

# Novell ZENworks® Linux Management

7.0

[www.novell.com](http://www.novell.com)

ADMINISTRATION GUIDE

March 23, 2007



Novell®

## Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. Please refer to [www.novell.com/info/exports/](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2007 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.novell.com/company/legal/patents/> and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.  
404 Wyman Street, Suite 500  
Waltham, MA 02451  
U.S.A.  
[www.novell.com](http://www.novell.com)

*Online Documentation:* To access the online documentation for this and other Novell products, and to get updates, see [www.novell.com/documentation](http://www.novell.com/documentation).

## **Novell Trademarks**

For a list of Novell trademarks, see the [Novell Trademark and Service Mark \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html) list at <http://www.novell.com/company/legal/trademarks/tmlist.html>.

## **Third-Party Materials**

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



# Contents

<b>About This Guide</b>	<b>15</b>
<b>Part I General Management</b>	<b>17</b>
<b>1 ZENworks Control Center</b>	<b>19</b>
1.1 Where the ZENworks Control Center is Installed	19
1.2 Accessing the ZENworks Control Center	19
1.3 Accessing the ZENworks Control Center through Novell iManager	20
<b>2 Command Line Administration Utilities</b>	<b>21</b>
<b>3 ZENworks Server</b>	<b>23</b>
3.1 ZENworks Services	23
3.1.1 Checking the Status of a ZENworks Service	24
3.1.2 Starting a ZENworks Service	24
3.1.3 Stopping a ZENworks Service	25
3.1.4 Restarting a ZENworks Service	25
3.2 RPM Package Repository	25
3.3 Uninstalling a ZENworks Server	26
<b>4 ZENworks Agent</b>	<b>29</b>
4.1 ZENworks Agent Filename and Location	29
4.2 ZENworks Agent (zmd) Cache Settings	29
4.3 File System Access	30
4.4 ZENworks Linux Management Update Client	30
4.5 Uninstalling the ZENworks Agent	30
<b>5 ZENworks Administrator Accounts</b>	<b>33</b>
5.1 Creating an Administrator Account	33
5.2 Modifying Account Rights	34
<b>6 ZENworks Database Maintenance</b>	<b>37</b>
6.1 Maintaining the ZENworks Object Store	37
6.1.1 Backing Up the ZENworks Object Store	37
6.1.2 Restoring the ZENworks Object Store	38
6.2 Maintaining the ZENworks Data Store on PostgreSQL	38
6.2.1 Understanding Automated Database Maintenance	38
6.2.2 Backing Up the ZENworks Data Store	39
6.2.3 Restoring the ZENworks Data Store	39
6.3 Maintaining the ZENworks Data Store on Oracle	40
6.3.1 Backup and Recovery Solutions	40
6.3.2 Setting Environment Variables	41
6.3.3 Connecting to the Database	41

6.3.4	Starting the Database . . . . .	41
6.3.5	Backing Up the Database . . . . .	42
6.3.6	Recovering the Database . . . . .	43
6.3.7	Shutting Down the Database . . . . .	44
6.4	Synchronizing the Object Store and Data Store . . . . .	44
<b>Part II Device Registration</b>		<b>47</b>
<b>7</b>	<b>Registration Overview</b>	<b>49</b>
<b>8</b>	<b>Registering Devices</b>	<b>51</b>
8.1	Installing the ZENworks Agent and Registering Devices . . . . .	51
8.2	Registering a Device after Installing the ZENworks Agent . . . . .	51
<b>9</b>	<b>Managing Registration Keys and Rules</b>	<b>53</b>
9.1	Managing Registration Keys . . . . .	54
9.1.1	Creating Keys to Register Devices . . . . .	54
9.1.2	Editing Existing Registration Keys . . . . .	57
9.1.3	Renaming, Copying, or Moving Registration Keys . . . . .	58
9.1.4	Deleting Registration Keys . . . . .	59
9.2	Managing Registration Rules . . . . .	59
9.2.1	Creating Rules to Register Devices . . . . .	59
9.2.2	Editing Existing Registration Rules . . . . .	63
9.2.3	Renaming or Copying Registration Rules . . . . .	64
9.2.4	Reordering Registration Rules . . . . .	65
9.2.5	Deleting Registration Rules . . . . .	65
9.3	Creating Folders . . . . .	65
<b>10</b>	<b>Unregistering and Reregistering Devices</b>	<b>67</b>
10.1	Possible Scenarios for Unregistering and Reregistering Devices . . . . .	67
10.2	Unregistering Devices . . . . .	68
10.3	Reregistering Devices . . . . .	68
<b>Part III Policy Management</b>		<b>69</b>
<b>11</b>	<b>Policy Management Overview</b>	<b>71</b>
11.1	Understanding Policies . . . . .	71
11.2	Creating Policies . . . . .	71
11.3	Managing Policies . . . . .	72
<b>12</b>	<b>Understanding Policies</b>	<b>73</b>
12.1	Types of Policies . . . . .	73
12.2	Assignments . . . . .	74
12.3	Schedules . . . . .	74
12.4	Groups . . . . .	75
12.5	System Requirements . . . . .	75
12.6	Effective Policies . . . . .	76

<b>13 Creating Policies</b>	<b>77</b>
13.1 Epiphany Policy .....	77
13.2 Evolution Policy .....	83
13.3 Firefox Policy .....	90
13.4 Generic GNOME Policy .....	97
13.5 Novell Linux Desktop Policy .....	103
13.6 Remote Execute Policy .....	111
13.7 Text File Policy .....	116
 <b>14 Managing Policies</b>	 <b>123</b>
14.1 Creating Policies .....	123
14.2 Creating Folders .....	124
14.3 Creating Policy Groups .....	125
14.4 Assigning Policies .....	128
14.5 Removing Policy Assignments .....	130
14.6 Adding Policies to Existing Groups .....	130
14.7 Editing Policies .....	131
14.7.1 Editing Epiphany, Evolution, Firefox, and NLD Policies .....	131
14.7.2 Editing Generic GNOME Policies .....	133
14.7.3 Editing Remote Execute Policies .....	136
14.7.4 Editing Text File Policies .....	138
14.7.5 Viewing Policy Enforcement Status .....	140
14.8 Editing System Requirements .....	141
14.9 Refreshing Policies .....	142
14.10 Verifying Policy Enforcement .....	143
14.11 Renaming, Copying, or Moving Policies .....	143
14.12 Deleting Policies, Policy Groups, and Folders .....	144
14.13 Unenforcing Policies .....	145
 <b>Part IV Package Management</b>	 <b>147</b>
 <b>15 Package Management Overview</b>	 <b>149</b>
15.1 Understanding RPM Bundles .....	149
15.2 Understanding Catalogs .....	150
15.3 Understanding the zlman Utility .....	150
15.4 Replicating Content in the ZENworks Management Zone .....	150
15.5 Mirroring Software .....	150
 <b>16 Using RPM Bundles</b>	 <b>153</b>
16.1 Understanding Bundles .....	153
16.1.1 RPM Bundles .....	154
16.1.2 Preboot Bundles .....	154
16.2 Creating RPM Bundles .....	154
16.3 Assigning Bundles .....	164
16.4 Editing Bundles .....	167
16.5 Adding Bundles to Catalogs .....	171
16.6 Creating Folders .....	171
16.7 Creating Bundle Groups .....	172
16.8 Adding Bundles to Existing Groups .....	178

16.9	Deleting Bundles, Bundle Groups, and Folders	178
16.10	Renaming, Copying, or Moving Bundles	179
16.11	Deploying a Different Version of a Bundle	180
16.11.1	Bundle Version Deployment Behavior (ZENworks Control Center vs. the zlman Utility)	181
16.12	Using a Remote Execute Policy to Remove Bundles and Packages from Devices	181
16.13	Generating Bundle Reports	185
<b>17</b>	<b>Using Catalogs</b>	<b>187</b>
17.1	Understanding Catalogs	187
17.2	Creating Catalogs	187
17.3	Assigning Catalogs	191
17.4	Adding Bundles to Catalogs	192
17.5	Renaming or Moving Catalogs	193
17.6	Deleting Catalogs	194
17.7	Creating Folders	194
<b>18</b>	<b>Replicating Content in the ZENworks Management Zone</b>	<b>197</b>
<b>19</b>	<b>Mirroring Software</b>	<b>199</b>
19.1	zlmirror	199
19.2	Configuring a Software Mirror	200
19.2.1	Creating Configuration Files	200
19.2.2	Testing and Performing the Mirroring Operation	203
19.3	Distributing Catalogs from a Public ZENworks Linux Management Server	204
19.3.1	Creating a Public ZENworks Linux Management Server	204
19.3.2	Accessing a Public ZENworks Linux Management Server	204
19.4	Deploying Red Hat Network Updates	204
19.4.1	Providing All RPM Packages and Package Bundles through a Catalog (Pulling)	205
19.4.2	Delivering Specific RPM Packages (Pushing)	205
<b>20</b>	<b>Creating RPM Packages From Tarballs</b>	<b>207</b>
20.1	Alien Package Converter Overview	207
20.2	Installing Alien Package Converter	207
20.3	Example Usage	208
<b>Part V</b>	<b>Preboot Services</b>	<b>209</b>
<b>21</b>	<b>Preboot Services Overview</b>	<b>211</b>
21.1	Preboot Services Functionality	211
21.2	Preboot Services Strategies	211
21.3	Preboot Bundles	212
21.4	Configuring Preboot Services	212
21.5	Setting Up Devices to Use Preboot Bundles	213
<b>22</b>	<b>Understanding Preboot Services in ZENworks Linux Management</b>	<b>215</b>
22.1	How Do You Implement Preboot Services?	215
22.2	What Is the Preboot Execution Environment (PXE)?	215



22.2.1	Understanding How Preboot Services Uses PXE . . . . .	215
22.2.2	Understanding the ZENworks NBPs . . . . .	216
22.2.3	Setting Up to Use PXE . . . . .	217
22.3	Preboot Services Functionality . . . . .	217
22.3.1	Preboot Bundles . . . . .	217
22.3.2	Preboot Services Menu . . . . .	219
22.3.3	Image Storage Security . . . . .	219
22.3.4	Non-registered Device Settings . . . . .	220
22.3.5	Preboot Work Assignment Rules . . . . .	220
22.3.6	Preboot Referral Lists . . . . .	222
22.3.7	Intel Active Management Technology (AMT) . . . . .	222
22.4	The Preboot Services Processes . . . . .	224
22.4.1	A Typical Preboot Services Operation . . . . .	224
22.4.2	Illustrating the Preboot Services Processes . . . . .	225
22.5	Preboot Strategies . . . . .	232
22.5.1	Automating Updates and Installations . . . . .	232
22.5.2	Creating, Installing, and Restoring Standard Images . . . . .	233
22.5.3	Reimaging Corrupted Devices . . . . .	234
22.5.4	Restoring Lab Devices to a Clean State . . . . .	234
22.5.5	Setting Up Devices for Future Reimaging . . . . .	235
22.5.6	Multicasting Device Images . . . . .	235

## **23 Setting Up Preboot Services 239**

23.1	Preparing a Preboot Services Server . . . . .	239
23.2	Setting Up the Preboot Services Methods . . . . .	240
23.2.1	Using Preboot Services (PXE) . . . . .	240
23.2.2	Preparing Imaging Boot CDs or DVDs . . . . .	240
23.2.3	Using the ZENworks Imaging Floppy Boot Disk Creator . . . . .	242
23.2.4	Managing ZENworks Partitions . . . . .	244
23.3	Deploying and Managing Preboot Services . . . . .	247
23.3.1	Checking the Preboot Services Imaging Server Setup . . . . .	247
23.3.2	Deploying Preboot Services In a Network Environment . . . . .	248
23.3.3	Administering Preboot Services . . . . .	256
23.3.4	Editing the Preboot Services Menu . . . . .	259
23.4	Configuring Preboot Services Defaults . . . . .	261
23.4.1	Configuring Preboot Menu Options . . . . .	262
23.4.2	Configuring Image Storage Security . . . . .	263
23.4.3	Configuring Non-registered Device Settings . . . . .	265
23.4.4	Configuring Preboot Work Assignments . . . . .	268
23.4.5	Configuring the Server Referral List . . . . .	275
23.4.6	Configuring Intel Active Management Technology (AMT) . . . . .	276
23.5	Overriding Preboot Services Defaults . . . . .	280
23.6	Enabling PXE on Devices . . . . .	282
23.6.1	Enabling PXE on a PXE-Capable Device . . . . .	282
23.6.2	Verifying That PXE Is Enabled on a Device . . . . .	283
23.7	Setting Up Devices for Imaging . . . . .	283
23.7.1	Device Requirements . . . . .	284
23.7.2	Enabling a Device for Imaging Operations . . . . .	284

## **24 Using Preboot Services 287**

24.1	Configuring AutoYaST or Kickstart Installation Script Bundles . . . . .	287
24.1.1	Configuring an AutoYaST Bundle . . . . .	287
24.1.2	Configuring a Kickstart Bundle . . . . .	292
24.2	Configuring ZENworks Script Bundles . . . . .	295
24.3	Imaging Devices . . . . .	298

24.3.1	Imaging Using the ZENworks Control Center	298
24.3.2	Performing Manual Imaging Tasks	304
24.3.3	Setting Up Disconnected Imaging Operations	314
24.4	Multicasting Images	319
24.4.1	Multicasting in the ZENworks Control Center	319
24.4.2	Multicasting Manually	325
24.5	Assigning Unassigned Preboot Bundles	330
24.6	Editing Preboot Services Work	332
<b>Part VI Hardware and Software Inventory</b>		<b>335</b>
<b>25 Inventory Overview</b>		<b>337</b>
<b>26 Reviewing Device Inventory</b>		<b>339</b>
26.1	Accessing the Device Inventory	339
26.2	Reviewing Device Inventory Summaries	339
26.3	Reviewing Hardware (General)	340
26.4	Reviewing Software (General)	340
26.5	Reviewing Hardware Details	340
<b>27 Rolling Up Hardware Inventory to the ZENworks 7 Server Management or ZENworks 7 Desktop Management Inventory Database</b>		<b>345</b>
27.1	Preparing to Roll Up Inventory	345
27.2	Configuring the Inventory Roll-Up Policy	345
27.3	Understanding the Roll-Up Process	347
27.4	Understanding the Components Involved in the Inventory Roll-Up	348
27.4.1	Understanding the Sender	348
27.4.2	Understanding the Compressed Scan Data File	348
27.5	Viewing the Inventory Data Stored in the ZENworks 7 Server Management or ZENworks 7 Desktop Management Inventory Database	349
<b>Part VII Remote Management</b>		<b>351</b>
<b>28 Remote Management Overview</b>		<b>353</b>
28.1	Remote Management Terminology	353
28.2	Understanding the Remote Management Components	353
28.2.1	Understanding Remote Control	354
28.2.2	Understanding Remote View	354
28.2.3	Understanding Remote Login	354
<b>29 Setting Up Remote Management</b>		<b>355</b>
29.1	Configuring the Remote Management Settings	355
29.1.1	Configuring Remote Management Settings at the Zone Level	355
29.1.2	Configuring Remote Management Settings at the Folder Level	357
29.1.3	Configuring Remote Management Settings at the Device Level	357
29.2	Configuring Remote Management Agent	358
29.2.1	Setting Up the Remote Management Agent Password on the Managed Device	359
29.2.2	Clearing the Remote Management Agent Password	359
29.2.3	Clearing Remote Management Agent Log Files	359

29.3	Starting Remote Management Operations Using the ZENworks Control Center . . . . .	359
29.3.1	Initiating a Remote Management Session from Common Tasks . . . . .	359
29.3.2	Initiating a Remote Management Session from the Device Context . . . . .	360
29.4	Starting Remote Management Operations Using the Native VNCViewer . . . . .	362
29.4.1	Starting Remote Management Operations Using the Windows VNC Viewer . . . . .	362
29.4.2	Starting Remote Management Operations Using the Linux VNC Viewer . . . . .	363
29.5	Establishing SSH Tunneling . . . . .	363
29.6	Improving Remote Management Performance . . . . .	364
<b>Part VIII Event Monitoring</b>		<b>365</b>
<b>30 Event Monitoring Overview</b>		<b>367</b>
30.1	Event Monitoring Terminology . . . . .	367
30.2	Monitoring Device Events . . . . .	367
30.3	Monitoring Policy Events . . . . .	368
30.4	Monitoring Bundle Events . . . . .	368
30.5	Using the Hot List . . . . .	368
<b>31 Working with Event Logs</b>		<b>371</b>
31.1	The Event Log Page . . . . .	371
31.2	Working with the Log Pages . . . . .	372
31.2.1	Viewing an Event Log . . . . .	372
31.2.2	Acknowledging an Event . . . . .	373
31.2.3	Using the Advanced Page . . . . .	375
31.2.4	Clearing the Event Log . . . . .	375
<b>32 Message Logger</b>		<b>377</b>
32.1	What Is Message Logger? . . . . .	377
32.2	Message Severity . . . . .	377
32.3	Message Format . . . . .	377
<b>33 Configuring Message Logger Settings</b>		<b>379</b>
33.1	Configuring Message Logger Settings for the Primary Server . . . . .	379
33.1.1	Configuring Database Maintenance Settings . . . . .	379
33.1.2	Configuring Centralized Log Settings . . . . .	380
33.1.3	Configuring SMTP Settings . . . . .	380
33.1.4	Configuring SNMP Settings . . . . .	381
33.2	Configuring Message Logger Settings for a Managed Device . . . . .	382
33.2.1	Configuring Local Log Settings . . . . .	382
33.2.2	Configuring System Log Settings . . . . .	383
<b>Part IX Reports</b>		<b>385</b>
<b>34 Reports Overview</b>		<b>387</b>
34.1	Bundle Reports . . . . .	387
34.2	Device Reports . . . . .	387

<b>35 Generating ZENworks Reports</b>	<b>389</b>
35.1 Creating a Folder	389
35.2 Creating a Report	390
35.3 Organizing Reports and Folders	392
35.3.1 Editing the Reports List	392
35.3.2 Deleting a Report or Folder	393
35.4 Modifying Report Details	393
35.5 Generating Reports	393
35.6 Resetting Default Reports	394
 <b>Part X Appendixes</b>	 <b>395</b>
 <b>A Bundle and Policy Schedules</b>	 <b>397</b>
A.1 No Schedule	397
A.2 Date Specific	397
A.3 Day of the Week Specific	398
A.4 Event	399
A.5 Monthly	399
A.6 Relative to Refresh	400
 <b>B Imaging Utilities and Components</b>	 <b>401</b>
B.1 Image Explorer (ImgExp.exe)	401
B.1.1 Opening Image Explorer (Imgexp.exe)	402
B.1.2 Opening an Image	402
B.1.3 Adding a File or Folder to an Open Image	402
B.1.4 Creating a Folder in an Open Image	402
B.1.5 Excluding a File or Folder from a File Set in the Open Image	403
B.1.6 Marking a File or Folder for Deletion in the Open Image	403
B.1.7 Purging Files and Folders Marked for Deletion from the Open Image	403
B.1.8 Extracting a File or Directory from the Open Image to a Folder	403
B.1.9 Extracting a File or Directory from the Open Image as an Add-On Image	403
B.1.10 Viewing a File from the Open Image in its Associated Application	404
B.1.11 Saving Your Changes to the Open Image	404
B.1.12 Creating an Add-On Image	404
B.1.13 Adding a Partition to a New Add-On Image	404
B.1.14 Compressing an Image	404
B.1.15 Splitting an Image	405
B.1.16 Resizing a Partition in an Image	406
B.2 Novell ZENworks Linux Management Imaging Agent (novell-zislnx)	406
B.3 Image-Safe Data Viewer and Editor (zisview and zisedit)	407
B.3.1 Information Displayed by the Image-Safe Data Viewer	407
B.3.2 Using the Image-Safe Data Viewer	409
B.3.3 Using the Image-Safe Data Editor	410
B.4 ZENworks Imaging Floppy Boot Disk Creator (zimboot.exe)	411
B.5 Imaging Configuration Parameters (settings.txt)	411
B.6 Imaging Boot Parameter for PCMCIA Cards	414
B.7 Imaging Server	414
B.7.1 Initiating the Imaging Processes	415
B.7.2 Viewing Information About Imaging Requests	423
B.7.3 Starting a Manual Multicast Session	423

<b>C</b>	<b>ZENworks Imaging Engine Commands</b>	<b>425</b>
C.1	Help Mode (img help) . . . . .	425
C.2	Automatic Mode (img auto) . . . . .	426
C.3	Make Mode (img make) . . . . .	427
C.3.1	Make Locally (img makel) . . . . .	427
C.3.2	Make to Proxy (img makep) . . . . .	428
C.4	Restore Mode (img restore) . . . . .	429
C.4.1	Restore from Local (img restorel) . . . . .	430
C.4.2	Restore from Proxy (img restorep) . . . . .	432
C.5	Session (Multicast) Mode (img session) . . . . .	433
C.6	Partition Mode (img part) . . . . .	435
C.6.1	Using the ZENworks Imaging Engine Menu . . . . .	435
C.6.2	Using the Bash Prompt . . . . .	436
C.7	ZENworks Partition Mode (img zenPartition) . . . . .	436
C.8	Dump Mode (img dump) . . . . .	437
C.9	Information Mode (img info) . . . . .	438
<b>D</b>	<b>Updating ZENworks Imaging Resource Files</b>	<b>441</b>
D.1	The Linux Distribution for Imaging . . . . .	441
D.2	Understanding Device Boot Processes in a ZENworks Imaging Environment . . . . .	442
D.2.1	linuxrc . . . . .	442
D.2.2	zenworks.s . . . . .	443
D.3	Understanding ZENworks Partitions and Command Line Parameters . . . . .	443
D.3.1	The ZENworks Partition . . . . .	443
D.3.2	Command Line Parameters and Variables . . . . .	444
D.4	Modifying ZENworks Imaging Resource Files . . . . .	444
D.4.1	Adding Files to an Imaging Boot CD . . . . .	445
D.4.2	Adding Files to the Initrd or Root File Systems . . . . .	446
D.4.3	Using the Driverupdate File Method . . . . .	447
D.5	Adding or Updating LAN Drivers . . . . .	449
D.5.1	Obtaining Drivers . . . . .	449
D.5.2	Building Drivers . . . . .	449
D.5.3	Loading Drivers with Parameters . . . . .	451
D.6	Using Uname . . . . .	451
D.7	Variables and Parameters . . . . .	452
D.7.1	Imaging Script Variables . . . . .	452
D.7.2	Linuxrc Parameters Specified in Settings.txt . . . . .	453
D.7.3	Image Engine Variables . . . . .	453
D.8	Troubleshooting Linux Driver Problems . . . . .	454
D.8.1	Troubleshooting During the Boot Process . . . . .	454
D.8.2	Troubleshooting at the Bash Prompt . . . . .	454
<b>E</b>	<b>Supported Ethernet Cards</b>	<b>455</b>
<b>F</b>	<b>Establishing SSH Tunneling</b>	<b>457</b>
F.1	SSH Tunneling between a Linux Management Console and a Linux Managed Device . . . .	457
F.1.1	Basic Use . . . . .	457
F.2	SSH Tunneling between a Windows Management Console and a Linux Managed Device .	458
F.3	Compression . . . . .	459

<b>G</b>	<b>Limited Support for SLES10 and SLED10 Managed Devices</b>	<b>461</b>
<b>H</b>	<b>License Agreement for libacl and libgconf</b>	<b>463</b>
H.1	Library GNU Public License . . . . .	463
<b>I</b>	<b>Documentation Updates</b>	<b>469</b>
I.1	March 23, 2007 . . . . .	469
I.2	January 2, 2007 . . . . .	470
I.3	September 29, 2006 . . . . .	470
I.4	August 18, 2006 . . . . .	470
I.5	July 18, 2006 . . . . .	471
I.6	June 29, 2006 . . . . .	471
I.7	Interim Release 1 . . . . .	472
I.8	December 23, 2005 . . . . .	473
I.9	December 9, 2005 . . . . .	473
I.9.1	Device Registration . . . . .	473
I.9.2	Establishing SSH Tunneling . . . . .	474
I.9.3	General Management . . . . .	474
I.9.4	Packages . . . . .	474

# About This Guide

This *ZENworks® 7 Linux Management Administration Guide* includes conceptual and task-based information to help you configure and maintain your ZENworks system.

---

**IMPORTANT:** Novell® ZENworks 7 Linux Management Interim Release 1 (IR1) was released July 17, 2006. The ISO image for IR1 is named `ZEN7_with_IR1_LinuxMgmt.iso`.

If you obtained the ISO image prior to July 17, 2006, and the ISO image is named `ZEN7_LinuxMgmt.iso`, you do not have IR1. If you do not have IR1, you should obtain and install it.

To update an existing installation of ZENworks 7 Linux Management with IR1, follow the download and installation instructions in TID 9183 in the [Novell Support site \(http://www.novell.com/support/supportcentral/supportcentral.do?id=m1\)](http://www.novell.com/support/supportcentral/supportcentral.do?id=m1). Ensure that you click the *Search by TID ID* check box before performing the search. This TID also includes a list of updates to ZENworks 7 Linux Management since its initial release.

For a brief overview of important features and additions to ZENworks 7 Linux Management with IR1, see [Interim Release 1](#) in [Appendix I, “Documentation Updates,”](#) on [page 469](#).

---

The guide is organized as follows:

- ♦ [Part I, “General Management,”](#) on [page 17](#)
- ♦ [Part II, “Device Registration,”](#) on [page 47](#)
- ♦ [Part III, “Policy Management,”](#) on [page 69](#)
- ♦ [Part IV, “Package Management,”](#) on [page 147](#)
- ♦ [Part V, “Preboot Services,”](#) on [page 209](#)
- ♦ [Part VI, “Hardware and Software Inventory,”](#) on [page 335](#)
- ♦ [Part VII, “Remote Management,”](#) on [page 351](#)
- ♦ [Part VIII, “Event Monitoring,”](#) on [page 365](#)
- ♦ [Part IX, “Reports,”](#) on [page 385](#)
- ♦ [Part X, “Appendixes,”](#) on [page 395](#)

## Audience

This guide is intended for ZENworks administrators.

## Feedback

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

## Documentation Updates

For the most recent, updated version of the *ZENworks 7 Desktop Management Administration Guide*, visit the [Novell ZENworks 7 documentation site \(http://www.novell.com/documentation/zenworks7\)](http://www.novell.com/documentation/zenworks7).

## Additional Documentation

ZENworks 7 Linux Management is supported with other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product:

- ♦ *Novell ZENworks 7 Installation Guide*

In addition, the other capabilities included in the ZENworks 7 suite have extensive documentation for your use. For a full list of this documentation, see the [Novell ZENworks 7 documentation site \(http://www.novell.com/documentation/zenworks7\)](http://www.novell.com/documentation/zenworks7).

## Documentation Conventions

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

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (\*) denotes a third-party trademark.

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



# General Management

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

- ♦ Chapter 1, “ZENworks Control Center,” on page 19
- ♦ Chapter 2, “Command Line Administration Utilities,” on page 21
- ♦ Chapter 3, “ZENworks Server,” on page 23
- ♦ Chapter 4, “ZENworks Agent,” on page 29
- ♦ Chapter 5, “ZENworks Administrator Accounts,” on page 33
- ♦ Chapter 6, “ZENworks Database Maintenance,” on page 37



# ZENworks Control Center

# 1

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

- ♦ [Section 1.1, “Where the ZENworks Control Center is Installed,” on page 19](#)
- ♦ [Section 1.2, “Accessing the ZENworks Control Center,” on page 19](#)
- ♦ [Section 1.3, “Accessing the ZENworks Control Center through Novell iManager,” on page 20](#)

## 1.1 Where the ZENworks Control Center is Installed

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

You can perform all management tasks on the primary server and most management tasks on the secondary servers. The one management exception on secondary servers is the manipulation (adding, deleting, modifying) of RPM packages in a bundle. This task is not supported because the primary server is the source server for RPM packages, meaning that packages are replicated from the primary server to secondary servers on a regularly scheduled basis. Manipulating an RPM package on a secondary server rather than on the primary server would result in the modified package being replaced (or removed) the next time the secondary server's packages were updated from the primary server. For more information about replication of RPM packages, see [Chapter 18, “Replicating Content in the ZENworks Management Zone,” on page 197](#).

## 1.2 Accessing the ZENworks Control Center

To access the ZENworks Control Center:

- 1 Using a Web browser that meets the requirements listed in “[Administration Workstation Requirements](#)” in “[System Requirements](#)” in the *Novell ZENworks 7 Linux Management Installation Guide*, enter the following URL:

```
https://ZENworks_Server_Address
```

Replace *ZENworks\_Server\_Address* with the IP address or DNS name of the ZENworks Server.

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

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

## 1.3 Accessing the ZENworks Control Center through Novell iManager

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

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

- 1 Copy the plug-in (`zlm7link.npm`) from either of the following CDs to a location on your iManager server.

*Novell ZENworks 7 Linux Management CD:* The `zlm7link.npm` file is located in the `/ImanagerPlugin` directory.

*Novell ZENworks 7 Companion 1 CD:* The `zlm7link.npm` file is located in the `/Novell iManager/ZLM Plugins NPM` directory.

- 2 Follow the instructions in the *Novell iManager 2.5 Installation Guide* ([http://www.novell.com/documentation/imanager25/imanager\\_install\\_25/data/bnptalr.html](http://www.novell.com/documentation/imanager25/imanager_install_25/data/bnptalr.html)) to install and configure the plug-in module.
- 3 If Tomcat did not restart during the installation and configuration process, restart Tomcat.
- 4 Log into iManager.
- 5 Click the *ZENworks* icon at the top of the page.
- 6 Enter the ZENworks Control Center URL:  
`https://ZENworks_Server_Address`  
Replace *ZENworks\_Server\_Address* with the IP address or DNS name of the ZENworks Server.
- 7 Click the *ZENworks* icon to launch the ZENworks Control Center.

# Command Line Administration Utilities

# 2

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

## zlman

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

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

For more information about zlman, view the zlman man page (man zlman) on the ZENworks Server or view the [HTML version \(http://www.novell.com/documentation/zenworks7/reference/zlman.html\)](http://www.novell.com/documentation/zenworks7/reference/zlman.html) of the man page.

## zlmirror

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

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

For more information about zlmirror, view the zlmirror man page (man zlmirror) on the ZENworks Server, view the [HTML version \(http://www.novell.com/documentation/zenworks7/reference/zlmirror.html\)](http://www.novell.com/documentation/zenworks7/reference/zlmirror.html) of the man page, or see [Chapter 19, “Mirroring Software,” on page 199](#).

## rug

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

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

For more information about rug, view the rug man page (man rug) on a managed device or view the [HTML version \(http://www.novell.com/documentation/zenworks7/reference/rug.html\)](http://www.novell.com/documentation/zenworks7/reference/rug.html) of the man page.

## zmd

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

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

For more information about zmd, view the zmd man page (man zmd) on a managed device or view the [HTML version \(http://www.novell.com/documentation/zenworks7/reference/zmd.html\)](http://www.novell.com/documentation/zenworks7/reference/zmd.html) of the man page.

## **zrmservice**

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

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

For more information about zrmservice, view the zrmservice man page (man zrmservice) on a managed device or view the [HTML version \(http://www.novell.com/documentation/zenworks7/reference/zrmservice.html\)](http://www.novell.com/documentation/zenworks7/reference/zrmservice.html) of the man page.

# ZENworks Server

# 3

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

- ♦ [Section 3.1, “ZENworks Services,” on page 23](#)
- ♦ [Section 3.2, “RPM Package Repository,” on page 25](#)
- ♦ [Section 3.3, “Uninstalling a ZENworks Server,” on page 26](#)

## 3.1 ZENworks Services

The ZENworks Server includes the following services:

**Table 3-1** *ZENworks Services*

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

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

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

- ♦ [Section 3.1.1, “Checking the Status of a ZENworks Service,” on page 24](#)
- ♦ [Section 3.1.2, “Starting a ZENworks Service,” on page 24](#)
- ♦ [Section 3.1.3, “Stopping a ZENworks Service,” on page 25](#)
- ♦ [Section 3.1.4, “Restarting a ZENworks Service,” on page 25](#)

### 3.1.1 Checking the Status of a ZENworks Service

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

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

Replace *servicename* with the name of the service as listed in the table in [Section 3.1, “ZENworks Services,” on page 23](#).

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

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

### 3.1.2 Starting a ZENworks Service

To start a service, use the following command:

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

Replace *servicename* with the name of the service as listed in the table in [Section 3.1, “ZENworks Services,” on page 23](#).



To start all services, use the following command:

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

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

### 3.1.3 Stopping a ZENworks Service

To stop a service, use the following command:

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

Replace *servicename* with the name of the service as listed in the table in [Section 3.1, “ZENworks Services,” on page 23](#).

To stop all services, use the following command:

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

### 3.1.4 Restarting a ZENworks Service

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

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

Replace *servicename* with the name of the service as listed in the table in [Section 3.1, “ZENworks Services,” on page 23](#).

To restart all services, use the following command:

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

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

## 3.2 RPM Package Repository

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

### Package Repository Location

The package repository is the `/var/opt/novell/zenworks/pkg-repo` directory on the ZENworks Server. When you add an RPM package to a bundle, the package is automatically uploaded to the package repository.

If you remove bundles or packages from devices as described in [Section 16.12, “Using a Remote Execute Policy to Remove Bundles and Packages from Devices,” on page 181](#), the packages are not automatically removed from the package repository. You can manually delete packages from the package repository. If, however, you leave the packages in the package repository, and you later include the same packages in another bundle, the packages are already on the Server and will not be automatically uploaded.

## Package Replication

To ensure that all ZENworks Servers have the same RPM packages to distribute, the ZENworks Primary Server can replicate all packages to any ZENworks Secondary Servers in the Management Zone. To enable replication, you need to establish a replication schedule (see [Chapter 18, “Replicating Content in the ZENworks Management Zone,”](#) on page 197).

During replication of packages to a secondary server, only a new packages and updates to existing packages are sent.

## Package Administration

Because of the way that packages are replicated from the primary server to secondary servers, you must run the ZENworks Control Center or `zlm` utility from the primary server to add a package to a bundle. Doing so causes the package to be added to the primary server's package repository and then be replicated to all secondary servers.

If you add a package to a secondary server, the package will not exist on the primary server and is therefore removed the next time the primary server replicates its packages to the secondary server.

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

## 3.3 Uninstalling a ZENworks Server

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

### Uninstalling a ZENworks Server Using `zlm-uninstall`

- 1 Make sure you know the password for the ZENworks Administrator account.
- 2 Log in to the ZENworks Server as `root`.
- 3 Run the following command:  

```
/opt/novell/zenworks/bin/zlm-uninstall
```
- 4 Follow the prompts.

### Uninstalling a Secondary ZENworks Server Using `zlm-config`

- 1 Make sure you know the password for the ZENworks Administrator account.
- 2 Log in to the Secondary ZENworks Server as `root`.
- 3 Run the following command:

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

where *secondary\_server* is the full NDS context of the secondary server.

The server is usually in the system context. For example, if your server name is ZEN216, the full command is:

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

## Manually Uninstalling a Primary or Secondary ZENworks Server

- 1 Stop the services on the ZENworks Server. If necessary, see [Section 3.1.3, “Stopping a ZENworks Service,” on page 25](#).

- 2 Remove the following directories:

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

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

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

```
/etc/init.d/postgresql startsu - postgresqldropdb  
zenworksdropuser zenadmin/etc/init.d/postgresql stop
```

- 5 (Conditional) If you are removing a secondary server, remove the secondary server object from the Object Store and Data Store. To do so:

- 5a Create a script file like the following one to create a CLASSPATH variable that includes all of the paths to the ZENworks classes:

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

- 5b Use the following command to remove the ZENworks secondary server object:

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

Replace *admin\_password* with the ZENworks Administrator account password.

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

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

Replace *admin\_password* with the ZENworks Administrator account password.

- 7 Remove the ZENworks RPM packages. To do so:

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

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

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

```
rpm -e | package_name
```

or

Use the following simple script to remove multiple packages:

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

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

**8** Remove the following directories:

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

# ZENworks Agent

# 4

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

- ♦ [Section 4.1, “ZENworks Agent Filename and Location,” on page 29](#)
- ♦ [Section 4.2, “ZENworks Agent \(zmd\) Cache Settings,” on page 29](#)
- ♦ [Section 4.3, “File System Access,” on page 30](#)
- ♦ [Section 4.4, “ZENworks Linux Management Update Client,” on page 30](#)
- ♦ [Section 4.5, “Uninstalling the ZENworks Agent,” on page 30](#)

## 4.1 ZENworks Agent Filename and Location

The ZENworks Agent is named `zmd`. It is sometimes referred to as the ZENworks Management Daemon. The ZENworks Agent is installed to the following directory:

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

## 4.2 ZENworks Agent (zmd) Cache Settings

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

The cleaning of cached information is always enabled. You can configure the following settings using the `rug set` command in the `rug` utility to manage the cache. For more information about the `rug` utility, see [“rug” on page 21](#).

**Table 4-1** ZENworks Management Daemon Cache Settings

Setting	Description
<i>max-cache-age</i>	<p>Defines the number of days the contents of the cache are retained, after which the contents are deleted. The default is 30 days. If this setting specifies 0 days, the cache content never expires.</p> <p>The cache cleanup is enforced on client startup and refresh. The contents of the cache are sorted by date (oldest to newest) and deleted by applying the <i>max-cache-age</i> setting, starting with the oldest content.</p> <p>To change the <i>max-cache-age</i> setting from the default of 30 days to 60 days, for example, you enter the following command from the managed device:</p> <pre>rug set max-cache-age 60</pre>

Setting	Description
<i>cache-max-size-in-mb</i>	<p>This setting is only enforced at cleanup time; not during bundle download. The default is 300 MB. If this is set to 0, there is no limit to the size of the cache; however, the <b>max-cache-age</b> setting still applies.</p> <p>If the cache size exceeds the maximum size specified with this setting, the cache contents are sorted by date and the oldest contents are deleted until the cache size is within the specified size limit.</p> <p>If this size limit is exceed while downloading bundles, the bundle contents are downloaded; however, the next time the device restarts or refreshes, the cache is cleaned until its size is within the specified size limit. The cache cleanup process will not delete files downloaded within the last 24 hours to get within the specified limit.</p> <p>To change the <i>cache-max-size-in-mb</i> setting from the default of 300 MB to 500 MB, for example, you enter the following command from the managed device:</p> <pre>rug set cache-max-size-in-mb 500</pre>

## 4.3 File System Access

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

## 4.4 ZENworks Linux Management Update Client

The ZENworks Linux Management Update Client is a component of the ZENworks Agent. It includes a user interface that can be launched from the client menu (Software Updates) or at the command line by using the following command:

```
/opt/novell/zenworks/bin/red-carpet
```

## 4.5 Uninstalling the ZENworks Agent

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

### Using zlm-uninstall to Uninstall the ZENworks Agent

- 1 Make sure you have unregistered the device. See [Chapter 10, “Unregistering and Reregistering Devices,”](#) on page 67.
- 2 Log in to the managed device as root.
- 3 Run the following command:  

```
/opt/novell/zenworks/bin/zlm-uninstall
```
- 4 Follow the prompts.

## Manually Uninstalling the ZENworks Agent

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

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

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

```
rpm -e package_name
```

or

Use the following simple script to remove multiple packages:

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

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

- 3 Remove the following directories:

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





# ZENworks Administrator Accounts

# 5

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

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

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

- ♦ [Section 5.1, “Creating an Administrator Account,” on page 33](#)
- ♦ [Section 5.2, “Modifying Account Rights,” on page 34](#)

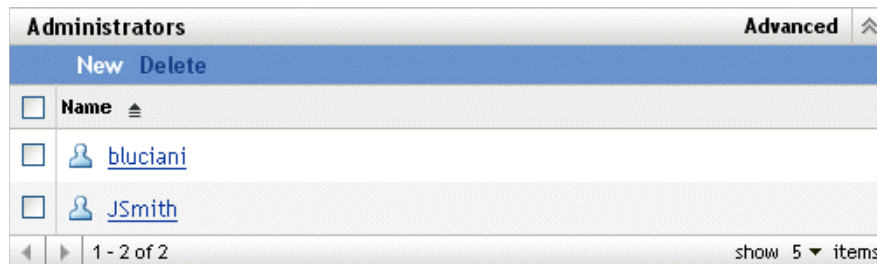

## 5.1 Creating an Administrator Account

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

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

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

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

Administrators		Advanced	⌵
New Delete			
<input type="checkbox"/>	Name		
<input type="checkbox"/>	 <a href="#">bluciani</a>		
<input type="checkbox"/>	 <a href="#">JSmith</a>		
1 - 2 of 2		show 5 items	

- 3 In the Administrators list, click *New* to display the Add new Administrator dialog box.
- 4 Provide a username and password for the account, then click *OK* to add the account to the Administrators list.

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

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

- 5 To change the administrator's rights, see the next section, [Modifying Account Rights](#).

## 5.2 Modifying Account Rights

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

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



To modify an administrator's rights:

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

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

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

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

Administrators		Advanced	⌵
New Delete			
<input type="checkbox"/>	Name		
<input type="checkbox"/>	 bluciani		
<input type="checkbox"/>	 JSmith		
1 - 2 of 2		show 5 items	

- 3 Click the account you want to modify.
- 4 Set the General options as desired:
  - ♦ **Can create and manage other administrators:** Select this option to enable the administrator to create additional administrator accounts, or to change the settings for existing administrator accounts.
  - ♦ **Can modify zone settings:** Select this option to enable the administrator to change the Management Zone settings, registration keys, registration rules, and licensing information included on the Configuration page.


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

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

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

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

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

- ♦ **Add:** By default, the Assigned Rights sections display only the root folders (/Bundles, /Devices, /Policies, and /Reports). To assign rights to a folder that is not listed, you need to add the folder to the list. To do so, click *Add* to display the Add Rights Folder dialog box. In the Folders field, click  to browse for and select the folder. After you select the folder, select the desired rights assignment (All, Modify, or View), then click *OK*.
- ♦ **Edit:** To modify the administrator's rights to a folder that already appears in the list (for example, the /Bundles folder), select the folder by checking the box in front of its name, then click *Edit*. Select the rights assignment you want (All, Modify, or View), then click *OK*.
- ♦ **Delete:** To delete a folder from the list, select the folder by checking the box in front of its name, then click *Delete*. This deletes the administrator's directly assigned rights to the folder. The administrator still inherits the rights assigned to the folder's parent. For example, assume the administrator has View rights in the /Bundles folder and All rights in the /Bundles/Workstations folder. You delete the /Bundles/Workstations folder from the list. The administrator's rights in the /Bundles/Workstations folder revert to the rights inherited from the /Bundles folder. Therefore, in this example, the administrator goes from having All rights in the /Bundles/Workstation folder to having View rights only.  
  
You cannot delete the root folders (/Bundles, /Devices, /Policies, and /Reports).

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



# ZENworks Database Maintenance

# 6

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

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

---

**IMPORTANT:** To restore a ZENworks Linux Management system after the failure of a ZENworks Primary Server, you need backups of the Object Store, Data Store, package repository, and zlmirror configuration files. Therefore, it is important that you complete the instructions in this section. For more information, see “[Disaster Recovery](#)” in the *ZENworks 7 Linux Management Troubleshooting Guide*.

---

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

- ♦ [Section 6.1, “Maintaining the ZENworks Object Store,” on page 37](#)
- ♦ [Section 6.2, “Maintaining the ZENworks Data Store on PostgreSQL,” on page 38](#)
- ♦ [Section 6.3, “Maintaining the ZENworks Data Store on Oracle,” on page 40](#)
- ♦ [Section 6.4, “Synchronizing the Object Store and Data Store,” on page 44](#)

## 6.1 Maintaining the ZENworks Object Store

The ZENworks Object Store is Novell eDirectory™ 8.7.3. The following sections provide information for backing up and restoring the Object Store:

- ♦ [Section 6.1.1, “Backing Up the ZENworks Object Store,” on page 37](#)
- ♦ [Section 6.1.2, “Restoring the ZENworks Object Store,” on page 38](#)

### 6.1.1 Backing Up the ZENworks Object Store

You use `zlm_ndsbackup.sh`, located in `/opt/novell/zenworks/sbin`, to back up the Object Store.

- 1 Make sure you are logged in as root to the ZENworks Server.
- 2 Enter the following command at the command prompt:  

```
# zlm_ndsbackup.sh -U admin.system
```
- 3 Enter the password to authenticate to the Object Store.

This is the password for the ZENworks Administrator account.

The backup program creates a directory in `/var/opt/novell/zenworks/backup/nds/month-yyyy/yyyy-mm-dd`. The directory name is the date on which the backup is taken. The

backup file is saved in this directory. The name of the backup file has the format *timestamp-backup*, and the time stamp indicates the time when the backup was taken. For example:

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

NDS Backup creates a directory with the current date in `/var/opt/novell/zenworks/backup/nds`. The backup file is saved in this directory.

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

## 6.1.2 Restoring the ZENworks Object Store

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

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

- 2 Enter the following command on the command prompt:

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

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

- 3 Enter the password to authenticate to the Object Store.

This is the password for the ZENworks Administrator account.

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

- 4 After the restore is complete, you need to ensure that the Data Store is synchronized with the Object Store. For instructions, see [Section 6.4, “Synchronizing the Object Store and Data Store,” on page 44](#).

## 6.2 Maintaining the ZENworks Data Store on PostgreSQL

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

- [Section 6.2.1, “Understanding Automated Database Maintenance,” on page 38](#)
- [Section 6.2.2, “Backing Up the ZENworks Data Store,” on page 39](#)
- [Section 6.2.3, “Restoring the ZENworks Data Store,” on page 39](#)

### 6.2.1 Understanding Automated Database Maintenance

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

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

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

## 6.2.2 Backing Up the ZENworks Data Store

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

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

- 1 Make sure you are logged in as root to a ZENworks Server.
- 2 Enter the following at the command prompt:

```
zlm_dbbackup.sh
```

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

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

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

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

## 6.2.3 Restoring the ZENworks Data Store

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

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

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

To restore the ZENworks Data Store:

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

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

Because all ZENworks Servers access the Data Store, you need to stop these services on all ZENworks Servers in your system.

- 2 Make sure you are logged in as root to a ZENworks Server.
- 3 Enter the following at command prompt:

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

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

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

- 4 If prompted, enter Y to stop the ZENworks Server (novell-zenserver).
- 5 If prompted, enter Y to stop the ZENworks Loader (novell-zenloader).
- 6 When prompted to supply a password to drop the database, enter the Administrator password.
- 7 When prompted to supply a password to create the new database, enter the Administrator password.

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

- 8 After the restore is complete, you need to ensure that the Data Store is synchronized with the Object Store. For instructions, see [Section 6.4, “Synchronizing the Object Store and Data Store,” on page 44](#).

## 6.3 Maintaining the ZENworks Data Store on Oracle

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

- ♦ [Section 6.3.1, “Backup and Recovery Solutions,” on page 40](#)
- ♦ [Section 6.3.2, “Setting Environment Variables,” on page 41](#)
- ♦ [Section 6.3.3, “Connecting to the Database,” on page 41](#)
- ♦ [Section 6.3.4, “Starting the Database,” on page 41](#)
- ♦ [Section 6.3.5, “Backing Up the Database,” on page 42](#)
- ♦ [Section 6.3.6, “Recovering the Database,” on page 43](#)
- ♦ [Section 6.3.7, “Shutting Down the Database,” on page 44](#)

### 6.3.1 Backup and Recovery Solutions

Oracle provides two methods of backup and recovery:

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

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

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



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

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

### 6.3.2 Setting Environment Variables

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

- ♦ ORACLE\_HOME: The directory where the Oracle software is installed. For example:  
`ORACLE_HOME=/home/oracle/product/9ir2`
- ♦ CLASSPATH: The paths to the libraries installed by Oracle. For example:  
`CLASSPATH=$CLASSPATH:/oracle/opt/oracle/product/9ir2/JRE:/oracle/opt/oracle/product/9ir2/jlib:/oracle/opt/oracle/product/9ir2/rdbms/jlib:/oracle/opt/oracle/product/9ir2/network/jlib`
- ♦ PATH: The Oracle installation's bin directory. For example:  
`PATH=$PATH:/home/oracle/product/9ir2/bin`

### 6.3.3 Connecting to the Database

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

- ♦ Start RMAN at the operating system command line without connecting to a database, by issuing the RMAN command without any connection options:  
`$ rmanRMAN> CONNECT TARGET /`
- ♦ Start the RMAN executable at the operating system command line while connecting to the database:  
`$ rman TARGET /`

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

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

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

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

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

### 6.3.4 Starting the Database

1 Start the database using the following command:

```
RMAN> startup mount
```

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

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

```
Oracle instance started
database mounted
```

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

### 6.3.5 Backing Up the Database

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

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

```
RMAN> BACKUP DATABASE;
```

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

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

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

`%U` generates a unique filename.

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

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

```
Starting backup at OCT 12 2001 19:09:48
using target database controlfile instead of recovery catalogal
located channel: ORA_DISK_1
channel ORA_DISK_1: sid=10 devtype=DISK
channel ORA_DISK_1: starting full datafile backupset
channel ORA_DISK_1: specifying datafile(s) in backupset
including current SPFILE in backupset
including current controlfile in backupset
input datafile fno=00001 name=/oracle/oradata/zenworks/system01.dbf
input datafile fno=00002 name=/oracle/oradata/zenworks/undotbs01.dbf
input datafile fno=00003 name=/oracle/oradata/zenworks/cwmlite01.dbf
input datafile fno=00004 name=/oracle/oradata/zenworks/drsys01.dbf
input datafile fno=00005 name=/oracle/oradata/zenworks/example01.dbf
input datafile fno=00006 name=/oracle/oradata/zenworks /indx01.dbf
input datafile fno=00007 name=/oracle/oradata/zenworks/tools01.dbf
input datafile fno=00008 name=/oracle/oradata/zenworks/users01.dbf
channel ORA_DISK_1: starting piece 1 at OCT 12 2001 19:09:56
channel ORA_DISK_1: finished piece 1 at OCT 12 2001 19:10:31
piece handle=/oracle/dbs/lvd6dtk1_1_1 comment=NONE
```

```
channel ORA_DISK_1: backup set complete, elapsed time: 00:00:39
Finished backup at OCT 12 2001 19:10:33
```

## 6.3.6 Recovering the Database

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

- ♦ “Complete Recovery” on page 43
- ♦ “Incomplete Recovery” on page 43

### Complete Recovery

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

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

```
RMAN> connect target /RMAN> run { 2> startup mount;3> restore
database;4> recover database;5> alter database open;6> }
```

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

- 2 After the restore is complete, you need to ensure that the Data Store is synchronized with the Object Store. For instructions, see [Section 6.4, “Synchronizing the Object Store and Data Store,” on page 44](#).

### Incomplete Recovery

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

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

- ♦ Media failure destroys some or all of the online redo logs.
- ♦ A user error causes data loss, for example, a user inadvertently drops a table.
- ♦ You cannot perform a complete recovery because an archived redo log is missing.

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

The database must be closed to perform an incomplete recovery.

To perform an incomplete recovery:

- 1 Set the time format environment variable:

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

- 2 Use the following sequence of steps:

```
$ rman target /RMAN> startup mount;RMAN> run {2> set until time  
"to_date('Mar 16 2005 10:24:00', 'MM DD YYYY HH24:MI:SS')";3>  
restore database;4> recover database;5> }
```

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

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

```
SET UNTIL SCN 1000
```

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

```
ALTER DATABASE OPEN RESETLOGS;
```

- 4 After the restore is complete, you need to ensure that the Data Store is synchronized with the Object Store. For instructions, see [Section 6.4, “Synchronizing the Object Store and Data Store,” on page 44](#).

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

### 6.3.7 Shutting Down the Database

- 1 Use the following command to shut down the database:

```
RMAN> SHUTDOWN NORMAL;
```

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

## 6.4 Synchronizing the Object Store and Data Store

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

- 1 Make sure you are logged in as root to the ZENworks Server.
- 2 Enter the following command on the command prompt:

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

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

**3** Enter the password to authenticate to the Object Store.

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



# Device Registration



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

- ♦ Chapter 7, “Registration Overview,” on page 49
- ♦ Chapter 8, “Registering Devices,” on page 51
- ♦ Chapter 9, “Managing Registration Keys and Rules,” on page 53
- ♦ Chapter 10, “Unregistering and Reregistering Devices,” on page 67





# Registration Overview

# 7

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

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

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

For Novell ZENworks to manage a device, you must install the ZENworks Agent software on the device. During installation of the ZENworks Agent software, the device is automatically registered as long as you (or whoever is installing the software) supplies the DNS name or IP address of a ZENworks Server in your Management Zone. You can also register devices at a later time. For more information, see [Chapter 8, “Registering Devices,” on page 51](#).

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

Using registration keys lets you define the keys that are used to register devices in the Management Zone. A registration key specifies a set of assignments that are applied to devices that register using that key. The key must be applied during installation of the ZENworks Agent on a device, either manually or by using a script. For more information, see [Section 9.1, “Managing Registration Keys,” on page 54](#).

If you do not want to use registration keys, you can create registration rules to determine a device's assignments when it registers without using a key. The major difference between using the default registration rules versus using a registration key is that the default registration rules use a filter to determine which set of device assignments to apply, but a key corresponds directly to a specific set of assignments to apply. For more information, see [Section 9.2, “Managing Registration Rules,” on page 59](#).

---

**NOTE:** You can register devices against only one ZENworks 7 Linux Management Server. However, you can register devices against one ZENworks 7 Server and multiple ZENworks 6.6.x Linux Management Servers. Registering devices against multiple Servers is useful, for example, during the transitional period while you deploy ZENworks 7.

---



# Registering Devices

# 8

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

The following sections contain additional information:

- [Section 8.1, “Installing the ZENworks Agent and Registering Devices,” on page 51](#)
- [Section 8.2, “Registering a Device after Installing the ZENworks Agent,” on page 51](#)

## 8.1 Installing the ZENworks Agent and Registering Devices

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

For more information about manually installing and registering the agent or automating installation and registration using a script, see “[Setting Up Managed Devices](#)” in “[Installation](#)” in the *Novell ZENworks 7 Linux Management Installation Guide*.

## 8.2 Registering a Device after Installing the ZENworks Agent

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

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

Replace *ZEN\_Server\_address* with the IP address or DNS name of the primary or secondary server.



# Managing Registration Keys and Rules

# 9

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

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

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

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

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

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

The two default rules are designed to ensure that no server or workstation registration fails. You can define additional rules that enable you to filter devices as they register and add them to different folders and groups. If, as recommended in **“Folders vs. Groups”** under **“Administration: A Quick Tutorial”** in the *Novell ZENworks 7 Linux Management Installation Guide*, you've established folders for devices with similar configuration settings and groups for devices with similar assignments, newly registered devices automatically receive the appropriate configuration settings and assignments.

The following sections contain additional information:

- ♦ **Section 9.1, “Managing Registration Keys,” on page 54**
- ♦ **Section 9.2, “Managing Registration Rules,” on page 59**

- ♦ [Section 9.3, “Creating Folders,” on page 65](#)

## 9.1 Managing Registration Keys

You can define the keys that are used to register devices in the Management Zone. A registration key specifies a set of assignments that are applied to devices that register using that key. The key must be applied during installation of the ZENworks Agent on a device, either manually or by using a script.

If you do not want to use registration keys, you can create registration rules to determine a device's assignments when it registers without using a key. The major difference between using the default registration rules versus using a registration key is that the default registration rules use a filter to determine which set of device assignments to apply, but a key corresponds directly to a specific set of assignments to apply. For more information, see [Section 9.2, “Managing Registration Rules,” on page 59](#).

The following sections contain additional information:

- ♦ [Section 9.1.1, “Creating Keys to Register Devices,” on page 54](#)
- ♦ [Section 9.1.2, “Editing Existing Registration Keys,” on page 57](#)
- ♦ [Section 9.1.3, “Renaming, Copying, or Moving Registration Keys,” on page 58](#)
- ♦ [Section 9.1.4, “Deleting Registration Keys,” on page 59](#)

### 9.1.1 Creating Keys to Register Devices

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

- 2 In the Registration Keys section, click *New*, then click *Registration* to launch the Create New Registration Key Wizard.

**Create New Registration Key** ?

**Step 1: Basic Information**

Supply the name, description, and the limit for the new registration key. A unique name can be generated by clicking on the "Generate unique key name" icon.

Name (used as the registration key code):

**Generate**

Folder: \*

Description:

Number of times this key can be used:

☒ Unlimited

☐ Limit to:

**<< Back** **Next >>** **Cancel**

- 3 Fill in the fields:

**Name (used as the registration key code):** Provide a name for the registration key. When devices register during installation or later using the `rug sa` command, this is the name the device provides to be assigned this registration. Any device that presents this name is given the assignments associated with this registration.

Choose something simple for reduced security, or click *Generate* to create a complex registration string that is difficult to guess. Use the Generate option along with a registration key limit for increased security.

The following characters cannot be used when creating a registration: # \* ( + \ ; ' " < > / ,

**Folder:** Specify the folder for this registration key. This is for organizational purposes only. Devices do not need to know where a registration key is located in order to register using it, they simply need to know the key name.

**Description:** Provide a description for the key. This description displays in the ZENworks Control Center, which is the administrative tool for ZENworks Linux Management.

**Number of times this key can be used:** Choose whether to allow the key to be used an unlimited number of times or specify a number of times that the key can be used.

For security purposes, this option lets you limit the number of devices that can register using this key.

- 4 Click *Next* to display the Naming and Containment Rules page.

Create New Registration Key sdf2 ?

Step 2: Naming and Containment Rules

Supply the template used to create the machine name, and the folder the machine should be placed in when imported.

Name given to imported machines:

Folder where imported machines should be placed:

---

<< Back    Next >>    Cancel

- 5 Fill in the fields to specify a naming scheme and the folder where the devices will be added:

**Name given to imported machines:** Provide a naming scheme for registering devices. To create a naming scheme, select one or more of the following machine variables:

CPU  
DNS  
GUID  
Hostname (default)  
OS

Avoid spaces in your naming scheme, because these spaces must be escaped when using the command line utilities. For example, use `${HostName}-${OS}` rather than `${HostName} ${OS}`.

**Folder where imported machines should be placed:** Specify the folder where devices should be placed.

As a general rule, devices with similar configuration settings (refresh intervals, logging settings, remote management settings, and so forth) should be grouped in the same folder so that you can specify the configuration settings on the folder and have the devices in the folder inherit them. You should not use the same folder for devices that require different configuration settings; doing so would prohibit you from using the folder to define the settings and force you to define them on each individual device.



- 6 Click *Next* to display the Group Membership page.

Create New Registration Key sdf2

Step 3: Group Membership

Supply the groups new machines should be placed in when imported.  
Note: only groups that are valid for the folder selected in the previous step will be selectable.

Add	Remove
<input type="checkbox"/>	Name In Folder

No items selected, click add to select items

<< Back Next >> Cancel

Adding groups causes registering devices to receive any assignments provided by membership in the groups. Assignments from group membership are additive, so if a device is assigned to both group A and group B, the device receives all assignments from both groups.

Click *Add* to add a group. You can only add groups that are valid for the type of device folder you specified on the previous page of the wizard. For example, if you specified the / Devices/Workstations folder, you can only choose workstation groups.

- 7 Click *Next* to display the Summary page.
- 8 Review the information on the Summary page, making any changes to the settings by using the *Back* button as necessary. Click *Finish* to create the registration key according to the settings on the Summary page.

## 9.1.2 Editing Existing Registration Keys

- 1 In the ZENworks Control Center, click the *Configuration* tab.
- 2 Click the underlined link for the registration key that you want to edit.

**NOTE:** If you edit an existing registration key, be aware that the changes you make apply only to newly registered devices. If the device is already registered, the original settings remain. For example, if you change the naming and folder containment settings, those devices already registered will retain the previous naming convention and remain in the original folder they were placed in. You could, however, unregister the devices and then reregister them to ensure that the new naming convention and folder containment settings are applied to the previously registered devices. For more information, see [Chapter 10, “Unregistering and Reregistering Devices,”](#) on page 67.

- 2a (Optional) In the General section, make the desired changes:

**Description:** Edit the description for the key. This description displays in the ZENworks Control Center, which is the administrative tool for ZENworks Linux Management.

**Number of times this key can be used:** Choose whether to allow the key to be used an unlimited number of times or specify a number of times that the key can be used.

For security purposes, this option lets you limit the number of devices that can register using this key.

**2b** (Optional) In the Values Applied to Imported Machines section, make the desired changes:

**Name given to imported machines:** Select one or more machine variables to provide a naming scheme for registering devices.

Avoid spaces in your naming scheme, because these spaces must be escaped when using the command line utilities. For example, use `${HostName}-${OS}` rather than `${HostName} ${OS}`.

**Folder where imported machines should be placed:** Specify the folder where devices should be placed.

As a general rule, devices with similar configuration settings (refresh intervals, logging settings, remote management settings, and so forth) should be grouped in the same folder so that you can specify the configuration settings on the folder and have the devices in the folder inherit them. You should not use the same folder for devices that require different configuration settings; doing so would prohibit you from using the folder to define the settings and force you to define them on each individual device.

**Group membership:** Click *Add* to add a group. You can only add groups that are valid for the type of device folder you specified on the previous page of the wizard. For example, if you specified the `/Devices/Workstations` folder, you can only choose workstation groups. To remove a group, select the box next to the group's name, then click *Remove*.

---

**NOTE:** If you change group membership for a device and then reregister it, the previous group membership is left intact and the new group membership is added. For example, deviceA is a member of group1. You then edit the key to change membership to group2. When the device is reregistered, the device will be a member of both groups.

---

**3** Click *Apply*.

### 9.1.3 Renaming, Copying, or Moving Registration Keys

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

**2** In the Registration Keys section, click *Advanced*.

**3** Select a registration key by selecting the box next to its name, click *Edit*, then click an option:

- ♦ **Rename:** Click *Rename*, type a new name for the registration key, then click *OK*.
- ♦ **Copy:** Click *Copy*, type a new name for the registration key, then click *OK*.

The copy option is useful to create a new registration key that is similar to an existing key. You can copy a key and then edit the new key's settings.

- ♦ **Move:** Click *Move*, choose a destination folder for the selected objects, then click *OK*.

The folder for registration keys is for organizational purposes only. Devices do not need to know where a registration key is located in order to register using it, they simply need to know the key name.

---

**NOTE:** Some actions cannot be performed on multiple objects. For example, if more than one check box is selected, the *Rename* and *Copy* options are not available from the *Edit* menu.

---

### 9.1.4 Deleting Registration Keys

- 1 In the ZENworks Control Center, click the *Configuration* tab.
- 2 Select the key by clicking the check box next to the key, then click *Delete*.

## 9.2 Managing Registration Rules

Registration rules let you determine a device's assignments when it registers without using a key. The major difference between using the default registration rules versus using a registration key is that the default registration rules use a filter to determine which set of device assignments to apply, but a key corresponds directly to a specific set of assignments to apply.

By default, the list includes a default registration rule for servers and another one for workstations. These two rules cause all servers to be added to the */Servers* folder and all workstations to the */Workstations* folder. The device hostname is used for its name. You cannot delete these two default rules, but you can modify the naming scheme and the groups to which the servers and workstation are added.

The two server and workstation default rules are designed to ensure that no server or workstation registration fails. You can, however, define additional rules that enable you to filter devices as they register and add them to different folders and groups. If you establish folders for devices with similar configuration settings and groups for devices with similar bundle and policy assignments, newly registered devices automatically receive the configuration settings and assignments appropriate to them.

If you do not want to use registration rules, you can create registration keys. Using registration keys lets you define the keys that are used to register devices in the Management Zone. For more information, see [Section 9.1, “Managing Registration Keys,” on page 54](#).

The following sections contain additional information:

- ♦ [Section 9.2.1, “Creating Rules to Register Devices,” on page 59](#)
- ♦ [Section 9.2.2, “Editing Existing Registration Rules,” on page 63](#)
- ♦ [Section 9.2.3, “Renaming or Copying Registration Rules,” on page 64](#)
- ♦ [Section 9.2.4, “Reordering Registration Rules,” on page 65](#)
- ♦ [Section 9.2.5, “Deleting Registration Rules,” on page 65](#)

### 9.2.1 Creating Rules to Register Devices

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

- 2 In the Default Registration Rules section, click *New* to launch the Create New Default Rule Wizard.

Create New Default Rule ?

Step 1: Basic Information

Supply the name and description for the new Default Rule.

Name:

Description:

<< Back Next >> Cancel

- 3 Fill in the fields:

**Name:** Provide a name for the registration rule.

**Description:** Provide a description if desired. The description is displayed on the rule's Details page. If you are creating several registration rules, you might want to use the description to detail each rule.

- 4 Click *Next* to display the Import Filters page.

Create New Default Rule ?

Step 2: Import Filters

Specify the criteria used for determining which machines should use this Default Registration Rule.

Add Filter Delete

Import machines matching the following criteria:

<< Back Next >> Cancel

- 5 Click *Add Filter* to specify the criteria used to determine which devices should use this Default Registration Rule.

**5a** Select an option from the drop-down list in the left field, select *Equal to*, *Contains*, *Starts with*, or *Ends with* from the drop-down list in the center field, then type a value in the right field.

The options you can use are listed below, along with possible values. The format for all values, with the exception of Device Type, is free form string.

Criteria	Possible Value
CPU	Intel Pentium M processor 1600MHz
DNS	abc.xyz.com
Device Type	Server or Workstation
GUID	5bf63fb9b1ed4cd880e1a428a1fcf737
Hostname	zenserver
IPAddress	123.456.78.99
OS	<p>The format for this value is not free form; the values for the supported OS platforms are:</p> <p>suse-93-i586  suse-93-x86_64  nld-9-i586  nld-9-x86_64  sles-9-i586  sles-9-x86_64  oes-9-i586  rhel-3as-i386  rhel-3es-i386  rhel-3ws-i386  rhel-4as-i386  rhel-4es-i386  rhel-4ws-i38</p>

**5b** (Conditional) Click *Add Filter* again to add an additional row of criteria and repeat **Step 5a** and **Step 5b**, as many times as necessary.

Be aware that the rows in the filter are separated by And. If you specify multiple rows in the filter, the criteria in all rows must be met for the rule to apply.

- 6 Click *Next* to display the Naming and Containment Rules page.

Create New Default Rule ?

Step 3: Naming and Containment Rules

Supply the template used to create the machine name, and the folder the machine should be placed in when imported.

Name given to imported machines:

Folder where imported machines should be placed:

<< Back Next >> Cancel

- 7 Fill in the fields:

**Name given to imported machines:** Provide a naming scheme for registering devices.

Avoid spaces in your naming scheme, because these spaces must be escaped when using the command line utilities. For example, use `${HostName}-${OS}` rather than `${HostName} ${OS}`.

**Folder where imported machines should be placed:** Specify the folder where devices should be placed.

As a general rule, devices with similar configuration settings (refresh intervals, logging settings, remote management settings, and so forth) should be grouped in the same folder so that you can specify the configuration settings on the folder and have the devices in the folder inherit them. You should not use the same folder for devices that require different configuration settings; doing so would prohibit you from using the folder to define the settings and force you to define them on each individual device.

- 8 Click *Next* to display the Group Membership page.

Create New Default Rule ?

Step 4: Group Membership

Supply the groups new machines should be placed in when imported. Note: only groups that are valid for the folder selected in the previous step will be selectable.

Add	Remove
<input type="checkbox"/>	<input type="checkbox"/>
Name	In Folder

No items selected, click add to select items

<< Back Next >> Cancel

Adding groups causes registering devices to receive any assignments provided by membership in the groups. Assignments from group membership are additive, so if a device is assigned to both group A and group B, the device receives all assignments from both groups.

Click *Add* to add a group. You can only add groups that are valid for the type of device folder you specified on the previous page of the wizard. For example, if you specified the / *Devices/Workstations* folder, you can only choose workstation groups.

- 9 Click *Next* to display the Summary page.
- 10 Review the information on the Summary page, making any changes to the settings by using the *Back* button as necessary. Click *Finish* to create the registration rule according to the settings on the Summary page.

## 9.2.2 Editing Existing Registration Rules

- 1 In the ZENworks Control Center, click the *Configuration* tab.
- 2 Click the underlined link for the registration rule that you want to edit.

---

**NOTE:** If you edit an existing registration rule, be aware that the changes you make apply only to newly registered devices. If the device is already registered, the original settings remain. For example, if you change the naming and folder containment settings, those devices already registered retain the previous naming convention and remain in the original folder they were placed in. You could, however, unregister the devices and then reregister them to ensure that the new naming convention and folder containment settings are applied to the previously registered devices. For more information, see [Chapter 10, “Unregistering and Reregistering Devices,”](#) on page 67.

---

- 3 (Optional) In the General section, make the desired changes:

**Description:** Edit the description for the rule. This description displays in the ZENworks Control Center, which is the administrative tool for ZENworks Linux Management.

- 4 (Optional) In the Import Filters section, make the desired changes.
  - 4a Select an option from the drop-down list in the left field, select *Equal to*, *Contains*, *Starts with*, or *Ends with* from the drop-down list in the center field, then type a value in the right field.

The criteria options you can use are listed below, along with possible values. The format for all values, with the exception of Device Type, is free form string.

Criteria	Possible Value
CPU	Intel Pentium M processor 1600MHz
DNS	abc.xyz.com
Device Type	Server or Workstation
GUID	5bf63fb9b1ed4cd880e1a428a1fcf737
Hostname	zenserver
IPAddress	123.456.78.99

Criteria	Possible Value
OS	<p>The format for this value is not free form; the values for the supported OS platforms are:</p> <p>suse-93-i586  suse-93-x86_64  nld-9-i586  nld-9-x86_64  sles-9-i586  sles-9-x86_64  oes-9-i586  rhel-3as-i386  rhel-3es-i386  rhel-3ws-i386  rhel-4as-i386  rhel-4es-i386  rhel-4ws-i386</p>

- 4b** (Conditional) Click *Add Filter* again to add an additional row of criteria and repeat **Step 4a** and **Step 4b**, as many times as necessary.

Be aware that the rows in the filter are separated by And. If you specify multiple rows in the filter, the criteria in all rows must be met for the rule to apply.

- 5** (Optional) In the Values Applied to Imported Machines section, make the desired changes:

**Name given to imported machines:** Select one or more machine variables to provide a naming scheme for registering devices.

Avoid spaces in your naming scheme, because these spaces must be escaped when using the command line utilities. For example, use `${HostName}-${OS}` rather than `${HostName} ${OS}`.

**Folder where imported machines should be placed:** Specify the folder where devices should be placed.

As a general rule, devices with similar configuration settings (refresh intervals, logging settings, remote management settings, and so forth) should be grouped in the same folder so that you can specify the configuration settings on the folder and have the devices in the folder inherit them. You should not use the same folder for devices that require different configuration settings; doing so would prohibit you from using the folder to define the settings and force you to define them on each individual device.

**Group membership:** Click *Add* to add a group. You can only add groups that are valid for the type of device folder you specified on the previous page of the wizard. For example, if you specified the `/Devices/Workstations` folder, you can only choose workstation groups. To remove a group, select the box next to the group's name, then click *Remove*.

- 6** Click *Apply*.

### 9.2.3 Renaming or Copying Registration Rules

- 1 In the ZENworks Control Center, click the *Configuration* tab.
- 2 In the Default Registration Rules section, click *Advanced*.



**3** Select a registration rule by selecting the box next to its name, click *Edit*, then click an option:

- ♦ **Rename:** Click *Rename*, type a new name for the registration rule, then click *OK*.
- ♦ **Copy:** Click *Copy*, type a new name for the registration rule, then click *OK*.

The copy option is useful to create a new registration rule that is similar to an existing rule. You can copy a key and then edit the new rule's settings.

---

**NOTE:** If more than one check box is selected, the *Rename* and *Copy* options are not available from the *Edit* menu.

---

## 9.2.4 Reordering Registration Rules

Rules are applied from the top down, and only the first matching rule is applied to a registering device. You should order the more restrictive rules first, then the more general rules, followed by the two default server and workstation rules (which always remain the last two rules).

To move a rule up or down in the list:

- 1** Select the rule by selecting the check box next to the rule.
- 2** Click *Move Up* or *Move Down*.

## 9.2.5 Deleting Registration Rules

- 1** In the ZENworks Control Center, click the *Configuration* tab.
- 2** Select the registration rule by selecting the check box next to the rule, then click *Delete*.

## 9.3 Creating Folders

A folder is an organization object that displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management. A folder can contain various objects, including subfolders, registration keys, registration rules, and more.

To create a folder:

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

- 2 Click *New*, then click *Folder* to display the New Folder dialog box.



The image shows a 'New Folder' dialog box with a blue title bar and a close button. It contains three input fields: 'Name: \*' (a text box), 'Folder: \*' (a text box containing '/Bundles' and a browse button), and 'Description:' (a large text area). Below the fields is a note: 'Fields marked with a blue asterisk are required.' At the bottom are 'OK' and 'Cancel' buttons.

- 3 Fill in the fields:
  - ♦ **Name:** Provide a unique name for your folder. This is a required field.
  - ♦ **Folder:** Type the name or browse to the folder that contains this folder in the ZENworks Control Center interface.
  - ♦ **Description:** Provide a short description of the folder's contents.
- 4 Click *OK*.

# Unregistering and Reregistering Devices

# 10

Under certain circumstances, it might be necessary to unregister devices from or reregister devices against the ZENworks® Server.

The following sections contain additional information:

- ♦ [Section 10.1, “Possible Scenarios for Unregistering and Reregistering Devices,” on page 67](#)
- ♦ [Section 10.2, “Unregistering Devices,” on page 68](#)
- ♦ [Section 10.3, “Reregistering Devices,” on page 68](#)

## 10.1 Possible Scenarios for Unregistering and Reregistering Devices

The following list illustrates possible scenarios in which you might want to unregister and reregister devices:

- ♦ You have secondary ZENworks Servers set up by job function (engineering, marketing, and so forth), an employee transfers to another job function, and you want to change the ZENworks Server that the device is registered against.
- ♦ You move a device from one physical location to another and you want to change the device's ZENworks Management Zone or the ZENworks Server that the device is registered against.
- ♦ You want to balance server load by changing the ZENworks Server that a device is registered against.

In these three scenarios, you could unregister the device and then reregister it in another ZENworks Management Zone or against another ZENworks Server. It is not necessary to remove the device object from the ZENworks Control Center because the updated Management Zone or ZENworks Server information is updated in the object's properties.

- ♦ You edit a registration key or registration rule to change the naming convention and folder containment settings as explained in [Section 9.1.2, “Editing Existing Registration Keys,” on page 57](#) and [Section 9.2.2, “Editing Existing Registration Rules,” on page 63](#) and you want all managed devices named and placed in folders according to the new settings.

In this scenario, only newly registered devices use the new settings. You can unregister devices, remove them from the ZENworks Control Center (click the *Devices* tab, navigate to and select devices by selecting the check box next to the their names, then click *Delete*), and then reregister them to ensure that the devices are renamed and placed in the proper folders according to the edited settings.

- ♦ You no longer want to manage a device using ZENworks Linux Management.

When you unregister a device, the device is no longer registered against a ZENworks Server and the device is no longer managed.

---

**IMPORTANT:** If you delete a device object in the ZENworks Control Center but do not unregister the device, when the device is refreshed according to its schedule or if the user runs the rug refresh command, the device reregisters and a corresponding device object is recreated

in the ZENworks Control Center. If you no longer want to manage the device using ZENworks Linux Management, ensure that you unregister the device, as explained below.

---

When you unregister a device, the ZENworks Agent software remains on the device. You can leave the ZENworks Agent on the device in case you want to reregister it, or you can uninstall the ZENworks Agent. For more information, see [Section 4.5, “Uninstalling the ZENworks Agent,” on page 30](#).

## 10.2 Unregistering Devices

To unregister a device, run the following rug command from the device:

```
/opt/novell/zenworks/bin/rug sd
```

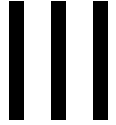
## 10.3 Reregistering Devices

To reregister a device, run the following rug command from the device:

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

Replace *ZEN\_Server\_address* with the IP address or DNS name of the primary or secondary server.

# Policy Management



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

- ♦ Chapter 11, “Policy Management Overview,” on page 71
- ♦ Chapter 12, “Understanding Policies,” on page 73
- ♦ Chapter 13, “Creating Policies,” on page 77
- ♦ Chapter 14, “Managing Policies,” on page 123



# Policy Management Overview

# 11

Novell® ZENworks® Linux Management lets you configure operating system settings and select application settings through the use of policies. By applying a policy to multiple devices, you can ensure that the devices have the same configuration. In addition, if you change a policy after it has already been applied to a device, the policy is reapplied to the device according to the defined schedule.

The following sections contain additional information:

- ♦ [Section 11.1, “Understanding Policies,” on page 71](#)
- ♦ [Section 11.2, “Creating Policies,” on page 71](#)
- ♦ [Section 11.3, “Managing Policies,” on page 72](#)

## 11.1 Understanding Policies

Before you start creating policies, you should have a basic understanding of policies, know the basic terminology, and know the different types of policies available in ZENworks Linux Management. For more information, see [Chapter 12, “Understanding Policies,” on page 73](#).

## 11.2 Creating Policies

ZENworks Linux Management Policies give you the ability to define and lockdown configuration settings on managed devices (servers and workstations). ZENworks Linux Management provides policies for a number of popular applications, including the Novell Linux Desktop. It also includes a policy to execute script, binary, or Java files and a policy to apply changes to text files.

ZENworks Linux Management lets you create the following policies:

**Table 11-1** ZENworks Linux Management Policies

Policy	Description
Epiphany Policy	Configures the Epiphany* Web browser. For step-by-step instructions to create this policy, see <a href="#">Section 13.1, “Epiphany Policy,” on page 77</a> .
Evolution Policy	Configures the Evolution™ e-mail client. For step-by-step instructions to create this policy, see <a href="#">Section 13.2, “Evolution Policy,” on page 83</a> .
Firefox Policy	Configures the Firefox* Web browser. For step-by-step instructions to create this policy, see <a href="#">Section 13.3, “Firefox Policy,” on page 90</a> .
Generic GNOME Policy	Configures the GNOME-based applications. For step-by-step instructions to create this policy, see <a href="#">Section 13.4, “Generic GNOME Policy,” on page 97</a> .
Novell Linux Desktop Policy	Configures the Novell Linux Desktop settings. For step-by-step instructions to create this policy, see <a href="#">Section 13.5, “Novell Linux Desktop Policy,” on page 103</a> .

Policy	Description
Remote Execute Policy	Executes a script, binary, or Java file. For step-by-step instructions to create this policy, see <a href="#">Section 13.6, “Remote Execute Policy,” on page 111</a> .
Text File Policy	Applies changes to a text file. For step-by-step instructions to create this policy, see <a href="#">Section 13.7, “Text File Policy,” on page 116</a> .

---

**NOTE:** The Epiphany, Evolution, Firefox, Generic GNOME, and Novell Linux Desktop policies are referred as GConf-based policies.

---

## 11.3 Managing Policies

In addition to creating policies, as described in [Chapter 13, “Creating Policies,” on page 77](#), you can create folders to organize policies, create policy groups to ease administration of policies, assign policies to devices, edit existing policies, and more.

For more information, see [Chapter 14, “Managing Policies,” on page 123](#).



Novell® ZENworks® Linux Management policies provide a mechanism of uniformly configuring applications. ZENworks policies let you configure system and application settings and then set them as Lockdown or Default. Lockdown lets you restrict users from changing settings, so the application must use the values that are configured in the policy. Default lets users change settings.

A policy applies to all users on assigned devices. You can use the Lockdown and Default mechanisms to configure applications in such a way that critical and important settings are locked and an appropriate default value is provided for other settings that might be relevant. Also, if you do not want to enforce a particular setting, you can exclude that setting while creating or editing a policy.

You can also use policies to modify configuration files and execute scripts or programs on managed devices.

Policies can be used to create a set of configurations that you can deploy on any number of managed devices, thereby providing the devices with a uniform configuration and eliminating the need to configure each device separately. You can also create policies with different settings and assign them appropriately to give a different configuration to a specific set of devices.

On managed devices, each policy type is enforced by a Policy Handler/Enforcer, which makes all the configuration changes necessary to enforce and unenforce the settings in a given policy. The Policy Handler/Enforcer executes with root privileges.

The following sections provide basic concepts you should understand as you begin using policies:

- ♦ [Section 12.1, “Types of Policies,” on page 73](#)
- ♦ [Section 12.2, “Assignments,” on page 74](#)
- ♦ [Section 12.3, “Schedules,” on page 74](#)
- ♦ [Section 12.4, “Groups,” on page 75](#)
- ♦ [Section 12.5, “System Requirements,” on page 75](#)
- ♦ [Section 12.6, “Effective Policies,” on page 76](#)

## 12.1 Types of Policies

ZENworks lets you create the following types of policies:

- ♦ **Epiphany policy:** Lets you disable certain Epiphany\* Web browser settings, such as automatic downloading and opening of files, loading contents from unsafe protocols, and accessing the browser's History. The Epiphany policy also lets you configure a default home page, configure cookie settings, and more. For step-by-step instructions to create this policy, see [Section 13.1, “Epiphany Policy,” on page 77](#).
- ♦ **Evolution policy:** Lets you disable certain Evolution™ e-mail client settings, such as signatures, showing only subscribed folders, and overriding the server-supplied folder namespace. The Evolution policy also lets you configure image settings, junk e-mail settings, Mime types settings, and more. For step-by-step instructions to create this policy, see [Section 13.2, “Evolution Policy,” on page 83](#).

- ♦ **Firefox policy:** Lets you disable certain Firefox\* Web browser settings, such as saving passwords and updating themes and extensions. The Firefox policy lets you configure pop-ups, JavaScript control, and more. For step-by-step instructions to create this policy, see [Section 13.3, “Firefox Policy,” on page 90](#).
- ♦ **Generic GNOME policy:** Lets you configure GConf-based applications. You can import settings from a device that is registered with the ZENworks Linux Management Server or you can define your own GConf settings. While importing settings from a device, the system imports all settings, including default settings, from that device. You must specify the name of a user on the device from where you are importing the GConf settings. Only those GConf settings are imported that are related to the user you have specified. For step-by-step instructions to create this policy, see [Section 13.4, “Generic GNOME Policy,” on page 97](#).
- ♦ **Novell Linux Desktop policy:** Lets you configure the Novell Linux Desktop settings. This policy lets you remove certain items from the system menu, program menu, and personal settings. It also lets you configure background image settings, shade settings, proxy settings, and more. For step-by-step instructions to create this policy, see [Section 13.5, “Novell Linux Desktop Policy,” on page 103](#).
- ♦ **Remote Execute policy:** Executes a script, binary, or Java file. The Remote Execute policy also lets you specify your own script to be executed on managed devices. For step-by-step instructions to create this policy, see [Section 13.6, “Remote Execute Policy,” on page 111](#).
- ♦ **Text File policy:** Applies changes to a text file. The Text File policy lets you append or prepend to a file and also lets you apply a search-based change in which a given string in the file can be replaced with another string, be deleted, and so forth. The search string can be specified using a regular expression.

This policy also allows you to execute a script, binary, or Java program before and after the text-file modification. It can be used for example, to change a configuration file. You might want to stop a service before the file is modified and restart the service after the file modification.

While creating a policy, only one file and one change can be specified. Editing a policy allows you to add multiple files and specify more than one change to a file. For step-by-step instructions to create this policy, see [Section 13.7, “Text File Policy,” on page 116](#).

## 12.2 Assignments

You can assign a policy directly to a device, or you can assign it to a folder or group in which the device is a member. As a general rule, you should try to assign policies to device groups rather than device folders.

## 12.3 Schedules

When assigning a policy to a device, you can specify the schedule for applying the policy. Depending on the type of policy being applied, the following schedules are available. Click the link in the left frame for details about each policy and its options, which vary, depending on the schedule.

**Table 12-1** Available Schedules

Schedule Type	Description	Applicable For
No Schedule	Use this option to indicate no schedule; no action occurs.	All policies
Date Specific	Select one or more dates on which to enforce the policy on devices and set other restrictions that might apply.	Remote Execute and Text File policies
Day of the Week Specific	Select one or more days of the week on which to enforce the policy on devices and set other restrictions that might apply.	Remote Execute and Text File policies
Event	Select the event that triggers the enforcement of the policy.	Epiphany, Evolution, Firefox, Generic GNOME, and Novell Linux Desktop policies.
Monthly	Select the day of the month on which to enforce the policy on devices and set other restrictions that might apply.	Remote Execute and Text File policies
Relative to Refresh	Schedule when the policy is enforced, either immediately after the device refreshes or a specified amount of time after the device refreshes. You can also specify whether the policy's enforcement is repeated and specify a time period when you do not want the policy enforced to help minimize network traffic during that time. For more information, see <a href="#">Section 14.9, "Refreshing Policies,"</a> on page 142.	Remote Execute and Text File policies

## 12.4 Groups

A policy group is a collection of one or more policies. You can create policy groups and assign them to devices the same way you would assign individual policies.

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create. For more information, see [Section 14.3, "Creating Policy Groups,"](#) on page 125.

## 12.5 System Requirements

System requirements specify the conditions that must be satisfied on the managed device for the policy to be effective. System requirements are specified for each policy to ensure that the conditions necessary for a proper enforcement of a policy are met.

The appropriate default system requirements are included in a policy when it is created. When you create or edit a policy, you can modify or remove the requirements. No default system requirement is available for the Text File and Remote Execute policies.

You can change the system requirement setting if the settings included in the policy are available on different versions or platforms. If not, all the settings configured in the policy are not effective. For example, if the Distribution  $\geq$  Novell Linux Desktop 9 requirement is removed from the Firefox policy and the policy is specified to be enforced on all platforms, the settings are not effective because the lockdown option for Firefox is available only for the Novell Linux Desktop.

You should remove the system requirement only if you are sure that it will not cause problems. For example, in a Generic GNOME policy created by importing settings from a device, the system requirement is set to the operating system of the device from which the settings were imported. If you have included settings in the policy that are available on other platforms, you can remove or change the system requirement.

---

**IMPORTANT:** Even if the requirements are removed and the application version or operating system is incompatible, the policy is enforced but a warning message is generated. If the appropriate application (Epiphany, Evolution, or Firefox) is not installed, the policy is not enforced and an error message is generated.

---




## 12.6 Effective Policies

A device inherits its policy assignments from its parent folders, its group memberships, and itself; when conflicting assignments occur, the assignments on the device override group assignments, which override folder assignments.

You can tell which policies are in effect for a device by viewing the Effective Policies section on the Device Summary page. To view the effective policies, click the *Devices* page, navigate the folders to find the device, click the device, then click the *Summary* tab.

All the effective policies are listed under the Effective Policies section on the Device Summary page. The following table provides a description of each icon that indicates the effectiveness of a policy:

**Table 12-2** Policy Status Icons

Icon	Description
	The policy is effective and will be enforced on the device.
	The policy might be effective. The policy will be enforced if the system requirements are met. Otherwise, the policy will not be enforced.
	The policy is not effective and will not be enforced.

For GConf-based policies, the first policy amongst the effective policies, whose system requirements are met, is applied on the device.

For the Text File and Remote Execute policies, all policies whose system requirements are met are applied on the device.

Novell® ZENworks® Linux Management lets you configure operating system settings and select application settings through the use of policies. By applying a policy to multiple devices, you can ensure that the devices have the same configuration. In addition, if you change a policy after it has already been applied to a device, the policy is reapplied to the device as per the defined schedule.

The following sections contain additional information about the available ZENworks Linux Management policies:

- ♦ [Section 13.1, “Epiphany Policy,” on page 77](#)
- ♦ [Section 13.2, “Evolution Policy,” on page 83](#)
- ♦ [Section 13.3, “Firefox Policy,” on page 90](#)
- ♦ [Section 13.4, “Generic GNOME Policy,” on page 97](#)
- ♦ [Section 13.5, “Novell Linux Desktop Policy,” on page 103](#)
- ♦ [Section 13.6, “Remote Execute Policy,” on page 111](#)
- ♦ [Section 13.7, “Text File Policy,” on page 116](#)

## 13.1 Epiphany Policy

The Epiphany policy is used to configure the Epiphany Web browser.

To configure the Epiphany policy:

- 1** In the ZENworks Control Center, click the *Policies* tab.
- 2** In the Policies list, click *New*, then click *Policy* to display the Create New Policy page.

- 3 In the Policy type list, click *Epiphany Policy*, then click *Next* to display the Policy Name page.

Create New Epiphany Policy ?

Step 2: Policy Name

Specify the name of the new policy:

Policy Name: \*

Folder: \*

/Policies

Description:

Fields marked with a blue asterisk are required.

<< Back Next >> Cancel

- 4 Fill in the fields:

- ♦ **Policy name:** (Required) Provide a unique name for the policy. The name you provide displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.
- ♦ **Folder:** (Required) Type the name or browse to the folder that this policy will be created in. Folders display in the ZENworks Control Center.
- ♦ **Description:** Provide a short description of the policy. This description displays on the policy's Summary page in the ZENworks Control Center interface.

5 Click *Next* to display the Epiphany Lockdown Settings page.

Create New Epiphany Policy Epiphany ?

Step 3: Epiphany Lockdown settings

Select the Epiphany settings:

- ☐ Disable Javascript control of window chrome
- ☐ Hide menu bar
- ☐ Disable automatic download and opening of files
- ☐ Disable manual URL entry
- ☐ Disable bookmark editing
- ☐ Disable toolbar editing
- ☐ Disable history
- ☐ Disable loading of content from unsafe protocols. Default safe protocols are HTTP and HTTPS

Safe Protocols list:

^

...

v

Add ...

Remove

<< Back

Next >>

Cancel

6 Select the desired options (by default, all options are disabled):

**Disable JavaScript control of window chrome:** Select this option to disable the JavaScript control and modification of the Epiphany Web browser's window chrome.

The chrome is part of an application window that is positioned outside of the window's content area. A Web page can use JavaScript to control and modify the window chrome. Several elements such as the toolbar, menu bar, progress bar, and title bar are part of the chrome.

**Hide menu bar:** Select this option to hide the menu bar of the Epiphany Web browser.

**Disable automatic download and opening of files:** Select this option to prevent users from downloading and opening files automatically.

If you include this setting in the policy, users are always asked if they want to save a file or open it. For example, if users want to download a file, they are prompted to specify the location to save or open the file. If the user clicks *Open*, the file is downloaded and opened with the corresponding application.

**Disable manual URL entry:** Select this option to prevent users from manually entering URLs in the address bar.

**Disable bookmark editing:** Select this option to prevent users from editing a bookmark.

**Disable toolbar editing:** Select this option to prevent users from editing the toolbar. A toolbar can contain buttons with images and menus, or a combination of both.

**Disable history:** Select this option to prevent users from accessing the history, which contains links to pages recently visited.

**Disable loading of contents from unsafe protocols. Default safe protocols are HTTP and HTTPS:** Select this option to prevent the downloading of data that is transmitted using an unsafe protocol. Unsafe protocols do not encrypt the data sent across a network.

After you check this option, the following buttons are available:

- ♦ **Add:** To add a protocol to the *Safe protocol* list, click *Add*, specify a protocol name, then click *OK*.
- ♦ **Remove:** To remove a protocol from the *Safe protocol* list, select the protocol, then click *Remove*.

7 Click *Next* to display the Epiphany Configuration Settings page.

**Create New Epiphany Policy** Epiphany ?

**Step 4: Epiphany Configuration settings**

Select any Epiphany configuration settings you would like to provide.  
For each setting you select, provide a value, and optionally, enable the lock to prevent the value from changing after it is set.

<input type="checkbox"/>	Homepage URL		<input type="text"/>
<input type="checkbox"/>	Download folder *		<input type="text"/>
<input type="checkbox"/>	Allow Popups		Yes ▾
<input type="checkbox"/>	Allow Java		Yes ▾
<input type="checkbox"/>	Allow Javascript		Yes ▾
<input type="checkbox"/>	Cookies		Always Accept ▾
<input type="checkbox"/>	Disk space for temporary files		50 MB

Fields marked with a blue asterisk are required.

<< Back   Next >>   Cancel

8 Select the desired options (by default, all options are disabled).

For each option you enable, provide a value. When you enable an option, it is locked by default. You can unlock the option by clicking . The options that are not enabled are excluded from the policy and are not applied to the device.

**Homepage URL:** Specify the URL to automatically display when users launch the Epiphany Web browser.

**Download folder:** Specify the directory where you want users to download data. If the folder you specify does not exist, it is created relative to all users' home directories. If you specify an absolute path, ensure that it is at a location where all users have Read and Write access to files.

**Allow popups:** Select this option to allow or disallow pop-ups to be displayed in the Epiphany Web browser.



**Allow Java:** Select this option to allow or disallow Java applications to run on the Epiphany Web browser.

**Allow JavaScript:** Select this option to allow or disallow JavaScript applications to run on the Epiphany Web browser.

**Cookies:** Select this option to configure how the Epiphany Web browser handles cookies.

A cookie is a piece of information given to a Web browser by a Web server. The browser, in turn, stores this information in a file. The available options are *Always accept*, *Only from the sites you visit*, and *Never accept*.

**Disk space for temporary files:** Specify the amount of disk space to allow for storing temporary files for the browser.

- 9 Click *Next* to display the Default System Requirements for Epiphany Policy page.

**Create New Epiphany Policy** Epiphany ?

**Step 5: Default system requirements for Epiphany policy**

The following condition is added as a default system requirement to this policy.  
If the minimum supported version requirement is removed or modified then the policy may not be fully applied and effective on the target device.

☒ Apply policy on devices with version of Epiphany >= 1.2.5 \*

Fields marked with a blue asterisk are required.

<< Back   Next >>   Cancel

- 10 Specify the minimum system requirements that must be satisfied for the Epiphany Web browser policy settings to be effective.

The *Apply policy on devices with version of Epiphany* field displays the minimum version of the Epiphany Web browser required for all policy settings to be effective. Epiphany 1.2.5 is the minimum required version. Policy settings are applied only if the user has the same or later version of the Epiphany Web browser installed. If the user does not have the Epiphany Web browser installed or has an earlier version than the specified version, the policy does not apply.

Even if you do not include this system requirement in the policy, the system checks whether the Epiphany Web browser is installed on a managed device or not. If the system finds that the Epiphany Web browser is installed on a device, it also checks the version. If it finds an earlier version than the specified one, the policy is enforced but a warning message is generated. If the Epiphany Web browser is not installed on a managed device, the policy is not enforced and an error message is generated.

- 11 Click *Next* to display the Summary page.
- 12 Click *Finish* to create the policy as configured according to the settings on the Summary page. If you click *Finish*, the Epiphany policy is created but it does not have devices assigned or a schedule specified. At some point in the future, you need to configure additional options for the policy by continuing with [Section 14.4, “Assigning Policies,” on page 128](#).

or

Click *Next* to display the Policy Assignment page to perform the following tasks:

- ♦ Specify assignments for this policy

- ♦ Specify the schedule for this policy
- ♦ Specify groups for this policy

Create New Epiphany Policy	Epiphany	?
Step 7: Policy Assignments		

Specify the assignments for this policy:

Add Remove	
<input type="checkbox"/>	Name In Folder
No items selected, click add to select items	

**13** Assign the policy to the devices.

**13a** Click *Add* to browse for and select the appropriate Server or Workstation objects.

You can also select Folder or Group objects.

**13b** Click the down-arrow next to Servers or Workstations to expand the list, then click the underlined link in the Name column to select the desired objects and display their names in the Selected list box.

Assigning a policy to a Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.

**13c** Click *OK*.

**14** Click *Next* to display the Policy Schedule page.

Create New Epiphany Policy	Epiphany	?
Step 8: Policy Schedule		

Select the schedule to apply to the policy assignments:

Schedule Type:

No Schedule

**15** Select the schedule to apply to the assignments from the drop-down list, then select the desired options, which vary, depending on the schedule type you select.

The settings you configure on this page determine when the policy is applied to devices.

See [Section 12.3, “Schedules,” on page 74](#) for information about the available schedules and their options.

- 16 Click *Next* to display the Policy Groups page.

Create New Epiphany Policy Epiphany ?

Step 9: Policy Groups

Specify the groups for this policy:

Add	Remove	Name	In Folder
No items selected, click add to select items			

<< Back Next >> Cancel

- 17 (Optional) Click *Add* to open the Select Groups dialog box, then click the underlined links in the Name column to select the desired policy groups and display their names in the Selected list box.

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create. For more information, see [Section 14.3, “Creating Policy Groups,” on page 125](#).

- 18 Click *Next* to display the Finish page.
- 19 Review the information on the Finish page, making any changes to the policy settings by using the *Back* button as necessary. Click *Finish* to create the policy as configured according to the settings on the Finish page.

## 13.2 Evolution Policy

The Evolution policy is used to configure the Evolution e-mail client.

To configure the Evolution policy:

- 1 In the ZENworks Control Center, click the *Policies* tab.
- 2 In the Policies list, click *New*, then click *Policy* to display the Create New Policy page.

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

**Create New Evolution Policy** **www** ?

**Step 2: Policy Name**

Specify the name of the new policy:

Policy Name: \*

Folder: \*

/Policies

Description:

Fields marked with a blue asterisk are required.

<< Back   Next >>   Cancel

- 4 Fill in the fields:

- ♦ **Policy name:** (Required) Provide a unique name for the policy. The name you provide displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.
- ♦ **Folder:** (Required) Type the name or browse to the folder that this policy will be created in. Folders display in the ZENworks Control Center.
- ♦ **Description:** Provide a short description of the policy. This description displays on the policy's Summary page in the ZENworks Control Center interface.

5 Click *Next* to display the Evolution Lockdown Settings page.

Create New Evolution Policy Evolution ?

Step 3: Evolution Lockdown Settings

Select the Evolution Mail Client settings that you do not want your users to change:

- ☐ Apply filters to new messages option
- ☐ Secure Socket Layer (SSL) option
- ☐ E-mail signature
- ☐ E-mail server authentication method
- ☐ Automatically check for new mail option
- ☐ Sent and draft mail folder locations
- ☐ Save password option
- ☐ Receive mail configuration
- ☐ Send mail configuration
- ☐ Show only subscribed folders (for IMAP Mail Accounts)
- ☐ Override server-supplied folder namespace (for IMAP Mail Accounts)

<< Back Next >> Cancel

6 Select the desired options (by default, all options are disabled):

The options on this page allow you to prevent users from changing the following Evolution e-mail client settings. Select an option to prevent users from changing that setting in the Evolution e-mail client.

**Apply filter to new messages option:** Applies the filter to all new messages users receive.

**Secure Socket Layer (SSL) option:** Specifies whether the Evolution e-mail client should connect to the server using SSL.

SSL is a protocol that provides encrypted communications on the network and enables secure communications between the Evolution client and the server.

**E-Mail signature:** Specifies whether an e-mail signature should be added to the contents of a message.

**E-mail server authentication method:** Specifies the kind of authentication to be used when users connect to the mail server.

**Automatically check for new mail option:** Specifies whether the Evolution client should automatically check for new mail.

**Sent and draft mail folder locations:** Specifies which folders users can select to store draft and sent mail.

**Save password option:** Specifies whether passwords should be saved so that users are not prompted for a password at every login.

**Receive mail configuration:** Configures the various options for receiving mail. For example, e-mail server and authentication details, checking for new mails, and applying filters.

**Send mail configuration:** Configures the various options for sending mail, for example, server and authentication details.

**Show only subscribed folders (for IMAP mail accounts):** Specifies that only the subscribed IMAP folders be shown to users. Internet Message Access Protocol (IMAP) lets users access e-mail messages that are stored on the mail server. Because the mail folders exist on the IMAP server and accessing them is time-consuming, Evolution lets users subscribe to certain IMAP folders.


**Override server-supplied folder namespace (for IMAP mail accounts):** Lets users change the IMAP name space that contains mail messages for the server.

**NOTE:** Users cannot create a new Evolution e-mail account if Receive Mail Configuration and Send Mail Configuration settings are included in the policy. These settings should be included in the policy only if the users' e-mail accounts have been created in the Evolution e-mail client.

- 7 Click *Next* to display the Evolution Configuration Settings page.








Create New Evolution Policy

Evolution

 **Step 4: Evolution Configuration Settings**

Select any e-mail configuration setting you would like to provide.

For each setting you select, provide a value, and optionally, enable the lock to prevent the value from changing after it is set.

<input type="checkbox"/>	Default character encoding for display		Western European (ISO-8859-1)
<input type="checkbox"/>	Default character encoding for composed mail		Western European (ISO-8859-1)
<input type="checkbox"/>	Empty Trash folders on exit		Never
<input type="checkbox"/>	Check inbox for junk mail		Yes
<input type="checkbox"/>	Include remote junk mail tests		No
<input type="checkbox"/>	Loading Images		Never load images off the net
<input type="checkbox"/>	Mime Types available for viewing Attachments		

Mime Types available

application/andrew-inset  
application/msword  
application/octet-stream  
application/oda  
application/pdf  
application/pgp


Mime Types selected

<< Back

Next >>

Cancel

- 8 Select the desired options (by default, all options are disabled).

For each option you enable, provide a value. When you enable an option, it is locked by default. You can unlock the option by clicking . The options that are not enabled are excluded from the policy and are not applied to the device.

**Default character encoding for display:** Lets you choose a character interpretation set for displaying e-mail messages. The default character interpretation set is Western European (ISO-8859-1).

**Default character encoding for composed mail:** Lets you choose a character interpretation set for composing e-mail messages. The default character interpretation set is Western European (ISO-8859-1).

**Empty trash folders on exit:** Lets you specify when to empty the Trash folder. The available options are Never, Every time, Once per day, Once per week, and Once per month.

**Check inbox for junk mail:** Lets you specify if the incoming mail must be checked for junk mail.

**Include remote junk mail tests:** Lets you specify if the remote junk filtering option should be used for filtering incoming mail.

For example, the Evolution client stores a message in the Junk Mail folder if it finds the mail address a blacklisted address.

**Loading Images:** Lets you decide how images embedded in e-mail messages are loaded in the Evolution client.

The following options are available:

- ♦ **Never load images off the Internet:** If you select this option, the Evolution e-mail client never loads images. If you select this option users can still view the images in the message by selecting the appropriate menu options in the Evolution e-mail client.
- ♦ **Load images if sender is in address book:** If you select this option, images are loaded only if the sender of the e-mail message is in the receiver's address book.
- ♦ **Always load images off the Internet:** If you select this option, images are loaded regardless of their source.

**Mime types available for viewing attachments:** Lets you select the MIME types that Evolution allows to be viewed using available Bonobo controls.

Evolution provides built-in support for opening certain MIME types. Those MIME types that are not supported by Evolution can be viewed by using certain available Bonobo controls. Bonobo controls provide a means to view both the MIME types that are supported and those that are not supported by Evolution.

After you select this option, you can select items from the *Mime types available* list and then use the arrow button to move the selected item to the *Mime types selected* list.

- 9 Click *Next* to display the Default System Requirements for Evolution Policy page.

**Create New Evolution Policy** Evolution ?

**Step 5: Default system requirements for Evolution policy**

The following condition is added as a default system requirement to this policy.  
If the minimum supported version requirement is removed or modified then the policy may not be fully applied and effective on the target device.

☒ Apply policy on devices with version of Evolution >= 2.0.1 \*

Fields marked with a blue asterisk are required.

<< Back Next >> Cancel

- 10 Specify the minimum system requirements that must be satisfied for the Evolution policy settings to be effective.

The *Apply policy on devices with version of Evolution* field displays the minimum version of the Evolution client required for all policy settings to be effective. Evolution 2.0.1 is the minimum required version. Policy settings are applied only if the user has the same or a later version of the Evolution e-mail client installed. If the user does not have the Evolution e-mail client installed or has an earlier version than the specified version, the policy does not apply.

Even if you do not include this system requirement in the policy, the system checks whether the Evolution client is installed on a managed device or not. If the system finds the Evolution client on a device, it also checks the version. If it finds an earlier version than the specified one, the policy is enforced but a warning message is generated. If the Evolution client is not installed on a managed device, the policy is not enforced and an error message is generated.

- 11 Click *Next* to display the Summary page.
- 12 Click *Finish* to create the policy as configured according to the settings on the Summary page. If you click *Finish*, the Evolution policy is created but it does not have devices assigned or a schedule specified. At some point in the future, you need to configure additional options for the policy by continuing with [Section 14.4, "Assigning Policies," on page 128](#).
- or

Click *Next* to display the Policy Assignment page to perform the following tasks:

- ◆ Specify assignments for this policy
- ◆ Specify the schedule for this policy
- ◆ Specify groups for this policy



Create New Evolution Policy

Evolution

?

Step 7: Policy Assignments

Specify the assignments for this policy:

Add	Remove
<input type="checkbox"/>	<input type="checkbox"/>
Name	In Folder
No items selected, click add to select items	

<< Back

Next >>

Cancel

**13** Assign the policy to the devices.

**13a** Click *Add* to browse for and select the appropriate Server or Workstation objects.

You can also select Folder or Group objects.

**13b** Click the down-arrow next to Servers or Workstations to expand the list, then click the underlined link in the Name column to select the desired objects and display their names in the Selected list box.

Assigning a policy to a Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.

**13c** Click *OK*.

**14** Click *Next* to display the Policy Schedule page.

Create New Evolution Policy

Evolution

?

Step 8: Policy Schedule

Select the schedule to apply to the policy assignments:

Schedule Type:

No Schedule

<< Back

Next >>

Cancel

**15** Select the schedule to apply to the assignments from the drop-down list, then select the desired options, which vary, depending on the schedule type you select.

The settings you configure on this page determine when the policy is applied to devices.

See [Section 12.3, “Schedules,” on page 74](#) for information about the available schedules and their options.

- 16 Click *Next* to display the Policy Groups page.

Create New Evolution Policy Evolution ?

Step 9: Policy Groups

Specify the groups for this policy:

Add	Remove	Name	In Folder
No items selected, click add to select items			

<< Back Next >> Cancel

- 17 (Optional) Click *Add* to open the Select Groups dialog box, then click the underlined links in the Name column to select the desired policy groups and display their names in the Selected list box.

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create. For more information, see [Section 14.3, “Creating Policy Groups,” on page 125](#).

- 18 Click *Next* to display the Finish page.
- 19 Review the information on the Finish page, making any changes to the policy settings by using the *Back* button as necessary. Click *Finish* to create the policy as configured according to the settings on the Finish page.

## 13.3 Firefox Policy

The Firefox policy is used to configure the Mozilla\* Firefox\* Web browser.

The Firefox policy is supported only if the lockdown version of Firefox is available on the Novell Linux Desktop.

To configure the Firefox policy:

- 1 In the ZENworks Control Center, click the *Policies* tab.
- 2 In the Policies list, click *New*, then click *Policy* to display the Create New Policy page.

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

Create New Firefox Policy ?

Step 2: Policy Name

Specify the name of the new policy:

Policy Name: \*

Folder: \*

/Policies

Description:

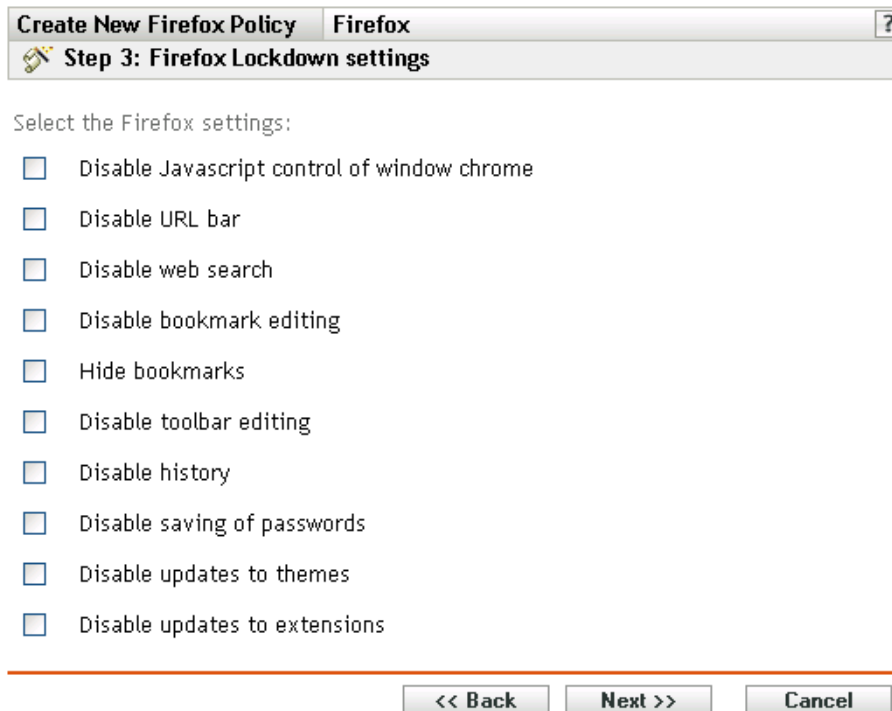
Fields marked with a blue asterisk are required.

<< Back Next >> Cancel

4 Fill in the fields:

- ♦ **Policy name:** (Required) Provide a unique name for the policy. The name you provide displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.
- ♦ **Folder:** (Required) Type the name or browse to the folder that this policy will be created in. Folders display in the ZENworks Control Center.
- ♦ **Description:** Provide a short description of the policy. This description displays on the policy's Summary page in the ZENworks Control Center interface.

- 5 Click *Next* to display the Firefox Lockdown Settings page.



**Create New Firefox Policy** Firefox ?

**Step 3: Firefox Lockdown settings**

Select the Firefox settings:

- ☐ Disable Javascript control of window chrome
- ☐ Disable URL bar
- ☐ Disable web search
- ☐ Disable bookmark editing
- ☐ Hide bookmarks
- ☐ Disable toolbar editing
- ☐ Disable history
- ☐ Disable saving of passwords
- ☐ Disable updates to themes
- ☐ Disable updates to extensions

<< Back   Next >>   Cancel

- 6 Select the desired options (by default, all options are disabled):

**Disable Javascript control of window chrome:** Select this option to disable the JavaScript control and modification of the Firefox Web browser's window chrome.

The chrome is part of an application window that is positioned outside of the window's content area. A Web page can use JavaScript to control and modify the window chrome. Several elements such as the toolbar, menu bar, progress bar, and title bar are part of the chrome.

**Disable URL bar:** Select this option to prevent users from manually entering URLs in the address bar.

**Disable web search:** Select this option to prevent users from using the Web search bar to search the Web pages. If you select this option, the search bar and Add Engine option are disabled.

**Disable bookmark editing:** Select this option to prevent users from editing a bookmark.

**Hide bookmarks:** Select this option to hide bookmarks, including all the bookmarks listed in the Bookmark menu and bookmarks toolbar. Make sure that you select Disable Bookmark Editing if you select the Hide Bookmarks option.

**Disable toolbar editing:** Select this option to prevent users from editing the toolbar. A toolbar can contain buttons with images and menus, or a combination of both.

**Disable history:** Select this option to prevent users from accessing the History, which contains links to pages recently visited.

**Disable saving of password:** Select this option to prevent Firefox from saving users' passwords. Whenever a user enters a password in Firefox, it prompts the user and asks if the password should be saved. If the user clicks Yes, Firefox saves the password and fills it in automatically whenever the user visits that page again.

**Disable updates to themes:** Select this option to prevent users from updating a theme file.

The theme file contains the Control, Window Border, and Icons elements, which determine the appearance of user's browser. Themes are skins for Firefox, and they allow you to change the look and feel of the browser and personalize it to your taste. A theme can simply change the colors of Firefox or it can change the entire browser appearance.

**Disable updates to extensions:** Select this option to prevent users from updating the extensions to add a new functionality to Firefox.

Extensions are add-ons that add new functionality to Firefox. They can add anything from a toolbar button to a completely new feature. Extensions customize the browser to fit the personal needs of each user. For example, an extension can be used to add an IRC client to Firefox or to automatically copy highlighted content to the clipboard.

7 Click *Next* to display the Firefox Configuration Settings page.

Create New Firefox Policy Firefox ?

Step 4: Firefox Configuration settings

Select any Firefox configuration settings you would like to provide.  
For each setting you select, provide a value, and optionally, enable the lock to prevent the value from changing after it is set.

☐ Homepage URL

☐ Allow Popups Yes ▾

☐ Allow Java Yes ▾

☐ Allow Javascript Yes ▾

☐ Allow sites to set cookies Yes ▾

☐ Keep Cookies  ▾

☐ Allow loading of images Anywhere ▾

☐ Disk space for temporary files 50 MB

☐ Download Folder

☒ Ask the user where to save every file

☐ Save all files to this folder  ▾

Folder path  \*

Fields marked with a blue asterisk are required.

<< Back Next >> Cancel

8 Select the desired options (by default, all options are disabled).

For each option you enable, provide a value. When you enable an option, it is locked by default. You can unlock the option by clicking . The options that are not enabled are excluded from the policy and are not applied to the device.

**Homepage URL:** Specify the URL to automatically display when users launch the Firefox Web browser.

**Allow popups:** Select this option to allow or disallow pop-ups to be displayed in the Firefox Web browser.

**Allow Java:** Select this option to allow or disallow Java applications to run on the Firefox Web browser.

**Allow JavaScript:** Select this option to allow or disallow JavaScript applications to run on the Firefox Web browser.

**Allow sites to set cookies:** Select this option to configure how Firefox handles cookies.

A cookie is a piece of information given to a Web browser by a Web server. The browser stores this information in a file.

You can select a value in the Keep Cookies drop-down list to specify if a Web server should be allowed to set cookies.

If you select Yes, specify how long to store the cookies:

- ♦ **Until they expire:** Firefox retains a cookie until it expires.
- ♦ **Ask me every time:** Firefox asks the user about the action to be taken with each cookie. Users can select *Allow*, *Allow for this session only*, or *Deny*.
- ♦ **Until I close Firefox:** Firefox retains cookies while the browser is open. When the browser is closed, Firefox removes all cookies.

**Allow loading of images:** Lets you specify the source from where images are loaded.

The following options are available:

- ♦ **Anywhere:** If you select this option, images are loaded regardless of their source.
- ♦ **From originating website only:** If you select this option, images are loaded only if the source of the images is the current site.
- ♦ **Never:** If you select this option, Firefox never loads images.

**Disk space for temporary files:** Specify the disk space allowed to store temporary files for the browser.

**Download folder:** Lets you specify the directory where you want users to save downloaded files.

The following options are available:

- ♦ **Ask the user where to save every file:** If you select this option, Firefox asks the users where to save files every time files are downloaded.
- ♦ **Save all files to this folder:** If you select this option, specify a location to save files.

The following options are available:

- ♦ **Desktop:** Select Desktop to save downloaded files on the Desktop.
- ♦ **My Downloads:** Select My Downloads to save downloaded files in the My Downloads folder.
- ♦ **Home:** Select Home to save the downloaded files in a folder in the Home directory.
- ♦ **Other:** Select Other to store the downloaded files in a location of your choice. Specify the complete path, including the directory where the downloaded files should be saved.

- 9 Click *Next* to display the Default System Requirements for Mozilla Firefox policy page.

The screenshot shows a dialog box titled 'Create New Firefox Policy' with a sub-tab 'Firefox'. Below the title bar, it says 'Step 5: Default system requirements for Mozilla Firefox policy'. The main text area contains the following information:

The following condition is added as a default system requirement to this policy.  
If the minimum supported version requirement is removed or modified then the policy may not be fully applied and effective on the target device.

☒ Apply policy on Novell Linux Desktop with Firefox version >=  \*

Fields marked with a blue asterisk are required.

At the bottom, there are three buttons: '<< Back', 'Next >>', and 'Cancel'.

- 10 Specify the minimum system requirements that must be satisfied for the Firefox Web browser policy settings to be effective.

The *Apply policy on Novell Linux Desktop with Firefox version* field displays the minimum version of Firefox required for all policy settings to be effective. Firefox 1.0.4 is the minimum required version. Policy settings are applied only if user has the same version or a later version of Firefox installed. If the user does not have Firefox installed or has an earlier version than the specified version, the policy does not apply.

Even if you do not include this system requirement in the policy, the system checks whether Firefox is installed on a managed device or not. If the system finds that Firefox is installed on a device, it also checks the version. If it finds an earlier version than the specified one, the policy is enforced but a warning message is generated. If Firefox is not installed on a managed device, the policy is not enforced and an error message is generated.

- 11 Click *Next* to display the Summary page.
- 12 Click *Finish* to create the policy as configured according to the settings on the Summary page. If you click *Finish*, the Firefox policy is created but it does not have devices assigned or a schedule specified. At some point in the future, you need to configure additional options for the policy by continuing with [Section 14.4, “Assigning Policies,” on page 128](#).

or

Click *Next* to display the Policy Assignment page to perform the following tasks:

- ♦ Specify assignments for this policy
- ♦ Specify the schedule for this policy
- ♦ Specify groups for this policy

Create New Firefox Policy Firefox ?

**Step 7: Policy Assignments**

Specify the assignments for this policy:

Add	Remove	Name	In Folder
No items selected, click add to select items			

<< Back Next >> Cancel

**13** Assign the policy to the devices.

**13a** Click *Add* to browse for and select the appropriate Server or Workstation objects.

You can also select Folder or Group objects.

**13b** Click the down-arrow next to Servers or Workstations to expand the list, then click the underlined link in the Name column to select the desired objects and display their names in the Selected list box.

Assigning a policy to a Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.

**13c** Click *OK*.

**14** Click *Next* to display the Policy Schedule page.

Create New Firefox Policy Firefox ?

**Step 8: Policy Schedule**

Select the schedule to apply to the policy assignments:

Schedule Type:  
No Schedule

<< Back Next >> Cancel

**15** Select the schedule to apply to the assignments from the drop-down list, then select the desired options, which vary, depending on the schedule type you select.

The settings you configure on this page determine when the policy is applied to devices.

See [Section 12.3, “Schedules,” on page 74](#) for information about the available schedules and their options.



- 16 Click *Next* to display the Policy Groups page.

Create New Firefox Policy Firefox ?

Step 9: Policy Groups

Specify the groups for this policy:

Add	Remove	Name	In Folder
No items selected, click add to select items			

<< Back Next >> Cancel

- 17 (Optional) Click *Add* to open the Select Groups dialog box, then click the underlined links in the Name column to select the desired policy groups and display their names in the Selected list box.

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create. For more information, see [Section 14.3, “Creating Policy Groups,” on page 125](#).

- 18 Click *Next* to display the Finish page.
- 19 Review the information on the Finish page, making any changes to the policy settings by using the *Back* button as necessary. Click *Finish* to create the policy as configured according to the settings on the Finish page.

## 13.4 Generic GNOME Policy

The Generic GNOME policy is used to configure GConf- based applications on a device.

To configure the GNOME policy:

- 1 In the ZENworks Control Center, click the *Policies* tab.
- 2 In the Policies list, click *New*, then click *Policy* to display the Create New Policy page.

- 3 In the Policy Type list, click *Generic GNOME Policy*, then click *Next* to display the Policy Name page.

Create New Generic GNOME Policy ?

Step 2: Policy Name

Specify the name of the new policy:

Policy Name: \*

Folder: \*

/Policies

Description:

Fields marked with a blue asterisk are required.

<< Back   Next >>   Cancel

- 4 Fill in the fields:
- ♦ **Policy name:** (Required) Provide a unique name for the policy. The name you provide displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.
  - ♦ **Folder:** (Required) Type the name or browse to the folder that this policy will be created in. Folders display in the ZENworks Control Center.
  - ♦ **Description:** Provide a short description of the policy. This description displays on the policy's Summary page in the ZENworks Control Center interface.

- 5 Click *Next* to display the Source page.

Create New Generic GNOME Policy GNOME ?

Step 3: Generic GNOME Policy, Source Page

To create a new Generic GNOME Policy, you need to define some Gconf settings. You can define Gconf Settings using one of the following options:

☒ Import the settings from a device

☐ Define a setting on your own

<< Back    Next >>    Cancel

- 6 Select the desired option, then click *Next*.

**Import the settings from a device:** Use this option to import the existing GConf settings from any device that is registered with the ZENworks Linux Management Server. The system obtains all settings, including default settings, from that device. You can enforce these settings on a desired managed device or group of devices at a later time.

Before you import settings to your device, make sure the GConf settings are correct on the device you are importing from.

If you choose this option, continue with [Step 7 on page 99](#).

**Define a setting on your own:** Create a directory and corresponding key settings such as key names, types, and values. At a later time, you can enforce these settings on a managed device or on a group of devices.

Make sure that you specify the correct key names and types.

If you choose this option, continue with [Step 8 on page 100](#).

- 7 (Conditional) If you chose the *Import the settings from a device* option in [Step 6 on page 99](#), choose the device from which you want to import the Gconf settings.

Create New Generic GNOME Policy GNOME ?

Step 4: Generic GNOME Policy, Device Page

Choose the device from which you want to import the Gconf settings

Import settings from:

☐ Selected machine

☒ DNS Name / IP Address

User Name: \*

Fields marked with a blue asterisk are required.

<< Back    Next >>    Cancel

**7a** Select one of the following options:

**Selected machine:** Browse to and select a device from which you want to import GConf settings, then click OK.

Only managed devices that are registered with the ZENworks Linux Management Server are displayed.

**DNS name / IP address:** Specify the DNS name or IP address of a managed device from which you are importing GConf settings. Ensure that the device is registered with the ZENworks Linux Management Server.


**7b** Specify the username of the managed device from which you are importing the GConf settings.

Only those GConf settings are imported that are related to the specified user. Ensure that the specified user has a valid account on the managed device from which you are importing the settings.


**7c** Click *Next* to import the top-level directories. The four top-level directories that are imported are Apps, Desktop, System, and GNOME.

**7d** Select one or more directory whose settings you want to import, then click *Next*.

**7e** (Optional) Add or delete the keys and their respective values from the imported GConf settings, then click *Next* and skip to [Step 9 on page 101](#).

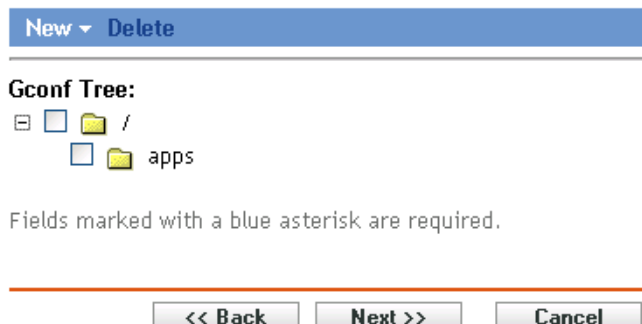
For detailed information about defining your own GConf settings, click the  button on the Built Gconf Tree page.

**8** (Conditional) If you chose the *Define a setting on your own* in [Step 6 on page 99](#), define your own Gconf Settings by adding and deleting keys on the Gconf Tree, then click *Next*.

For detailed information about defining your own Gconf settings, click the  button on the Built Gconf Tree page.



You can define your own Gconf Settings by Adding / Deleting the keys on the Gconf Tree.  
Deleting a directory, will delete all the sub-directories and keys in it.



- 9 Click *Next* to display the Default system requirements for Generic GNOME Policy page.

Create New Generic GNOME Policy GNOME ?

Step 5: Default system requirements for Generic GNOME policy

The following condition is added as a default system requirement to this policy.  
If the minimum supported version requirement is removed then the policy may not be fully applied and effective on the target device.

☒ Apply policy on devices with distribution >= SUSE LINUX 9.3

<< Back Next >> Cancel

- 10 Specify the minimum system requirements for Generic GNOME policy settings to be effective.

The value you specify in the *Apply policy on devices with distribution* field indicates the distribution and minimum version that is required for the policy settings to be effective. The policy is applied if the device has the same version or a later version of the distribution.

If you chose the *Import from a device* option in [Step 6 on page 99](#), the default value is the operating system of a device from which you have imported GConf settings. If you have not included this setting in the policy, and if the operating system of a managed device (where the policy is to be applied) is different than the operating system of the device from which the settings have been imported, a warning message is generated. However, the policy settings are enforced.

If you chose the *Define a setting on your own* option in [Step 6 on page 99](#), and you want to include the default system requirement in the policy, you must specify the distribution and version of the operating system. If you do not include this setting in the policy, the system does not check for minimum operating system requirements and immediately enforces the policy.

Refer to the contents of the `/etc/SuSE-release` or `/etc/redhat-release` file to obtain the correct string for your platform.

- 11 Click *Next* to display the Summary page.
- 12 Click *Finish* to create the policy as configured according to the settings on the Summary page. If you click *Finish*, the Generic GNOME policy is created but it does not have devices assigned or a schedule. At some point in the future, you need to configure additional options for the policy by continuing with [Section 14.4, “Assigning Policies,” on page 128](#).

or

Click *Next* to display the Policy Assignment page to perform the following tasks:

- ◆ Specify assignments for this policy
- ◆ Specify the schedule for this policy
- ◆ Specify groups for this policy

Create New Generic GNOME Policy

GNOME

?

**Step 7: Policy Assignments**

Specify the assignments for this policy:

Add	Remove	
<input type="checkbox"/>		<div>Name</div> <div>In Folder</div>
No items selected, click add to select items		

<< Back

Next >>

Cancel

**13** Assign the policy to the devices.

**13a** Click *Add* to browse for and select the appropriate Server or Workstation objects.

You can also select Folder or Group objects.

**13b** Click the down-arrow next to Servers or Workstations to expand the list, then click the underlined link in the Name column to select the desired objects and display their names in the Selected list box.

Assigning a policy to a Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.

**13c** Click *OK*.

**14** Click *Next* to display the Policy Schedule page.

Create New Generic GNOME Policy

GNOME

?

**Step 8: Policy Schedule**

Select the schedule to apply to the policy assignments:

Schedule Type:

No Schedule

<< Back

Next >>

Cancel

**15** Select the schedule to apply to the assignments from the drop-down list, then select the desired options, which vary, depending on the schedule type you select.

The settings you configure on this page determine when the policy is applied to devices.

See [Section 12.3, “Schedules,” on page 74](#) for information about the available schedules and their options.

- 16 Click *Next* to display the Policy Groups page.

Create New Generic GNOME Policy GNOME ?

Step 9: Policy Groups

Specify the groups for this policy:

Add	Remove	Name	In Folder
No items selected, click add to select items			

<< Back Next >> Cancel

- 17 (Optional) Click *Add* to open the Select Groups dialog box, then click the underlined links in the Name column to select the desired policy groups and display their names in the Selected list box.

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create. For more information, see [Section 14.3, “Creating Policy Groups,” on page 125](#).

- 18 Click *Next* to display the Finish page.
- 19 Review the information on the *Finish* page, making any changes to the policy settings by using the *Back* button as necessary. Click *Finish* to create the policy as configured according to the settings on the Finish page.

## 13.5 Novell Linux Desktop Policy

The Novell Linux Desktop policy is used to configure the GNOME Novell Linux Desktop settings on a device.

To configure the Novell Linux Desktop policy:

- 1 In the ZENworks Control Center, click the *Policies* tab.
- 2 In the Policies list, click *New*, then click *Policy* to display the Create New Policy page.

- 3 In the Policy Type list, click *Novell Linux Desktop Policy*, then click *Next* to display the Policy Name page.

Create New Novell Linux Desktop Policy ?

Step 2: Policy Name

Specify the name of the new policy:

Policy Name: \*

Folder: \*

/Policies

Description:

Fields marked with a blue asterisk are required.

<< Back Next >> Cancel

- 4 Fill in the fields:
- ♦ **Policy name:** (Required) Provide a unique name for the policy. The name you provide displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.
  - ♦ **Folder:** (Required) Type the name or browse to the folder that this policy will be created in. Folders display in the ZENworks Control Center.
  - ♦ **Description:** Provide a short description of the policy. This description displays on the policy's Summary page in the ZENworks Control Center interface.



- 5 Click *Next* to display the Novell Linux Desktop Lockdown Settings page.

**Create New Novell Linux Desktop Policy** NLD ?

**Step 3: Novell Linux Desktop Lockdown Settings**

Selecting an item from the list below will disable or remove the associated feature on the users desktop. The user will be unable to access menu items or controls associated with the feature.

- ☐ Disable panel configuration
- ☐ Disable launcher creation
- ☐ Remove computer icon from desktop
- ☐ Remove trash icon from desktop
- ☐ Remove user's home icon from desktop

<< Back    Next >>    Cancel

- 6 Select the desired options (by default, all options are disabled):

Selecting an item from the list disables or removes the associated feature on the user's desktop. The user cannot access menu items or controls associated with the feature.

**Disable panel configuration:** Lets you prevent users from configuring a panel. If you select this option, users cannot add and remove the icons on the panel.

**Disable launcher creation:** Lets you prevent users from creating application launchers.

**Remove computer icon from desktop:** Lets you remove the computer icon from users' desktops.

**Remove trash icon from desktop:** Lets you remove the trash icon from users' desktops.

**Remove user's home icon from desktop:** Lets you remove the Home icon from users' desktops.

- 7 Click *Next* to display the Novell Linux Desktop Menu Lockdown page.

**Create New Novell Linux Desktop Policy** NLD ?

**Step 4: Novell Linux Desktop Menu Lockdown**

Selecting an item from the list below will remove the associated feature on the users desktop. The user will be unable to access menu items associated with the feature.

☐ Remove from system menu

System menu items

Log Off  
Lock Screen  
Run Program  
Search for Files

Menu items to be removed. \*

☐ Remove from program menu

Program menu items

Gnome Terminal  
File Manager  
Find Files  
System Monitor

Menu items to be removed. \*

Fields marked with a blue asterisk are required.

<< Back Next >> Cancel

- 8 Select the items that you want to remove from desktops so that users cannot access menu items associated with the feature (by default, all options are disabled):

**Remove from System menu:** Lets you remove items from the System menu of the Novell Linux Desktop. Select an item you want to remove and move it to the box on the right side. The item is removed from the users' System menus.

**Remove from Program Menu:** Lets you remove items from the Program menu of the Novell Linux Desktop. Select an item you want to remove and move it to the box on the right side. The item is removed from the users' Program menus.

- 9 Click *Next* to display the Novell Linux Desktop Personal Settings and Applets Lockdown page.

- 10 Select the items that you want to remove from desktops so that users cannot access menu items associated with the feature (by default, all options are disabled):

**Remove from personal settings:** Lets you remove items from the Personal Settings of Novell Linux Desktop. Select an item you want to remove and move it to the box on the right side. The item is removed from the users' Personal Settings.


**Remove applets:** Lets you prevent the applets from being displayed on users' Novell Linux Desktop. Select an applet from the Applets list and move it to the box on the right side. Selected applets are not displayed on users' Novell Linux Desktop.

- 11 Click *Next* to display the Novell Linux Desktop Configuration Settings page.

Create New Novell Linux Desktop Policy

NLD


?

 Step 6: Novell Linux Desktop Configuration Settings

Click the checkboxes to select settings which will be enforced on the desktop.  
For each setting you select, provide a value, and optionally, lock the setting to prevent the value from changing after it is set.

☐


Background image file name \*



(eg. /opt/gnome/share/images/roses.jpeg)

☐

Background position




Centered

▼

☐

Background shade




Solid

▼

☐


Theme file name \*



(eg. /opt/gnome/share/themes/metacity/index.theme)

☐

Proxy Settings



☐

Direct internet connection

☒

Manual proxy configuration

HTTP Proxy \*

Port \*

8080

Authentication

HTTP Secure Proxy

Port \*

0

FTP Proxy

Port \*

0

Socks Proxy

Port \*

0

☐

Automatic proxy configuration

Autoconfiguration URL


Fields marked with a blue asterisk are required.

<< Back

Next >>

Cancel

- 12 Select the desired options (by default, all options are disabled).

For each option you enable, provide a value. When you enable an option, it is locked by default. You can unlock the option by clicking . The options that are not enabled are excluded from the policy and are not applied to the device.

**Background image filename:** Lets you specify the filename and complete location of a background image. This image file is displayed as a background on users' desktops. The file should exist on the managed device at the specified location.

**Background position:** Lets you specify background image display options. Center displays an image in the center of the screen, Fill Screen stretches the image to cover the entire screen, Scaled enlarges the image until the image meets the screen edges, and Tiled repeats the image

over the screen. Select No Background to prevent the image from being displayed on the desktop.

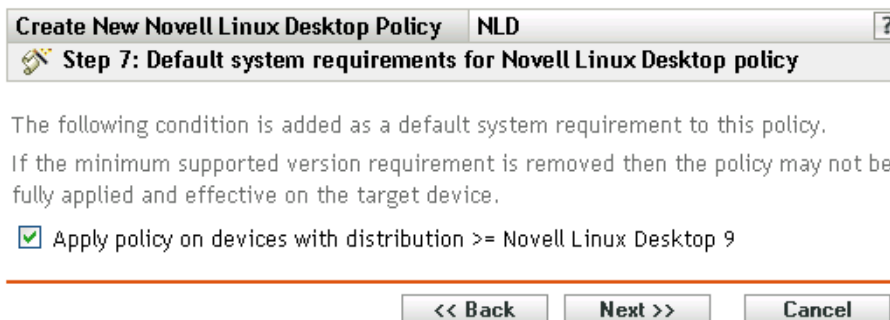
**Background shade:** Lets you choose an available shade to decorate the background. Select Solid to have the background image uniform across the desktop. Select Vertical to have the image become darker as you go up, and select Horizontal to have the image become darker as you go from left to right.

**Theme filename:** Lets you specify a theme file name and its complete location. The appearance of the windows, icons, buttons, and other graphical user interface controls are changed according to the selected theme.

**Proxy settings:** Specify a proxy setting:

- ♦ **Direct internet connection:** Lets users connect to the Internet without using the proxy server.
- ♦ **Manual proxy configuration:** Lets you manually configure the proxy. Specify the HTTP Proxy value, HTTP Secure Proxy value, FTP Proxy value, Socks Proxy value, and corresponding port numbers.  
  
To authenticate the user before proxy configuration, click Authentication. In the HTTP Proxy Authentication dialog box, select Use Authentication, specify the username and password, then click OK.
- ♦ **Automatic proxy configuration:** Lets you automatically configure the proxy from a certain URL by specifying the URL.

- 13 Click *Next* to display the Default System Requirements for the Novell Linux Desktop Policy page.



- 14 Specify the minimum version of Novell Linux Desktop required for all policy settings to be effective. Policy settings are applied only if a device has the same version or a newer version of the Novell Linux Desktop. If a device does not have Novell Linux Desktop 9 or newer, the policy does not apply correctly.

Even if you do not include this setting in the policy, the system checks for Novell Linux Desktop. If it does not find Novell Linux Desktop, an error message is generated and the policy is not applied.

---

**NOTE:** To ensure successful enforcement of all configured items, you need Novell Linux Desktop 9 with Support Pack 2 with GNOME.

---

- 15 Click *Next* to display the Summary page.
- 16 Click *Finish* to create the policy as configured according to the settings on the Summary page. If you click *Finish*, the Novell Linux Desktop policy is created but it does not have devices

assigned or a schedule specified. At some point in the future, you need to configure additional options for the policy by continuing with [Section 14.4, “Assigning Policies,” on page 128](#).

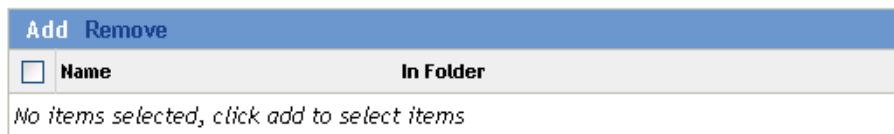
or

Click *Next* to display the Policy Assignment page to perform the following tasks:

- ♦ Specify assignments for this policy
- ♦ Specify the schedule for this policy
- ♦ Specify groups for this policy



Specify the assignments for this policy:



<< Back

Next >>

Cancel

**17** Assign the policy to the devices.

**17a** Click *Add* to browse for and select the appropriate Server or Workstation objects.

You can also select Folder or Group objects.

**17b** Click the down-arrow next to Servers or Workstations to expand the list, then click the underlined link in the Name column to select the desired objects and display their names in the Selected list box.

Assigning a policy to a Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.

**17c** Click *OK*.

**18** Click *Next* to display the Policy Schedule page.



Select the schedule to apply to the policy assignments:

Schedule Type:

No Schedule

<< Back

Next >>

Cancel

- 19 Select the schedule to apply to the assignments from the drop-down list, then select the desired options, which vary, depending on the schedule type you select.

The settings you configure on this page determine when the policy is applied to devices.

See [Section 12.3, “Schedules,” on page 74](#) for information about the available schedules and their options.

- 20 Click *Next* to display the Policy Groups page.

Create New Novell Linux Desktop Policy NLD ?

Step 11: Policy Groups

Specify the groups for this policy:

Add	Remove	Name	In Folder
No items selected, click add to select items			

<< Back Next >> Cancel

- 21 (Optional) Click *Add* to open the Select Groups dialog box, then click the underlined links in the Name column to select the desired policy groups and display their names in the Selected list box.

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create. For more information, see [Section 14.3, “Creating Policy Groups,” on page 125](#).

- 22 Click *Next* to display the Finish page.
- 23 Review the information on the Finish page, making any changes to the policy settings by using the *Back* button as necessary. Click *Finish* to create the policy as configured according to the settings on the Finish page.

## 13.6 Remote Execute Policy

The Remote Execute policy is used to execute any Script, Binary, or Java file.

To configure the Remote Execute policy:

- 1 In the ZENworks Control Center, click the *Policies* tab.
- 2 In the Policies list, click *New*, then click *Policy* to display the Create New Policy page.

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

Create New Remote Execute Policy ?

Step 2: Policy Name

Specify the name of the new policy:

Policy Name: \*

Folder: \*

/Policies

Description:

Fields marked with a blue asterisk are required.

<< Back Next >> Cancel

- 4 Fill in the fields:

- ♦ **Policy name:** (Required) Provide a unique name for the policy. The name you provide displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.
- ♦ **Folder:** (Required) Type the name or browse to the folder that this policy will be created in. Folders display in the ZENworks Control Center.
- ♦ **Description:** Provide a short description of the policy. This description displays on the policy's Summary page in the ZENworks Control Center interface.



5 Click *Next*.

Create New Remote Execute Policy

Remote\_Execute

?

Step 3: Remote Execute Policy

Executable Type:

Script

▼

Maximum Waiting Time:

☐ Do not wait

☒ Wait till the program completes the execution

☐ Wait For  sec

Script to run:

Specify a file

▼

Script file name: \*

(e.g. /usr/local/xyz.pl)

Script parameters:

(e.g. abc efg)

Script engine: \*

(e.g. /usr/local/bin/perl)

Script engine parameters:

(e.g. -c abc -s efg)

Fields marked with a blue asterisk are required.

<< Back

Next >>

Cancel

6 Select the desired options:

**Executable type:** Select an executable type to run on a managed device (script, binary, or Java). Depending on the executable type you select, different options are available, as described below.

**Maximum waiting time:** Indicate the waiting time after starting the script, binary, or Java program. The following table explains the available options:

Option	Description
Do not wait	The Remote Execute enforcer does not wait for the program to be completed.
Wait till the program completes the execution	The Remote Execute enforcer waits for the program to be completed.
Wait for <n> sec	Indicates how many seconds the Remote Execute enforcer should wait after starting the program.

**NOTE:** The launched program is not terminated by the enforcer if you select the Do Not Wait or Wait for <n>Sec options.

(Conditional) If you chose Script in the Executable Type field in [Step 6 on page 113](#), the following options are available:

**Script to run:** Select an option from the drop-down list:

- ♦ **Specify a file:** Fill in the fields:

**Script filename:** Specify the complete path, including the filename, of the script you want to run on a managed device.

**Script parameters:** Specify any parameters to be passed to the specified script file.

**Script engine:** Specify the name and location of the script engine that runs the script. For example, `/user/bin/perl`.

**Script engine parameters:** Specify any parameters to be passed to the specified script engine.

- ♦ **Define your own script:** Type your script in the box.

(Conditional) If you chose Binary in the Executable Type field in [Step 6 on page 113](#), the following options are available:

**Executable file name:** Specify the complete path, including the filename, of the binary program you want to run on a managed device.

**Executable file parameters:** Specify any parameters to be passed to the specified binary program.

---

**NOTE:** You cannot perform shell operations, such as redirection using the executable type Binary. You can use *Executable file parameters* to pass only those parameters that are required by the executable specified in the *Executable file name* field. If you want to use shell operations, define your own script.

---

(Conditional) If you chose Java in the Executable Type field in [Step 6 on page 113](#), the following options are available:

**Java program name:** Specify the Java program you want to run on a managed device.

**Program parameters:** Specify any parameters to be passed to the specified Java program.

**Java Runtime Executable (JRE):** Specify the complete path, including the Java Runtime Executable (JRE) name. JRE is used to interpret the Java binary file.

**JRE parameters:** Specify the parameters to be passed to the Java Runtime Executable (JRE).

---

**NOTE:** The Own Defined Script specified in the Remote Execute policy is executed in the shell specified by the environment variable SHELL. The value of the variable SHELL is taken from the environment in which ZENworks Management daemon runs. If a value is not specified, then `/bin/sh` is used, which is a default value.

---

**7** Click *Next* to display the Summary page.

**8** Click *Finish* to create the policy as configured according to the settings on the Summary page. If you click *Finish*, the Remote Execute policy is created but it does not have devices assigned or a schedule specified. At some point in the future, you need to configure additional options for the policy by continuing with [Section 14.4, “Assigning Policies,” on page 128](#).

or

Click *Next* to display the Policy Assignment page to perform the following tasks:

- ♦ Specify assignments for this policy
- ♦ Specify the schedule for this policy

- ♦ Specify groups for this policy

Create New Remote Execute Policy	Remote_Execute	?
Step 5: Policy Assignments		

Specify the assignments for this policy:

Add	Remove
<input type="checkbox"/>	<b>Name</b>
	<b>In Folder</b>
No items selected, click add to select items	

<< Back	Next >>	Cancel
---------	---------	--------

**9** Assign the policy to the devices.

- 9a** Click *Add* to browse for and select the appropriate Server or Workstation objects.

You can also select Folder or Group objects.

- 9b** Click the down-arrow next to Servers or Workstations to expand the list, then click the underlined link in the Name column to select the desired objects and display their names in the Selected list box.

Assigning a policy to a Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.

- 9c** Click *OK*.

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

The settings you configure on this page determine when the policy is applied to devices.

See [Section 12.3, “Schedules,” on page 74](#) for information about the available schedules.

**11** Click *Next* to display the Policy Groups page.

Create New Remote Execute Policy	Remote_Execute	?
Step 7: Policy Groups		

Specify the groups for this policy:

Add	Remove
<input type="checkbox"/>	<b>Name</b>
	<b>In Folder</b>
No items selected, click add to select items	

<< Back	Next >>	Cancel
---------	---------	--------

**12** (Optional) Click *Add* to open the Select Groups dialog box, then click the underlined links in the Name column to select the desired policy groups and display their names in the Selected list box.

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create. For more information, see [Section 14.3, “Creating Policy Groups,” on page 125](#).

- 13 Click *Next* to display the Finish page.
- 14 Review the information on the Finish page, making any changes to the policy settings by using the *Back* button as necessary. Click *Finish* to create the policy as configured per settings on the Finish page.

## 13.7 Text File Policy

The Text File policy is used to make changes to any text file on a device.

To configure the Text File policy:

- 1 In the ZENworks Control Center, click the *Policies* tab.
- 2 In the Policies list, click *New*, then click *Policy* to display the Create New Policy page.
- 3 In the Policy Type list, click *Text File Policy*, then click *Next* to display the Policy Name page.

The screenshot shows a dialog box titled "Create New Text File Policy" with a question mark icon in the top right corner. Below the title bar, it says "Step 2: Policy Name" with a small icon. The main area contains the text "Specify the name of the new policy:" followed by three fields: "Policy Name: \*" with an asterisk and a text input box; "Folder: \*" with an asterisk, a text input box containing "/Policies", and a folder selection icon; and "Description:" with a large text area. At the bottom, a note states "Fields marked with a blue asterisk are required." Below this is a horizontal line and three buttons: "<< Back", "Next >>", and "Cancel".

- 4 Fill in the fields:
  - ♦ **Policy name:** (Required) Provide a unique name for the policy. The name you provide displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.

- ♦ **Folder:** (Required) Type the name or browse to the folder that this policy will be created in. Folders display in the ZENworks Control Center.
- ♦ **Description:** Provide a short description of the policy. This description displays on the policy's Summary page in the ZENworks Control Center interface.

5 Click *Next* to display the General page.

Create New Text File Policy

Text\_File

?

Step 3: Text File Policy, General Page

**File details:**

File Name: \*   
(e.g. /etc/samba/smb.conf)

Maximum number of version(s) to retain [1 to 25]: \*

---

**Change details:**

Enter the search string as a regular (or) normal expression.  
Refer the Administration document for further information on regular expressions.

Change Name: \*

Change Mode:

Search String: \*   
(e.g. ^abc\*\$)

Case Sensitive: ☒

Search Occurrence:

Result Action:

New String: \*

Fields marked with a blue asterisk are required.

<< Back

Next >>

Cancel


6 Select the desired options:

**Filename:** Specify the name and the complete path of a file you want to change.

**Maximum number of versions to retain:** Specify the maximum number of backups to be maintained for a file that has been changed. If the maximum limit of backups is reached, the oldest backup of a file is deleted. The backup is created in the same location as the specified file.

**Change name:** Specify the name of the change you want to perform in the file. If you want to make more than one change in the same file, go to the Settings page.

**Change mode:** Select an option from the drop-down list:

- ♦ **Search file:** Lets you search for the given text in the entire file. Fill in the fields:
  - ♦ **Search string:** Specify the text you want to search for in a given file. The search string can be simple text or a regular expression. For detailed information on regular expressions, click the  button.
  - Case sensitive:** Select this option to distinguish between uppercase and lowercase characters. When Case Sensitive is selected, the system finds only those instances in which the capitalization matches the text you have specified in the search string.
  - Search occurrence:** Indicates the occurrence of the search text you have given. The available options are First Occurrence, Last Occurrence, and Find All Occurrences. For example, if you select First Occurrence, the system finds the first occurrence of the search string and performs the specified action on it.
  - Result action:** Select the operation from the drop-down list that you want perform on the specified search text.
- ♦ **Append lines to file:** Lets you append the given lines of text to the file
- ♦ **Prepend lines to file:** Lets you prepend the given lines of text to the file.

**New string:** Specify the text to be used for carrying out the specified action in the file. For example, you can select to replace a search string with a new string.

7 Click *Next* to display the Script Page.

**Create New Text File Policy** **Text\_File** ?

**Step 4: Text File Policy, Script Page**

**Pre-change action:**  
Execute the following before modifying the text file(s)

Executable Type:

Action when the execution fails:

---

**Post-change action:**  
Execute the following after modifying the text file(s)

Executable Type:

Fields marked with a blue asterisk are required.

<< Back   Next >>   Cancel

8 Fill in the fields:

**Pre-change action:** Specify the actions to perform before modifying the text files:

- ♦ **Executable type:** Select the executable type from the drop-down list that you want to run before modifying the file. The available options are None, Binary, Java, and Script.  
(Conditional) If you chose Script in the *Executable type* field, the following options are available:

**Script to run:** Select an option from the drop-down list (Specify a File or Define Your Own Script):

- ♦ **Specify a file:** Fill in the fields:

**Script filename:** Specify the complete path, including the filename, of the script you want to run on a managed device.

**Script parameters:** Specify any parameters to be passed to the specified script file.

**Script engine:** Specify the name and location of the script engine that runs the script. For example, /user/bin/perl.

**Script engine parameters:** Specify any parameters to be passed to the specified script engine.

- ♦ **Define your own script:** Type your script in the box.

(Conditional) If you chose Binary in the *Executable type* field, the following options are available:

**Executable file name:** Specify the complete path, including the filename, of the binary program you want to run on a managed device.

**Executable file parameters:** Specify any parameters to be passed to the specified binary program.

(Conditional) If you chose Java in the *Executable type* field, the following options are available:

**Java program name:** Specify the Java program you want to run on a managed device.

**Program parameters:** Specify any parameters to be passed to the specified Java program.

**Java Runtime Executable (JRE):** Specify the complete path, including the Java Runtime Executable (JRE) name. JRE is used to interpret the Java binary file.

**JRE parameters:** Specify the parameters to be passed to the Java Runtime Executable (JRE).

---

**NOTE:** The Own Defined Script specified in the Remote Execute policy is executed in the shell specified by the environment variable SHELL. The value of the variable SHELL is taken from the environment in which ZENworks Management daemon runs. If a value is not specified, then `/bin/sh` is used, which is a default value.

---

**Action when the execution fails:** Select an action you want the system to perform when an execution fails. You can continue modifying the file by selecting *Continue modifying the text file* or you can stop the modifications in the file by selecting *Do not modify the text file*.

---

**NOTE:** The backup of the text file is taken after the pre-change action completes the execution and before the text file modification starts.

---

**Post-change action:** Specify the actions to perform after the actual changes are done in the file.

- ♦ **Executable type:** Select the executable type you want to run after modifying the file. Select Binary, Java, Script, or None from the drop-down list. Depending on which type you select, the available options vary. For more information about the specific options, see the descriptions in the Pre-Change Action section directly above.

**9** Click *Next* to display the Summary page.

**10** Click *Finish* to create the policy as configured according to the settings on the Summary page. If you click *Finish*, the Text File policy is created but it does not have devices assigned or a schedule specified. At some point in the future, you need to configure additional options for the policy by continuing with [Section 14.4, “Assigning Policies,” on page 128](#).

or

Click *Next* to display the Policy Assignment page to perform the following tasks:

- ♦ Specify assignments for this policy
- ♦ Specify the schedule for this policy
- ♦ Specify groups for this policy



Create New Text File Policy

Text\_File

?

**Step 6: Policy Assignments**

Specify the assignments for this policy:

Add Remove	
<input type="checkbox"/> Name	In Folder
No items selected, click add to select items	

---

<< Back

Next >>

Cancel

**11** Assign the policy to the devices.

**11a** Click *Add* to browse for and select the appropriate Server or Workstation objects.

You can also select Folder or Group objects.

**11b** Click the down-arrow next to Servers or Workstations to expand the list, then click the underlined link in the Name column to select the desired objects and display their names in the Selected list box.

Assigning a policy to a Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.

**11c** Click *OK*.

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

The settings you configure on this page determine when the policy is applied to devices.

See [Section 12.3, “Schedules,” on page 74](#) for information about the available schedules.

**13** Click *Next* to display the Policy Groups page.

Create New Text File Policy

Text\_File

?

**Step 8: Policy Groups**

Specify the groups for this policy:

Add Remove	
<input type="checkbox"/> Name	In Folder
No items selected, click add to select items	

---

<< Back

Next >>

Cancel

**14** (Optional) Click *Add* to open the Select Groups dialog box, then click the underlined links in the Name column to select the desired policy groups and display their names in the Selected list box.

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create. For more information, see [Section 14.3, “Creating Policy Groups,” on page 125](#).

- 15** Click *Next* to display the Finish page.
- 16** Review the information on the Finish page, making any changes to the policy settings by using the *Back* button as necessary. Click *Finish* to create the policy as configured according to the settings on the Finish page.

Novell® ZENworks® Linux Management Policies give you the ability to define and lock down configuration settings of various applications on managed devices. ZENworks Linux Management provides policies for a number of popular applications, including the Novell Linux Desktop, plus powerful tools to create customized policies for other applications. In addition to creating policies, as described in [Chapter 13, “Creating Policies,” on page 77](#), you can create groups and folders to assign policies to, edit existing policies, and more.

The following sections contain additional information:

- ♦ [Section 14.1, “Creating Policies,” on page 123](#)
- ♦ [Section 14.2, “Creating Folders,” on page 124](#)
- ♦ [Section 14.3, “Creating Policy Groups,” on page 125](#)
- ♦ [Section 14.4, “Assigning Policies,” on page 128](#)
- ♦ [Section 14.5, “Removing Policy Assignments,” on page 130](#)
- ♦ [Section 14.6, “Adding Policies to Existing Groups,” on page 130](#)
- ♦ [Section 14.7, “Editing Policies,” on page 131](#)
- ♦ [Section 14.8, “Editing System Requirements,” on page 141](#)
- ♦ [Section 14.9, “Refreshing Policies,” on page 142](#)
- ♦ [Section 14.10, “Verifying Policy Enforcement,” on page 143](#)
- ♦ [Section 14.11, “Renaming, Copying, or Moving Policies,” on page 143](#)
- ♦ [Section 14.12, “Deleting Policies, Policy Groups, and Folders,” on page 144](#)
- ♦ [Section 14.13, “Unenforcing Policies,” on page 145](#)

## 14.1 Creating Policies

Step-by-step instructions to create policies are contained in [Chapter 13, “Creating Policies,” on page 77](#).

ZENworks lets you create seven types of policies:

- ♦ **Epiphany policy:** Configures the Epiphany Web browser. For step-by-step instructions to create this policy, see [Section 13.1, “Epiphany Policy,” on page 77](#).
- ♦ **Evolution policy:** Configures the Evolution™ e-mail client. For step-by-step instructions to create this policy, see [Section 13.2, “Evolution Policy,” on page 83](#).
- ♦ **Firefox policy:** Configures the Firefox Web browser. For step-by-step instructions to create this policy, see [Section 13.3, “Firefox Policy,” on page 90](#).
- ♦ **Generic GNOME policy:** Configures GConf applications. For step-by-step instructions to create this policy, see [Section 13.4, “Generic GNOME Policy,” on page 97](#).
- ♦ **Novell Linux Desktop policy:** Configures the Novell Linux Desktop settings. For step-by-step instructions to create this policy, see [Section 13.5, “Novell Linux Desktop Policy,” on page 103](#).

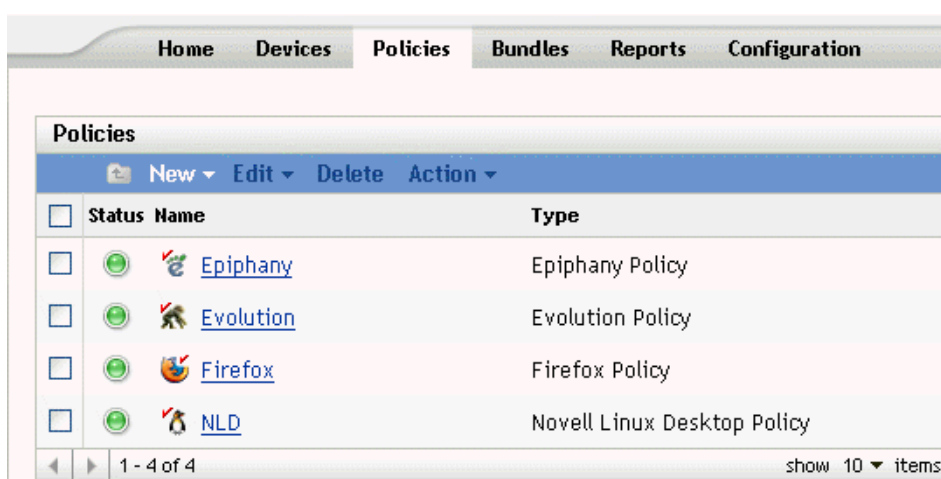
- ♦ **Remote Execute policy:** Executes a script, binary, or Java file. For step-by-step instructions to create this policy, see [Section 13.6, “Remote Execute Policy,” on page 111](#).
- ♦ **Text File policy:** Applies changes to a text file. For step-by-step instructions to create this policy, see [Section 13.7, “Text File Policy,” on page 116](#).

## 14.2 Creating Folders

A folder is an organization object that displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management. A folder can contain various objects, including subfolders, Policy, and Policy Group objects.

To create a folder:

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



- 2 Click *New*, then click *Folder* to display the New Folder dialog box.



The image shows a 'New Folder' dialog box with a blue title bar and a close button. It contains three fields: 'Name: \*' with an empty text box, 'Folder: \*' with a text box containing '/Policies' and a browse button, and 'Description:' with a large empty text area. At the bottom, there is a note 'Fields marked with a blue asterisk are required.' and two buttons: 'OK' and 'Cancel'.

- 3 Fill in the fields:

- ♦ **Name:** Provide a unique name for your folder. This is a required field.
- ♦ **Folder:** Type the name or browse to the folder that contains this folder in the ZENworks Control Center interface.
- ♦ **Description:** Provide a short description of the folder's contents.

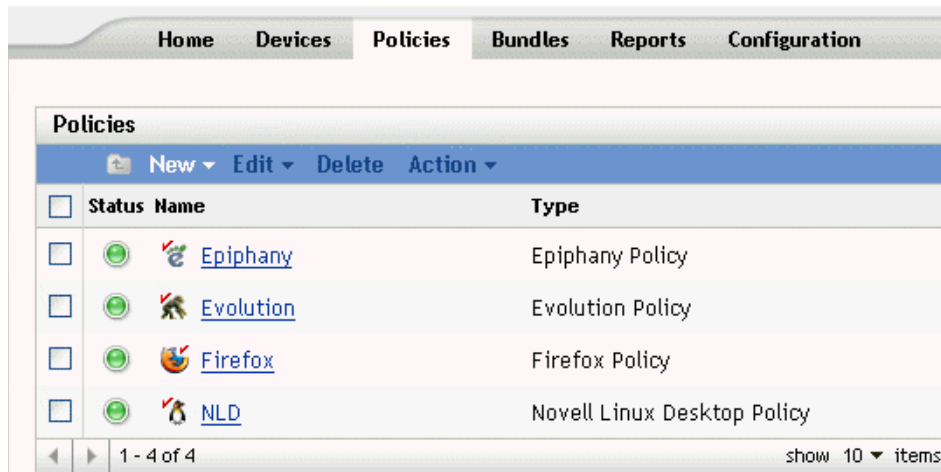
- 4 Click *OK*.

## 14.3 Creating Policy Groups

A policy group lets you organize policies to ease administration and to provide easier assigning and scheduling of the policies in the policy group.

To create a policy group:

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



- 2 Click *New*, then click *Policy Group* to display the Basic Information page.

A screenshot of the 'Create New Group' dialog box, Step 1: Basic Information. The dialog has a title bar 'Create New Group' with a help icon. Below the title bar is a section 'Step 1: Basic Information'. It contains three fields: 'Group Name: \*' with a text input box, 'Folder: \*' with a text input box containing '/Policies' and a browse button, and 'Description:' with a large text area. At the bottom, there is a note 'Fields marked with a blue asterisk are required.' and three buttons: '<< Back', 'Next >>', and 'Cancel'.

- 3 Fill in the fields:

- ♦ **Group name:** (Required) Provide a unique name for your policy group. The name you provide displays in the ZENworks Control Center interface (the administrative tool for ZENworks Linux Management) and in the user interface.
- ♦ **Folder:** (Required) Type the name or browse to the folder that contains this policy group.

- ♦ **Description:** Provide a short description of the policy group's contents. This description displays in the ZENworks Control Center.

**4** Click *Next* to display the Summary page.

Review the information on the Summary page, making any changes to the policy-group settings by using the *Back* button as necessary.

Depending on your needs, you can create the policy group now or you can specify members, assignments, and schedules for this policy group.

**5** Click *Finish* to create the policy as configured according to the settings on the Summary page. If you click *Finish*, the policy group is created but it does not have members, devices assigned, a schedule, and so forth. At some point in the future, you need to configure additional options for the policy group by continuing with [Section 14.4, “Assigning Policies,” on page 128](#).

or

Click *Next* to display the Add Group Members page to perform the following tasks:

- ♦ Specify members for this policy group
- ♦ Specify assignments for this policy group
- ♦ Specify the schedule to apply the policy-group assignments

Create New Group Policies ?

Step 3: Add Group Members

Specify the members for this group:

Add Remove	
<input type="checkbox"/>	In Folder
No items selected, click add to select items	

---

<< Back

Next >>

Cancel

**6** Specify the policies to include in this policy group.

- 6a** Click *Add* to browse for and select the appropriate policy objects.
- 6b** Click the underlined link in the Name column to select the desired policies and display their names in the Selected list box.
- 6c** Click *OK*.

- 7 Click *Next* to display the Add Assignments page.

Create New Group Policies ?

Step 4: Add Assignments

Specify the assignments for this group:

Add	Remove
<input type="checkbox"/>	Name In Folder

No items selected, click add to select items

<< Back Next >> Cancel

- 8 Assign the policy group to the desired devices.

- 8a Click *Add* to browse for and select the appropriate device objects.

You can also select Folder or Group objects.

- 8b Click the down-arrow next to Servers or Workstations to expand the list, then click the underlined link in the Name column to select the desired objects and display their names in the Selected list box.

Assigning a policy to a Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.

- 8c Click *OK*.

- 9 Click *Next* to display the Schedule page.

- 10 Select the schedule to apply to the assignments.

The settings you configure on this page determine when the policies in the policy group are assigned to devices.

See [Section 12.3, “Schedules,” on page 74](#) for information about the available schedules.

- 11 Click *Next* to display the Summary page, then review the information, making any changes to the settings by using the Back button as necessary.

- 12 Click *Finish*.

## 14.4 Assigning Policies

When you assign policies, you specify device assignments and assignment schedules for an existing policy.

When you created policies, midway through the Create Policy Wizard, you were given the choice of clicking *Finish* or *Next*.

If you clicked *Finish*, the policy was created without assigning devices to it, specifying assignment schedules, or specifying groups for the policy. Before the policy can be applied to assigned devices,



you must complete the following steps. If you clicked *Next*, you have already performed the following procedure as part of the policy-creation process.

- 1 In the ZENworks Control Center, click the *Policies* tab, select the desired policy in the Policies list by checking the box next to its name, click *Action*, then click *Assign Policy* to display the Policy Assignments page.

The screenshot shows the 'Assign Policy' dialog box with the title bar 'Assign Policy' and a help icon. Below the title bar is a sub-header 'Step 1: Devices to be Assigned'. The main area contains the instruction 'Select the devices to be assigned to the previously selected policies.' Below this is a table with two columns: 'Name' and 'In Folder'. The table is currently empty, with a message 'No items selected, click add to select items' at the bottom. At the top left of the table area are buttons 'Add' and 'Remove'. At the bottom of the dialog are three buttons: '<< Back', 'Next >>', and 'Cancel'.

Name	In Folder
No items selected, click add to select items	

- 2 Assign the policy to the desired devices.
  - 2a Click *Add* to browse for and select the appropriate Server or Workstation objects.

You can also select Folder or Group objects.
  - 2b Click the down-arrow next to Servers or Workstations to expand the list, then click the underlined link in the Name column to select the desired objects and display their names in the Selected list box.

Assigning a policy to a Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.
  - 2c Click *OK*.
- 3 Click *Next* to display the Schedule page.

The screenshot shows the 'Assign Policy' dialog box with the title bar 'Assign Policy' and a help icon. Below the title bar is a sub-header 'Step 2: Schedule'. The main area contains the instruction 'Specify the schedule to use for the assignments.' Below this is a label 'Schedule Type:' followed by a dropdown menu currently showing 'No Schedule'. At the bottom of the dialog are three buttons: '<< Back', 'Next >>', and 'Cancel'.

- 4 Select the schedule to apply to the assignments.

The settings you configure on this page determine when the policy is applied to devices. Depending on the type of policy you are assigning, the available schedules vary. See [Section 12.3, “Schedules,” on page 74](#) for information about the available schedules.

- 5 Click *Next* to display the Finish page.
- 6 Review the information on the Finish page, making any changes to the policy settings by using the *Back* button as necessary. Click *Finish* to assign the policy as configured according to the settings on the Finish page.

In addition to the preceding steps to assign policies, the following are other options to assign a policy to devices:

- By selecting a policy and then using the Assignments section of the policy's Summary page.
- By selecting a device, device group, or folder and then selecting *Assign Policy* in the Action menu.
- By using the Effective Policy section on the device's Summary page.

## 14.5 Removing Policy Assignments

You can remove the policy assignments by selecting a policy and then removing the device from the Assignments section on the Policy Summary page. You can also do this by clicking the appropriate device on the Devices page and disassociating a policy by using the Effective Policies section.

After a policy is disassociated from a device, it is unenforced on the device. For more details on unenforcement of a policy, see [Section 14.13, “Unenforcing Policies,” on page 145](#).

You do not need to delete a policy to disassociate it from a device.

## 14.6 Adding Policies to Existing Groups

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create.

- 1 In the ZENworks Control Center, click the *Policies* tab, select the desired policy in the Policies list by selecting the box next to its name, click *Action*, then click *Add to Group* to display the Targets page.

**Add To Group** ?

**Step 1: Targets**

Select the groups that will contain the items.

Add	Remove	Name	In Folder
No items selected, click add to select items			

<< Back    Next >>    Cancel

- 2 Click *Add* to open the Select Groups dialog box, click the desired objects to add them to the Selected list, then click *OK* to display the selected groups in the list on the Targets page.
- 3 Click *Next* to display the Finish page.

- 4 Review the information on the Finish page, making any changes to the settings by using the *Back* button as necessary, then click *Finish* to add the policy to the group.

## 14.7 Editing Policies

You can edit an existing policy to change its description, add or remove assignments, add or remove the policy from existing policy groups, change configuration settings, and more.

Following sections describes how you can edit different types of policies:

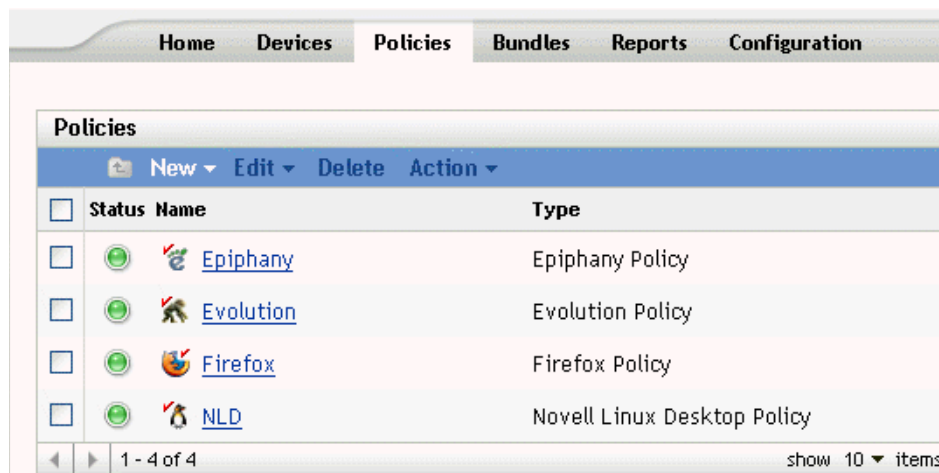
- ♦ [Section 14.7.1, “Editing Epiphany, Evolution, Firefox, and NLD Policies,” on page 131](#)
- ♦ [Section 14.7.2, “Editing Generic GNOME Policies,” on page 133](#)
- ♦ [Section 14.7.3, “Editing Remote Execute Policies,” on page 136](#)
- ♦ [Section 14.7.4, “Editing Text File Policies,” on page 138](#)
- ♦ [Section 14.7.5, “Viewing Policy Enforcement Status,” on page 140](#)

### 14.7.1 Editing Epiphany, Evolution, Firefox, and NLD Policies

You can edit, include, or remove lockdown settings, configuration settings, and system requirements of the application policies. Epiphany, Evolution, Firefox, and Novell Linux Desktop policies are the application policies.

To edit the application policies:

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



- 2 Click the policy's name to display the Summary page, then make the desired configuration changes.

If you do not want to edit any item on the Summary page, skip to [Step 3 on page 133](#).

Use the Summary page to view detailed information about the selected policy. This page provides general information about the policy, lists the individual devices that are assigned to the policy, displays an event log, shows upcoming events, and lists the groups that the policy belongs to.

You can also use this page to edit the policy's description, add or remove assignments for the policy, and change other configuration settings, as described below.

- 2a** Review the information in the General section, then make the desired configuration changes (you can edit only the Revision and Description options in this section).

**Policy type:** Displays the policy type (Novell Linux Desktop Policy, Firefox Policy, and so forth).

**Revision:** Displays the policy's revision number. To change the revision number, click Increment Revision.

**Number of errors not acknowledged:** Displays the number of errors not acknowledged.

**Number of warnings not acknowledged:** A warning is anything that does not cause the application of the policy to fail, but indicates minor problems. The number displayed indicates the number of unacknowledged warnings, which display in the Event Log section below.

**GUID:** Lists the selected object's GUID (global unique identifier), a randomly generated string that provides a unique identifier for the policy. You cannot edit the object's GUID.

**Description:** Displays the selected object's description, if one was provided when the policy was created. The description provides a short description of the policy's purpose.

Click *Edit* to change the description, if necessary.

- 2b** Review the information in the Assignments section, then make the desired configuration changes.

The Assignments section lists the devices, device groups, and device folders to which the selected policy is assigned. You can also view the folder to which the device belongs and the schedule. You can click the device object name to view information about that device object.

You can also use the following options:

**Advanced:** Click *Advanced* to display the Edit Assignments page to display a list of the devices that are assigned to the selected policy, the folder that contains each device, and each device's schedule. You can use the Edit Assignments page to edit certain settings, such as the schedule.

**Add:** Click *Add* to launch the Assign Policy Wizard to select the devices to be assigned to the selected policy. For more information, see [Section 14.4, "Assigning Policies," on page 128](#).

**Remove:** Select the device by selecting the check box next to the appropriate device name, then click *Remove* to remove the device's assignment from this policy.

- 2c** Review the information in the Event Log section, then make the desired changes.

The Event Log section lists all unacknowledged errors and warnings.

The Status column displays an icon indicating each item's status. Position the mouse pointer over each icon to display a short message describing the status of the item.

To acknowledge an error or warning, click its name in the Event Column, then click *Acknowledged* in the Message Detail Information dialog box that displays. You can also click *Advanced*, select the check box next to the appropriate event, then click *Acknowledge* (a check mark displays on the right side of the Date column to indicate that the item has been acknowledged).

- 2d** Review the information in the Upcoming Events section.

The Upcoming Events section lists events scheduled for the selected policy. You can click the calendar icon to display a calendar to view events for the desired date. You can also use the arrows to view events for the previous or next day, week, or month.

- 2e** Review the information in the Groups section, then make the desired configuration changes.

The Groups section lists the groups that contain the selected policy.

You can also use the following options:

**Advanced:** Click *Advanced* to display the Edit Groups page to display a list of the groups that contain the selected policy. You can click *Add* to open the Select Groups dialog box to add the selected policy to existing groups. You can also remove a group by selecting the check box next to the Name column, then clicking *Remove* to remove.

**Add:** Click *Add* to open the Select Groups dialog box, then click the blue arrow in the Select column to select the desired group and display its name in the Selected list box.

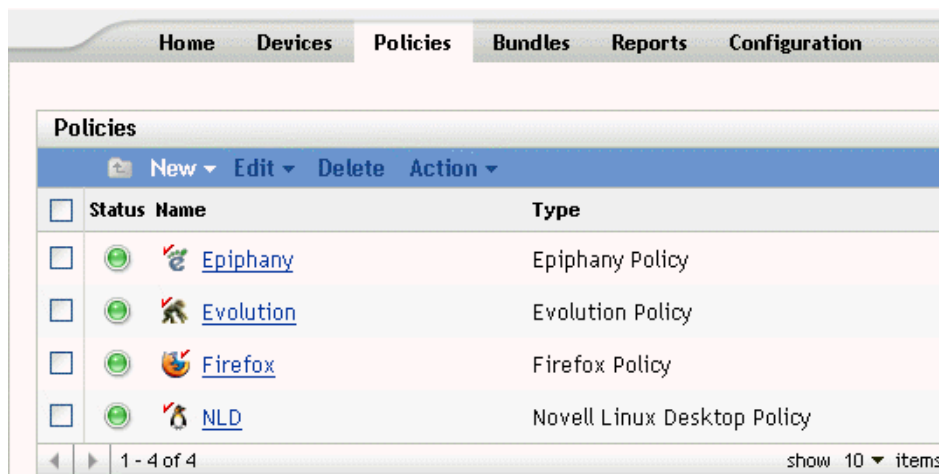
**Remove:** Select the check box next to the appropriate group name, then click *Remove* to remove the selected policy from the group.

- 3** Click the Details tab, then make the desired configuration changes. For more information about the available options, see the section about the appropriate policy in [Chapter 13, “Creating Policies,”](#) on page 77.
  - 3a** To edit the system requirements of a policy, see [Section 14.8, “Editing System Requirements,”](#) on page 141.
  - 3b** Click *Apply* to save any changes you have made.
- 4** After a policy is modified, the Revision field of the policy, which is available under the General section of the Summary page, must be incremented for the updated policy to be applied to associated devices. If the policy revision is not incremented, the changes made to the policy are not applied on the device.

## 14.7.2 Editing Generic GNOME Policies

To edit a Generic GNOME policy:

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



- 2 Click the policy's name to display the Summary page, then make the desired configuration changes.

If you do not want to edit any item on the Summary page, skip to [Step 3 on page 135](#).

Use the Summary page to view detailed information about the selected policy. This page provides general information about the policy, lists the individual devices that are assigned to the policy, displays an event log, shows upcoming events, and lists the groups that the policy belongs to.

You can also use this page to edit the policy's description, add or remove assignments for the policy, and change other configuration settings, as described below.

- 2a Review the information in the General section, then make the desired configuration changes (you can edit only the Revision and Description options in this section).

**Policy type:** Displays the policy type as Generic GNOME policy.

**Revision:** Displays the policy's revision number. To change the revision number, click *Increment Revision*.

**Number of errors not acknowledged:** Displays the number of errors that are not acknowledged.

**Number of warnings not acknowledged:** A warning is anything that does not cause the application of the policy to fail, but indicates minor problems. The number displayed indicates the number of unacknowledged warnings, which display in the Event Log section below.

**GUID:** Lists the selected object's GUID (global unique identifier), a randomly generated string that provides a unique identifier for the policy. You cannot edit the object's GUID.

**Description:** Displays the selected object's description, if one was provided when the policy was created. The description provides a short description of the policy's purpose. This description displays in the ZENworks Control Center interface.

Click *Edit* to change the description, if necessary.

- 2b Review the information in the Assignments section, then make the desired configuration changes.

The Assignments section lists the devices, device groups and device folders to which the selected policy is assigned. You can also view the folder to which the device belongs and the schedule. You can click the device object name to view information about that device object.

You can also use the following options:

**Advanced:** Click *Advanced* to display the Edit Assignments page to display a list of the devices that are assigned to the selected policy, the folder that contains each device, and each device's schedule. You can use the Edit Assignments page to edit certain settings, such as the schedule.

**Add:** Click *Add* to launch the Assign Policy Wizard to select the devices to be assigned to the selected policy. For more information, see [Section 14.4, "Assigning Policies," on page 128](#).

**Remove:** Select the device by clicking the check box next to the appropriate device name, then click *Remove* to remove the device's assignment from this policy.

- 2c Review the information in the Event Log section, then make the desired changes.

The Event Log section lists all unacknowledged errors and warnings.

The Status column displays an icon indicating each item's status. Position the mouse pointer over each icon to display a short message describing the status of the item.

To acknowledge an error or warning, click its name in the Event Column, then click *Acknowledged* in the Message Detail Information dialog box that displays. You can also click *Advanced*, select the check box next to the appropriate event, then click *Acknowledge* (a check mark displays on the right side of the Date column to indicate that the item has been acknowledged).

**2d** Review the information in the Upcoming Events section.

The Upcoming Events section lists events scheduled for the selected policy. You can click the calendar icon to display a calendar to view events for the desired date. You can also use the arrows to view events for the previous or next day, week, or month.

**2e** Review the information in the Groups section, then make the desired configuration changes.

The Groups section lists the groups that contain the selected policy.

You can also use the following options:

**Advanced:** Click *Advanced* to display the Edit Groups page to display a list of the groups that contain the selected policy. You can click *Add* to open the Select Groups dialog box to add the selected policy to existing groups. You can also remove a group by selecting the check box next to the Name column, then clicking *Remove* to remove.

**Add:** Click *Add* to open the Select Groups dialog box, then click the blue arrow in the Select column to select the desired group and display its name in the Selected list box.

**Remove:** Select the check box next to the appropriate group name, then click *Remove* to remove the selected policy from the group.

**3** Click the Details tab, then make the desired configuration changes.

**3a** You can add a new key or directory by selecting the directory under which you want to add the new key or directory. You can use the New menu to add a new key or directory.

If you want to configure more application keys using the same policy, the Import From a Device option is more appropriate. You can configure the device, test it, and then import the settings to update the policy.

You can import from the same device that was used to create the original policy or you can import from any other device. When you import settings, you have additional options, such as the following:

**Add the new imported settings that are not present in the policy:** Adds only those GConf settings that are not part of existing policy settings. This is selected by default. Use this option to update the policy by including more directories and keys.

**Override the settings that are already present in the policy with the imported settings:** Overrides the existing settings with the imported policy settings. Use this option to use the newly imported settings instead of the ones configured in the policy.

**Remove settings from the policy that are not present among the imported settings:**

Removes those policy settings that are not present in the imported settings. Use this feature to discard any additional settings that might be present in the original policy and that you do not want as a part of the updated policy.

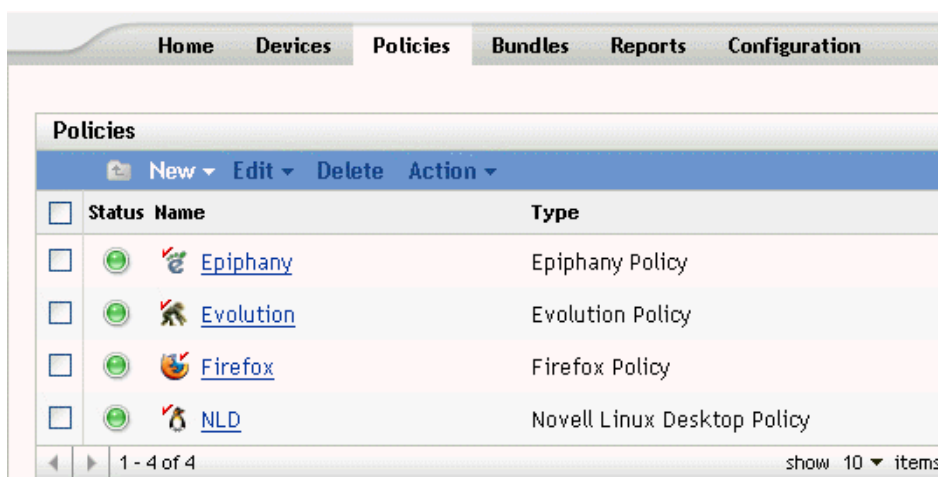
**3b** Edit the minimum system requirements according to your preferences. To edit the System Requirements of the Generic GNOME policy, see [Section 14.8, “Editing System Requirements,” on page 141](#).

- 3c Click *Apply* to save any changes you have made.
- 4 After a policy is modified, the Revision field of the policy (under the General section of the Summary page), must be incremented for the updated policy to be applied to associated devices. If the policy revision is not incremented, the changes made to the policy are not applied on the device.

### 14.7.3 Editing Remote Execute Policies

To edit the Remote Execute policy:

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



- 2 Click the policy's name to display the Summary page, then make the desired configuration changes.

If you do not want to edit any item on the Summary page, skip to **Step 3 on page 138**.

Use the Summary page to view detailed information about the selected policy. This page provides general information about the policy, lists the individual devices that are assigned to the policy, displays an event log, shows upcoming events, and lists the groups that the policy belongs to.

You can also use this page to edit the policy's description, add or remove assignments for the policy, and change other configuration settings, as described below.

- 2a Review the information in the General section, then make the desired configuration changes (you can edit only the Revision and Description options in this section).

**Policy type:** Displays the policy type as Remote Execute policy.

**Revision:** Displays the policy's revision number. To change the revision number, click *Increment Revision*.

**Number of errors not acknowledged:** Displays the number of unacknowledged errors.

**Number of warnings not acknowledged:** A warning is anything that does not cause the application of the policy to fail, but indicates minor problems. The number displayed indicates the number of unacknowledged warnings, which display in the Event Log section below.

**GUID:** Lists the selected object's GUID (global unique identifier), a randomly generated string that provides a unique identifier for the policy. You cannot edit the object's GUID.



**Description:** Displays the selected object's description, if one was provided when the policy was created. The description provides a short description of the policy's purpose. This description displays in the ZENworks Control Center interface.

Click *Edit* to change the description, if necessary.

- 2b** Review the information in the Assignments section, then make the desired configuration changes.

The Assignments section lists the devices, device groups and device folders to which the selected policy is assigned. You can also view the folder to which the device belongs and the schedule. You can click the device object name to view information about that device object.

You can also use the following options:

**Advanced:** Click *Advanced* to display the Edit Assignments page to display a list of the devices that are assigned to the selected policy, the folder that contains each device, and each device's schedule. You can use the Edit Assignments page to edit certain settings, such as the schedule.

**Add:** Click *Add* to launch the Assign Policy Wizard to select the devices to be assigned to the selected policy. For more information, see [Section 14.4, "Assigning Policies," on page 128](#).

**Remove:** Select the device by selecting the check box next to the appropriate device name, then click *Remove* to remove the device's assignment from this policy.

- 2c** Review the information in the Event Log section, then make the desired changes.

The Event Log section lists all unacknowledged errors and warnings.

The Status column displays an icon indicating each item's status. Position the mouse pointer over each icon to display a short message describing the status of the item.

To acknowledge an error or warning, click its name in the Event Column, then click *Acknowledged* in the Message Detail Information dialog box that displays. You can also click *Advanced*, select the check box next to the appropriate event, then click *Acknowledge* (a check mark displays on the right side of the Date column to indicate that the item has been acknowledged).

- 2d** Review the information in the Upcoming Events section.

The Upcoming Events section lists events scheduled for the selected policy. You can click the calendar icon to display a calendar to view events for the desired date. You can also use the arrows to view events for the previous or next day, week, or month.

- 2e** Review the information in the Groups section, then make the desired configuration changes.

The Groups section lists the groups that contain the selected policy.

You can also use the following options:

**Advanced:** Click *Advanced* to display the Edit Groups page to display a list of the groups that contain the selected policy. You can click *Add* to open the Select Groups dialog box to add the selected policy to existing groups. You can also remove a group by selecting the check box next to the Name column, then clicking *Remove*.

**Add:** Click *Add* to open the Select Groups dialog box, then click the blue arrow in the Select column to select the desired group and display its name in the Selected list box.

**Remove:** Select the check box next to the appropriate group name, then click *Remove* to remove the selected policy from the group.

- 3 Click the Details tab, then make the desired configuration changes. For more information about the available options, see [Section 13.6, “Remote Execute Policy,” on page 111](#).

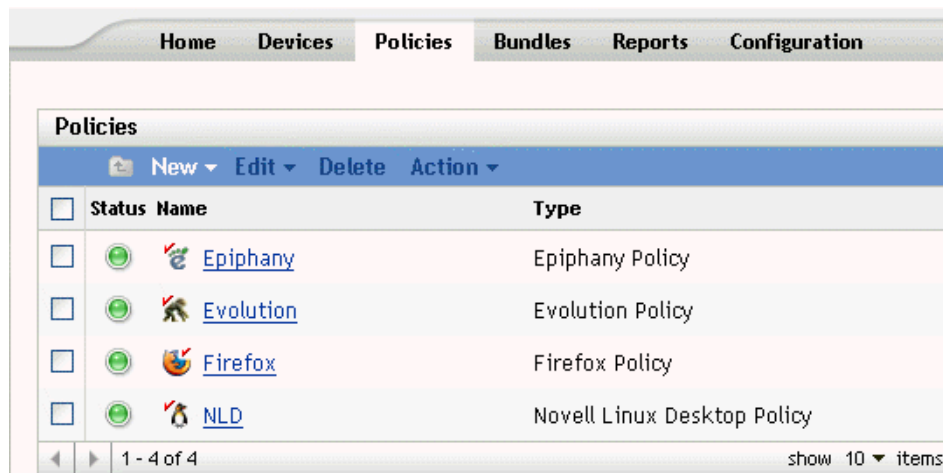
You can add system requirements to a policy. For more information, see [Section 14.8, “Editing System Requirements,” on page 141](#).

- 3a Click *Apply* to save any changes you have made.
- 4 After a policy is modified the Revision field of the policy (available under the General section of the Summary page), must be incremented for the updated policy to be applied to associated devices. If the policy revision is not incremented, the changes made to the policy are not applied on the device.

## 14.7.4 Editing Text File Policies

To edit the Text File Policy:

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



- 2 Click the policy's name to display the Summary page, then make the desired configuration changes.

If you do not want to edit any item on the Summary page, skip to [Step 3 on page 140](#).

Use the Summary page to view detailed information about the selected policy. This page provides general information about the policy, lists the individual devices that are assigned to the policy, displays an event log, shows upcoming events, and lists the groups that the policy belongs to.

You can also use this page to edit the policy's description, add or remove assignments for the policy, and change other configuration settings, as described below.

- 2a Review the information in the General section, then make the desired configuration changes (you can edit only the Revision and Description options in this section).

**Policy type:** Displays the policy type as Text File policy.

**Revision:** Displays the policy's revision number. To change the revision number, click *Increment revision*.

**Number of errors not acknowledged:** Displays the number of unacknowledged errors.

**Number of warnings not acknowledged:** A warning is anything that does not cause the application of the policy to fail, but indicates minor problems. The number displayed indicates the number of unacknowledged warnings, which display in the Event Log section below.

**GUID:** Lists the selected object's GUID (global unique identifier), a randomly generated string that provides a unique identifier for the policy. You cannot edit the object's GUID.

**Description:** Displays the selected object's description, if one was provided when the policy was created. The description provides a short description of the policy's purpose. This description displays in the ZENworks Control Center interface.

Click *Edit* to change the description, if necessary.

- 2b** Review the information in the Assignments section, then make the desired configuration changes.

The Assignments section lists the devices, device groups and device folders to which the selected policy is assigned. You can also view the folder to which the device belongs and the schedule. You can click the device object name to view information about that device object.

You can also use the following options:

**Advanced:** Click *Advanced* to display the Edit Assignments page to display a list of the devices that are assigned to the selected policy, the folder that contains each device, and each device's schedule. You can use the Edit Assignments page to edit certain settings, such as the schedule.

**Add:** Click *Add* to launch the Assign Policy Wizard to select the devices to be assigned to the selected policy. For more information, see [Section 14.4, “Assigning Policies,” on page 128](#).

**Remove:** Select the device by selecting the check box next to the appropriate device name, then click *Remove* to remove the device's assignment from this policy.

- 2c** Review the information in the Event Log section, then make the desired changes.

The Event Log section lists all unacknowledged errors and warnings.

The Status column displays an icon indicating each item's status. Position the mouse pointer over each icon to display a short message describing the status of the item.

To acknowledge an error or warning, click its name in the Event Column, then click *Acknowledged* in the Message Detail Information dialog box that displays. You can also click *Advanced*, select the check box next to the appropriate event, then click *Acknowledge* (a check mark displays on the right side of the Date column to indicate that the item has been acknowledged).

- 2d** Review the information in the Upcoming Events section.

The Upcoming Events section lists events scheduled for the selected policy. You can click the calendar icon to display a calendar to view events for the desired date. You can also use the arrows to view events for the previous or next day, week, or month.

- 2e** Review the information in the Groups section, then make the desired configuration changes.

The Groups section lists the groups that contain the selected policy.

You can also use the following options:

**Advanced:** Click *Advanced* to display the Edit Groups page to display a list of the groups that contain the selected policy. You can click *Add* to open the Select Groups dialog box to

add the selected policy to existing groups. You can also remove a group by selecting the check box next to the Name column, then clicking Remove to remove.

**Add:** Click *Add* to open the Select Groups dialog box, then click the blue arrow in the Select column to select the desired group and display its name in the Selected list box.

**Remove:** Select the check box next to the appropriate group name, then click *Remove* to remove the selected policy from the group.

- 3 Click the Details page. This page lets you perform the following actions:

Editing Item	Description
Edit the existing change(s) to be made	Lets you update the modifications to be made.
Add a new change to the same file	Lets you make multiple changes to the same file.
Add a new file to be changed and the corresponding changes	Lets you modify multiple files using the same policy.
Rename the change	Lets you keep the changed name consistent with the changes made.
Edit the file to be modified	Lets you edit the filename to apply the changes to another file or update the filename.
Delete files and changes	Lets you delete the files and changes.
Reorder files and changes	<p>A file is modified in the order of the changes shown in the ZENworks Control Center, you can use this option to order the sequence of changes. Because the second modification will be done on the updated file after the first modification is complete, and so on, ordering changes lets you perform logical operations.</p> <p>Ordering of files lets you modify files in a logical order.</p>
Edit the pre- and post-change actions	Lets you add, edit, or remove the pre- and post-change actions for the policy. You can also edit the action to be taken when a pre-change action fails.

You can add system requirements to a policy. For more information, see [Section 14.8, “Editing System Requirements,” on page 141](#).

**3a** Click *Apply* to save any changes you have made.

- 4 After a policy is modified, the Revision field of the policy (available under the General section of the Summary page) must be incremented for the updated policy to be applied to associated devices. If the policy revision is not incremented, the changes made to the policy are not applied on the device.

## 14.7.5 Viewing Policy Enforcement Status

You can view the status of a policy by looking at the icon located next to each policy. The following table describes each color code and its description:

Color Code	Policy Status
Green	Normal. The policy has been successfully enforced on all associated devices.
Yellow	Warning. A device has encountered a warning when trying to apply this policy.
Red Cross	Critical. A device has encountered an error when trying to apply this policy.

To view more information about a warning or error, click the policy to review the event log.

## 14.8 Editing System Requirements

The purpose of the system requirements is to limit some policies to run on devices that have the necessary requirements to enforce the policy. When more than one GConf-based policy of the same type is assigned, the first policy that meets the requirements is enforced on managed devices. All effective Remote Execute and Text File policies are enforced on managed devices.

You can specify the system requirements by defining certain conditions, called filters. You can set up simple system requirements that contain only one filter, or you can set up complex system requirements containing multiple filters or groups of filters. If you set up system requirements using more than one filter, you must also specify the logical relationship between the filters.

To set up a filter:

- 1 In the ZENworks Control Center, click the *Policies* tab.
- 2 Select a policy for which you want to edit the system requirements.
- 3 Click the *Details* tab.
- 4 In the Combine Filters Using field, select AND or OR.

This setting lets you specify the logical relationship between filter sets and filters. Select And to satisfy all the sets of filters and select Or to satisfy any one of the filter sets. By default, the filters are defined in one filter set. Within a filter set, select OR to satisfy any one of the filter conditions and select AND to satisfy all the filter conditions.

- 5 (Optional) Click *Add filter*. The new filter is added and it is applied based on the logical relationship you have defined in [Step 4 on page 141](#).
- 6 (Optional) Click *Add filter set* to add a new filter set. This filter is also applied based on the logical relationship you have defined in [Step 4 on page 141](#).
- 7 Select a value from the first drop-down list.

The operator list and other text boxes are displayed based on the value you have selected in the first drop-down list.

- 8 Specify a value in the text box. The following table describes values you can select in the first drop-down list and corresponding examples you can specify:

Criteria	Field 1	Field 2	Field 3
Date of File	Filename with complete path	Logical condition	Date
Distribution	Logical condition	Distribution name with version number	-

Criteria	Field 1	Field 2	Field 3
Environment	Environment Variable	Logical condition	Value
Find File	Filename with full path	Logical condition	-
Find RPM	RPM name  Make sure that the RPM name you specify is case-sensitive.	Logical condition	-
Free Disk Space	File system. For example, /dev/hda1.	Logical condition	Value in KB
Kernel	Logical condition	Linux kernel_version. For example, Linux 2.6.5-7.111	-
Processor	Logical condition		-
Size of file	Filename with complete path	Logical condition	Size in bytes
Total Disk Space	File system. For example, /dev/hda1.	Logical condition	Value in KB
Used Disk Space	File System. For example, /dev/hda1	Logical condition	Value in KB
Version of RPM	RPM name  Make sure that the RPM name you specify is case-sensitive.	Logical condition	Version (2.0.1)

**9** Select an operator from the drop-down list.

The operator drop-down list is displayed based on the value you have selected in the first drop-down list. For example, if you select *Version of RPM*, the available operators are *Equal to*, *Not Equal to*, *Less Than*, *Greater than*, *Greater than or equal to*, and *Less than or equal to*. If you select *Size of file*, the available operators are *Less than*, *Greater than*, *Greater than or equal to*, and *Less than or equal to*. If you select *Date of file*, the available options are *On*, *After*, *On or after*, *Before*, and *On or before*. If you select *Date of file*, you can also select a specific date.

**10** Click *Apply*.

## 14.9 Refreshing Policies

If you assign a new policy to a device or update a policy, you can ensure that the policy is updated on managed devices by refreshing the policies. Each device periodically refreshes its settings. It is not necessary to manually refresh each device after updating a policy. To ensure that the updated

policy is immediately pulled down, you can manually refresh the device using the following methods:

- ♦ In the ZENworks Control Center, go to the Devices page, select the appropriate device, click *Actions*, then click *Refresh Device*.
- ♦ On a managed device, start a console session and execute the following command: `/opt/novell/zenworks/bin/rug refresh`

Performing either action results in the managed device refreshing its policies and other settings. A newly assigned or updated policy is delivered to the device and is applied according to its schedule.

## 14.10 Verifying Policy Enforcement

ZENworks Linux Management lets you verify the enforcement of a policy after it has been assigned to a device or updated and the device has been refreshed (either manually or automatically by ZENworks). After a policy has been enforced, a message is logged indicating the success or failure of the policy enforcement. These messages can be seen in the Event log of the device on which the policy was applied or can be seen in the Event log of the policy that was applied.

To verify the enforcement of the GConf-based policies, you need to re-login to the assigned device. You can then start the application and verify that the policy has been enforced correctly.

If a desktop or user interface session is in progress on a managed device with GConf-based policies assigned to it, and an updated policy is enforced on that device by a console login or an `su` command, all updated settings may not be immediately applicable on the desktop session. The updated settings are reflected only when the user logs in via the user interface session again.

In the Novell Linux Desktop policy, some of the configuration settings are file-permission-based, and hence for a root user, these settings such as items in the Program menu and System menu will be accessible even if it is locked.

For the Remote Execute and Text File policies, the enforcement occurs according to the schedule. To verify the enforcement, check the managed device to ensure that the specified changes or actions have taken place.

You can also verify the enforcement status or check for errors by looking at the `zmd` log on the managed device (`/var/opt/novell/log/zenworks/zmd-messages.log`).

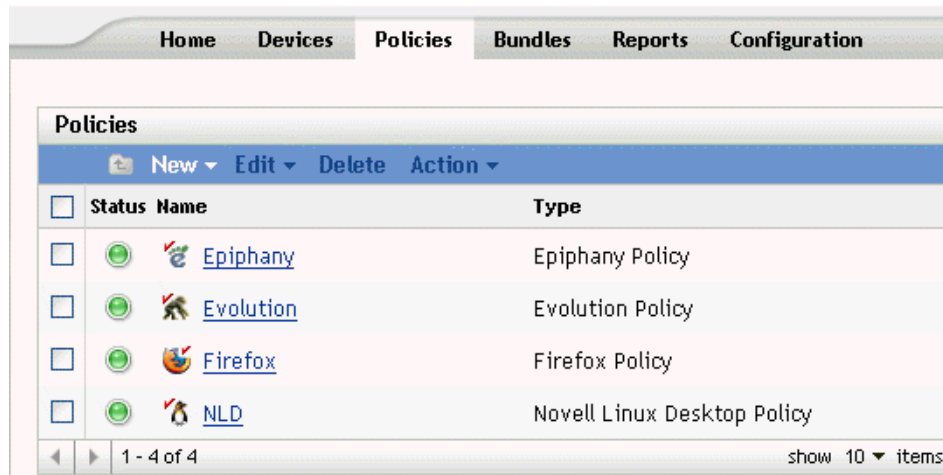
## 14.11 Renaming, Copying, or Moving Policies

Use the Edit drop-down list on the Policies page to edit an existing object. To access the Edit drop-down list, you must select an object by clicking the check box next to the object's name in the list.

Depending on the type of object you select, you can rename, copy, or move the object. For example, if you select a Policy object, you can rename, copy, and move the policy. If you select a Policy Group object, you can rename or move the Policy Group object, but not copy it. If the option is dimmed, that option is not available for the selected object type.

Some actions cannot be performed on multiple objects. For example, if more than one check box is selected, the Rename option is not available from the Edit menu.

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



- 2 In the Policies list, select the box next to the policy's name, click *Edit*, then click an option.

- ♦ **Rename:** Click *Rename*, type a new name for the policy, then click *OK*.
- ♦ **Copy:** Click *Copy*, type a new name for the copy, then click *OK*.

The copy option is useful to create a new policy that is similar to an existing policy. You can copy a policy and then edit the new policy's settings.

Only policy settings are copied; policy groups and assignments are not copied.

- ♦ **Move:** Click *Move*, select a destination folder for the selected objects, then click *OK*.

If you rename or move a policy, its assignments are still in place. ZENworks Linux Management does not reapply the policy to devices because of the name or location change.

## 14.12 Deleting Policies, Policy Groups, and Folders

Before you delete policies, policy groups, and folders from the ZENworks Control Center, review the following information to ensure that you obtain the desired results.

**Deleting Policies:** Depending on your needs, you can delete a policy from your ZENworks Linux Management system or remove a policy's assignments from devices.

If you delete a policy from your ZENworks Linux Management system, the policy does not display on the Policies or Devices pages in the ZENworks Control Center. When a policy is deleted, it is unassigned and unenforced from the device with which it was assigned. For more information, see [Section 14.13, "Unenforcing Policies," on page 145](#).

**Deleting Policy Groups:** The results of deleting a policy group is similar to that of deleting a policy.

If you delete a policy group from your ZENworks Linux Management system, the policy group does not display on the Policies page in the ZENworks Control Center and the policy group's assignments



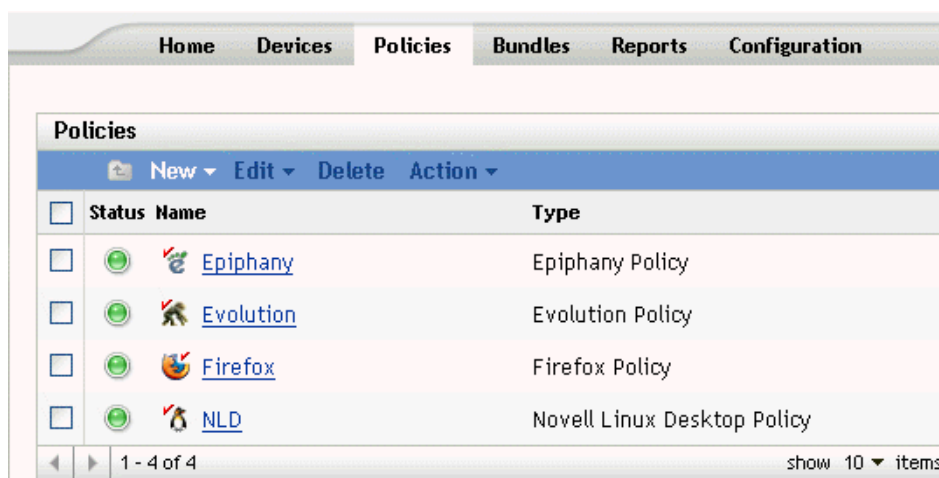
are removed. However, the individual policies contained in the group are not removed from the ZENworks Control Center and still display on the Policies page.

When a policy group is deleted, its member policies are not deleted, but the associations are removed. The policies of a policy group are unenforced from the devices to which the policy group was associated. For more information, see [Section 14.13, “Unenforcing Policies,” on page 145](#).

**Deleting Folders:** If you delete a folder that contains policies from your ZENworks Linux Management system, both the folder and its policies are removed from the ZENworks Control Center. The policies contained in the folder are unenforced from the device to which they were assigned. For more information, see [Section 14.13, “Unenforcing Policies,” on page 145](#).

To delete a policy, policy group, or folder:

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



- 2 In the Policies list, select the box next to the desired item's name, then click *Delete*.

If the item you are deleting is a folder, you are prompted whether or not to delete the folder and its contents.

When a policy folder is deleted, each of its policies and subfolders are also deleted.

## 14.13 Unenforcing Policies

Policies are unenforced when either a policy is deleted or it is unassigned from a device. On the next refresh, the policy data is removed from the managed device. For GConf-based policies, when a user logs in after a refresh, the configuration changes made by the policy are undone. Unenforcement is not supported for the Remote Execute and Text File policies.



# Package Management

# IV

The following sections provide information about Novell® ZENworks® Linux Management Package and Content Management features and procedures:

- ♦ Chapter 15, “Package Management Overview,” on page 149
- ♦ Chapter 16, “Using RPM Bundles,” on page 153
- ♦ Chapter 17, “Using Catalogs,” on page 187
- ♦ Chapter 18, “Replicating Content in the ZENworks Management Zone,” on page 197
- ♦ Chapter 19, “Mirroring Software,” on page 199
- ♦ Chapter 20, “Creating RPM Packages From Tarballs,” on page 207



Novell® ZENworks® Linux Management lets you install software using either a bundle or a catalog. Software included in a bundle that is directly assigned is considered mandatory; the software is installed on all assigned devices. A catalog is a collection of RPM bundles; software bundles included in a catalog are usually considered optional.

ZENworks Linux Management also provides content replication and mirroring to replicate content (packages, bundles, and catalogs) from one server to other servers in your system.

The content replication feature in ZENworks Linux Management lets you replicate content from the primary ZENworks server to secondary servers in a single ZENworks Management Zone.

The mirroring feature (zlmmirror) lets you replicate content between Management Zones or from remote servers.

The following sections contain additional information:

- ♦ [Section 15.1, “Understanding RPM Bundles,” on page 149](#)
- ♦ [Section 15.2, “Understanding Catalogs,” on page 150](#)
- ♦ [Section 15.3, “Understanding the zlman Utility,” on page 150](#)
- ♦ [Section 15.4, “Replicating Content in the ZENworks Management Zone,” on page 150](#)
- ♦ [Section 15.5, “Mirroring Software,” on page 150](#)

## 15.1 Understanding RPM Bundles

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

ZENworks Linux Management uses Red Hat Package Manager (RPM). RPM is a powerful package management system capable of installing, uninstalling, verifying, querying, and updating computer software packages on different devices.

ZENworks Linux Management supports the RPM format.

Software included in a bundle that is directly assigned is considered mandatory; the software is installed on all devices assigned to the bundle (the bundle is directly assigned to devices, device groups, or device folders).

When you create a bundle using the Create New Bundle Wizard, you are given the choice of creating an RPM package bundle or a preboot bundle. A preboot bundle performs operations before the operating system boots. If you are familiar with ZENworks Desktop Management, preboot bundles are similar to imaging operations. For more information, see [Part V, “Preboot Services,” on page 209](#).

You can also create bundle groups to collect several bundles to ease administration and to provide easier assigning and scheduling of the bundles in the bundle group.

For more information and step-by-step instructions, see [Chapter 16, “Using RPM Bundles,” on page 153](#).

## 15.2 Understanding Catalogs

A catalog is a collection of bundles; software bundles included in a catalog are usually considered optional. You can use catalogs to deploy and install optional or dependent packages to assigned devices. If you deploy optional packages to devices by using a catalog, users can choose whether to deploy and install the software packages included in the bundles inside the catalog. Users use the ZENworks Linux Management Update Manager to manage the software on managed devices. To access the ZENworks Linux Management Update Manager from the device, click *System*, then click *Software Update*.

You can also use bundles in a catalog to provide dependent packages for a primary package contained in a bundle or in another catalog. For example, suppose you want to include Java\* Runtime in a catalog and, optionally, hide the catalog from the user interface. If a package contained in a bundle or in another catalog needs Java Runtime (it is listed as a dependency for the primary package), the package containing Java Runtime becomes mandatory and is deployed and installed on all devices that the primary package is deployed and installed on.

For more information and step-by-step instructions, see [Chapter 17, “Using Catalogs,” on page 187](#).

## 15.3 Understanding the zlman Utility

The zlman utility is the command-line interface to ZENworks Linux Management. If you need to create and configure a large number of bundles or catalogs, or if you want to automate the process using scripts, you can use zlman.

The zlman utility lets you create and modify bundles, including adding packages to bundles and creating patch bundles. You can also use zlman to create and modify catalogs, including adding bundles to catalogs.

For more information, see [zlman \(http://www.novell.com/documentation/zenworks7/zlmref/zlman.html\)](http://www.novell.com/documentation/zenworks7/zlmref/zlman.html).

## 15.4 Replicating Content in the ZENworks Management Zone

ZENworks Linux Management uses a hierarchical organization to simplify device management. At the top level, a ZENworks Management Zone provides an autonomous unit of ZENworks Servers and managed devices (workstations and servers). The ZENworks Servers manage the devices.

Each ZENworks Management Zone has one primary server, and optionally, one or more secondary servers to help distribute workload.

All RPM packages must reside on the primary server. ZENworks Linux Management uses content replication to replicate packages to each secondary server in your Management Zone.

For more information, see [Chapter 18, “Replicating Content in the ZENworks Management Zone,” on page 197](#).

## 15.5 Mirroring Software

ZENworks Linux Management lets you connect to a remote server and copy software catalogs, bundles, or packages from the remote server to your server using a few simple commands.

Depending on your needs, you might have more than one ZENworks Management Zone in your system. To replicate content across Management Zones, you must use `zlmirror`.

For more information, see [Chapter 19, “Mirroring Software,” on page 199](#).





Using Novell® ZENworks® Linux Management, you can install software using either a bundle or a catalog.

Software included in a bundle that is directly assigned is considered mandatory; the software is installed on all assigned devices (the bundle is directly assigned to devices, the device group, or the device folder).

A catalog is a collection of RPM bundles or bundle groups; software bundles included in a catalog are usually considered optional. For more information about catalogs, see [Chapter 17, “Using Catalogs,” on page 187](#).

The `zlm` utility is the command-line interface to ZENworks Linux Management. If you need to create and configure a large number of bundles or catalogs, or if you want to automate the process using scripts, you can use `zlm`. For more information, see [zlm](http://www.novell.com/documentation/zenworks7/zlmref/zlm.html) (<http://www.novell.com/documentation/zenworks7/zlmref/zlm.html>).

The following sections contain additional information:

- ♦ [Section 16.1, “Understanding Bundles,” on page 153](#)
- ♦ [Section 16.2, “Creating RPM Bundles,” on page 154](#)
- ♦ [Section 16.3, “Assigning Bundles,” on page 164](#)
- ♦ [Section 16.4, “Editing Bundles,” on page 167](#)
- ♦ [Section 16.5, “Adding Bundles to Catalogs,” on page 171](#)
- ♦ [Section 16.6, “Creating Folders,” on page 171](#)
- ♦ [Section 16.7, “Creating Bundle Groups,” on page 172](#)
- ♦ [Section 16.8, “Adding Bundles to Existing Groups,” on page 178](#)
- ♦ [Section 16.9, “Deleting Bundles, Bundle Groups, and Folders,” on page 178](#)
- ♦ [Section 16.10, “Renaming, Copying, or Moving Bundles,” on page 179](#)
- ♦ [Section 16.11, “Deploying a Different Version of a Bundle,” on page 180](#)
- ♦ [Section 16.12, “Using a Remote Execute Policy to Remove Bundles and Packages from Devices,” on page 181](#)
- ♦ [Section 16.13, “Generating Bundle Reports,” on page 185](#)

## 16.1 Understanding Bundles

ZENworks Linux Management lets you create the following types of bundles:

- ♦ [Section 16.1.1, “RPM Bundles,” on page 154](#)
- ♦ [Section 16.1.2, “Preboot Bundles,” on page 154](#)

## 16.1.1 RPM Bundles

An RPM bundle is a grouping of one or more software packages. ZENworks Linux Management ships all software in this format. Bundles contain one or more files that are installed to particular locations on a system, plus information about the bundle, such as version, description, what applications must also be present for it to be installed, and more.

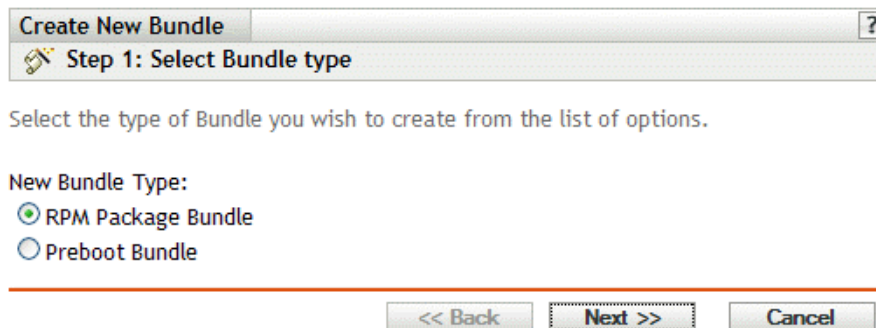
ZENworks Linux Management supports only the RPM format.

## 16.1.2 Preboot Bundles

A preboot bundle performs operations before the operating system boots. If you are familiar with ZENworks Desktop Management, preboot bundles are similar to imaging operations. For more information about preboot bundles, see [Part V, “Preboot Services,” on page 209](#).

## 16.2 Creating RPM Bundles

- 1 In the ZENworks Control Center, click the *Bundles* tab.
- 2 In the Bundle list, click *New*, then click *Bundle* to display the Select Bundle Type page.



The screenshot shows a dialog box titled "Create New Bundle" with a question mark icon in the top right corner. Below the title bar, it says "Step 1: Select Bundle type" with a small icon of a wrench and screwdriver. The main text reads: "Select the type of Bundle you wish to create from the list of options." Below this, under the heading "New Bundle Type:", there are two radio button options: "RPM Package Bundle" (which is selected with a green dot) and "Preboot Bundle". At the bottom of the dialog, there are three buttons: "<< Back", "Next >>" (which is highlighted with a dashed border), and "Cancel".

- 3 Select *RPM package bundle* (the default option), then click *Next* to display the Name and Description page.

For more information about preboot bundles, see [Part V, “Preboot Services,”](#) on page 209.

The screenshot shows a dialog box titled "Create New Bundle" with a question mark icon in the top right corner. Below the title bar is a subtitle "Step 2: Name and Description" with a wrench icon. The main area contains the instruction "Enter a name, display name, location, and description for this new Bundle." followed by four input fields: "Name:" (a single-line text box), "Display Name:" (a single-line text box), "Folder:" (a text box containing "/Bundles" with a browse button icon to its right), and "Description:" (a multi-line text area). At the bottom of the dialog are three buttons: "<< Back", "Next >>", and "Cancel".

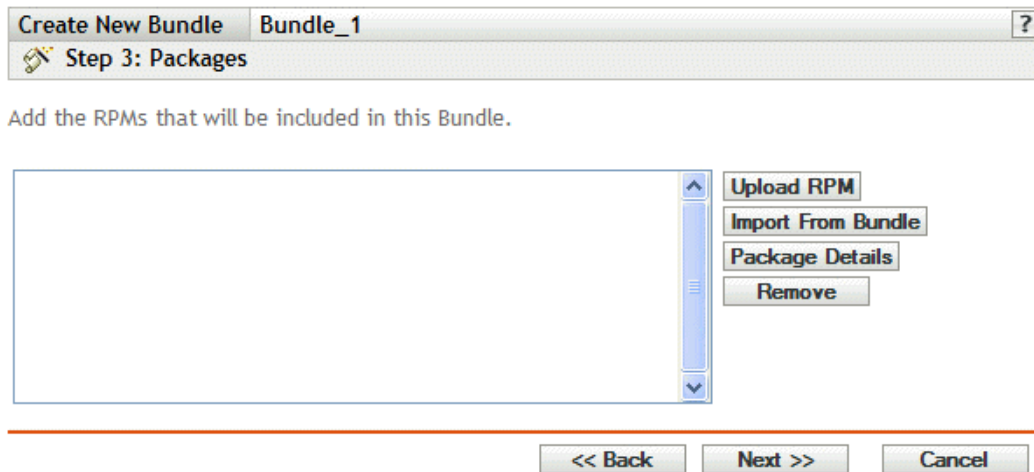
**4** Fill in the fields:

- ♦ **Name:** (Required) Provide a unique name for the RPM bundle. The name you provide displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.
- ♦ **Display name:** Provide a name that displays for users when they update software. The display name can be the same name that you provided in the Name field; however, you can choose to make the name more intuitive for users.
- ♦ **Folder:** Type the name or browse to the folder that this bundle will be created in. Folders display in the ZENworks Control Center. The default folder is /Bundles.
- ♦ **Description:** Provide a short description of the bundle's contents. This description displays in the ZENworks Control Center interface and in the ZENworks Linux Management Update Manager, which is the user interface for updating software.

**5** Click *Next* to display the Packages page.

Use the Packages page to add RPM packages to the bundle or to import RPM packages contained in an existing bundle. The packages that you add to a bundle must already exist on the local device on which you are running the ZENworks Control Center. During the bundle-creation process, packages are copied to the ZENworks Server and placed in the package

repository (/var/opt/novell/zenworks/pkg-repo). You can also import packages from an existing RPM bundle.

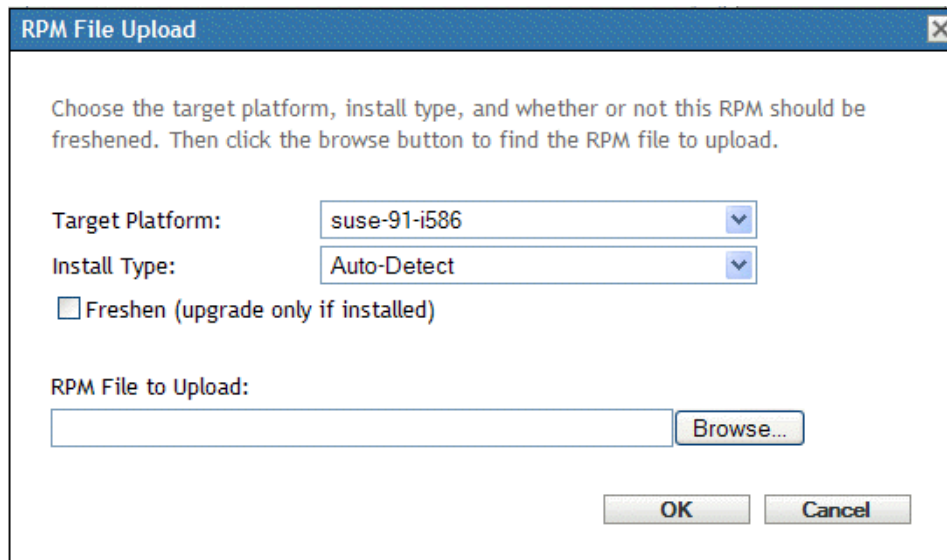


- 6 Add the RPM packages to include in the bundle using the *Upload RPM* and the *Import from Bundle* options.

You can use either the *Upload RMP* option or the *Import from Bundle* option, or you can use both options, depending on your needs.

After you upload or import packages into the list, you can view the details of a selected package by using the *Package Details* option. You can remove a selected package from the list by using the *Remove* option.

- 6a (Optional) Click the *Upload RPM* button to open the RPM File Upload dialog box, then fill in the fields:



**Target platform:** Select the desired platform from the *Target platform* drop-down list.

The target platform is the platform of the devices that the package will be installed on. ZENworks Linux Management does not auto-detect the target platform by examining the RPM packages because RPM packages are not limited to working on only one platform;

RPM packages can be created to work on multiple platforms. For this reason, the administrator must select the platform of the target devices.

---

**NOTE:** Bundles can be installed on any platform; bundles are not platform-specific. The packages contained in bundles are platform-specific and can be installed only on devices supporting the specified platform.

You can, however, create a bundle containing several packages that apply to various Linux platforms. When the bundle is assigned to a group of devices or to a folder that contains devices running on different platforms, each managed device gets the appropriate packages installed.

For example, you could create a bundle containing two packages: PackageA and PackageB. PackageA applies to suse-93-i586, nld-9-i586, and sles-9-i586. PackageB applies to nld-9-i586 only. If you assign the bundle to a folder containing three devices, with each device running one of these platforms, the bundle will be installed on all three devices; however, PackageA will be installed on all three devices and PackageB will be installed only on the device running nld-9-i586.

For this reason, the ZENworks Control Center might indicate that a bundle is effective for a device even if one or several packages contained in the bundle was not installed.

If you want a bundle to be platform-specific, you must use a script and have the script verify the target platform before deploying and installing the bundle.

---

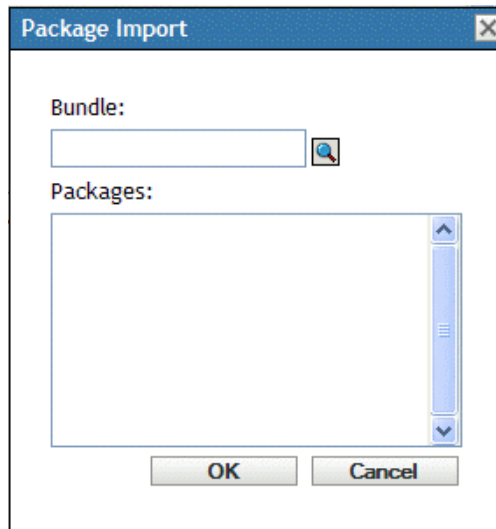
**Install type:** Use the Install type drop-down list to choose from the following installation options:

- ♦ **Auto-detect:** Automatically detects whether the bundle is already installed on assigned devices and either installs the bundle or updates an existing bundle, if necessary. Basically, the *Auto-detect* option determines whether the *Update* or the *Install* option functionality (explained below) is best, and then performs that operation. Any kernel packages are installed using the *Install* option functionality; other packages are installed using the *Update* option functionality. This is the default option and should be used in most situations.
- ♦ **Update:** Updates the packages on assigned devices if the packages in the bundle are newer than what is installed on the devices. If the packages are not installed on the assigned devices, ZENworks Linux Management installs them. With the *Update* option, you don't need to worry whether a package is already installed because the package is either updated (if needed) or installed on the device. Parallel installation of a package is not possible with the Update option.
- ♦ **Install:** Installs the bundle on all assigned devices. If previous versions of the packages exist on the devices, ZENworks Linux Management does not update the existing packages. As a result, packages can be installed multiple times (parallel installations), which might cause overlap issues. This option is rarely used; you should use the default option, *Auto-detect*, under most circumstances. You should use this option almost exclusively to install kernel packages.

**Freshen (upgrade only if installed):** Use this option to transact a package only if a previous version of the package is already installed on the device. You can use the *Freshen* option in conjunction with the *Auto-detect*, *Update*, or *Install* options.

**RPM file to upload:** Browse to and select the RPM packages that you want to add to the bundle. The RPM packages must be located on the local device on which you are running the ZENworks Control Center. Click *OK* to upload the packages to the ZENworks Linux Management server.

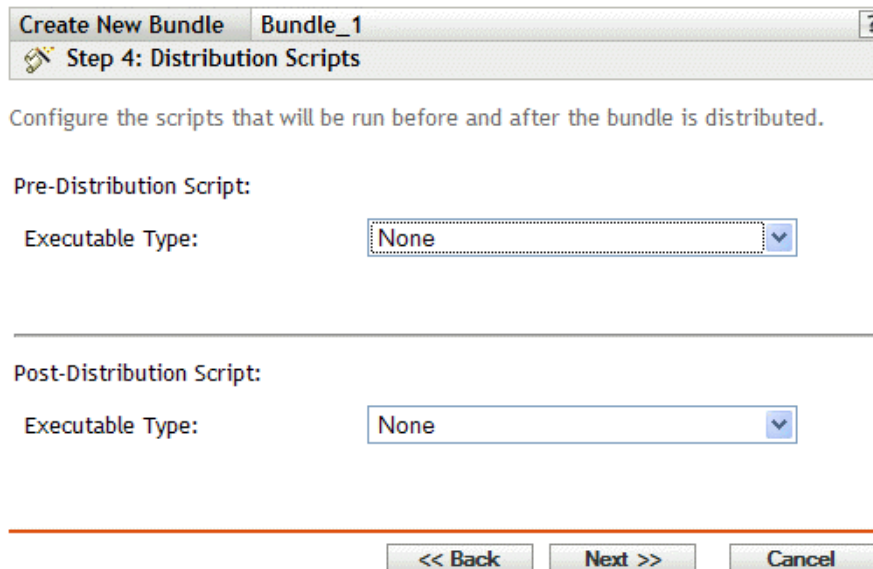
- 6b** (Optional) Click the *Import from Bundle* button to open the Package Import dialog box, fill in the fields, then click *OK*.



**Bundle:** Browse to and select the bundle you want to import packages from.

**Packages:** Select the packages to import.

- 7** Click *Next* to display the Distribution Scripts page.



- 8** Select a script engine from one or both of the *Executable type* drop-down lists, as needed.
- As part of the process of distributing a bundle, ZENworks Linux Management can launch a script engine to execute a “before distribution” script and an “after distribution” script. Distribution scripts let you perform tasks that must be done before or after a bundle is distributed. For example, you can log in to other servers or trees, provide dynamic mappings, run applications, and so forth.

Select one of the following script engines from the *Executable type* drop-down list:

- ♦ Script
- ♦ Binary
- ♦ Java
- ♦ None

Depending on the type of distribution script you select, different fields display to specify the filename and various parameters.

- 9 Click *Next* to display the Installation Scripts page.

Create New Bundle Bundle\_1 ?

Step 5: Installation Scripts

Configure the scripts that will be run before and after the bundle is installed.

Pre-Installation Script:

Executable Type: None

Post-Installation Script:

Executable Type: None

<< Back Next >> Cancel

- 10 Select a script engine from one or both of the *Executable type* drop-down lists, as needed.

As part of the process of distributing a bundle, ZENworks Linux Management can launch a script engine to execute a “before installation” script and an “after installation” script. Installation scripts let you perform tasks that must be done before or after a bundle is installed. For example, you can log in to other servers or trees, provide dynamic mappings, run applications, and so forth.

Select one of the following script engines from the *Executable type* drop-down list:

- ♦ Script
- ♦ Binary
- ♦ Java
- ♦ None

Depending on the type of distribution script you select, different fields display to specify the filename and various parameters.

- 11 Click *Next* to display the Summary page, then review the information on the Summary page, making any changes to the bundle settings by using the *Back* button as necessary.

Depending on your needs, you can create the bundle now or you can configure additional options for this bundle.

- 12** Click *Finish* to create the bundle as configured per settings on the Summary page. If you click *Finish*, the bundle is created but it does not have devices assigned, a schedule, and so forth. At some point in the future, you need to configure additional options for the bundle by continuing with [Section 16.3, “Assigning Bundles,” on page 164](#).

or

Click *Next* to display the Bundle Assignment page to perform the following tasks:

- ◆ Specify assignments for this bundle
- ◆ Specify the deployment schedule for this bundle
- ◆ Specify the installation schedule for this bundle
- ◆ Specify special flags, such as flags to specify to remove conflicting packages or trying a dry run to test a bundle's deployment
- ◆ Specify groups for this bundle

Create New Bundle Bundle\_1 ?

Step 7: Bundle Assignments

Specify the assignments for this bundle:

Add	Remove
<input type="checkbox"/>	Name In Folder

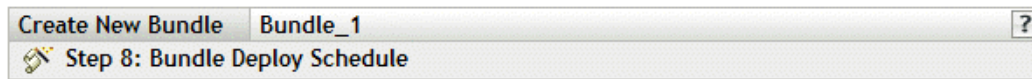
No items selected, click add to select items

<< Back Next >> Cancel

- 13** Assign the bundle to the devices that you want to distribute the bundle to.
- 13a** Click *Add* to browse for and select the appropriate Server or Workstation objects.  
You can also select Folder or Group objects.
- 13b** Click the down-arrow next to Servers or Workstations to expand the list, then click the underlined link in the Name column to select the desired objects and display their names in the Selected list box.  
Assigning a bundle to a Folder or Group object is the preferred method of assigning the bundle. Assigning the bundle to a large number of objects (for example, more than 250) might cause increased server utilization.
- 13c** Click *OK*.

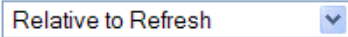


- 14 Click *Next* to display the Bundle Deploy Schedule page.



Select the schedule to apply to the bundle assignments:

Schedule Type:



Select the initial delay and repeat frequency to run the scheduled event and set other restrictions that may apply

- 15 Select a bundle-deployment schedule type from the drop-down list, then select the desired options, which vary, depending on the schedule type you select.

For more information on the various options, click the desired link in the Schedule Type column in the following table.

The settings you configure on this page determine when the bundle is deployed to assigned devices. The next page in this wizard, Bundle Install Schedule, lets you configure when the software packages in the bundle are actually installed on assigned devices.

The deployment schedule determines when the packages inside the bundle are downloaded from the server to the assigned devices. The software packages are not yet installed and available for use. The installation schedule determines when the software packages are installed to assigned devices so the software will be available for use.

The following schedules are available. Click the link in the left column in the table below for more information about each schedule type and its options.

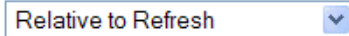
Schedule Type	Description
<a href="#">No Schedule</a>	Use this option to indicate no schedule; no action occurs.
<a href="#">Date Specific</a>	Select one or more dates on which to deploy the bundle to assigned devices and set other restrictions that might apply.
<a href="#">Day of the Week Specific</a>	Select one or more days of the week on which to deploy the bundle to assigned devices and set other restrictions that might apply.
<a href="#">Event</a>	Select the event that triggers the deployment of the bundle.
<a href="#">Monthly</a>	Select the day of the month on which to deploy the bundle to assigned devices and set other restrictions that might apply.
<a href="#">Relative to Refresh</a>	Schedule when the bundle is deployed, either immediately after the device refreshes or a specified amount of time after the device refreshes. You can also specify whether the bundle's deployment is repeated and specify a time period when you do not want the bundle deployed to help minimize network traffic during that time.

- 16 Click *Next* to display the Bundle Install Schedule page.



Select the schedule to apply to the bundle assignments:

Schedule Type:



Select the initial delay and repeat frequency to run the scheduled event and set other restrictions that may apply

- 17 Select a bundle-installment schedule type from the drop-down list, then select the desired options, which vary, depending on the schedule type you select.

For more information on the various options, click the desired link in the Schedule Type column in the following table.

The settings you configure on this page determine when the bundle is installed on assigned devices.

The following schedules are available. Click the link in the left column in the table below for more information about each schedule type and its options.

Schedule Type	Description
<a href="#">No Schedule</a>	Use this option to indicate no schedule; no action occurs.
<a href="#">Date Specific</a>	Select one or more dates on which to install the bundle on assigned devices and set other restrictions that might apply.
<a href="#">Day of the Week Specific</a>	Select one or more days of the week on which to install the bundle on assigned devices and set other restrictions that might apply.
<a href="#">Event</a>	Select the event that triggers the installation of the bundle.
<a href="#">Monthly</a>	Select the day of the month on which to install the bundle on assigned devices and set other restrictions that might apply.
<a href="#">Relative to Refresh</a>	Schedule when the bundle is installed, either immediately after the device refreshes or a specified amount of time after the device refreshes. You can also specify whether the bundle's installation is repeated and specify a time period when you do not want the bundle installed to help minimize network traffic during that time.

18 Click *Next* to display the Special Flags page.

Create New Bundle bunde\_1 ?

Step 10: Special Flags

Specify whether conflicting packages should be overwritten. Selecting Dry Run pretends to install as a test to see if there would be any issues. Check the log file for results.

☐ Remove conflicting packages  
☐ Attempt a dry run

<< Back Next >> Cancel

19 (Optional) Specify the following options:

- **Remove conflicting packages:** Select this option to specify that conflicting packages are uninstalled from devices before installing new packages. By default, this option is selected, so conflicting packages (previous versions of the same package, for example) are uninstalled before the current package is installed. If this option is not selected, packages will not be installed if a conflict is detected.
- **Attempt a dry run:** Select this option to have ZENworks Linux Management perform a test to determine if the RPM bundle can be successfully deployed. If there are any issues that could prevent the RPM bundle from being deployed, you can look at the log file to troubleshoot the bundle-creation process. The log file is located in `/var/opt/novell/logs/zenworks`.

A successful dry run ensures that the bundle can be successfully deployed or installed on assigned devices (packages are available, dependencies are met, etc.).

20 Click *Next* to display the Bundle Groups page.

Create New Bundle bunde\_1 ?

Step 11: Bundle Groups

Specify the groups for this bundle:

Add	Remove	Name	In Folder
<input type="checkbox"/>			

No items selected, click add to select items

<< Back Next >> Cancel

21 (Optional) Click *Add* to open the Select Groups dialog box, then click the underlined links in the Name column to select the desired bundle groups and display their names in the Selected list box.

Using bundle groups eases administration efforts by letting you group several bundles so you can use common assignments, schedules, and so forth, rather than configuring these settings for each bundle you create.

- 22** Click *Next* to display the Summary page.
- 23** Review the information on the Summary page, making any changes to the bundle settings by using the *Back* button as necessary. Click *Finish* to create the bundle as configured per settings on the Summary page.
- 24** Click *OK*.

## 16.3 Assigning Bundles

When you assign bundles, you specify device assignments, deployment and installation schedules, special flags, and groups for an existing bundle.

In [Step 12](#) under [Section 16.2, “Creating RPM Bundles,” on page 154](#), you were given the choice of clicking *Finish* or *Next*.

If you clicked *Finish*, the bundle was created without assigning devices to it, specifying deployment and installation schedules, setting special flags, or specifying groups for the bundle. Before the bundle can be deployed and installed on assigned devices, you must complete the following steps. If you clicked *Next*, you have already performed the following procedure as part of the bundle-creation process.

- 1** In the ZENworks Control Center, click the *Bundles* tab, select the desired bundle in the Bundles list by checking the box next to its name, click *Action*, then click *Assign Bundle* to display the Bundle Assignments page.

**Assign Bundle** ?

**Step 1: Devices to be Assigned**

Select the devices to be assigned to the previously selected bundles.

Add	Remove	Name	In Folder
<input type="checkbox"/>			

No items selected, click add to select items


<< Back    Next >>    Cancel

- 2** Assign the bundle to the devices that you want to distribute the bundle to.
  - 2a** Click *Add* to browse for and select the appropriate Server or Workstation objects.  
You can also select Folder or Group objects.
  - 2b** Click the down-arrow next to Servers or Workstations to expand the list, then click the underlined link in the Name column to select the desired objects and display their names in the Selected list box.  
Assigning a bundle to a Folder or Group object is the preferred method of assigning the bundle. Assigning the bundle to a large number of objects (for example, more than 250) might cause increased server utilization.
  - 2c** Click *OK*.

- 3 Click *Next* to display the Schedule page.

Assign Bundle

?

 Step 2: Schedule

Specify the schedule to use for the assignments.

Schedule Type:

Relative to Refresh

Select the initial delay and repeat frequency to run the scheduled event and set other restrictions that may apply

- 4 Select the schedule to apply to the assignments, then select the desired options, which vary, depending on the schedule type you select.

For more information on the various options, click the desired link in the Schedule Type column in the following table.

The settings you configure on this page determine when the bundle is assigned to devices. The next page in this wizard, Install Schedule, lets you configure when the software packages in the bundle are actually installed on assigned devices.

The following schedules are available. Click the link in the left column in the table below for more information about each schedule type and its options.

Schedule Type	Description
<a href="#">No Schedule</a>	Use this option to indicate no schedule; no action occurs.
<a href="#">Date Specific</a>	Select one or more dates on which to assign the bundle to devices and set other restrictions that might apply.
<a href="#">Day of the Week Specific</a>	Select one or more days of the week on which to assign the bundle to devices and set other restrictions that might apply.
<a href="#">Event</a>	Select the event that triggers the assignment of the bundle.
<a href="#">Monthly</a>	Select the day of the month on which to assign the bundle to devices and set other restrictions that might apply.
<a href="#">Relative to Refresh</a>	Schedule when the bundle is assigned, either immediately after the device refreshes or a specified amount of time after the device refreshes. You can also specify whether the bundle's assignment is repeated and specify a time period when you do not want the bundle assigned to help minimize network traffic during that time.

- 5 Click *Next* to display the Install Schedule page.



RPM Package Bundles can specify a second schedule for installation.

Schedule Type:

Relative to Refresh

Select the initial delay and repeat frequency to run the scheduled event and set other restrictions that may apply

- 6 Select a bundle-install schedule type from the drop-down list, then select the desired options, which vary, depending on the schedule type you select.

For more information on the various options, click the desired link in the Schedule Type column in the following table.

The settings you configure on this page determine when the bundle is installed on assigned devices.

The following schedules are available. Click the link in the left column in the table below for more information about each schedule type and its options.

Schedule Type	Description
<a href="#">No Schedule</a>	Use this option to indicate no schedule; no action occurs.
<a href="#">Date Specific</a>	Select one or more dates on which to install the bundle on assigned devices and set other restrictions that might apply.
<a href="#">Day of the Week Specific</a>	Select one or more days of the week on which to install the bundle on assigned devices and set other restrictions that might apply.
<a href="#">Event</a>	Select the event that triggers the installation of the bundle.
<a href="#">Monthly</a>	Select the day of the month on which to install the bundle on assigned devices and set other restrictions that might apply.
<a href="#">Relative to Refresh</a>	Schedule when the bundle is installed, either immediately after the device refreshes or a specified amount of time after the device refreshes. You can also specify whether the bundle's installation is repeated and specify a time period when you do not want the bundle deployed to help minimize network traffic during that time.

7 Click *Next* to display the Special Flags page.

**Assign Bundle** ?

**Step 4: Special Flags**

Specify whether conflicting packages should be overwritten. Selecting Dry Run pretends to install as a test to see if there would be any issues. Check the log file for results.

☒ Remove conflicting packages  
☐ Attempt a dry run

<< Back   Next >>   Cancel

8 (Optional) Specify the following options:

- ♦ **Remove conflicting packages:** Select this option to specify that conflicting packages are uninstalled from devices before installing new packages. By default, this option is selected, so conflicting packages (previous versions of the same package, for example) are uninstalled before the current package is installed. If this option is not selected, packages will not be installed if a conflict is detected.
- ♦ **Attempt a dry run:** Select this option to have ZENworks Linux Management perform a test to determine if the RPM bundle can be successfully deployed. If there are any issues that could prevent the RPM bundle from being deployed, you can look at the log file to troubleshoot the bundle-creation process. The log file is located in `/var/opt/novell/logs/zenworks`.

A successful dry run ensures that the bundle can be successfully deployed or installed on assigned devices (packages are available, dependencies are met, etc.).

9 Click *Next* to display the Finish page.

10 Review the information on the Finish page, making any changes to the bundle settings by using the *Back* button as necessary. Click *Finish* to create the bundle as configured per settings on the Finish page.

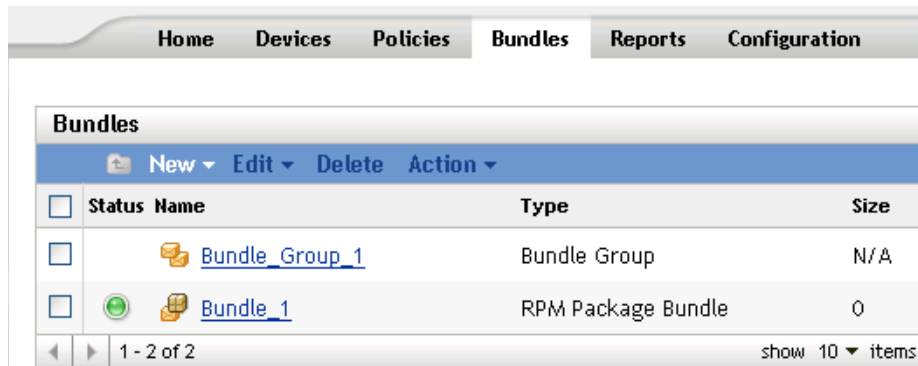
11 Click *OK*.



## 16.4 Editing Bundles

You can edit an existing bundle to change its description, add or remove assignments, add or remove the bundle from existing catalogs or bundle groups, add or remove packages from the bundle, deploy a different version of the bundle, and more.

To edit a bundle:

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



Status	Name	Type	Size
<input type="checkbox"/>	 <a href="#">Bundle_Group_1</a>	Bundle Group	N/A
<input type="checkbox"/>	 <a href="#">Bundle_1</a>	RPM Package Bundle	0

- 2 Click the bundle's name to display the Summary page, then make the desired configuration changes as explained below.

Use the Summary page to view detailed information about the selected bundle. This page provides general information about the bundle, lists the individual devices that are assigned to the bundle, displays an event log, shows upcoming events, and lists the catalogs or groups that the bundle belongs to.

You can also use this page to edit the bundle group's description, add or remove assignments for the bundle, and change other configuration settings, as described below.

- 2a Review the information in the General section, then make the desired configuration changes (you can edit only the Description in this section).

**Size:** Displays the number of packages that make up the bundle.

**Version:** Displays the bundle's version number. You can have multiple versions of the same bundle. If you click the *Details* tab on this page and make any configuration changes, the version number increments.

**Number of errors not acknowledged:** A warning is anything that does not cause the deployment or installation of the bundle to fail, but indicates minor problems with the packages or bundle. The number displayed indicates the number of unacknowledged warnings, which display in the Event Log section below.

**GUID:** Lists the selected object's GUID (global unique identifier), a randomly generated string that provides a unique identifier for the bundle. You cannot edit the object's GUID.

**Description:** Displays the selected object's description, if one was provided when the bundle was created. The description provides a short description of the bundle's contents. This description displays in the ZENworks Control Center interface and in the user interface.

Click *Edit* to change the bundle group's description, if necessary.

- 2b Review the information in the Assignments section, then make the desired configuration changes.

The Assignments section lists the devices that are assigned to the selected bundle. You can click the device name to view information about each device that is directly assigned to the bundle, including its schedule and other options.

You can also use the following options:



**Advanced:** Click *Advanced* to display the Edit Assignments page to display a list of the devices that are assigned to the selected bundle, the folder that contains each device, each device's deployment and installation schedule, and whether the *Allow remove* and *Dry run* options are enabled. You can use the Edit Assignments page to edit certain settings, such as the deployment and installation schedules as well as the *Allow remove* and *Dry run* options.

**Add:** Click *Add* to launch the Assign Bundle Wizard to select the devices to be assigned to the selected bundle. For more information, see [Section 16.3, "Assigning Bundles," on page 164](#).

**Remove:** Select the device by clicking the check box next to the appropriate device name, then click *Remove* to remove the device's assignment from this bundle.

**2c** Review the information in the Event Log section, then make the desired changes.

The Event Log section lists all unacknowledged errors and warnings.

The Status column displays an icon indicating each item's status. Position the mouse pointer over each icon to display a short message describing the status of the item.

To acknowledge an error or warning, click its name in the Event Column, then click *Acknowledged* in the Message Detail Information dialog box that displays. You can also click *Advanced*, select the check box next to the appropriate event, then click *Acknowledge* (a check mark displays on the right side of the Date column to indicate that the item has been acknowledged).

**2d** Review the information in the Upcoming Events section.

The Upcoming Events section lists events scheduled for the selected bundle. You can click the calendar icon to display a calendar to view events for the desired date. You can also use the arrows to view events for the previous or next day, week, or month.

**2e** Review the information in the Catalogs/Groups section, then make the desired configuration changes.

The Catalogs/Groups section lists the catalogs and groups that contain the selected bundle.

You can also use the following options:

**Advanced:** Click *Advanced* to display the Edit Catalogs/Groups page to display a list of the catalogs and groups that contain the selected bundle. You can click *Add* to open the Select Groups dialog box to add the selected bundle to existing catalogs or groups. You can also remove a bundle or group by clicking the check box next to the Name column, then clicking *Remove* to remove the bundle from that catalog or group.

**Add:** Click *Add* to open the Select Groups dialog box, then click the blue arrow in the Select column to select the desired catalog or group and display its name in the Selected list box.

**Remove:** Select the device by clicking the check box next to the appropriate catalog or bundle name, then click *Remove* to remove the selected bundle from the catalog or group.

**3** Click the *Details* tab, then make the desired configuration changes.

Use the Details page to view detailed information about the selected bundle, such as the bundle's version number, name and display name, folder, description, a list of the individual RPM packages that make up the bundle, and the distribution and installation scripts that the bundle will use.

You can also use the options on this page to deploy a different version of the selected bundle to assigned devices, delete a particular version of the bundle, add or remove packages from the bundle, and change the script engine and scripts that you want to use for the bundle.

- 3a** Review the information in the RPM Package Bundle Settings section, then make the desired configuration changes.

**Version:** Displays the selected bundle's version number. You can have multiple versions of the same bundle. If you make any configuration changes on this page (changing the display name or description, adding a package to or removing a package from the bundle, or adding or modifying a script), the version number increments. You can use the *Version* drop-down list to view the details of each version of the selected bundle. Text below the Version box informs you which version of the bundle is deployed on assigned devices.

**Deploy:** Lets you deploy a different version of the currently deployed bundle. Use the *Version* drop-down list to select the desired version number, then click *Deploy*.

Only one version of a bundle can be deployed at any given time. For example, suppose a bundle has multiple versions: 1, 2, and 3. If version 1 is currently deployed, all associated devices have version 1 of the bundle deployed. If you then make version 3 the deployed version, all devices with version 1 deployed and still associated to that bundle will be automatically upgraded to version 3.

**Delete:** Lets you delete a version of the currently deployed bundle. Use the *Version* drop-down list to select the desired version number, then click *Delete*.

**Name:** Displays the unique name of the RPM bundle that was provided when the bundle was created. The name displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.

**Display name:** Displays the name that displays for users when they update software. The display name, which can be more intuitive for users, was provided when the bundle was created. You can edit the display name.

**Folder:** Displays the name of the folder that contains this bundle in the ZENworks Control Center interface.

**Description:** Displays a short description of the bundle's contents. This description displays in the ZENworks Control Center interface and in the ZENworks Linux Management Update Client, which is the user interface. You can edit the description.

**Packages:** The Packages section displays the RPM packages contained in the selected bundle. Use the Packages section to add RPM packages to the bundle, to import RPM packages contained in a bundle, or to remove packages from a bundle. The packages that you add to a bundle must already exist on the local device on which you are running the ZENworks Control Center, or you can import packages from an existing RPM bundle.

You can use the following options if you want to add packages to or remove packages from the selected bundle:

- ♦ **Upload RPM:** Click the *Upload RPM* button to open the RPM File Upload dialog box. For more information, see [Step 6a on page 156](#).
- ♦ **Import from bundle:** Click the *Import from bundle* button to open the Package Import dialog box. For more information, see [Step 6b on page 158](#).
- ♦ **Remove:** Click *Remove* to remove the selected package from the bundle, as needed.

---

**NOTE:** To view details about each package, select it and then click *Package Details*.

---

**Scripts:** As part of the process of distributing or installing a bundle, ZENworks Linux Management can also launch a script engine to execute scripts that let you perform tasks that must be done before or after a bundle is distributed or installed. For example, you can log in to other servers or trees, provide dynamic mappings, run applications, and so forth.

Each *Executable type* box displays the script engine that was specified when the bundle was created. You can use any of the script drop-down lists to change the script engine that you want to use and to change the scripts you want executed.

- 4 Click *Apply* to save any changes you have made.

## 16.5 Adding Bundles to Catalogs

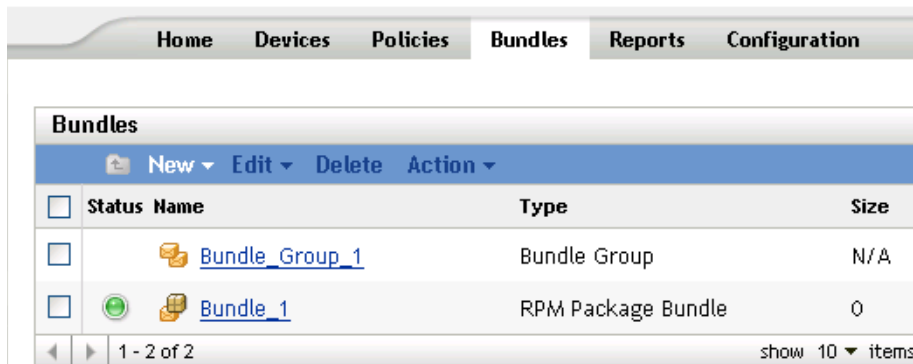
Instructions to add bundles to existing catalogs are included in the [Using Catalogs](#) section. For more information, see [Section 17.4, “Adding Bundles to Catalogs,” on page 192](#).

## 16.6 Creating Folders



A folder is an organization object that displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management. A folder can contain various objects, including subfolders, Bundle, Bundle Group, and Catalog objects.

To create a folder:

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

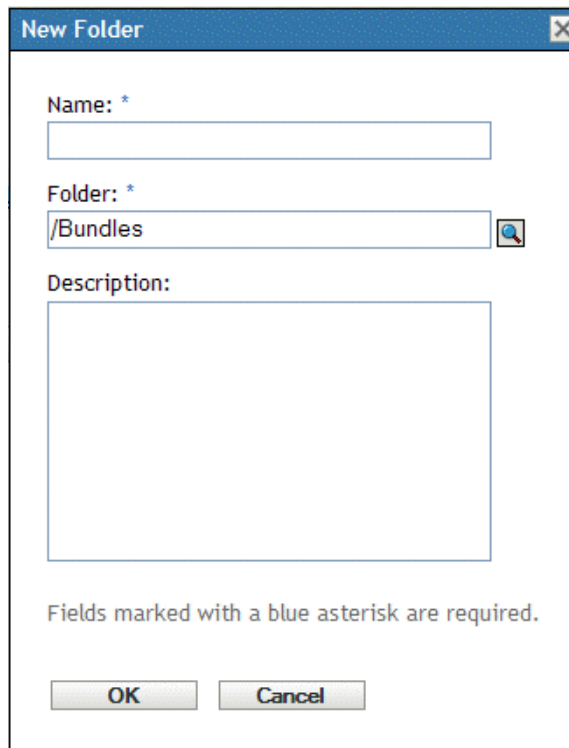


The screenshot shows the ZENworks Control Center interface with the 'Bundles' tab selected. The interface includes a navigation bar with tabs: Home, Devices, Policies, Bundles, Reports, and Configuration. Below the navigation bar is a 'Bundles' section with a table. The table has columns for Status, Name, Type, and Size. There are two bundles listed: 'Bundle\_Group\_1' (Bundle Group) and 'Bundle\_1' (RPM Package Bundle). The table also includes a 'New' button and a 'Delete' button. The status of 'Bundle\_Group\_1' is 'N/A' and the status of 'Bundle\_1' is '0'.

Status	Name	Type	Size
<input type="checkbox"/>	 <a href="#">Bundle_Group_1</a>	Bundle Group	N/A
<input type="checkbox"/>	 <a href="#">Bundle_1</a>	RPM Package Bundle	0

1 - 2 of 2 show 10 items

- 2 Click *New*, then click *Folder* to display the New Folder dialog box.



The image shows a 'New Folder' dialog box with a blue title bar and a close button. It contains three input fields: 'Name: \*' with an empty text box, 'Folder: \*' with a text box containing '/Bundles' and a browse button, and 'Description:' with a large empty text area. Below the fields is a note: 'Fields marked with a blue asterisk are required.' At the bottom are 'OK' and 'Cancel' buttons.

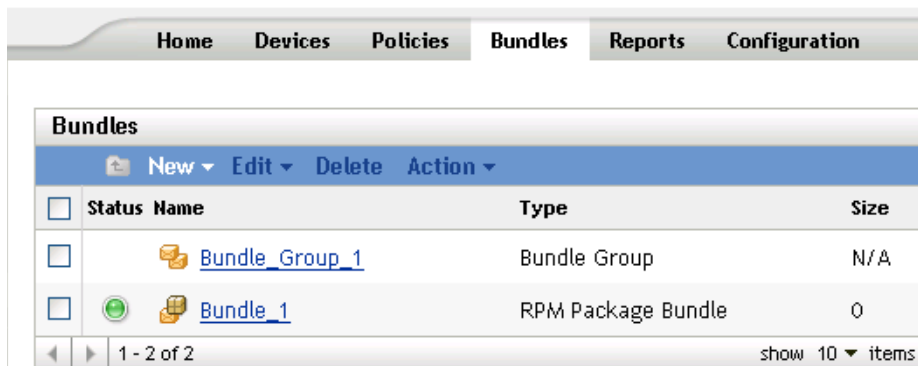
- 3 Fill in the fields:
  - ♦ **Name:** Provide a unique name for your folder. This is a required field.
  - ♦ **Folder:** Type the name or browse to the folder that contains this folder in the ZENworks Control Center interface.
  - ♦ **Description:** Provide a short description of the folder's contents.
- 4 Click *OK*.

## 16.7 Creating Bundle Groups

A bundle group lets you group bundles to ease administration and to provide easier assigning and scheduling of the bundles in the bundle group.

To create a bundle group:

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



- 2 Click *New*, then click *Bundle Group* to display the Basic Information page.

The screenshot shows the 'Create New Group' dialog box, Step 1: Basic Information. The dialog has a title bar 'Create New Group' with a question mark icon. Below the title bar is a section 'Step 1: Basic Information'. There are three fields: 'Group Name: \*' with a text input box, 'Folder: \*' with a text input box containing '/Bundles' and a browse button (magnifying glass icon), and 'Description:' with a large text area. Below the fields is a note: 'Fields marked with a blue asterisk are required.' At the bottom of the dialog are three buttons: '<< Back', 'Next >>', and 'Cancel'.

- 3 Fill in the fields:

- ♦ **Group name:** (Required) Provide a unique name for your bundle group. The name you provide displays in the ZENworks Control Center interface (the administrative tool for ZENworks Linux Management) and in the user interface.
- ♦ **Folder:** (Required) Type the name or browse to the folder that contains this bundle group.
- ♦ **Description:** Provide a short description of the bundle group's contents. This description displays in the ZENworks Control Center interface and in the ZENworks Linux Management Update Manager, which is the user interface for updating software.

**4** Click *Next* to display the Summary page.

Review the information on the Summary page, making any changes to the bundle-group settings by using the *Back* button as necessary.

Depending on your needs, you can create the bundle group now or you can specify members, assignments, and schedules for this bundle group and configure other options for this bundle group.

**5** Click *Finish* to create the bundle group as configured per settings on the Summary page. If you click *Finish*, the bundle group is created but it does not have members, devices assigned, a schedule, and so forth. At some point in the future, you need to configure additional options for the bundle group by continuing with [Section 16.3, “Assigning Bundles,” on page 164](#).

or

Click *Next* to display the Add Group Members page to perform the following tasks:

- ♦ Specify members for this bundle group
- ♦ Specify assignments for this bundle group
- ♦ Specify the schedule to apply the bundle-group assignments
- ♦ Specify the schedule to install the bundles on assigned devices
- ♦ Set special flags, such as flags to remove conflicting packages and attempt a dry run of the package installation

Create New Group Group\_1 ?

Step 3: Add Group Members

Specify the members for this group:

Add	Remove
<input type="checkbox"/>	Name In Folder
No items selected, click add to select items	

<< Back Next >> Cancel

**6** Specify the bundles to include in this bundle group.

**6a** Click *Add* to browse for and select the appropriate bundle objects.

**6b** Click the underlined link in the Name column to select the desired bundles and display their names in the Selected list box.

**6c** Click *OK*.

- 7 Click *Next* to display the Add Assignments page.

Create New Group Group\_1 ?

Step 4: Add Assignments

Specify the assignments for this group:

Add	Remove
<input type="checkbox"/>	Name
	In Folder
No items selected, click add to select items	

<< Back Next >> Cancel

- 8 Assign the bundle group to the devices that you want to distribute the bundle group to.
- 8a** Click *Add* to browse for and select the appropriate device objects.
- You can also select Folder or Group objects.
- 8b** Click the down-arrow next to Servers or Workstations to expand the list, then click the underlined link in the Name column to select the desired objects and display their names in the Selected list box.
- Assigning a bundle to a Folder or Group object is the preferred method of assigning the bundle. Assigning the bundle to a large number of objects (for example, more than 250) might cause increased server utilization.
- 8c** Click *OK*.
- 9 Click *Next* to display the Schedule page.
- 10 Select the schedule to apply to the assignments, then select the desired options, which vary, depending on the schedule type you select.

For more information on the various options, click the desired link in the Schedule Type column in the following table.

The settings you configure on this page determine when the bundle group is assigned to devices. The next page in this wizard, Install Schedule, lets you configure when the software packages in the bundle are actually installed.

The following schedules are available. Click the link in the left column in the table below for more information about each schedule type and its options.

Schedule Type	Description
No Schedule	Use this option to indicate no schedule; no action occurs.
Date Specific	Select one or more dates on which to assign the bundle group to devices and set other restrictions that might apply.
Day of the Week Specific	Select one or more days of the week on which to assign the bundle group to devices and set other restrictions that might apply.
Event	Select the event that triggers the assignment of the bundle group.
Monthly	Select the day of the month on which to assign the bundle group to devices and set other restrictions that might apply.

Schedule Type	Description
Relative to Refresh	Schedule when the bundle group is assigned, either immediately after the device refreshes or a specified amount of time after the device refreshes. You can also specify whether the bundle group's assignment is repeated and specify a time period when you do not want the bundle assigned to help minimize network traffic during that time.

- 11 Click *Next* to display the Install Schedule page.
- 12 Select a bundle group-install schedule type from the drop-down list, which vary, depending on the schedule type you select.

For more information on the various options, click the desired link in the Schedule Type column in the following table.

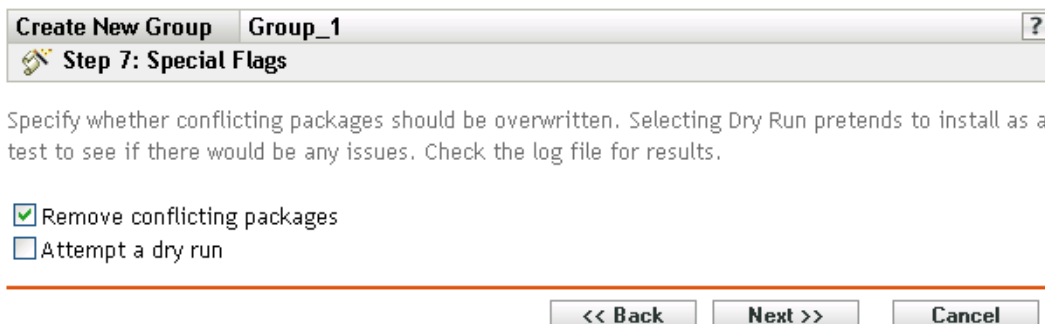
The settings you configure on this page determine when the bundles in the bundle group are installed on assigned devices.

The following schedules are available. Click the link in the left column in the table below for more information about each schedule type and its options.


Schedule Type	Description
No Schedule	Use this option to indicate no schedule; no action occurs.
Date Specific	Select one or more dates on which to install the bundles in the bundle group on assigned devices and set other restrictions that might apply.
Day of the Week Specific	Select one or more days of the week on which to install the bundles in the bundle group on assigned devices and set other restrictions that might apply.
Event	Select the event that triggers the installation of the bundles in the bundle group.
Monthly	Select the day of the month on which to install the bundles in the bundle group on assigned devices and set other restrictions that might apply.
Relative to Refresh	Schedule when the bundle group is installed, either immediately after the device refreshes or a specified amount of time after the device refreshes. You can also specify whether the bundle group's installation is repeated and specify a time period when you do not want the bundle group installed to help minimize network traffic during that time.



- 13 Click *Next* to display the Special Flags page.



Create New Group Group\_1 ?

 Step 7: Special Flags

Specify whether conflicting packages should be overwritten. Selecting Dry Run pretends to install as a test to see if there would be any issues. Check the log file for results.

☒ Remove conflicting packages  
☐ Attempt a dry run

<< Back Next >> Cancel

- 14 (Optional) Specify the following options:

- ♦ **Remove conflicting packages:** Select this option to specify that conflicting packages are uninstalled from devices before installing new packages. By default, this option is selected, so conflicting packages (previous versions of the same package, for example) are uninstalled before the current package is installed. If this option is not selected, packages will not be installed if a conflict is detected.
- ♦ **Attempt a dry run:** Select this option to have ZENworks Linux Management perform a test to determine if the RPM bundle can be successfully deployed. If there are any issues that could prevent the RPM bundle from being deployed, you can look at the log file to troubleshoot the bundle-creation process. The log file is located in `/var/opt/novell/logs/zenworks`.

A successful dry run ensures that the bundle can be successfully deployed or installed on assigned devices (packages are available, dependencies are met, etc.).

- 15 Click *Next* to display the Summary page, then review the information, making any changes to the bundle settings by using the *Back* button as necessary.
- 16 Click *Finish*.
- 17 Click *OK*.

## 16.8 Adding Bundles to Existing Groups

Using bundle groups eases administration efforts by letting you group several bundles so you can use common assignments, schedules, and so forth, rather than configuring these settings for each bundle you create.

- 1 In the ZENworks Control Center, click the *Bundles* tab, select the desired bundle in the Bundles list by checking the box next to its name, click *Action*, then click *Add to Group* to display the Targets page.

**Add To Group** ?

**Step 1: Targets**

Select the groups that will contain the items.

Add	Remove
<input type="checkbox"/>	Name In Folder

No items selected, click add to select items

<< Back Next >> Cancel

- 2 Click *Add* to open the Select Groups dialog box, click the desired groups to add them to the Selected list, then click *OK* to display the selected groups in the list on the Targets page.
- 3 Click *Next* to display the Finish page.
- 4 Review the information on the Finish page, making any changes to the settings by using the *Back* button as necessary, then click *Finish* to add the bundle to the group.

## 16.9 Deleting Bundles, Bundle Groups, and Folders

Before you delete bundles, bundle groups, and folders from the ZENworks Control Center, review the following information before performing the procedure in this section to ensure that you obtain the desired results.

**Deleting Bundles:** Depending on your needs, you can delete a bundle from your ZENworks Linux Management system or remove a bundle's assignments from devices.

If you delete a bundle from your ZENworks Linux Management system, the bundle does not display on the Bundles or Devices pages in the ZENworks Control Center; however, the software contained in that bundle remains on the previously assigned devices.

If you remove a bundle's assignments, the previously assigned devices are no longer assigned to the bundle; however, the software in the bundle remains on those devices.

**Deleting Bundle Groups:** The results of deleting a bundle group is similar to that of deleting a bundle.

If you delete a bundle group from your ZENworks Linux Management system, the bundle group does not display on the Bundles page in the ZENworks Control Center and the bundle group's assignments are removed. However, the individual bundles contained in the group are not removed

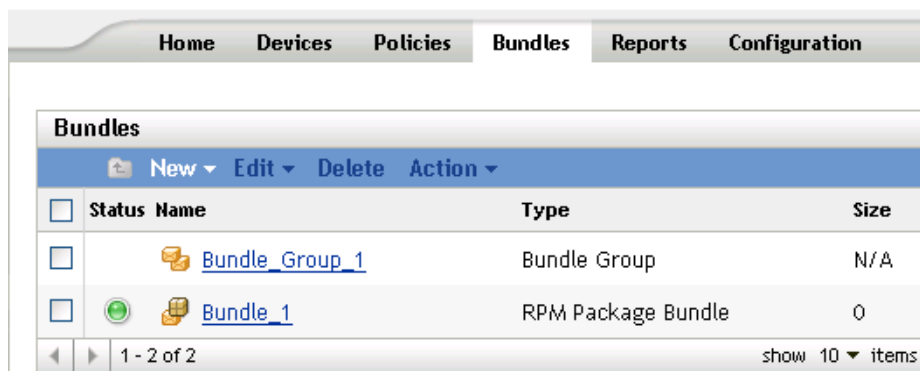
from the ZENworks Control Center and still display on the Bundles page. As with bundles, when you delete a bundle group from the ZENworks Control Center, the software contained in that bundle group remains on the previously assigned devices.

**Deleting Folders:** If you delete a folder that contains bundles from your ZENworks Linux Management system, both the folder and its bundles are removed from the ZENworks Control Center. However, the software contained in those bundles remain on the previously assigned devices.

**Removing Packages from Devices:** To remove RPM packages from devices, you can configure a Remote Execute policy to run a script. You can then assign the policy to devices. For more information, see [Section 16.12, “Using a Remote Execute Policy to Remove Bundles and Packages from Devices,”](#) on page 181.

To delete a bundle, bundle group, or folder:

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



- 2 In the Bundles list, check the box next to the desired item's name, then click *Delete*.

If the item you are deleting is a folder, you are prompted whether or not to delete the folder and its contents.

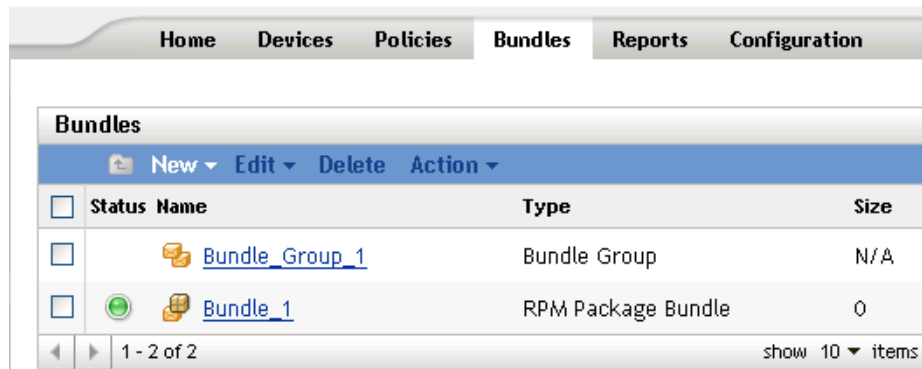
## 16.10 Renaming, Copying, or Moving Bundles

Use the *Edit* drop-down list on the Bundles page to edit an existing object. To access the *Edit* drop-down list, you must select an object by clicking the check box next to the object's name in the list.

Depending on the type of object you select, you can rename, copy, or move the selected object. For example, if you select a Bundle object, you can rename, copy, and move the bundle. If you select a Bundle Group object, you can rename or move the Bundle Group object, but not copy it. If the option is dimmed, that option is not available for the selected object type.

Some actions cannot be performed on multiple objects. For example, if more than one check box is selected, the Rename option is not available from the Edit menu.

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



- 2 In the Bundles list, check the box next to the bundle's name, click *Edit*, then click an option.
  - ♦ **Rename:** Click *Rename*, type a new name for the bundle, then click *OK*.
  - ♦ **Copy:** Click *Copy*, type a new name for the copy, then click *OK*.

The copy option is useful to create a new bundle that is similar to an existing bundle. You can copy a bundle and then edit the new bundle's settings.
  - ♦ **Move:** Click *Move*, choose a destination folder for the selected objects, then click *OK*.

If you rename or move a bundle, its assignments are still in place and ZENworks Linux Management does not redistribute the catalog to devices because of the name or location change.

## 16.11 Deploying a Different Version of a Bundle

You can have multiple versions of the same bundle; although, only one version of a bundle can be deployed at any given time. If you make any configuration changes to an existing bundle (changing the display name or description, adding a package to or removing a package from the bundle, or adding or modifying a script), the version number increments.

Only one version of a bundle can be deployed at any given time. For example, suppose a bundle has multiple versions: 1, 2, and 3. If version 1 is currently deployed, all associated devices have version 1 of the bundle deployed. If you then make version 3 the deployed version, all devices with version 1 deployed and still associated to that bundle will be automatically upgraded to version 3.

For more information about editing bundles, which might cause version numbers to increment, see [Section 16.4, “Editing Bundles,” on page 167](#). Note that only changes made on the Details page cause the version number to increment, as described in [Step 3 on page 169](#).

The following section contains more information:

- ♦ [Section 16.11.1, “Bundle Version Deployment Behavior \(ZENworks Control Center vs. the zlman Utility\),” on page 181](#)

## 16.11.1 Bundle Version Deployment Behavior (ZENworks Control Center vs. the `z1man` Utility)

You can modify an existing bundle using either the ZENworks Control Center or the `z1man` utility, which causes the bundle's version number to increment. Depending on the method you use to modify a bundle, the deployment behavior of the new version varies.

If you use the ZENworks Control Center to modify a bundle, the version number increments but the new version of the bundle is not automatically deployed; you must manually deploy the new version, as described in [Step 3a on page 170](#).

If you use the `z1man` utility to modify a bundle, the version number increments and the new version of the bundle is automatically deployed; you do not have to manually deploy the edited bundle.

## 16.12 Using a Remote Execute Policy to Remove Bundles and Packages from Devices

If you remove a bundle's assignments, the previously assigned devices are no longer assigned to the bundle; however, the software in the bundle remains on those devices. Likewise, if you delete a bundle by clicking the Bundles tab, checking the box next to a bundle's name, and then clicking Delete, the software is not removed from assigned devices.

To remove the bundles and software packages from devices, you can configure a Remote Execute policy to run a script and then assign the policy to devices. You can remove a bundle, a package, or a list of packages.

You cannot remove a catalog by using a Remote Execute policy, but you can remove the bundles and packages contained in a catalog.

To configure a Remote Execute policy to remove bundles and packages from devices:

- 1 In the ZENworks Control Center, click the *Policies* tab.
- 2 In the Policies list, click *New*, then click *Policy* to display the Create New Policy page.
- 3 In the Policy Type list, click *Remote Execute Policy*, then click *Next* to display the Policy Name page.
- 4 Fill in the fields:
  - ♦ **Name:** (Required) Provide a unique name for the policy. The name you provide displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.
  - ♦ **Folder:** (Required) Type the name or browse to the folder that this bundle will be created in. Folders display in the ZENworks Control Center.
  - ♦ **Description:** Provide a short description of the policy. This description displays on the policy's Summary page in the ZENworks Control Center interface.

5 Click *Next*.

**Create New Remote Execute Policy** Remote\_Execute ?

**Step 3: Remote Execute Policy**

Executable Type:

Maximum Waiting Time: ☐ Do not wait  
☒ Wait till the program completes the execution  
☐ Wait For  sec

Script to run:

Script file name: \*   
(e.g. /usr/local/xyz.pl)

Script parameters:   
(e.g. abc efg)

Script engine: \*   
(e.g. /usr/local/bin/perl)

Script engine parameters:   
(e.g. -c abc -s efg)

Fields marked with a blue asterisk are required.

<< Back   Next >>   Cancel

6 Select *Script* from the *Executable type* drop-down list.

7 Specify the waiting time after starting the script.

8 Select *Specify your own script* from the *Script to run* drop-down list.

9 Type your script in the script box.

The following table provides example scripts that you can use, depending on your needs:

Sample Script	Description
<code>rug bundle-remove bundle1</code>	Removes bundle1 from all devices that you assign the policy to.
<code>rug rm package1</code>	Removes package1 from all devices that you assign the policy to.
<code>rug rm package1 package2 package3</code>	Removes package1, package2, and package3 from all devices that you assign the policy to. Separate the package name with spaces.

Sample Script	Description
<code>rug rm bundle1 --allow-removals</code>	Removes bundle1 and all of its dependencies, even if they are not contained in the bundle.  If you attempt to remove a bundle that has outside dependencies without using this flag, you receive the following error message: "Error: Could not remove the bundle because of RPM dependency chain. Removing this bundle will require ZMD to remove additional packages not contained in this bundle."

**NOTE:** If you use `rug rm package_name` to remove a package that is contained in an installed bundle that contains other packages, only the specified package is removed from assigned devices. The other packages in the bundle are not removed.

If a bundle has multiple packages, when one or more package is removed, the bundle is still marked as installed in the ZENworks Control Center. Depending on the bundle's schedule, the server may re-install the package.

- 10 Click *Next* to display the Summary page.
- 11 Click *Finish* to create the policy as configured per settings on the Summary page. If you click *Finish*, the Remote Execute policy is created but it does not have devices assigned or a schedule. At some point in the future, you need to configure additional options for the policy by continuing with [Section 14.4, "Assigning Policies," on page 128](#).

or

Click *Next* to display the Policy Assignments page to perform the following tasks:

- ♦ Specify assignments for this policy
- ♦ Specify the schedule for this policy
- ♦ Specify groups for this policy

Create New Remote Execute Policy	Remote_Execute	?
 Step 5: Policy Assignments		

Specify the assignments for this policy:

Add Remove	
<input type="checkbox"/>	Name In Folder
No items selected, click add to select items	

- 12 Assign the policy to the devices.
  - 12a Click *Add* to browse for and select the appropriate Server or Workstation objects.  
You can also select Folder or Group objects.

- 12b** Click the down-arrow next to Servers or Workstations to expand the list, then click the underlined link in the Name column to select the desired objects and display their names in the Selected list box.

Assigning a policy to a Folder or Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.

- 12c** Click *OK*.

- 13** Click *Next* to display the Policy Schedule page, select the schedule to apply to the assignments from the drop-down list, which vary, depending on the schedule type you select.

The settings you configure on this page determine when the policy is assigned to devices.

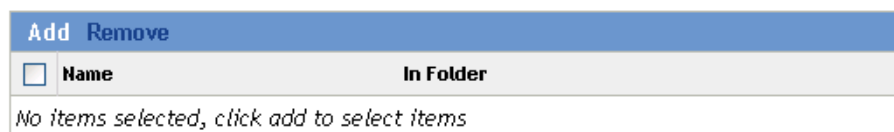
The following schedules are available. Click the link in the left column for more information about each schedule type and its options.

Schedule Type	Description
<a href="#">No Schedule</a>	Use this option to indicate no schedule; no action occurs.
<a href="#">Date Specific</a>	Select one or more dates on which to assign the policy to devices and set other restrictions that might apply.
<a href="#">Day of the Week Specific</a>	Select one or more days of the week on which to assign the policy to devices and set other restrictions that might apply.
<a href="#">Monthly</a>	Select the day of the month on which to assign the policy to devices and set other restrictions that might apply.
<a href="#">Relative to Refresh</a>	Schedule when the policy is assigned, either immediately after the device refreshes or a specified amount of time after the device refreshes. You can also specify whether the policy's assignment is repeated and specify a time period when you do not want the policy assigned to help minimize network traffic during that time.

- 14** Click *Next* to display the Policy Groups page.



Specify the groups for this policy:



- 15** (Optional) Click *Add* to open the Select Groups dialog box, then click the underlined links in the Name column to select the desired policy groups and display their names in the Selected list box.



Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create.

- 16 Click *Next* to display the Finish page.
- 17 Review the information on the Finish page, making any changes to the policy settings by using the *Back* button as necessary. Click *Finish* to create the policy as configured per settings on the Finish page.

## 16.13 Generating Bundle Reports

Reports let you create custom views for your ZENworks environment. Reports can contain details from a large volume of inventory, packaging, and other device information. You can create new reports, edit existing reports, delete reports, or generate one or multiple reports simultaneously. You can also create folders that let you organize and store reports based on your own criteria.

The following bundle reports are provided with ZENworks Linux Management:

- ♦ **Bundle Delivery Failure:** Lists bundle delivery failures per device.
- ♦ **Bundle Delivery in the Past 24 Hours:** Displays the previous day's bundle deliveries.
- ♦ **Bundle Delivery Information per Device:** Lists information consisting of error, warning, and success counts, as well as the last bundle delivery message and status.
- ♦ **Last Bundle Delivery per Device:** Displays the last bundle delivery that took place per device.

For more information, see [Part IX, “Reports,” on page 385](#).



Using Novell® ZENworks® Linux Management, you can install software using either a catalog or a bundle. A catalog is a collection of RPM bundles; software bundles included in a catalog are usually considered optional. Software included in a bundle that is directly assigned is considered mandatory; the software is installed on all assigned devices (the bundle is directly assigned to devices, the device group, or the device folder). For more information about bundles, see [Chapter 16, “Using RPM Bundles,” on page 153](#).

The `zlman` utility is the command-line interface to ZENworks Linux Management. If you need to create and configure a large number of bundles or catalogs, or if you want to automate the process using scripts, you can use `zlman`. For more information, see [zlman \(http://www.novell.com/documentation/zenworks7/zlmanref/zlman.html\)](http://www.novell.com/documentation/zenworks7/zlmanref/zlman.html).

The following sections contain additional information:

- ♦ [Section 17.1, “Understanding Catalogs,” on page 187](#)
- ♦ [Section 17.2, “Creating Catalogs,” on page 187](#)
- ♦ [Section 17.3, “Assigning Catalogs,” on page 191](#)
- ♦ [Section 17.4, “Adding Bundles to Catalogs,” on page 192](#)
- ♦ [Section 17.5, “Renaming or Moving Catalogs,” on page 193](#)
- ♦ [Section 17.6, “Deleting Catalogs,” on page 194](#)
- ♦ [Section 17.7, “Creating Folders,” on page 194](#)

## 17.1 Understanding Catalogs

A catalog is a collection of bundles; software bundles included in a catalog are usually considered optional. You can use catalogs to deploy and install optional or dependent packages to assigned devices. If you deploy optional packages to devices using a catalog, users can choose whether to deploy and install the software packages included in the bundles inside the catalog. Users use the ZENworks Linux Management Update Manager to manage the software on managed devices. To access the ZENworks Linux Management Update Manager, from the device, click *System*, then click *Software Update*.

You can also use bundles in a catalog to provide dependent packages for a primary package contained in a bundle or in another catalog. For example, suppose you want to include Java Runtime in a catalog and, optionally, hide the catalog from the user interface. If a package contained in a bundle or in another catalog needs Java Runtime (it is listed as a dependency for the primary package), the package containing Java Runtime becomes mandatory and is deployed and installed on all devices that the primary package is deployed and installed on.

## 17.2 Creating Catalogs

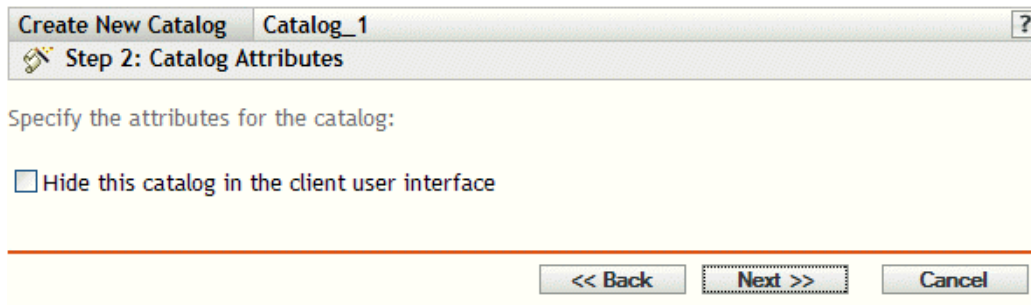
- 1 In the ZENworks Control Center, click the *Bundles* tab.

- 2 In the Bundle list, click *New*, then click *Catalog* to display the Catalog Name page.

- 3 Fill in the fields:

- ♦ **Catalog name:** (Required) Provide a unique name for your catalog. The name you provide displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.
- ♦ **Display name:** (Required) Provide a name that displays for users when they update software. The display name can be the same name that you provided in the Name box; however, you can choose to make the name more intuitive for users. In the next step in this wizard, Catalog Attributes, you can specify to hide this catalog in the ZENworks Linux Management Update Manager, which is the user interface for updating software.
- ♦ **Folder:** (Required) Type or browse to the folder that contains this catalog in the ZENworks Control Center interface.
- ♦ **Description:** Provide a short description of the catalog's contents. This description displays in the ZENworks Control Center interface and in the user interface. In the next step in this wizard, Catalog Attributes, you can specify to hide this catalog in the user interface.

- 4 Click *Next* to display the Catalog Attributes page.



- 5 (Optional) Select the *Hide this catalog in the client user interface* option to hide the catalog from users; the catalog displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management, but is hidden from users.

This option is useful if you have a bundle or catalog containing a primary package that has dependent packages that must already be installed on devices. You can hide the catalog containing these dependent packages from users. When the primary package in a bundle or catalog is deployed and installed, all dependent packages in the hidden catalog are also deployed and installed.

For example, suppose you have an anti-virus application that you want to deploy and install using a catalog. You could make this catalog visible to users. Suppose that you also need to install updated definition files on devices before the primary package in the bundle or catalog can be installed. You could hide the catalog containing the definition files from users. When users deploy and install the primary package in the bundle or in the visible catalog, the dependent packages in the hidden catalog are also deployed and installed.

---

**IMPORTANT:** If you hide an optional catalog (none of the packages contains dependent packages) from the user interface, the catalog is never deployed and installed. For this reason, you should only hide catalogs that contain dependent packages. When the primary package contained in a bundle or catalog is deployed and installed, the dependent packages contained in the hidden catalog are also deployed and installed.

---

- 6 Click *Next* to display the Summary page, then Review the information on the Summary page, making any changes to the bundle settings by using the *Back* button as necessary.

Depending on your needs, you can create the catalog now or you can configure additional settings for this catalog.


- 7 Click *Finish* to create the Catalog as configured per settings on the Summary page. If you click *Finish*, the catalog is created but it does not contain bundles or have any assignments. At some time in the future, you need to perform the steps under [Section 17.3, “Assigning Catalogs,” on page 191](#).

or

Click *Next* to display the Select Bundles page to perform the following tasks:

- ♦ Specify bundles and bundle groups to place in this catalog
- ♦ Specify the assignments for this catalog

Create New Catalog Catalog\_1 ?

 Step 4: Select Bundles

Specify the bundles and bundle groups to place in this catalog:

Add Remove	
<input type="checkbox"/> Name	In Folder
No items selected, click add to select items	

<< Back Next >> Cancel

8 Specify bundles and bundle groups for this catalog.


**8a** Click *Add* to display the Select Bundles dialog box, then browse for and select the bundles and bundle groups you want to assign to this catalog.

Click the underlined link in the Name column to select the bundles or bundle groups and to display their names in the Selected list box.

**8b** Click *OK*.

9 Click *Next* to display the Catalog Assignments page.

Create New Catalog Catalog\_1 ?

 Step 5: Catalog Assignments

Specify the assignments for this catalog:

Add Remove	
<input type="checkbox"/> Name	In Folder
No items selected, click add to select items	

<< Back Next >> Cancel

10 Assign this catalog to the devices that you want to distribute the catalog to.

**10a** Click *Add* to display the Select Assignments dialog box.

**10b** Click the blue arrow next to Servers or Workstations to expand the list, then click the underlined link in the Name column to select the desired objects and display their names in the Selected list box.

You can also select Folder or Group objects.

Assigning a catalog to a Folder or Group object is the preferred method of associating the catalog. Assigning the catalog to a large number of objects (for example, more than 250) might cause increased server utilization.

**10c** Click *OK*.

11 Click *Next* to display the Finish page, review the information on the Finish page, make any changes to the settings by using the *Back* button as necessary, then click *Finish* to create the item as configured per settings on the Finish page.

12 Click *OK*.

## 17.3 Assigning Catalogs

When you assign bundles, you specify device assignments and special flags for an existing catalog.

In [Step 7](#) under [Section 17.2, “Creating Catalogs,” on page 187](#), you were given the choice of clicking *Finish* or *Next*.

If you clicked *Finish*, the catalog was created without assigning devices to it or setting special flags for the catalog. Before the catalog can be deployed and installed on assigned devices, you must complete the following steps. If you clicked *Next*, you have already performed the following procedure as part of the catalog-creation process.

- 1 In the ZENworks Control Center, click the *Bundles* tab, select the desired catalog in the Bundles list by checking the box next to its name, click *Action*, then click *Assign Catalog* to display the Devices To Be Assigned page.

The screenshot shows a dialog box titled "Assign Catalog" with a question mark icon in the top right corner. Below the title bar is a section labeled "Step 1: Devices to be Assigned" with a wrench icon. The main area contains the instruction "Select the devices to be assigned to the previously selected catalogs." Below this is a table with two columns: "Name" and "In Folder". The "Name" column has a checkbox next to it. The table is currently empty, and a message below it says "No items selected, click add to select items". At the bottom of the dialog are three buttons: "<< Back", "Next >>" (which is highlighted with a dashed border), and "Cancel".

- 2 Assign the catalog to the devices that you want to distribute the catalog to.

**2a** Click *Add* to browse for and select the appropriate device objects.

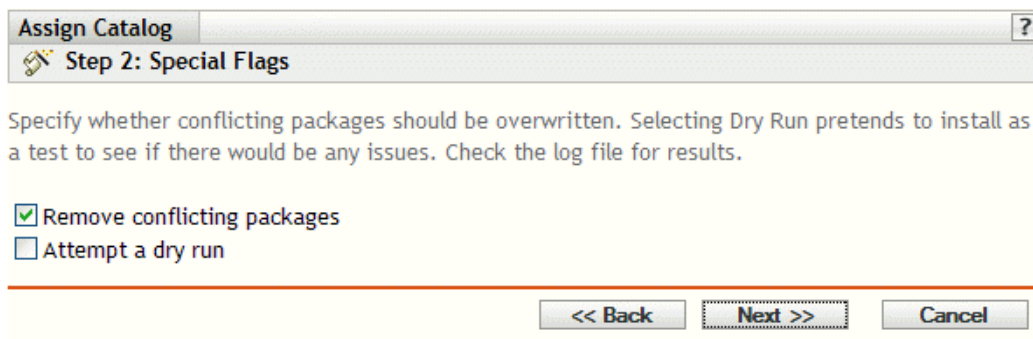
You can also select Folder or Group objects.

**2b** Click the down-arrow next to Servers or Workstations to expand the list, then click the underlined link in the Name column to select the desired objects and display their names in the Selected list box.

Assigning a catalog to a Folder or Group object is the preferred method of assigning the catalog. Assigning the catalog to a large number of objects (for example, more than 250) might cause increased server utilization.

**2c** Click *OK*.

- 3 Click *Next* to display the Special Flags page.



The dialog box titled "Assign Catalog" has a sub-header "Step 2: Special Flags". It contains a text instruction: "Specify whether conflicting packages should be overwritten. Selecting Dry Run pretends to install as a test to see if there would be any issues. Check the log file for results." Below this are two checkboxes: "Remove conflicting packages" (checked) and "Attempt a dry run" (unchecked). At the bottom are three buttons: "<< Back", "Next >>" (highlighted with a dashed border), and "Cancel".

- 4 (Optional) Specify the following options:

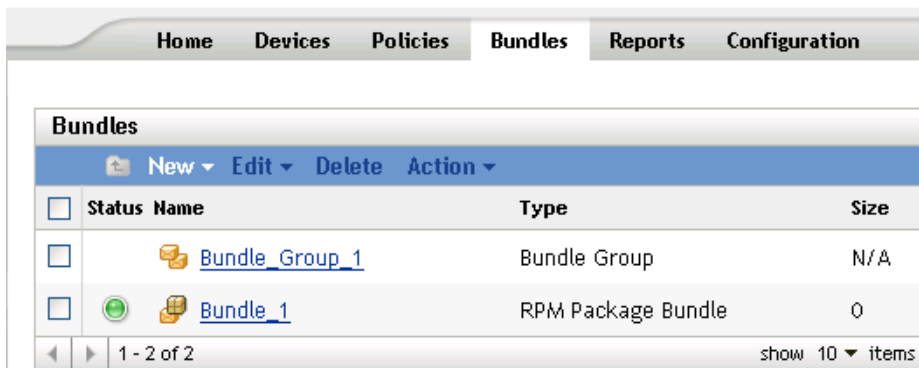
- ♦ **Remove conflicting packages:** Select this option to specify that conflicting packages are uninstalled from devices before installing new packages. By default, this option is selected, so conflicting packages (previous versions of the same package, for example) are uninstalled before the current package is installed. If this option is not selected, packages will not be installed if a conflict is detected.
- ♦ **Attempt a dry run:** Select this option to have ZENworks Linux Management perform a test to determine if the RPM bundle can be successfully deployed. If there are any issues that could prevent the RPM bundle from being deployed, you can look at the log file to troubleshoot the bundle-creation process. The log file is located in `/var/opt/novell/logs/zenworks`.

A successful dry run ensures that the bundle can be successfully deployed or installed on assigned devices (packages are available, dependencies are met, etc.).

- 5 Click *Next* to display the Finish page, review the information on the Finish page, make any changes to the settings by using the *Back* button as necessary, then click *Finish* to assign the catalog as configured per settings on the Finish page.
- 6 Click *OK*.

## 17.4 Adding Bundles to Catalogs

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



The screenshot shows the ZENworks Control Center interface with the "Bundles" tab selected. The top navigation bar includes "Home", "Devices", "Policies", "Bundles", "Reports", and "Configuration". Below the navigation bar is a table titled "Bundles" with columns "Status", "Name", "Type", and "Size". The table contains two entries: "Bundle\_Group\_1" (Bundle Group, N/A) and "Bundle\_1" (RPM Package Bundle, 0). The table has a footer showing "1 - 2 of 2" and "show 10 items".

Status	Name	Type	Size
	<a href="#">Bundle_Group_1</a>	Bundle Group	N/A
	<a href="#">Bundle_1</a>	RPM Package Bundle	0



- 2 In the Bundles list, select the box next to the bundle's name, click *Action*, then click *Add to Catalog* to display the Targets page.

Add To Catalog ?

Step 1: Targets

Select the catalogs that will contain the items.

Add	Remove	Name	In Folder
No items selected, click add to select items			

<< Back   Next >>   Cancel

- 3 Select the catalog to contain the selected bundles.
  - 3a Click *Add* to open the Select Catalogs dialog box, then click the desired catalogs to add them to the Selected list.
  - 3b Click *OK* to display the selected catalogs in the list on the Targets page.
- 4 Click *Next* to display the Finish page, review the information on the Finish page, make any changes to the settings by using the *Back* button as necessary, then click *Finish* to add the bundle to the catalog.

## 17.5 Renaming or Moving Catalogs

Use the *Edit* drop-down list on the Bundles page to edit an existing object. To access the *Edit* drop-down list, you must select an object by clicking the check box next to the object's name in the list.

Depending on the type of object you select, you can rename, copy, or move the selected object. For example, if you select a catalog object, you can rename and move the catalog, but you cannot copy it. If you select a bundle object, you can rename, copy, or move the object. If the option is dimmed, that option is not available for the selected object type.

Some actions cannot be performed on multiple objects. For example, if more than one check box is selected, the *Rename* option is not available from the Edit menu.

- 1 From the ZENworks Control Center, click the *Bundles* tab.

Home   Devices   Policies   Bundles   Reports   Configuration

**Bundles**

New ▾   Edit ▾   Delete   Action ▾

Status	Name	Type	Size
<input type="checkbox"/>	Bundle_Group_1	Bundle Group	N/A
<input type="checkbox"/>	Bundle_1	RPM Package Bundle	0

1 - 2 of 2   show 10 ▾ items

2 In the Bundles list, select the box next to the catalog's name, click *Edit*, then click an option.

- ♦ **Rename:** Click *Rename*, type a new name for the catalog, then click *OK*.
- ♦ **Move:** Click *Move*, choose a destination folder for the selected objects, then click *OK*.

If you rename or move a catalog, its assignments are still in place and ZENworks Linux Management does not redistribute the catalog to devices because of the name or location change.

## 17.6 Deleting Catalogs

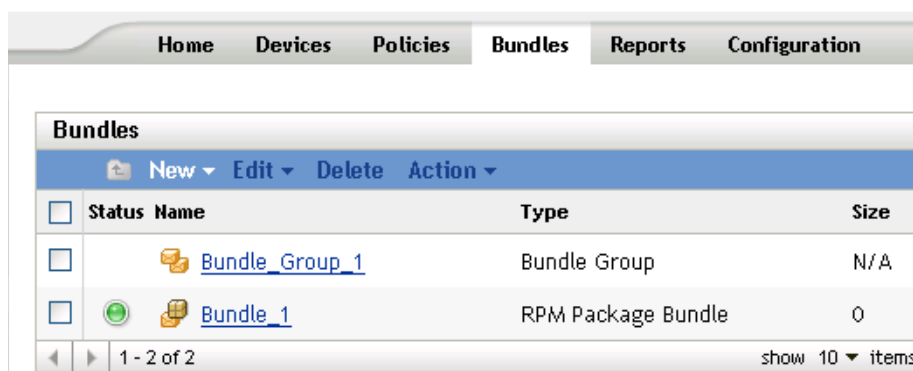
If you delete a catalog from your ZENworks Linux Management system, the catalog does not display on the Bundles or Devices pages in the ZENworks Control Center; however, the software contained in that catalog remains on the previously assigned devices.

If you remove a catalog's assignments, the previously assigned devices are no longer assigned to the catalog; however, the software in the catalog remains on those devices.

To remove the software contained in catalogs from devices, see [Section 16.12, “Using a Remote Execute Policy to Remove Bundles and Packages from Devices,”](#) on page 181.

To delete a catalog from the ZENworks Control Center:

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



2 In the Bundles list, check the box next to the catalog's name, then click *Delete* to remove the catalog from the ZENworks Control Center.

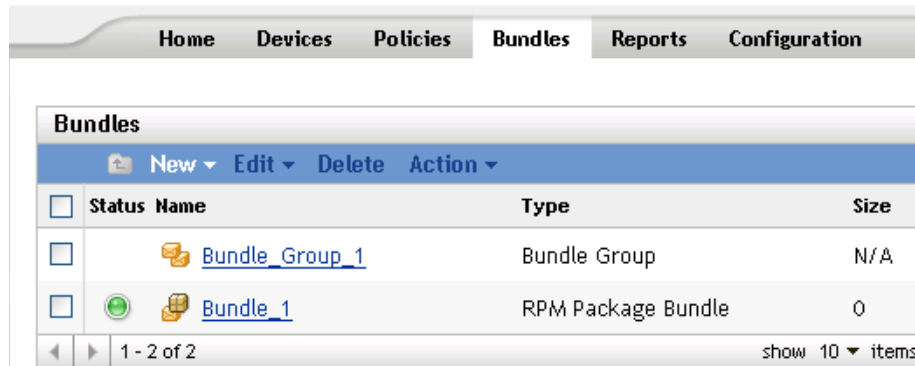
3 Click *OK* on the warning window that displays.

## 17.7 Creating Folders

A folder is an organization object that displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management. A folder can contain various objects, including subfolders, Bundle, Bundle Group, Catalog, Device, and Device Group objects.

To create a folder:

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



- 2 Click *New*, then click *Folder* to display the New Folder dialog box.

The 'New Folder' dialog box is shown. It has a title bar with 'New Folder' and a close button. The form contains three fields: 'Name: \*' with a text input field, 'Folder: \*' with a text input field containing '/Bundles' and a browse button, and 'Description:' with a large text area. At the bottom, there is a note: 'Fields marked with a blue asterisk are required.' and two buttons: 'OK' and 'Cancel'.

- 3 Fill in the fields:

- ♦ **Name:** Provide a unique name for your folder. This is a required field.
- ♦ **Folder:** Type the name or browse to the folder that contains this folder in the ZENworks Control Center interface.
- ♦ **Description:** Provide a short description of the folder's contents.

- 4 Click *OK*.



# Replicating Content in the ZENworks Management Zone

# 18

Novell® ZENworks® Linux Management uses a hierarchical organization to simplify device management. At the top level, a ZENworks Management Zone provides an autonomous unit of ZENworks servers and managed devices (workstations and servers). The ZENworks servers manage the devices.

Each ZENworks Management Zone has one primary server, and optionally, one or more secondary servers to help distribute the workload.

All RPM packages must reside on the primary server. ZENworks Linux Management uses content replication to replicate packages to each secondary server in your system.

---

**NOTE:** Depending on your needs, you might have more than one ZENworks Management Zone in your system. The content replication procedure in this section helps you replicate content from the primary server to secondary servers in a particular Management Zone. To replicate content across Management Zones, you must use `zlmirror`. For more information, see [Chapter 19, “Mirroring Software,”](#) on page 199.

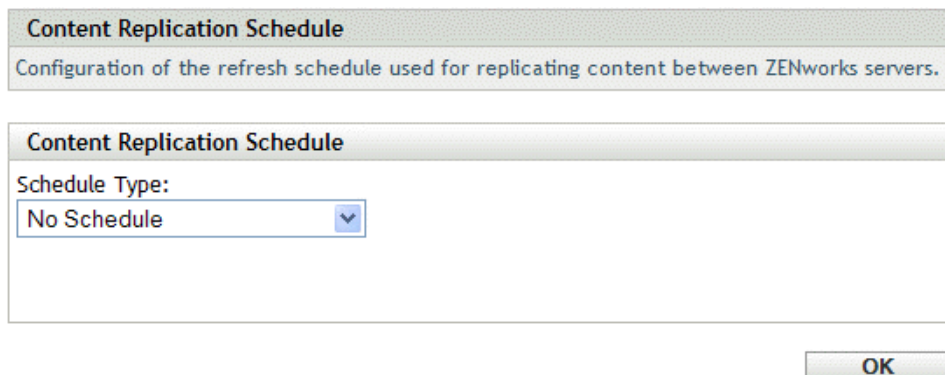
---

To configure the content replication schedule:

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



- 2 Click *Content Replication Schedule* to display the Content Replication Schedule page.



- 3 Select a schedule type from the drop-down list.

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

The following schedules are available:

Schedule Type	Description
No Schedule	Use this option to indicate no schedule. The content is not replicated to the secondary servers.
Date Specific	Select one or more dates on which to replicate the content to secondary servers and set other restrictions that might apply.
Day of the Week Specific	Select one or more days of the week on which to replicate content to secondary servers and set other restrictions that might apply.
Monthly	Select the day of the month on which to replicate content to secondary servers and set other restrictions that might apply.

- 4 Click *Apply*.

Novell® ZENworks® Linux Management lets you connect to a remote server and copy software catalogs, bundles, or packages from the remote server to your server using a few simple commands.

Depending on your needs, you might have more than one ZENworks Management Zone in your system. The information in this section helps you mirror content across Management Zones. For information about replicating content from a ZENworks primary server to ZENworks secondary servers in a particular Management Zone, see [Chapter 18, “Replicating Content in the ZENworks Management Zone,”](#) on page 197.

You can mirror software using the `zlmirror` command line application. Software can be mirrored from the following servers:

- ♦ ZENworks Linux Management (from the servers in one ZENworks Management Zone to another Management Zone)
- ♦ YaST Online Updates
- ♦ Red Hat Network
- ♦ Red Carpet Enterprise or ZENworks 6.x Linux Management

---

**NOTE:** To mirror from a ZENworks 6.6.x Linux Management server to a ZENworks 7 Linux Management server, the 6.6.x server must also be a YaST Online Update (YOU) server.

---

Novell, SUSE®, and Red Hat each maintain servers of their respective types, enabling you to simply mirror the catalogs and bundles you are interested in without needing to maintain or update these repositories.

Mirroring is the preferred method of obtaining the majority of the software you distribute to managed devices.

ZENworks 7 Linux Management automatically looks for SUSE Linux Enterprise Server (SLES) Service Packs and creates Bundle Groups to contain them. Because of this new functionality, you can now mirror SLES Service Packs.

The following sections contain additional information:

- ♦ [Section 19.1, “zlmirror,”](#) on page 199
- ♦ [Section 19.2, “Configuring a Software Mirror,”](#) on page 200
- ♦ [Section 19.3, “Distributing Catalogs from a Public ZENworks Linux Management Server,”](#) on page 204
- ♦ [Section 19.4, “Deploying Red Hat Network Updates,”](#) on page 204

## 19.1 zlmirror

All of the software components necessary to use `zlmirror` are installed during the ZENworks Linux Management installation process.

The `zlmirror` executable is located in `/opt/novell/zenworks/bin/`. You can view help for `zlmirror` at any time by running the following command:

```
zlmirror --help
```

You can also view an HTML version of the zlmirror man page.

## 19.2 Configuring a Software Mirror

Configuring a software mirror consists of the following:

1. Creating a separate XML configuration file for each remote server you want to mirror.

See [Section 19.2.1, “Creating Configuration Files,” on page 200](#)

2. Testing and run the mirroring operation using zlmirror.

See [Section 19.2.2, “Testing and Performing the Mirroring Operation,” on page 203](#)

### 19.2.1 Creating Configuration Files

In this early access release, no default configuration file is supplied. Run the following command to generate an empty configuration file:

```
zlmirror conf-generate zlmirror-config.xml
```

This command generates a template configuration file named zlmirror-config.xml in the current directory.

You can also convert the configuration file from an earlier version of ZENworks Linux Management or Red Carpet, or create configuration files manually. Configuration files are specified using the -c flag:

```
zlmirror command -c zlmirror-config.xml
```

If no configuration file is specified, the default configuration file location is /etc/opt/novell/zenworks/zlmirror.xml.

You can check the configuration file for errors and display the parsed configuration information by using the conf-validate (cv) *filename* command.

After you have a base configuration file created, the following tasks walk you through adding the necessary configuration information:

- ♦ [“Step 1: Servers” on page 200](#)
- ♦ [“Step 2: Catalog and Bundle Configuration” on page 202](#)

#### Step 1: Servers

You must provide details about a remote server containing the software you want to mirror, and a local server, which is your ZENworks Linux Management server receiving the mirrored software.

##### RemoteServer

```
<RemoteServer>
  <Base>http://red-carpet.ximian.com/</Base>
  <Type>rce</Type>
  <User />
  <Password />
</RemoteServer>
```



Configuration Element	Description
Base	<p>Path to the server you want to mirror, in the following format depending on Type:</p> <p><b>ZLM:</b> <code>https://server</code></p> <p><b>RCE:</b> <code>https://server/path</code></p> <p><b>YAST:</b> <code>http(s)://server/path</code> or <code>ftp://server/path</code></p> <p><b>RHN:</b> <code>http(s)://server/path</code></p> <p><b>STATIC:</b> <code>/path/on/filesystem</code></p>
Type	<p>Type of server you want to mirror:</p> <p><b>ZLM:</b> ZENworks 7 Linux Management</p> <p><b>RCE:</b> Red Carpet Enterprise, or ZENworks 6.x Linux Management</p> <p><b>YAST:</b> YAST Online Updates</p> <p><b>RHN:</b> Red Hat Network</p> <p><b>STATIC:</b> Mirrors packages from a directory containing the output of a static mirror session and adds them to ZENworks</p>
User	<p>Name to use when connecting to the remote server. If no user is specified, zlmirror reads the identity from the following location depending on Type:</p> <p><b>ZLM:</b> <code>/etc/opt/novell/zenworks/zmd/deviceid</code></p> <p><b>RCE:</b> <code>/etc/ximian/mcookie</code></p> <p><b>YAST:</b> <code>/etc/sysconfig/onlineupdate</code></p> <p>When connecting to an RHN server, leave this element empty.</p>
Password	<p>Password to use when connecting to the remote server. If no password is specified, zlmirror reads the password from the following location depending on Type:</p> <p><b>ZLM:</b> <code>/etc/opt/novell/zenworks/zmd/secret</code></p> <p><b>RCE:</b> <code>/etc/ximian/partnernet</code></p> <p><b>YAST:</b> <code>/etc/sysconfig/onlineupdate</code></p> <p>When connecting to an RHN server, leave this element empty.</p>

## LocalServer

```

<LocalServer>
  <Base></Base>
  <Type>zlm</Type>
  <User>Administrator</User>
  <Password>password</Password>
</LocalServer>

```

Configuration Element	Description
Base	<p>If the Type element indicates STATIC mirroring, use the Base element to define the destination path where files will be stored (<code>/path/on/filesystem</code>, for example).</p> <p>If the Type element indicates ZLM mirroring, leave the Base element empty.</p>
Type	<p>Type of mirroring you want performed:</p> <p><b>ZLM:</b> Mirrors catalogs and bundles directly to your ZENworks Linux Management server. After mirroring, mirrored catalogs and bundles are displayed in the ZENworks Control Center.</p> <p><b>STATIC:</b> Mirrors packages to the file system of your ZENworks Linux Management server, but does not add them to ZENworks.</p>
User	Name to use when connecting to your ZENworks Linux Management (local) server. The Administrator user should be specified if you want to use the default administrator account.
Password	Password for the account provided in User. If you are using the Administrator account, this is the password you specified during the server installation.

## Step 2: Catalog and Bundle Configuration

You must provide details about the catalogs and bundles you want mirrored to your server.

### CatalogConf

Each catalog you want to mirror must have a separate CatalogConf section:

```
<CatalogConf>
  <Name>Red Carpet 2</Name>
  <LocalName>Red Carpet 2</LocalName>
  <Target>sles-9-i586</Target>
  <Package>lib.*</Package>
</CatalogConf>
```

Configuration Element	Description
Name	<p>Name of the catalog you want to mirror from this remote server.</p> <p>This is the only required parameter.</p>
Local Name	Name of the catalog you want the mirrored software placed in. If no Local Name is specified, the catalog name from the remote server is used.
Folder	Specifies the eDirectory folder (for example, <code>/folder1/folder2</code> ) where bundles and catalogs are created and updated. If not specified, the catalogs and bundles are created and updated in the <code>/zlmirror</code> folder.
Target	<p>Restricts the mirroring operation on this catalog to packages and patches that support the specified target platforms. If no target is specified, packages for all platforms are mirrored.</p> <p>This element can be specified multiple times, and can contain either a target name or a regular expression string for wildcard matching of target names.</p>

Configuration Element	Description
ExcludeTarget	<p>Same as Target, except packages and patches supporting the specified target platform(s) are excluded.</p> <p>ExcludeBundle is performed after Target, so platforms appearing in a Target and ExcludeTarget are ultimately excluded.</p>
Bundle	<p>Restricts the mirroring operation on this catalog to the specified bundles. If not specified, all bundles are mirrored.</p> <p>This option is valid only for ZENworks Linux Management and YAST remote servers. It can be specified multiple times and can contain either a bundle name or a regular expression string for wildcard matching of bundle names.</p>
ExcludeBundle	<p>Same as Bundle, except packages and patches contained in the specified bundles are excluded.</p> <p>This option is valid only for ZENworks Linux Management and YAST remote servers. It can be specified multiple times and can contain either a bundle name or a regular expression string for wildcard matching of bundle names.</p> <p>ExcludeBundle is performed after Bundle, so bundles appearing in a Bundle and ExcludeBundle are ultimately excluded.</p>
Package	<p>Restricts the mirroring operation on this catalog to the specified packages. If not specified, all packages are mirrored.</p> <p>This option is valid only for ZENworks Linux Management and YAST remote servers. It can be specified multiple times and can contain either a bundle name or a regular expression string for wildcard matching of bundle names.</p>
ExcludePackage	<p>Same as Package, except specified packages are excluded.</p> <p>This option is valid only for ZENworks Linux Management and YAST remote servers. It can be specified multiple times and can contain either a bundle name or a regular expression string for wildcard matching of bundle names.</p> <p>ExcludePackage is performed after Package, so packages appearing in a Package and ExcludePackage are ultimately excluded.</p>

## 19.2.2 Testing and Performing the Mirroring Operation

After you have created the configuration file for a remote server, run the following command to perform a dry run of the mirroring operation, and optionally add the verbose flag to see detailed messages:

```
zlmirror mirror -c zlmirror-config.xml --dryrun --verbose
```

If this operation provides the intended results, run the mirror command without the dry run flag to complete the operation:

```
zlmirror mirror -c zlmirror-config.xml
```

## 19.3 Distributing Catalogs from a Public ZENworks Linux Management Server

The following sections contain additional information:

- [Section 19.3.1, “Creating a Public ZENworks Linux Management Server,” on page 204](#)
- [Section 19.3.2, “Accessing a Public ZENworks Linux Management Server,” on page 204](#)

### 19.3.1 Creating a Public ZENworks Linux Management Server

- 1 Create a default registration rule on the ZENworks Linux Management Server that creates a device in a specified folder.

For more information, see [Part II, “Device Registration,” on page 47](#) and [Section 14.2, “Creating Folders,” on page 124](#).

- 2 Assign all catalogs that you want to make public to that folder.

For more information, see [Section 17.3, “Assigning Catalogs,” on page 191](#).

### 19.3.2 Accessing a Public ZENworks Linux Management Server

- 1 Create a `zlmirror.conf` file.

For more information, see [Section 19.2.1, “Creating Configuration Files,” on page 200](#).

- 2 Install the ZENworks Linux Management agent on a workstation and register against the public ZENworks Linux Management Server using no registration key (to use the default registration rule).

For more information, see “[Installing the ZENworks Agent and Registering the Device](#)” under “[Installation](#)” in the *Novell ZENworks 7 Linux Management Installation Guide*.

- 3 Copy the contents of the deviceid and secret file from that workstation (`/etc/opt/novell/zenworks/zmd`) to the `zlmirror.conf` file in the `<User>` and `<Password>` tags of the `<RemoteServer>` section.

- 4 Mirror using the configuration file you created in [Step 1](#) to [Step 3](#).

For more information, see [Section 19.2.2, “Testing and Performing the Mirroring Operation,” on page 203](#).

## 19.4 Deploying Red Hat Network Updates

When you use ZENworks Linux Management to mirror a Red Hat distribution from the Red Hat Network, the mirroring process creates a single bundle containing all of the RPM packages. This bundle is not usually assigned directly to a managed device because it contains the entire Red Hat distribution, which will cause significant network traffic and the bundle might contain RPM packages that conflict with each other.

Following are two scenarios for updating devices with RPM packages:

- [Section 19.4.1, “Providing All RPM Packages and Package Bundles through a Catalog \(Pulling\),” on page 205](#)

- ♦ [Section 19.4.2, “Delivering Specific RPM Packages \(Pushing\),” on page 205](#)

## 19.4.1 Providing All RPM Packages and Package Bundles through a Catalog (Pulling)

If you want to provide all RPM packages via a catalog, create a catalog and add the mirrored Red Hat Network bundle to it, then assign the catalog to the managed devices. This allows users to have access through the catalog to all of the RPM packages contained in the Red Hat Network bundle.

For more information on mirroring and catalogs, see [Section 19.2, “Configuring a Software Mirror,” on page 200](#) and [Section 17.2, “Creating Catalogs,” on page 187](#).

From a managed device, there are two ways that you can force deployment and installation of the updates included in the Red Hat Network bundles contained in a catalog:

- ♦ **Using the ZENworks Linux Management Update Manager:** From the managed device, click *System > Software Update*, then select the catalog and click *Mark for installation > Run now*.
- ♦ **Using rug:** On a managed device, start a console session and enter the following command:  

```
/opt/novell/zenworks/bin/rug up
```

For more information, see [“rug” on page 21](#).

## 19.4.2 Delivering Specific RPM Packages (Pushing)

If you want to provide specific RPM packages, you can create a custom bundle by selecting the desired subset of RPM packages from the initial bundle that was created when mirroring the Red Hat Network. Or, you can create several custom bundles, each containing one or more RPM packages. It is best to test your custom bundles on a single device to verify that there are no conflicts within a bundle. If the test is successful, you can then assign the bundles to your managed devices.

To ensure that the packages contained in the custom bundle can meet all of their dependencies, you can create a catalog containing the mirrored Red Hat Network bundle and make it available to the desired managed devices. During the catalog creation process, you can hide this catalog from users. After you assign the custom bundle to devices, if a package requires other packages for dependency resolution, the device has access to the packages in the hidden catalog. For more information, see [Section 17.2, “Creating Catalogs,” on page 187](#).

Managed devices refresh on a schedule. Also, an administrator can trigger a device refresh through the ZENworks Control Center. When a device refreshes, it downloads the bundle automatically from the server and installs it.

The managed device requests one or more bundles from the server. In other words, the server does not actually push the bundle. However, the server can tell the managed device to refresh immediately. You can also modify the refresh interval centrally from the server for one or more managed devices. Otherwise, the client refreshes on its own schedule to look for a scheduled action.

From a managed device, you can use rug to force a refresh by entering the following command:

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

For more information, see [“rug” on page 21](#).



# Creating RPM Packages From Tarballs

# 20

Novell® ZENworks® Linux Management uses Red Hat Package Manager (RPM). RPM is a powerful package management system capable of installing, uninstalling, verifying, querying, and updating computer software packages on different devices.

ZENworks Linux Management supports only the RPM format.

RPM Packages are traditionally created using a `.rpm spec` file. This is the native RPM method, and includes a number of steps, including building the software to be packaged from sources. This method is the most powerful and flexible because it can exercise all of the options available in RPM. However, it is also the most complex.

This section describes the simplest method to create a `.rpm` file. At the same time, it is also the least flexible.

The following sections contain additional information:

- ♦ [Section 20.1, “Alien Package Converter Overview,” on page 207](#)
- ♦ [Section 20.2, “Installing Alien Package Converter,” on page 207](#)
- ♦ [Section 20.3, “Example Usage,” on page 208](#)

## 20.1 Alien Package Converter Overview

The Alien package converter is a simple program to convert packages from one format to another format. Note that, in general, converting package formats does not work very well; package dependencies and other metadata do not carry over from one distribution to another, much less across packaging systems.

For our purposes, however, it will work nicely. The Alien package converter allows the transformation from a tarball to a `.rpm` file, which can then be added to a ZENworks Server for distribution.

Additional information and download information about Alien package converter can be found on the [Alien Package Converter page \(http://www.kitenet.net/programs/alien/\)](http://www.kitenet.net/programs/alien/).

## 20.2 Installing Alien Package Converter

- 1 Ensure that you Perl version 5.004 or later.
- 2 Download the Alien package converter utility from the [Alien Package Converter page \(http://www.kitenet.net/programs/alien/alien\\_8.53.tar.gz\)](http://www.kitenet.net/programs/alien/alien_8.53.tar.gz).
- 3 Unpack, make, and install the utility using the following commands:

```
$ tar zxvf alien_8.53.tar.gz
$ cd alien
$ perl Makefile.PL
$ make
```

- 4 Log in as root or use sudo:

```
$ sudo make install
```

## 20.3 Example Usage

The following example describes the procedure to deliver a file called `readme` to the `/usr/share/myapp` directory:

- 1 Enter the following commands to create the directory structure and create the `.tar` file:

```
$ mkdir -p usr/share/myapp
$ echo "Hello World" >usr/share/myapp/readme
$ tar zcvf helloworld.tgz usr
```

When the tarball is unpacked, it will create the `/usr/share/myapp` directory containing the `readme` file.

- 2 Use Alien package converter to make an RPM package of the tarball by entering the following command:

```
$ alien -r helloworld.tgz
```

The Alien package converter creates the `helloworld-1-2.noarch.rpm` package.

- 3 Verify that the package is valid and list its contents by entering the following commands:

```
$ rpm -qlp helloworld-1-2.noarch.rpm
/usr
/usr/share
/usr/share/myapp
/usr/share/myapp/README
```

The `alien` utility has other options, for example to set the version and description of the package. See “`man alien`” for more information.



# Preboot Services



The following sections provide information on Novell® ZENworks® Linux Management Preboot Services features and procedures:

- ♦ [Chapter 21, “Preboot Services Overview,” on page 211](#)
- ♦ [Chapter 22, “Understanding Preboot Services in ZENworks Linux Management,” on page 215](#)
- ♦ [Chapter 23, “Setting Up Preboot Services,” on page 239](#)
- ♦ [Chapter 24, “Using Preboot Services,” on page 287](#)



# Preboot Services Overview

# 21

Novell® ZENworks® Linux Management Preboot Services contains functionality that allows you to perform tasks on devices before their operating systems boot. Currently for ZENworks Linux Management, “devices” are servers and workstations.

The following sections provide an overview of Preboot Services:

- ♦ [Section 21.1, “Preboot Services Functionality,” on page 211](#)
- ♦ [Section 21.2, “Preboot Services Strategies,” on page 211](#)
- ♦ [Section 21.3, “Preboot Bundles,” on page 212](#)
- ♦ [Section 21.4, “Configuring Preboot Services,” on page 212](#)
- ♦ [Section 21.5, “Setting Up Devices to Use Preboot Bundles,” on page 213](#)

## 21.1 Preboot Services Functionality

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

- ♦ Run AutoYaST and kickstart installations
- ♦ Run ZENworks scripts on the device
- ♦ Make an image of the device’s hard drives
- ♦ Restore an image to the device
- ♦ Apply an existing image to multiple devices

To accomplish these tasks automatically using the ZENworks Control Center, you simply need to have PXE (Preboot Execution Environment) enabled on your devices, and have preboot bundles configured and assigned to the devices. Then, the devices can automatically execute these bundles when they boot.

You can also execute some Preboot tasks on devices using CDs, DVDs, or a ZENworks partition, rather than using PXE.

## 21.2 Preboot Services Strategies

The following are some ways you can use Preboot Services:

- ♦ **Automate Linux installations.** You can automate kickstart or AutoYaST installations.
- ♦ **Create and restore base images.** You can create base images from existing devices, as well as restoring images to any manageable device.
- ♦ **Restore devices to a clean state.** You can quickly and efficiently reset devices to an initial state, such as in a lab.
- ♦ **Set up devices for future reimaging.** You can set up devices so that the next time they reboot, they do the imaging work that is contained in their assigned bundle.
- ♦ **Multicast images.** You can apply an image of one device to many other devices. This is an excellent feature for initially setting up a lab.

## 21.3 Preboot Bundles

In the ZENworks Control Center, Preboot Services tasks are contained in Preboot bundles. The following five Preboot bundle types are available:

- ♦ **AutoYaST bundle:** Describes the location and access protocol of an AutoYaST response file and network installation directory for SUSE® Linux. This bundle allows you to launch an AutoYaST automated installation of SUSE Linux using Preboot Services. This is only available for Linux devices that are PXE-enabled.
- ♦ **Kickstart bundle:** Describes the location and access protocol for a kickstart response file. This bundle allows you to launch an automated kickstart installation of Red Hat Linux using Preboot Services. This is only available for Linux devices that are PXE-enabled.
- ♦ **ZENworks Image bundle:** Lists one or more ZENworks images (base plus add-ons) that can be restored on a device. This bundle allows you to define simple imaging operations.
- ♦ **ZENworks Multicast bundle:** Specifies an image that can be sent using the multicast protocol. This bundle allows you to send an image to a large number of devices in a single operation, thus minimizing network traffic. It is ideal for labs, classrooms, and staging areas.
- ♦ **ZENworks Script bundle:** Allows you to write a custom Linux bash script. This provides detailed control over ZENworks imaging operations, as well as most Linux-based preboot tasks.

To create one of these bundles, in the ZENworks Control Center interface, click *Bundles > New > Bundle > Preboot bundle > Next*, then select a bundle type. For more information, see [Chapter 24, “Using Preboot Services,”](#) on page 287.

## 21.4 Configuring Preboot Services

In the ZENworks Control Center, you can set up default Preboot Services configurations for all of your devices. Some settings can be overridden at the device, group, or folder level.

You can configure the following settings per [ZENworks Management Zone](#):

- ♦ **Preboot Menu options:** The Preboot Menu contains five options: 1) *Start ZENworks imaging* (automatically executes the bundle); 2) *Start ZENworks imaging maintenance* (accesses the bash prompt); 3) *Disable ZENworks partition*; 4) *Enable ZENworks partition*; and, 5) *Exit* (resumes booting). You can configure whether the Preboot Menu is displayed upon booting, not displayed, or allowed to be displayed only when Ctrl+Alt is pressed during booting.
- ♦ **Image storage security:** You can restrict where to save image files on the imaging server.
- ♦ **Non-registered device settings:** You can use Preboot Services to automatically name your non-registered devices using such criteria as prefixes, BIOS information (like asset tags or serial numbers), DNS suffixes, and you can set up DHCP or IP addresses.
- ♦ **Preboot work assignment rules:** Work assignment rules are used to determine which bundle should be applied to which device. The work rules use logic to determine whether a device meets the requirements for applying the Preboot bundle. A rule is comprised of filters that are used to determine whether a device complies with the rule. The AND and OR logical operators are used for creating complex filters for the rule.
- ♦ **Preboot referral lists:** When a device boots, it is necessary for it to find its home ZENworks Management Zone to get its assigned preboot work. If multiple management zones exist on the network, referral lists provide a method for allowing a managed device to find its home zone.

- ♦ **Intel Active Management Technology (AMT):** Intel\* AMT provides Preboot Services with persistent device identification.

To configure these settings, click *Configuration > Preboot Services*. For more information, see [Section 23.4, “Configuring Preboot Services Defaults,” on page 261](#).

## 21.5 Setting Up Devices to Use Preboot Bundles

In order for a device to automatically use a Preboot bundle, there are 2 steps: 1) assign a Preboot bundle to the device, its parent folder, or its group; and 2) set up the device to apply the bundle.

Preboot Services utilizes PXE and other boot mechanisms and media to trigger the preboot work.

The following paths represent many of the methods for accessing the Add button to assign bundles to devices, or devices to bundles:

- ♦ Click *Devices*, select the box next to *Name*, then click *Action > Assign bundle*.  
Assigns bundles to all of the devices in the *Servers* and *Workstations* folders.
- ♦ Click *Devices*, select the box next to *Servers*, then click *Action > Assign bundle*.  
Assigns bundles to all of the devices in the *Servers* folder.
- ♦ Click *Devices*, select the box next to *Workstations*, then click *Action > Assign bundle*.  
Assigns bundles to all of the devices in the *Workstations* folder.
- ♦ Click *Devices > Servers*, select the box next to *Status Name*, then click *Action > Assign bundle*.  
Assigns bundles to all of the devices in the *Servers* folder.
- ♦ Click *Devices > Servers*, select the box next to one or more servers, then click *Action > Assign bundle*.  
Assigns bundles to all of the devices in the selected *Servers* and *Workstations* folders.
- ♦ Click *Devices > Workstations*, select the box next to *Status Name*, then click *Action > Assign bundle*.  
Assigns bundles to all of the devices in the *Workstations* folder.
- ♦ Click *Devices > Workstations*, select the box next to one or more workstations, then click *Action > Assign bundle*.  
Assigns bundles to all of the devices in the selected *Workstations* folder.
- ♦ Click *Devices > Servers*, select a server, then click *Advanced (in Effective Bundles)*.  
Assigns bundles to the selected server.
- ♦ Click *Devices > Workstations*, select a workstation, then click *Advanced (in Effective Bundles)*.  
Assigns bundles to the selected workstation.
- ♦ Click *Bundles*, select the box next to *Status Name*, then click *Action > Assign bundle*.  
Assigns all bundles to the devices that you select in the wizard.
- ♦ Click *Bundles*, select the box next to one or more bundle names, then click *Action > Assign bundle*.  
Assigns the selected bundles to the devices that you select in the wizard.

For more information, see [Section 23.2, “Setting Up the Preboot Services Methods,” on page 240](#).



# Understanding Preboot Services in ZENworks Linux Management

# 22

This section provides an understanding of Novell® ZENworks® Linux Management Preboot Services and how you can use it in your Linux network:

- ♦ [Section 22.1, “How Do You Implement Preboot Services?” on page 215](#)
- ♦ [Section 22.2, “What Is the Preboot Execution Environment \(PXE\)?” on page 215](#)
- ♦ [Section 22.3, “Preboot Services Functionality,” on page 217](#)
- ♦ [Section 22.4, “The Preboot Services Processes,” on page 224](#)
- ♦ [Section 22.5, “Preboot Strategies,” on page 232](#)

## 22.1 How Do You Implement Preboot Services?

Preboot Services utilizes any of the following to make its functions possible:

- ♦ **PXE (Preboot Execution Environment):** An Intel specification that allows a device to boot from the network, instead of its hard drive or other local media. ZENworks Linux Management can use PXE to launch Preboot Services.
- ♦ **Preboot Services bootable CD or DVD:** Used where PXE is not installed or where you want to manually perform a Preboot Services operation.
- ♦ **Preboot Services bootable diskette:** Enables using the Preboot Services bootable CD or DVD when the device doesn't support booting from a CD or DVD.
- ♦ **ZENworks partition:** Enables you to set up a device for unattended imaging operations where the device is not PXE enabled or does not have access to PXE network services.

## 22.2 What Is the Preboot Execution Environment (PXE)?

The following sections provide information on using PXE in Linux Management:

- ♦ [Section 22.2.1, “Understanding How Preboot Services Uses PXE,” on page 215](#)
- ♦ [Section 22.2.2, “Understanding the ZENworks NBPs,” on page 216](#)
- ♦ [Section 22.2.3, “Setting Up to Use PXE,” on page 217](#)

### 22.2.1 Understanding How Preboot Services Uses PXE

PXE uses DHCP (Dynamic Host Configuration Protocol) and TFTP (Trivial File Transfer Protocol) to locate and load bootstrap programs from the network. The PXE environment is loaded from the BIOS on the NIC.

In ZENworks Linux Management, Preboot Services uses PXE to discover if there is Preboot Services work specified for a device and to provide the device with the files necessary to execute the assigned work.

Using Preboot Services, you can automatically place an image on a device, even if the device's hard disk is blank. You do not need to use the CD or DVD, or a ZENworks partition on the device.

## 22.2.2 Understanding the ZENworks NBPs

The Intel PXE specification defines mechanisms and protocols that allow PXE devices to use their network interface cards (NICs) to find bootstrap programs located on network servers. In the PXE specification, these programs are called Network Bootstrap Programs (NBPs).

NBPs are analogous to the bootstrap programs found in the Master Boot Records (MBRs) of other boot media, such as hard drives, floppy disks, CDs, and DVDs. The purpose of a bootstrap program is to find and load a bootable operating system. MBRs on traditional boot media accomplish this by locating the necessary data on their respective media. NBPs accomplish this by using files found on network servers, usually TFTP servers.

ZENworks Preboot Services uses two separate NBPs working in concert:

- ♦ “`nvlmbp.sys`” on page 216
- ♦ “`pxelinux.0`” on page 216

### **nvlmbp.sys**

This NBP has the following responsibilities:

- ♦ Detect various SMBIOS parameters and local hardware
- ♦ Read the ZENworks identity information from the hard drives
- ♦ Communicate with novell-zmgprebootpolicy to determine if there is any preboot work applicable to the device
- ♦ Present and manage the Preboot Services menu
- ♦ If necessary, launch `pxelinux.0` to execute the assigned preboot work

### **pxelinux.0**

The primary purpose of this NBP is to load the operating system that is required to execute the assigned preboot work.

The `pxelinux.0` file is a modified version of part of an open-source project called syslinux. While `pxelinux.0` is primarily a Linux loader, it is capable of loading other operating systems. It operates by using configuration files located on a TFTP server to provide boot instructions. The various `pxelinux.0` configuration files used by Linux Management can be found on your imaging server in the `/srv/tftp` directory.

In Linux Management, when PXE devices are assigned preboot work, they are also told which `pxelinux.0` configuration file they should use to execute that work. Similarly, when using the Preboot Services Menu, each menu option corresponds to a `pxelinux.0` configuration file. For more information, see [Section 23.3.4, “Editing the Preboot Services Menu,” on page 259](#).

For more information on `pxelinux.0` and its configuration files, see the [syslinux home page \(http://syslinux.zytor.org/pxe.php\)](http://syslinux.zytor.org/pxe.php).

For a copy of the Novell modifications to the syslinux open-source project, see [Novell Forge \(http://forge.novell.com\)](http://forge.novell.com).



## 22.2.3 Setting Up to Use PXE

Before you can use Preboot Services with PXE, you need to do the following:

1. Install ZENworks 7 Linux Management on your imaging server.
2. Enable PXE on your ZENworks Linux Management devices.
3. Have a standard DHCP server, either on your imaging server or on another network server.

## 22.3 Preboot Services Functionality

Review the following sections to understand Preboot Services functionality:

- ♦ [Section 22.3.1, “Preboot Bundles,” on page 217](#)
- ♦ [Section 22.3.2, “Preboot Services Menu,” on page 219](#)
- ♦ [Section 22.3.3, “Image Storage Security,” on page 219](#)
- ♦ [Section 22.3.4, “Non-registered Device Settings,” on page 220](#)
- ♦ [Section 22.3.5, “Preboot Work Assignment Rules,” on page 220](#)
- ♦ [Section 22.3.6, “Preboot Referral Lists,” on page 222](#)
- ♦ [Section 22.3.7, “Intel Active Management Technology \(AMT\),” on page 222](#)

### 22.3.1 Preboot Bundles

In ZENworks Linux Management, Preboot Services uses bundles to apply Preboot Services work to devices. For example, Preboot bundles can contain tasks, such as to restore an image, that are performed at the time a device boots.

In order for a device to utilize a Preboot bundle, the bundle must be assigned to the device, its group, or its folder.

The available Preboot bundles are:

- ♦ [“AutoYaST Bundle” on page 217](#)
- ♦ [“Kickstart Bundle” on page 217](#)
- ♦ [“ZENworks Image Bundle” on page 218](#)
- ♦ [“ZENworks Multicast Bundle” on page 218](#)
- ♦ [“ZENworks Script Bundle” on page 219](#)

#### AutoYaST Bundle

Provides the location and access protocol for installing using AutoYaST, including the network installation directory for SUSE Linux. This bundle allows you to launch an automated installation of SUSE Linux using Preboot Services.

#### Kickstart Bundle

Provides the location and access protocol for installing using kickstart. This bundle allows you to launch an automated installation of Red Hat Linux using Preboot Services.

## ZENworks Image Bundle

Lists one or more ZENworks images that can be restored on a computer. This bundle allows you to quickly define simple image restoration operations.

### Scope

You can restore an image all of a device's hard disks, specific add-on images, and file sets.

### Boot Manager Limitation

If the device you want to image has an unsupported boot manager running, such as System Commander, you must disable or remove it before attempting to image those devices. This is because boot managers create their own information in the MBR and overwrite the ZENworks boot system, preventing ZENworks imaging from being performed.

### Base Images

A base image contains descriptions of all partitions and files on a hard drive. When it is restored, all existing partitions are deleted, new partitions are created from the descriptions in the base image, and all files are restored from the image.

Base images are created by taking an image of a device. You can use an [option in the ZENworks Control Center](#) or [imaging commands on a bash prompt](#) to create a base image.

### Add-On Images

These images are a collection of files added non-destructively to existing partitions. The existing partitions and files are left intact, except for any files that the add-on image might update.

Add-on images allow you to customize a device after a base image is restored. This allows you to use a base image for multiple purposes.

You can create add-on images using the [Image Explorer](#) utility.

## ZENworks Multicast Bundle

Specifies an image that can be sent using the multicast protocol. This bundle allows you to send an existing image to a large number of devices in a single operation. It is ideal for labs, classrooms, and staging areas.

For more information, see [Section 22.5.6, “Multicasting Device Images,” on page 235](#).

### Benefits

You can image multiple devices with the least amount of overhead. Devices to be imaged can have a variety of operating systems installed on them, or even no operating system installed.

Using the multicast capabilities of your network, you minimize network traffic by sending the image file across the network once for all devices to be imaged, rather than individually per device.

### Limitations

Using the same image on multiple devices means they all have the same network identities. However, you can install the ZENworks Linux Management Imaging Agent ([novell-zislnx](#)) on these

devices prior to performing the multicast, because this agent saves each device's network identity settings and restores them after the multicast image is applied.

### ZENworks Script Bundle

Allows you to write a custom Linux bash script that is executed on PXE-enabled Linux devices. This provides detailed control over ZENworks imaging operations, as well as most Linux-based preboot tasks.

## 22.3.2 Preboot Services Menu

Where PXE is enabled on a device, the Preboot Services Menu can be displayed during the boot process. The following menu choices are displayed on the Preboot Services Menu:

- ♦ **Start ZENworks Imaging:** Executes the effective Preboot Services imaging bundle.
- ♦ **Start ZENworks Imaging maintenance:** Displays the bash prompt, where you can execute imaging commands.
- ♦ **Disable ZENworks partition:** Prevents an existing ZENworks partition from being used during booting to execute the assigned Preboot bundles.
- ♦ **Enable ZENworks partition:** Allows an existing ZENworks partition to be used during booting to execute the effective Preboot bundle.
- ♦ **Exit:** Resumes normal booting of the device.

You can use the ZENworks Control Center to configure whether this menu should be displayed on a PXE-enabled device by selecting one of the following options:

*Always Show Preboot Menu*

*Never Show Preboot Menu*

*Show Preboot Menu if CTRL+ALT is Pressed*

For the procedures in configuring whether to display the menu, see [Section 23.4.1, “Configuring Preboot Menu Options,” on page 262](#).

## 22.3.3 Image Storage Security

You can determine the degree of security you want by restricting where to save image files on your imaging server. The following options in the ZENworks Control Center provide this storage security:

- ♦ **Allow Preboot Services to overwrite existing files when uploading:** Select this option only if you want existing image files to be overwritten during imaging.
- ♦ **Only allow uploads to the following directories:** This option allows you to determine where images can be restored on the imaging server. You specify a full path to the directory in the *Add* field, then click *Add* to enter it into the list box. These are the directories where images are allowed to be saved on the imaging server. These are the locations that can be selected when configuring where to store image files.

For the procedures in configuring imaging storage, see [Section 23.4.2, “Configuring Image Storage Security,” on page 263](#).

## 22.3.4 Non-registered Device Settings

Devices that are new to the ZENworks Management Zone and have received their first image, need certain IP configuration information to successfully access the network and network services. You can use Preboot Services to automatically name your non-registered devices using such criteria as prefixes, BIOS information (like asset tags or serial numbers), DNS suffixes, and you can set up DHCP or IP addresses.

For example, the device needs a unique IP address and the address of at least one DNS name server. In many networks, this information is distributed through the DHCP services, but can also be configured through the default Preboot Services configuration settings in the ZENworks Control Center.

After a device has registered with ZENworks, its configuration is set and the non-registered device settings in the ZENworks Management Zone no longer apply to it, because the ZENworks Linux Management server now knows its identity. After the device is imaged, whether it becomes a member of the zone or continues to be a non-registered device depends on whether the image applied to the device contains the ZENworks Linux Management Imaging Agent (**novell-zislnx**).

The settings that can be adjusted for a ZENworks Management Zone are:

- ♦ **DNS suffix:** Provides a suffix for all of your devices' names. For example, provo.novell.com.
- ♦ **Name servers:** This controls which DNS servers a device uses. You can specify multiple DNS name servers.
- ♦ **Device name:** Configured device names can include a prefix, the BIOS asset tag, the BIOS serial number, or none of these.
- ♦ **IP configuration:** For the IP configuration, you can specify to use DHCP or a specific IP address. If you select to use IP addresses, you can provide a list using a range or by specifying specific IP addresses. As devices are registered, they assume one of the available addresses. For IP addresses, you can also specify a subnet mask and a default gateway.

For the procedures in configuring defaults for non-registered devices, see [Section 23.4.3, “Configuring Non-registered Device Settings,”](#) on page 265.

## 22.3.5 Preboot Work Assignment Rules

You can set up hardware-based rules for your Preboot bundles. Work assignment rules are used to apply bundles to devices with specific hardware, or match a broad set of hardware requirements.

For example, you can create a rule that applies a bundle to any device with a specific MAC address or BIOS serial number. Rules like this can only match to a single device. On the other hand, you can create a rule that applies to any device with at least 512 MB of RAM and 150 GB of hard drive space.

A work rule is comprised of filters that are used to determine whether a device complies with the rule. The rules use logic to determine whether a device meets the requirements for applying the Preboot bundle. The AND and OR logical operators are used for creating complex filters for the rule.

When a device is seeking work to be done, it scans the rules until it finds a rule where all of the rule's filters match the device, then executes the bundle assigned to the rule.

Filter information that you can provide:

- ♦ **Device component:** Any of the following:

- BIOS Asset Tag
- BIOS Serial Number
- BIOS Version
- CPU Chipset
- Hard Drive Controller
- Hard Drive Size (in MB)
- IP Address
- MAC Address
- Network Adapter
- RAM (in MB)
- Sound Card
- System Manufacturer
- Video Adapter

- ♦ **Relationship:** This defines the relationship for a filter between the *Device component* field and the value you specify for it.

Possibilities for the *Hard drive size* and *RAM* fields:

- < (less than)
- > (greater than)
- = (equal to)
- >= (greater than or equal to)
- <= (less than or equal to)
- ≠ (not equal to)

Possibilities for all other device components:

- Contains
- Equal To
- Starts With

- ♦ **Component value:** This corresponds to the match you want for the component. For example, you select *RAM (in MB)* for the filter and enter 512 for its value. Then, the relationship you select determines whether it's less than, less than or equal to, equal to, not equal to, greater than or equal to, or just greater than 512 MB.

You can have multiple filters and sets of filters in a single rule, using the AND and OR operators, and you can have multiple rules associated with the same Preboot bundle. This allows you to specify exactly to which devices a particular Preboot bundle can be applied.

For the procedures in configuring work assignment rules, see [Section 23.4.4, “Configuring Preboot Work Assignments,”](#) on page 268.

## 22.3.6 Preboot Referral Lists

When a PXE device boots, it makes a broadcast request on the network for PXE services. The ZENworks Proxy DHCP server (novell-proxydhcp) responds to this request with information that includes the IP address of an imaging server where the device can send requests for assigned preboot work.

It is essential that the PXE device contact PXE services associated with its home zone so that it can correctly determine if there is any preboot work assigned to it. When there is only a single ZENworks Management Zone, this is fairly easy to do as all Proxy DHCP servers provide addresses to services that belong to the same zone. Any device can request preboot work from any imaging server in the same zone and get the same response. However, when multiple ZENworks management zones exist in the same network, things become more difficult, particularly when each zone has its own set of PXE services.

The PXE device's initial request for PXE services is sent as a broadcast to the network, and all Proxy DHCP servers respond with information pertaining to their respective zones. Because it is impossible to determine which Proxy DHCP server responds first, if multiple Proxy DHCP servers respond, or which response is used by the device, it is impossible to ensure that each PXE device will contact servers in its home zone.

A Preboot Referral List allows you to ensure that all devices contact their home zone for preboot work assignments. The list should contain the IP address of an imaging server in each known ZENworks management zone. When a device requests preboot work from a server, the server first determines if the device belongs to the same zone as the server. If it does not, the server refers the request to each server in its referral list until it finds the device's home zone. The device is then instructed to send all future requests to the correct daemon.

After you have specified all of the necessary servers in the referral list, you must place certain files in the `\tftp` directories of each server in the list. Which files are copied and modified depends on the version of ZENworks running on that server.

Note that the Preboot Referral Lists are only used by PXE devices, and only one ZENworks Management Zone needs to have an active Proxy DHCP server and Preboot Referral List.

For the procedures in configuring referral lists, see [Section 23.4.5, "Configuring the Server Referral List," on page 275](#).

## 22.3.7 Intel Active Management Technology (AMT)

Review the following to understand how the Intel AMT functionality is used by ZENworks Linux Management:

- ♦ ["Using AMT in ZENworks Linux Management" on page 223](#)
- ♦ ["Understanding AMT Provisioning" on page 223](#)
- ♦ ["Accessing AMT Resources" on page 224](#)

For more information on Intel AMT, see the [Intel Web site \(http://www.intel.com/technology/manage/iamt/\)](http://www.intel.com/technology/manage/iamt/).

## Using AMT in ZENworks Linux Management

The Intel AMT functionality allows you to accurately identify devices, even if they have had physical drive replacements. This provides ZENworks Preboot Services with persistent device identification by providing ZENworks with nonvolatile memory for storing the unique device identity.

With AMT and Preboot Services, if a device has a new, unformatted hard drive, ZENworks Linux Management can instantly and accurately identify the device and apply the appropriate Preboot bundle. If a device's hard drive is inactive or its drive is replaced, ZENworks can automatically identify the device in a preboot environment and provide the appropriate ZENworks Linux Management-created image during a system rebuild.

AMT with ZENworks also provides easier hardware upgrading capability. For example, to upgrade applications, some of your device hardware might not meet the minimum requirements. With AMT and Preboot Services, as soon as the hard drives are replaced and before any agents or operating systems are installed, you can continue to assign Preboot bundles using the device's ZENworks identity without having to re-register the device.

If you are using Intel AMT, support for it should be enabled in the `novell-zmgprebootpolicy.conf` file.

## Understanding AMT Provisioning

For security purposes, AMT devices generally ship with all AMT features disabled. In this configuration, AMT devices act like normal computers, but none of the AMT features are available. To enable the AMT features, each device must go through a process that Intel refers to as “provisioning,” which sets up the device's AMT resources for access.

- ♦ “The Provisioning Modes” on page 223
- ♦ “The Provisioning Process” on page 223

### The Provisioning Modes

An AMT device may be provisioned into one of two modes: enterprise or small business. Both modes offer the same off-line and remote management capabilities, but in enterprise mode AMT devices use local Certificate Authority credentials to grant remote access, and may require HTTPS protocol for communication rather than just HTTP. In small business mode, remote access is granted through standard HTTP authentication services.

While ZENworks Linux Management works equally well with devices provisioned in either enterprise or small business mode, only the small business mode is required. Therefore, ZENworks Linux Management does not provide a mechanism to provision AMT devices in enterprise mode.

If you use another AMT-enabled application that does require provisioning in enterprise mode, you should use the provisioning utilities of that application. Make sure you provision each AMT device with at least one “enterprise name.”

### The Provisioning Process

The provisioning process for AMT devices allows you to specify many AMT-related configuration settings. Examples include users, passwords, enterprise names, and allocation of NVRAM space to specific AMT-enabled applications.

To use the AMT features in ZENworks Linux Management, all that is necessary is each AMT device be provisioned with at least one valid enterprise name, which is used to access the NVRAM where Linux Management stores the ZENworks identity information.

Intel suggests that the enterprise name be chosen to indicate the device's general location. For example, all the devices in the home office may be given an enterprise name of "Company\_HQ," and all devices in field offices may be given enterprise names reflecting their geographical locations.

While it is not required, it is assumed that large numbers of devices will have the same Enterprise name. Each AMT device itself may have up to four different enterprise names.

ZENworks Linux Management provides a utility (`smb-provisioning.exe`) to help provision AMT-devices in small business mode with enterprise names. This utility can be found in the `/opt/novell/zenworks/zdm/imaging/winutils` directory on your imaging server. It requires .NET framework.

For the procedures in providing Intel AMT enterprise names to ZENworks Linux Management, see [Section 23.4.6, "Configuring Intel Active Management Technology \(AMT\)," on page 276](#).

### Accessing AMT Resources

For more information, see ["Downloading and Installing the iAMT Redirection Drivers" on page 276](#).

## 22.4 The Preboot Services Processes

The following sections explain how the Preboot Services processes work:

- [Section 22.4.1, "A Typical Preboot Services Operation," on page 224](#)
- [Section 22.4.2, "Illustrating the Preboot Services Processes," on page 225](#)

### 22.4.1 A Typical Preboot Services Operation

A typical Preboot Services operation can flow as follows:

1. A Preboot bundle is created in the ZENworks Control Center and assigned to a PXE-enabled device.
2. The PXE-enabled device starts to boot.
3. The device sends a DHCP discovery request to determine the IP address of the Preboot Services imaging server.
4. The DHCP server responds with an IP address for the device to use.
5. The `novell-proxydhcp` daemon responds with the IP addresses of the TFTP server, as well as the filename of the Preboot Services bootstrap program (`novlntp.sys`).
6. The PXE device downloads the Preboot Services bootstrap program using `novell-tftp`.
7. After the Preboot Services bootstrap program is downloaded and executed, the device checks `novell-zmgprebootpolicy` to see if there is any imaging work to do.
8. If there is imaging work to do (as contained in a Preboot bundle that is assigned to the device), the device downloads the Linux Management imaging environment from the server so that the it can be booted to Linux.
9. Any imaging tasks contained in the Preboot bundle are performed.



10. If there are no imaging tasks to perform, files are not downloaded and the device proceeds to boot to its operating system.

In addition to using PXE for automation, you can also execute Preboot work manually using one of the following:

- Preboot Menu (if enabled for the device)
- Preboot Services bootable CD or DVD
- ZENworks partition

## 22.4.2 Illustrating the Preboot Services Processes

The following illustrations show the interaction between a Preboot Services (PXE) device and a Preboot Services imaging server, starting when the PXE device is turned on and begins to boot, and ending when imaging work begins on that device.

The following example assumes that the devices and imaging servers are in the same network segment.

- ♦ [“Phase 1: Beginning the Process” on page 225](#)
- ♦ [“Phases 2 through 8: Continuing the Process” on page 228](#)

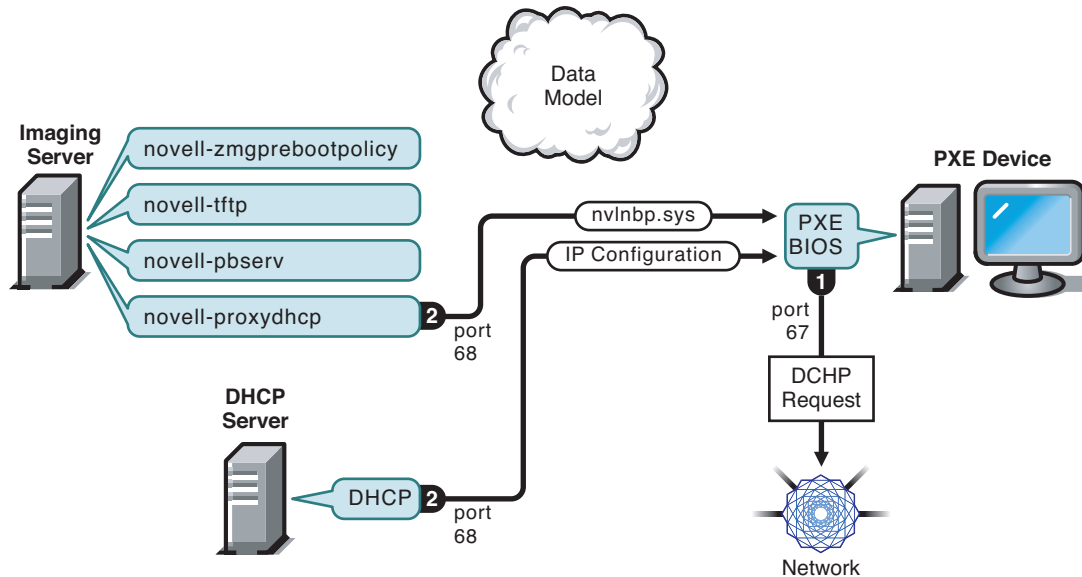
### Phase 1: Beginning the Process

Depending on whether novell-proxydhcp is configured on the same server as the standard DHCP server or on a different server, the imaging process begins differently. The following sections illustrate how the process begins for each configuration, then the phases illustrated in [“Phases 2 through 8: Continuing the Process” on page 228](#) are the same for both.

## Standard DHCP and Novell Proxy DHCP Configured on Separate Servers

For this example, the DHCP server and the Preboot Services imaging server are two separate servers on the network.

**Figure 22-1** DHCP Configuration on Separate Servers



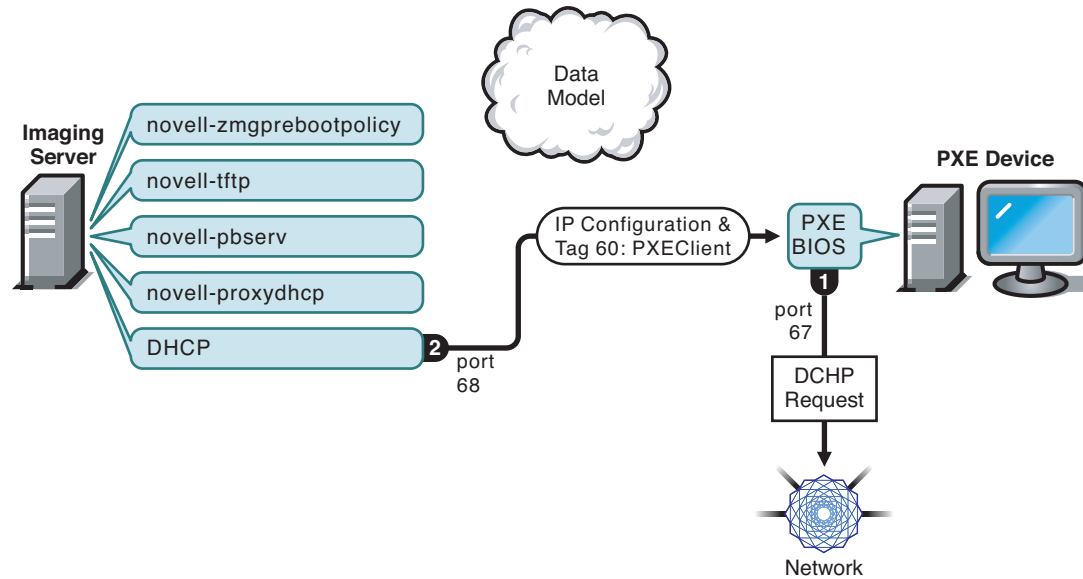
Processes:

1. When the device boots, the PXE BIOS issues a DHCP request with PXE extensions. The request is broadcast on port 67.
2. The DHCP server responds with IP configuration information on port 68, and the Proxy DHCP server responds on port 68 with the name of the bootstrap program (`nvlnbp.sys`) and the IP address of the TFTP daemon where it can be found.
3. Continue with [“Phases 2 through 8: Continuing the Process” on page 228](#).

## Standard DHCP and Novell Proxy DHCP Configured on the Same Server: Part A

For this example, the DHCP server and the Preboot Services imaging server are configured on the same server on the network. This example contains parts A and B.

**Figure 22-2** DHCP Configuration on the Same Server; Part A

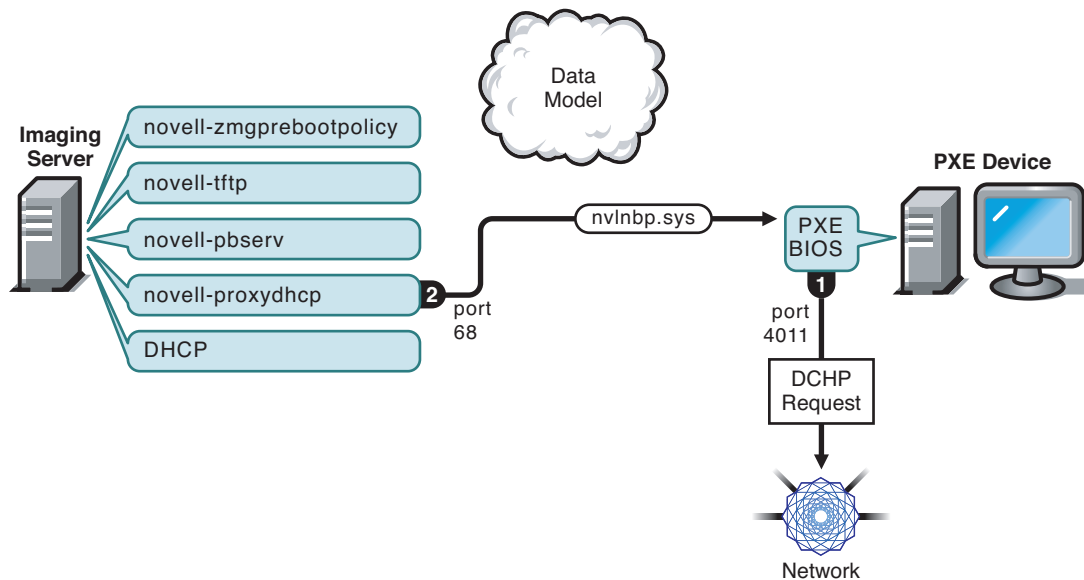


Processes:

1. When the device boots, the PXE BIOS issues a DHCP request with PXE extensions. The request is broadcast on port 67.
2. The DHCP server responds with IP configuration information on port 68, including **tag 60 for PXEClient**, which indicates that novell-proxydhcp is running on the same server.

## Standard DHCP and Novell Proxy DHCP Configured on the Same Server: Part B

**Figure 22-3** DHCP Configuration on the Same Server, Part B



Processes:

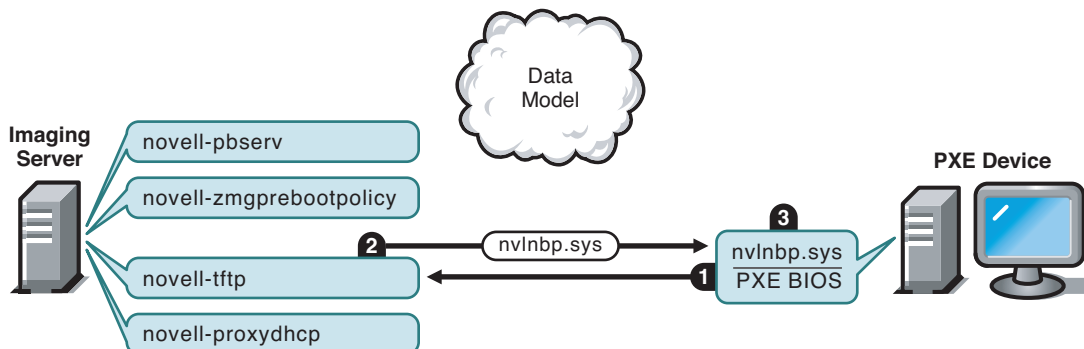
1. When the device sees tag 60 in the DHCP response, the PXE BIOS reissues the DHCP request on port 4011.
2. The Proxy DHCP server responds on port 68 with the name of the bootstrap program (`nvlnbp.sys`) and the IP address of the TFTP daemon where it can be found.
3. Continue with [“Phases 2 through 8: Continuing the Process” on page 228](#).

### Phases 2 through 8: Continuing the Process

The following phases are continued after one of the Phase 1 sections above.

#### Phase 2

**Figure 22-4** Phase 2 of the Preboot Services Process

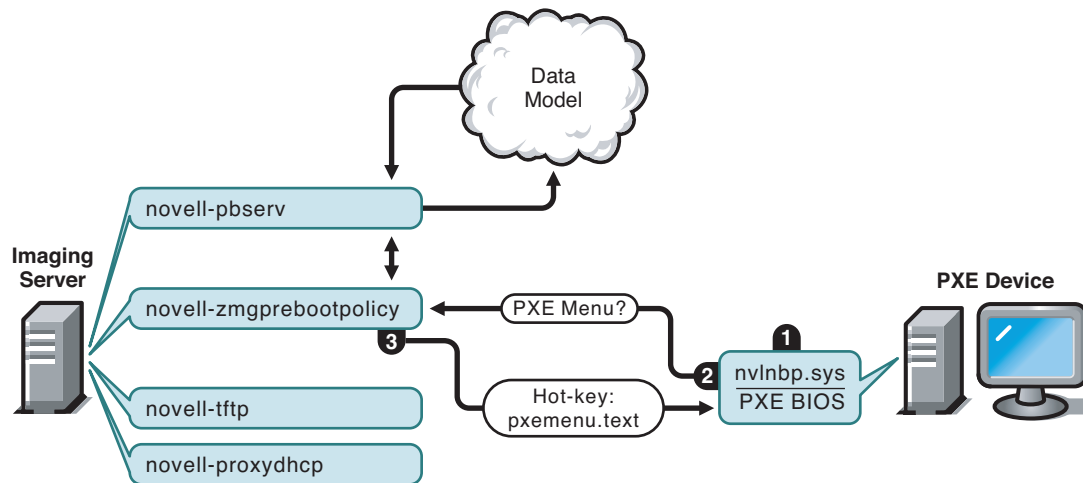


Processes:

1. The PXE BIOS requests `nvlnbp.sys` from the TFTP server.
2. The TFTP server sends `nvlnbp.sys` to the PXE device.
3. The PXE device loads `nvlnbp.sys` into memory.

### Phase 3

**Figure 22-5** Phase 3 of the Preboot Services Process

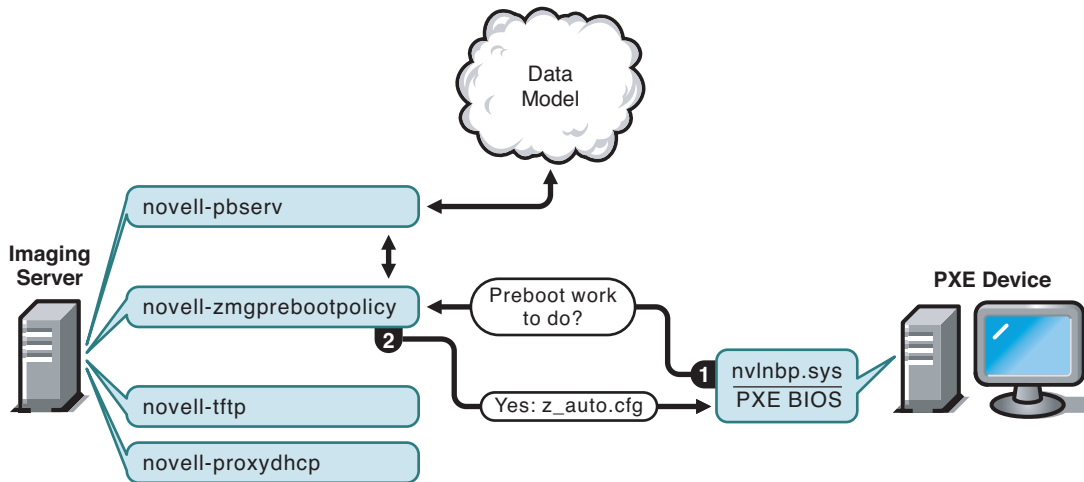


Processes:

1. Hardware detection is performed by `nvlnbp.sys` and it reads the image-safe data.
2. `Nvlnbp.sys` requests the PXE Menu configuration from the Data Model via the `novell-zmgprebootpolicy` daemon.
3. The `novell-zmgprebootpolicy` daemon returns the PXE Menu configuration. In this case, the menu described in `pxemenu.txt` is displayed when a user presses the hot key.

## Phase 4

**Figure 22-6** Phase 4 of the Preboot Services Process

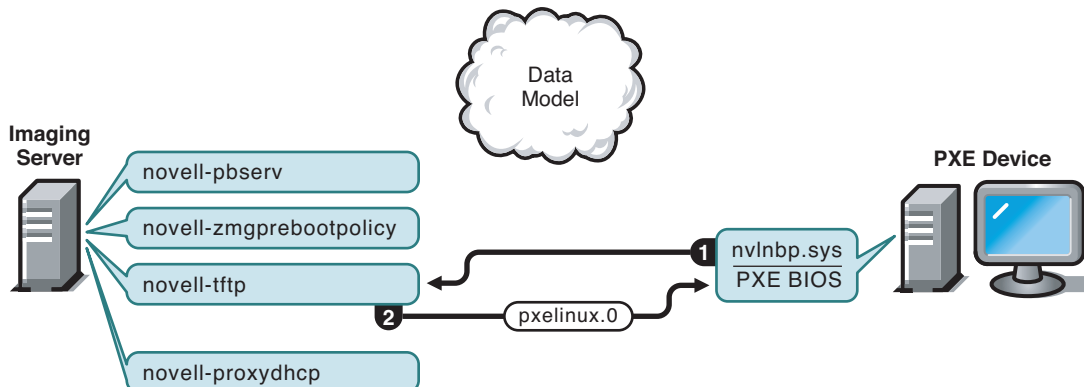


Processes:

1. Assuming no PXE Menu is displayed, the device asks the Data Model (via `novell-zmgprebootpolicy`) if any work is assigned.
2. Assuming work is assigned, the `novell-zmgprebootpolicy` daemon responds with the name of the configuration file to use in performing the preboot work (`z_auto.cfg` in this example).

## Phase 5

**Figure 22-7** Phase 5 of the Preboot Services Process

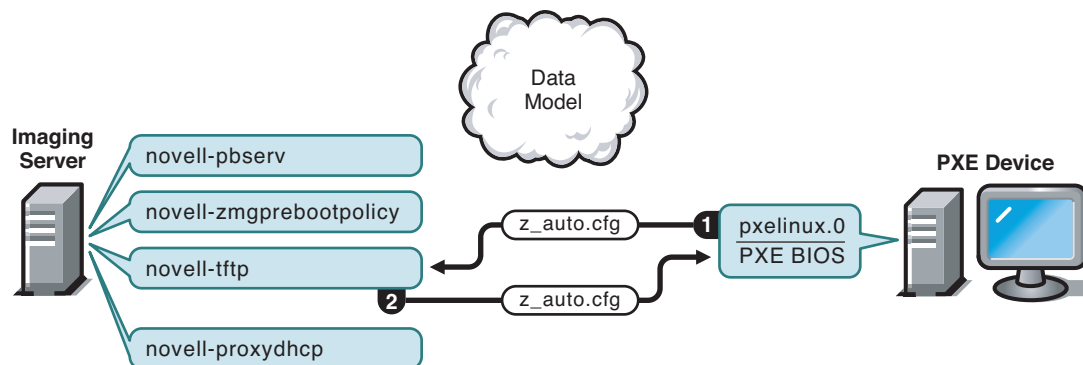


Processes:

1. The PXE device requests `pxelinux.0` from the TFTP server.
2. The TFTP server sends `pxelinux.0` to the device.

## Phase 6

**Figure 22-8** Phase 6 of the Preboot Services Process

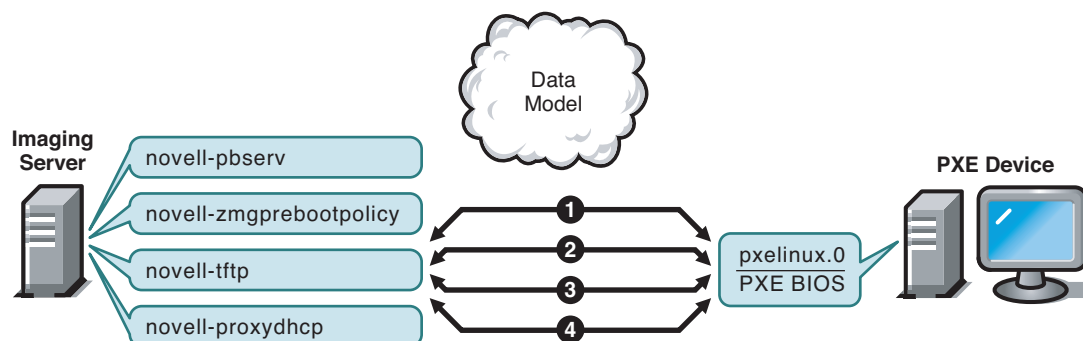


Processes:

1. `Pxelinux.0` replaces `nvlnbp.sys` in memory and requests `z_auto.cfg` from the TFTP server.
2. The TFTP server sends the `z_auto.cfg` file to the device.

## Phase 7

**Figure 22-9** Phase 7 of the Preboot Services Process

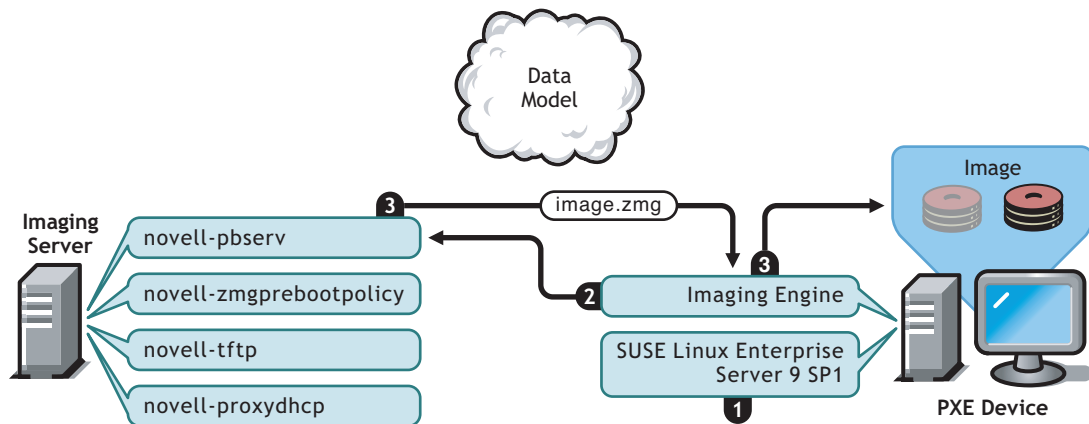


Processes:

1. `Pxelinux.0` requests and receives `/boot/kernel` from the TFTP server.
2. `Pxelinux.0` requests and receives `/boot/initid` from the TFTP server.
3. `Pxelinux.0` requests and receives `/boot/root` from the TFTP server.
4. `Pxelinux.0` requests and receives `/boot/updateDrivers.tgz` from the TFTP server, but is denied because the file does not exist (it is used to provide post-release software updates).

## Phase 8

**Figure 22-10** Phase 8 of the Preboot Services Process



Processes:

1. SUSE Linux Enterprise Server (SLES) 9 SP1 is loaded and run on the device.
2. The ZENworks Imaging Engine (img) requests the assigned Preboot Services work details and performs the work.
3. The image is laid down on the device and it automatically reboots.

## 22.5 Preboot Strategies

The following sections present possible approaches to using Preboot Services. Use the following sections to determine which procedures to perform. The steps are documented in subsequent sections.

- ♦ [Section 22.5.1, “Automating Updates and Installations,” on page 232](#)
- ♦ [Section 22.5.2, “Creating, Installing, and Restoring Standard Images,” on page 233](#)
- ♦ [Section 22.5.3, “Reimaging Corrupted Devices,” on page 234](#)
- ♦ [Section 22.5.4, “Restoring Lab Devices to a Clean State,” on page 234](#)
- ♦ [Section 22.5.5, “Setting Up Devices for Future Reimaging,” on page 235](#)
- ♦ [Section 22.5.6, “Multicasting Device Images,” on page 235](#)

### 22.5.1 Automating Updates and Installations

You can automate Linux installations and software updates using Preboot Services in the following ways:

- ♦ **SUSE Linux installation:** The AutoYaST bundle can automate installation of SUSE Linux on a Linux device.
- ♦ **Red Hat Linux installation:** The kickstart bundle can automate installation of Red Hat Linux on a Linux device.
- ♦ **ZENworks script execution:** The ZENworks Script bundle can automate execution of any ZENworks script on a Linux device, including imaging commands.



- ♦ **Device imaging:** The ZENworks Imaging bundle can be used to place an image on a Linux device.
- ♦ **Imaging multiple devices:** The ZENworks Multicast bundle can be used to place an image on multiple Linux devices with one pass of the image file over the network, such as in resetting lab devices.

All you need to do to accomplish the above is to create and configure one of the five Preboot bundle types, then assign the bundle to the desired devices.

When a device boots, the assigned bundle is automatically applied before the device's operating system starts.

You can also manually accomplish these tasks per device using the Preboot Services Menu's *Start ZENworks Imaging Maintenance* option to access the bash prompt, if you have enabled the Preboot Services Menu for the device. Or, you can use a Preboot Services bootable CD or DVD, which does not require PXE to be enabled on the device.

## 22.5.2 Creating, Installing, and Restoring Standard Images

As new devices are purchased and before deploying them, you can install a standard software platform and enable the device for future unattended reimaging.

1. Create a model device of each type that you'll deploy.
2. Create an image of each model device on a ZENworks Linux Management imaging server. For more information, see [“Manually Taking an Image of a Device” on page 305](#).

These images should include the Novell ZENworks Linux Management Imaging Agent (`novell-zslnx`).

3. Optionally, you may create a preboot imaging bundle for this image. This allows the image to be assigned automatically for later use.
4. If you are using Preboot Services, install ZENworks Linux Management on your imaging server. For more information, see [Section 23.1, “Preparing a Preboot Services Server,” on page 239](#).

or

If you are using a bootable CD or DVD, or a ZENworks partition, create a boot CD or DVD that points to the ZENworks Linux Management imaging server where the model images are stored. For more information, see [Section 23.2, “Setting Up the Preboot Services Methods,” on page 240](#).

As each new device comes in, if you are using Preboot Services do the following:

1. Check to see if the device is PXE capable. Enable PXE if it isn't enabled by default. For more information, see [Section 23.6, “Enabling PXE on Devices,” on page 282](#).
2. Physically connect the device to the network.
3. Boot the device from the Preboot Services imaging server.

If you are not using Preboot Services, boot the device with the imaging boot CD or DVD and consider installing the ZENworks partition to enable auto-imaging without needing to supply the CD or DVD. For more information, see [Step 3 on page 245](#) of [Section 23.7.2, “Enabling a Device for Imaging Operations,” on page 284](#). After you have installed the partition, reboot the device from the ZENworks partition.

### 22.5.3 Reimaging Corrupted Devices

Without data loss or undue disruption to users, you can fix devices that have become misconfigured or corrupted.

1. When a device needs to be fixed, have the user back up any files to the network that he or she wants to keep (if possible).
2. Create and/or assign an appropriate imaging bundle to the device.
3. If it is a device with a ZENworks partition or it is PXE-enabled, the user should boot the device from the ZENworks partition or the Preboot Services imaging server (via PXE) to find and execute the assigned bundle. If you are using PXE, make sure that Preboot Services is installed on your imaging server. For more information, see [Chapter 24, “Using Preboot Services,” on page 287](#).

or

If the device does not have a ZENworks partition and is not PXE-enabled, the user should boot the device with the imaging boot CD or DVD and restore the appropriate images manually.

4. After the image is laid down, restore any user files that were backed up to the network.

### 22.5.4 Restoring Lab Devices to a Clean State

You can restore devices to a clean state, removing any changes or additions made since the last time you restored the image on that device. This is useful for updating lab devices.

The following steps assume that the devices are unregistered.

1. Create an image of a clean model device and store it on a ZENworks Linux Management imaging server. For more information, see [“Manually Taking an Image of a Device” on page 305](#).
2. If you are using Preboot Services, make sure that ZENworks Linux Management is installed on your imaging server. For more information, see [Section 23.1, “Preparing a Preboot Services Server,” on page 239](#).
3. If you are using Preboot Services and the devices are PXE capable, make sure that PXE is enabled. For more information, see [Section 23.6, “Enabling PXE on Devices,” on page 282](#).

or

If you are not using Preboot Services or the Linux partition, create an imaging boot CD or DVD that points to the ZENworks Linux Management imaging server where the clean image is stored. For more information, see [Section 23.2, “Setting Up the Preboot Services Methods,” on page 240](#).

Deploy each lab device as follows:

1. Physically connect the device to the lab network.
2. If you are using Preboot Services, boot the device from the Preboot Services imaging server.

or

If you are not using Preboot Services, boot the device with the imaging boot CD or DVD and install the ZENworks partition. For more information, see [Step 3 on page 245 of Section 23.7.2, “Enabling a Device for Imaging Operations,” on page 284](#). After you have installed the partition, reboot the device from the ZENworks partition.

3. At the end of each lab session, assign the Preboot bundle to the lab devices.
4. Reboot each device and let it be auto-imaged by its assignment to a ZENworks Preboot bundle.

## 22.5.5 Setting Up Devices for Future Reimaging

With minimal disruption to users, you can enable existing devices for possible future reimaging.

This process might need to be phased in by local administrators. Each administrator could do the following:

1. Install the Novell ZENworks Linux Management Imaging Agent (**novell-zislnx**) on each device.
2. If the devices are PXE capable, make sure PXE is enabled (see [Section 23.6, “Enabling PXE on Devices,” on page 282](#)) and make sure that ZENworks Linux Management is installed on your imaging server (see [Section 23.1, “Preparing a Preboot Services Server,” on page 239](#)).  
or  
Prepare a few sets of imaging CDs or DVDs that users can use when they run into trouble (see [Section 23.2, “Setting Up the Preboot Services Methods,” on page 240](#)). These devices could point to an imaging server that contains the same clean images used for new devices.
3. If a user runs into trouble, use the strategy for reimaging corrupted devices. For more information, see [Section 22.5.3, “Reimaging Corrupted Devices,” on page 234](#).

## 22.5.6 Multicasting Device Images

The following sections explain the multicasting images feature:

- ♦ [“Understanding Multicasting” on page 235](#)
- ♦ [“What Are Practical Uses For Multicasting?” on page 236](#)
- ♦ [“Automatic Multicasting Example” on page 237](#)

For instructions on using multicasting, see [Section 24.4, “Multicasting Images,” on page 319](#).

### Understanding Multicasting

Multicasting is a way to send the same image to multiple devices without sending that image multiple times across the network. It is done by inviting participants to join a multicast session. Multicasting is similar to broadcasting on the network, in that you send the image once to the network and only those devices belonging to the multicast session can see and receive it. This saves on network bandwidth usage.

For example, if you have 10 devices in the multicast session and the image is 3 GB in size, your network experiences only 3 GB of network traffic to image all 10 devices. Without Multicasting, the network experiences 30 GB of network traffic to image all 10 devices individually.

The devices to be imaged must be physically connected to the network. They can be devices with existing operating systems of any kind, or they can be new devices with no operating system installed.

---

**IMPORTANT:** For multicasting to work properly, all routers and switches on the network must have their multicast features configured. Otherwise, multicast packets might not be routed properly.

---

Multicasting can be done automatically or manually:

- ♦ [“Automatic Multicasting” on page 236](#)
- ♦ [“Manual Multicasting” on page 236](#)

### Automatic Multicasting

In the ZENworks Control Center, multicasting is accomplished by configuring a Multicast bundle. The bundle contains a base image that is taken previously from a device and is stored on an imaging server. This base image is applied to all multicast session participants.

When using a Preboot bundle to perform multicasting, the imaging server is the session master, which sends the `.zmg` image file to the session participants. The `novell-pbserv` daemon is used in this process. All problems are reported and displayed on the session master device.

For more information, see [Section 24.4, “Multicasting Images,” on page 319](#).

### Manual Multicasting

At a bash prompt, you can enter commands to configure and initiate a multicasting session. You enter the appropriate commands on a bash prompt at each device, specifying one of them to be the session master. An image of the session master’s hard drive is sent to each of the session participants.

For more information on the imaging commands, see [Section C.5, “Session \(Multicast\) Mode \(img session\),” on page 433](#).

If you plan to set up multicasting by visiting each device, you need either an imaging boot CD or DVD, or the devices must be PXE-enabled. For more information, see [Section 23.2, “Setting Up the Preboot Services Methods,” on page 240](#).

## What Are Practical Uses For Multicasting?

Multicasting is ideal for labs, classrooms, and staging areas, or for any place where you need to quickly create the same configuration on multiple devices, instead of taking the time to set up each device individually.

### Benefits of Multicasting Images

Multicasting is the way to use ZENworks Imaging Engine for mass reimaging with the least amount of overhead. It is useful if you have one device with a clean software configuration that you want to duplicate on several other devices, or if you have a single image that you want to set up on multiple devices.

### Limitations of Multicasting Images

One significant limitation of using multicast without installing any ZENworks Linux Management software is that it results in a set of devices that have duplicate network identities. The IP addresses (if the network is using static IP addressing) and device hostname are all the same and can cause conflicts if deployed on the network without change.

For a handful of devices, this might not be a problem. But for a larger number of devices, you should install the Novell ZENworks Linux Management Imaging Agent (`novell-zislnx`) on them before doing the multicast (see [Section 23.7.2, “Enabling a Device for Imaging Operations,” on page 284](#)).

The Imaging Agent saves the device's network identity settings before the multicast session and restores them afterwards.

## Automatic Multicasting Example

To automatically multicast an image to multiple devices using the ZENworks Control Center:

1. In the ZENworks Control Center, create a Multicast bundle using a wizard.
2. Specify the source image for the bundle.

You can multicast an existing image from your imaging server.

3. Configure the trigger for multicasting the bundle. Trigger examples:

**Client count:** When the specified number of clients specified in the bundle have booted and registered, the multicast session begins.

**Time count:** When the specified length of time has passed with no new clients having registered, the multicast session begins regardless of the number of client participating.

The first trigger to be realized causes the multicast session to begin.

4. Assign the Multicast bundle to the desired devices.

The ZENworks Control Center provides a way to enable or disable a Multicast bundle, allowing you to temporarily stop the bundle from executing. This is more efficient than unassigning the bundle from many devices.

5. Wait for the trigger to happen.

Each device booting into the session has its boot process delayed until the session begins, which timing is determined by fulfillment of one of the triggers.

The multicast happens automatically when a device assigned to the Multicast bundle boots, according the configuration you set up for the Multicast bundle and for the devices you assigned to the bundle. This bundle is applied to each session device before it boots its operating system. The ZENworks Multicast bundle is sent over the wire just once, using the multicast capability of your network, and executed simultaneously on all participating devices.



# Setting Up Preboot Services

# 23

The section provides instructions for setting up Novell® ZENworks® Linux Management Preboot Services:

- ♦ [Section 23.1, “Preparing a Preboot Services Server,” on page 239](#)
- ♦ [Section 23.2, “Setting Up the Preboot Services Methods,” on page 240](#)
- ♦ [Section 23.3, “Deploying and Managing Preboot Services,” on page 247](#)
- ♦ [Section 23.4, “Configuring Preboot Services Defaults,” on page 261](#)
- ♦ [Section 23.5, “Overriding Preboot Services Defaults,” on page 280](#)
- ♦ [Section 23.6, “Enabling PXE on Devices,” on page 282](#)
- ♦ [Section 23.7, “Setting Up Devices for Imaging,” on page 283](#)

---

**IMPORTANT:** The Preboot Services software is automatically installed when you install ZENworks Linux Management.

---

## 23.1 Preparing a Preboot Services Server

When you install Novell ZENworks Linux Management on a server, the server is nearly ready to act as a Preboot Services server. To avoid confusion, the Proxy DHCP daemon (novell-proxydhcp) is installed, but not enabled. For PXE devices to be able to communicate with Preboot Services, this daemon must be started manually on at least one server on each network segment. Exactly how many servers and which specific servers should run this daemon is dictated by your network topology. As a rule of thumb, for every DHCP server deployed in your network, you should have a corresponding Proxy DHCP server.

For information on setting up management of your devices, see [Section 23.3, “Deploying and Managing Preboot Services,” on page 247](#) and [Section 23.4, “Configuring Preboot Services Defaults,” on page 261](#).

In addition to the specific hardware requirements for a ZENworks Linux Management server, the server used to store image files must meet the following requirements:

- ♦ **A fixed IP address:** When you connect to the imaging server during an imaging operation, you must do so using the fixed IP address or DNS name of the imaging server.
- ♦ **Enough space to store device images:** Unless you use compression (which is enabled by default) for your device images, they are nearly the same size as the data on the device hard disk, which could be many gigabytes.

If you want to store an image locally (on a CD, DVD, or hard disk) rather than on an imaging server, see [“Using a CD or DVD for Disconnected Imaging Operations” on page 314](#) and [“Using a Hard Disk for Disconnected Imaging Operations” on page 316](#).

## 23.2 Setting Up the Preboot Services Methods

The Novell ZENworks Imaging Engine that performs the actual imaging of a device is a Linux application. Unless you use automated Preboot Services with PXE-enabled devices, you need to prepare a boot medium that has the Linux kernel, ZENworks Imaging Engine, and network drivers installed.

The following sections contain additional information:

- ♦ [Section 23.2.1, “Using Preboot Services \(PXE\),” on page 240](#)
- ♦ [Section 23.2.2, “Preparing Imaging Boot CDs or DVDs,” on page 240](#)
- ♦ [Section 23.2.3, “Using the ZENworks Imaging Floppy Boot Disk Creator,” on page 242](#)
- ♦ [Section 23.2.4, “Managing ZENworks Partitions,” on page 244](#)

### 23.2.1 Using Preboot Services (PXE)

Preboot Execution Environment (PXE) is an Intel specification that allows a device to boot off the network, instead of its hard drive or other local media. ZENworks Linux Management can use PXE to launch Preboot Services.

In ZENworks Linux Management, Preboot Services uses PXE to find out if there is imaging work specified for a device and to provide the device with the files necessary to boot to the ZENworks Linux Management imaging environment.

Before you can use Preboot Services with automated Preboot bundles, you need to do the following:

- ♦ Install the ZENworks Linux Management Imaging and Preboot Services (PXE Support) components on your imaging server.
- ♦ Enable PXE on the device.
- ♦ Have a standard DHCP server, either on your imaging server or on another network server.

Automated Preboot Services functions can also be performed using a ZENworks partition. For more information, see [“Creating a ZENworks Partition” on page 245](#).

Manual Preboot Services functions can be performed using CDs or DVDs. For more information, see [Section 23.2.2, “Preparing Imaging Boot CDs or DVDs,” on page 240](#).

### 23.2.2 Preparing Imaging Boot CDs or DVDs

If you have software for burning CDs or DVDs, you can create an imaging boot CD or DVD for imaging operations. You have two options:

- ♦ [“Creating a Boot CD or DVD with Additional Files” on page 241](#)
- ♦ [“Creating a Boot CD or DVD without Additional Files” on page 241](#)

For information on how to use the CD or DVD to perform disconnected imaging operations, see [Section 24.3.3, “Setting Up Disconnected Imaging Operations,” on page 314](#).



## Creating a Boot CD or DVD with Additional Files

This section describes how to create an imaging CD or DVD that contains more than the files provided in the `bootcd.iso` image.

This method allows you to include the `settings.txt` file on the boot CD or DVD to provide the required imaging parameters. For more information on the `settings.txt` file, see [Section B.5, “Imaging Configuration Parameters \(settings.txt\),” on page 411](#).

This method also allows you to add other files and drivers that you need to do the imaging.

To create an imaging boot CD or DVD that includes `settings.txt` and other files:

- 1 Copy the `bootcd.iso` file to a temporary location.

The `bootcd.iso` file is located in the `/opt/novell/zenworks/zdm/imaging/winutils` directory on the imaging server where ZENworks Linux Management is installed.

- 2 In an ISO editor, open the temporary copy of the `bootcd.iso` file.

If you experience ISO corruption after adding files into the ISO, such as a checksum error, use a more reliable ISO editor. Also, some ISO editors do not work very well with DVDs.

- 3 Using the temporary `bootcd.iso` file, copy the `settings.txt` file to the root of the `bootcd.iso` image.

The `settings.txt` file is located in the `/opt/novell/zenworks/zdm/imaging/winutils` directory on the imaging server where ZENworks Linux Management is installed.

- 4 Copy any other files or drivers that you want included on the CD or DVD to the `/addfiles` directory in the temporary `bootcd.iso` image.

Any files or subdirectories that you add under the `/addfiles` directory are placed at the root of the client when booting the CD or DVD.

---

**IMPORTANT:** When booting from the CD or DVD, the imaging engine is read into RAM. Because the imaging engine uses some of the RAM that exists on the client device, the combined size of any files that you add under the `/addfiles` directory cannot exceed amount of remaining RAM.

---

- 5 Save the updated `bootcd.iso` image file to its temporary location.
- 6 Use your software for burning CDs or DVDs to burn the updated `bootcd.iso` image onto the CD or DVD.
- 7 Boot the device to be imaged from your newly created imaging boot CD or DVD.

Bootimg from a SCSI CD-ROM device is currently not supported.

## Creating a Boot CD or DVD without Additional Files

If you do not want to include the `settings.txt` file or any other files or drivers in the imaging boot CD or DVD, you can simply create the imaging boot CD or DVD from the `bootcd.iso` image provided with ZENworks.

However, you will need to provide the `settings.txt` file on a floppy diskette to provide the required imaging parameters. For more information on the `settings.txt` file, see [Section B.5, “Imaging Configuration Parameters \(settings.txt\),” on page 411](#).

To create an imaging boot CD or DVD that contains only the `bootcd.iso` image:

- 1 Copy the `settings.txt` file containing the settings you want for the imaging boot process onto a floppy diskette.

This file is located in the `/opt/novell/zenworks/zdm/imaging/winutils` directory on the imaging server where ZENworks Linux Management is installed.

- 2 Use your software for burning CDs or DVDs to burn the `bootcd.iso` image onto the CD or DVD.

The `bootcd.iso` file is located in the `/opt/novell/zenworks/zdm/imaging/winutils` directory on the imaging server where ZENworks Linux Management is installed

- 3 Boot the device to be imaged from your newly created imaging boot CD or DVD.

You will be prompted for the diskette that contains the `settings.txt` file.

Booting from a SCSI CD-ROM device is currently not supported.

### 23.2.3 Using the ZENworks Imaging Floppy Boot Disk Creator

This utility allows you to do the following:

- ♦ “Creating a Floppy Boot Diskette” on page 242
- ♦ “Managing the `settings.txt` File” on page 243

#### Creating a Floppy Boot Diskette

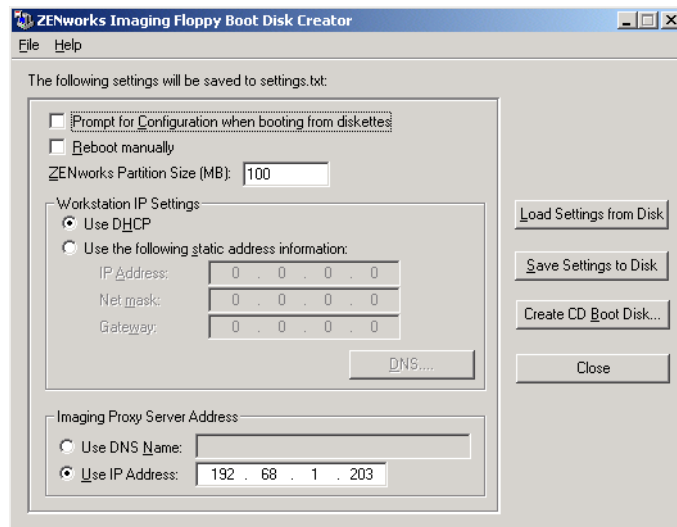
If you have devices that cannot normally boot a CD or DVD, but has the CD or DVD hardware installed, you can use the ZENworks Imaging Floppy Boot Disk Creator utility to create a diskette that enables the device to boot from a CD or DVD.

To create a boot diskette:

- 1 Format one high-density diskette, or use a preformatted blank diskette.
- 2 On a Windows machine, browse to the `opt/novell/zenworks/zdm/imaging/winutils` directory on your Linux imaging server and run `zimboot.exe`.

You might need to configure Samba on the Linux server in order for the Windows machine to have access to this directory.

The following dialog box is displayed:



- 3 Click *Create CD Boot Disk*.
- 4 After the diskette is created, click *Close*.
- 5 Insert both this diskette and the imaging CD or DVD on the device to be imaged, then boot the device.

The diskette enables the imaging CD or DVD to be booted by the device.

## Managing the settings.txt File

There two `settings.txt` files shipped with ZENworks Linux Management:

- ♦ **/srv/tftp/boot/settings.txt:** PXE devices use this version of the file for automated preboot work. This file exists on the imaging server and usually does not need to be modified. During the boot process, this `settings.txt` file is read and the necessary settings information is discovered and used.
- ♦ **/opt/novell/zenworks/zdm/imaging/winutils/settings.txt:** The imaging server copy of this file needs to be modified for your network environment and a working copy of it should be maintained at the root of the imaging boot device (imaging CD or DVD, or a blank floppy diskette). When burning the imaging CD or DVD, be sure to include the edited copy of this `settings.txt` file.

You can manage the content of this copy of the `settings.txt` file with the ZENworks Imaging Floppy Boot Disk Creator utility, as outlined in the following steps.

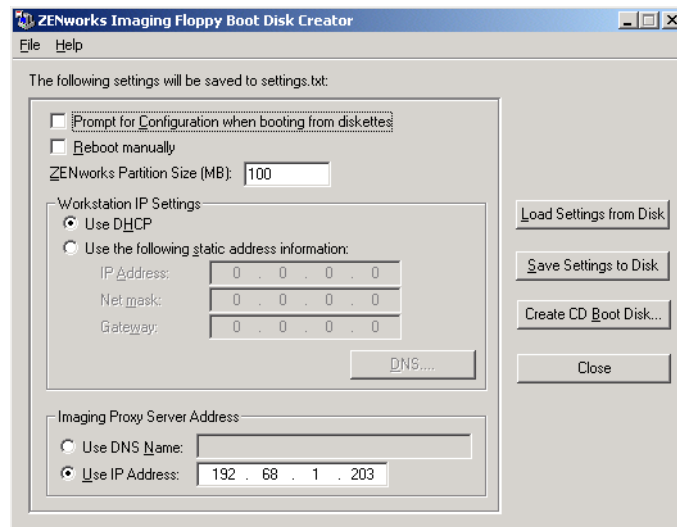
To manually edit the `settings.txt` file, see [Section B.5, “Imaging Configuration Parameters \(settings.txt\),” on page 411](#).

To manage the `settings.txt` file using the ZENworks Imaging Floppy Boot Disk Creator utility:

- 1 On a Windows machine, browse to the `opt/novell/zenworks/zdm/imaging/winutils` directory on your Linux imaging server and run `zimboot.exe`.

You might need to configure Samba on the Linux server in order for the Windows machine to have access to this directory.

The following dialog box is displayed:



**2** Click *Load settings from disk*.

This allows you to browse for the `settings.txt` file. Then, it populates the fields in this dialog box from information in the `settings.txt` file after you locate it in the next step, which you can modify in subsequent steps.

**3** Browse for the `settings.txt` file, then click *Open*.

The default location is `A:\`. Browse to the `/opt/novell/zenworks/zdm/imaging/winutils/` directory for the copy to be modified.

**4** (Required) In the ZENworks Imaging Floppy Boot Disk Creator dialog box (in the Imaging Proxy Server Address section), specify either the fixed IP address or the full DNS name of your imaging server (where novell-pbserv is running).

**5** (Optional) For the other fields and options on the dialog box, keep the default settings, unless you have a specific reason to change a setting, such as to specify a particular device's IP Address in the Workstation IP Settings section.

Click *Help* for details on the specific settings, or see [Section B.5, “Imaging Configuration Parameters \(settings.txt\),” on page 411](#).

**6** Click *Save settings to disk*.

**7** Browse for where you want to save the `settings.txt` file, then click *Save*.

The default location is `A:\`. You can save to a different location for use in burning it to an imaging CD or DVD.

**8** When you are finished using this utility, click *Close*.

## 23.2.4 Managing ZENworks Partitions

A ZENworks partition is used by a device when booting for automated Preboot Services work when the device does not have PXE available. The following sections explain how to manage ZENworks partitions:

- [“Creating a ZENworks Partition” on page 245](#)
- [“Disabling a ZENworks Partition” on page 245](#)

- ♦ [“Removing a ZENworks Partition” on page 246](#)

## Creating a ZENworks Partition

If you want to set up a device for unattended imaging operations and are unable to use Preboot Services (PXE), you can create a ZENworks partition on the hard disk. If you make the partition large enough, you can even store an image of the device’s hard disk, which can be useful if the device becomes misconfigured or corrupted when the network connection is lost.

---

**WARNING:** Installing the ZENworks partition destroys all data on that hard drive. Use this only on devices where you plan to reinstall the operating system and software programs.

---

To create a ZENworks partition, you must first create an imaging CD or DVD to boot the device from. (If the device cannot boot from a CD or DVD, see [Section 23.2.3, “Using the ZENworks Imaging Floppy Boot Disk Creator,” on page 242.](#)) Then, do the following:

- 1 Boot the device with the imaging CD or DVD, then select *Install/Update ZEN partition* from the menu.

This starts the process of creating the ZENworks partition in the first partition slot. It destroys all existing partitions, except an existing ZENworks partition or the Dell or Compaq configuration partitions. By default, the ZENworks partition size is 150 MB.

If the ZENworks partition already exists, it is upgraded, and your existing partitions are left intact.

- 2 After the ZENworks partition is installed or updated, remove the CD or DVD and press any key to continue.
- 3 After removing the CD or DVD and reboot the device, install the operating system on the device.

---

**IMPORTANT:** During installation of the operating system, you must install the boot loader where the root partition is being installed.

---

- 4 To take an image of the device using the ZENworks partition, see [“Creating an Image Using the Bash Prompt” on page 316.](#)
- 5 When the bash prompt is displayed, reboot the device.

The device should boot to Linux. If the bash prompt is displayed again, enter `lilo.s` and reboot a second time.

## Disabling a ZENworks Partition

If you decide to enable PXE on a device, but have previously installed a ZENworks partition on it, you can disable or delete the partition, because it is then no longer necessary. For information on deleting the partition, see [“Removing a ZENworks Partition” on page 246.](#)

When you boot to Linux using any imaging boot device or method other than booting from the ZENworks partition, you can disable (or enable) the ZENworks partition. Just select the menu option to do so when the PXE menu is presented.

## Removing a ZENworks Partition

Because you should not delete the ZENworks partition if you booted using the partition, you should boot the device from an imaging boot method other than the ZENworks partition.

---

**WARNING:** After you have deleted the ZENworks partition, you need to make sure that the image you put on the device was made on a device without a ZENworks partition. Otherwise, the wrong MBR (Master Boot Record) is restored, and the device fails to boot. You should only remove the ZENworks partition if you are going to restore an image that does not have the partition to the device.

---

The following are ways you can remove a ZENworks partition from a device:

- ♦ “Using an Imaging CD or DVD” on page 246
- ♦ “Using a ZENworks Script Bundle” on page 246
- ♦ “Using FDISK” on page 247

### Using an Imaging CD or DVD

If you cannot perform a full restoration at this time, you should consider disabling the ZENworks partition.

To remove a ZENworks partition:

- 1 Boot the device using the ZENworks 7 Linux Management imaging CD or DVD.
- 2 Select the *Manual mode* option.
- 3 On the bash prompt, enter:  

```
img zenPart remove
```
- 4 After the removal is complete, eject the CD or DVD (if you are not going to use it to reimage the device).
- 5 Reboot the device when ready.
- 6 Restore an image or install an operating system.

When the device boots, its ZENworks partition is removed, then the device can be imaged from the CD or DVD without a ZENworks partition.

If the device is assigned to a Preboot Services bundle, it is imaged according to that bundle.

### Using a ZENworks Script Bundle

If you are using Preboot Services, but formerly booted from the ZENworks partition on the device, you can delete the ZENworks partition at the same time you put down an image. However, the new image should not contain a ZENworks partition.

For example, you can do the following:

- 1 In the ZENworks Control Center, create a ZENworks Script bundle.
- 2 In the *Script text* field in the Create New Preboot Bundle wizard, enter:  

```
img zenPart remove
```
- 3 In the *Script text* field (after the above command), enter the other commands necessary for the imaging work you want for this device.

For more information, see [Appendix C, “ZENworks Imaging Engine Commands,” on page 425](#).

- 4 On the Summary page of the wizard, click *Finish* (not *Next*).
- 5 Reboot the device.

## Using FDISK

You can remove a ZENworks partition by simply using FDISK to reconfigure the device’s hard drive. Then, you can either image the device using a ZENworks imaging CD or DVD, or enable PXE on the device and assign a Preboot bundle to it, then reboot it to use that bundle.

# 23.3 Deploying and Managing Preboot Services

The following sections explain how to set up, deploy, and manage Preboot Services:

- ♦ [Section 23.3.1, “Checking the Preboot Services Imaging Server Setup,” on page 247](#)
- ♦ [Section 23.3.2, “Deploying Preboot Services In a Network Environment,” on page 248](#)
- ♦ [Section 23.3.3, “Administering Preboot Services,” on page 256](#)
- ♦ [Section 23.3.4, “Editing the Preboot Services Menu,” on page 259](#)

For information on using Preboot, see [Chapter 24, “Using Preboot Services,” on page 287](#).

## 23.3.1 Checking the Preboot Services Imaging Server Setup

This section provides information on how to check the configuration of Preboot Services after it is installed, and how to set up standard DHCP and novell-proxydhcp daemons on the same server.

- ♦ [“Overview of Preboot Services Components” on page 247](#)
- ♦ [“Checking the Setup” on page 248](#)

## Overview of Preboot Services Components

The following components are installed as part of Preboot Services:

**Table 23-1** *Preboot Service Components*

Daemon	Description
novell-pbserv	The novell-pbserv daemon provides imaging services to devices.
novell-proxydhcp	The novell-proxydhcp daemon runs alongside a standard DHCP server to inform PXE devices of the IP address of the TFTP server. The Proxy DHCP server also responds to PXE devices to indicate which bootstrap program ( <code>nvlnbp.sys</code> ) to use.
novell-tftp	<p>The novell-tftp daemon is used by PXE devices to request files that are needed to perform imaging tasks. The TFTP server also provides a central repository for these imaging files, such as the Linux kernel, <code>initrd</code>, and <code>nvlnbp.sys</code>.</p> <p>A PXE device uses this server to download the bootstrap program (<code>nvlnbp.sys</code>).</p>

Daemon	Description
novell-zmgprebootpolicy	The PXE devices use the novell-zmgprebootpolicy daemon to check if there are any Preboot bundles that are assigned to the device.

The novell-proxydhcp daemon must be started manually and does not need to be run on all imaging servers.

The other three daemons are started automatically when installing ZENworks Linux Management, or any time the server is rebooted, and must run on all imaging servers.

For more information on these daemons, see [Section B.7, “Imaging Server,” on page 414](#).

## Checking the Setup

After the Preboot Services components are installed, the following daemons should be installed and running on the server:

**Table 23-2** Preboot Services Daemons

Service	Command to Check Its Status
novell-pbserv	<code>/etc/init.d/novell-pbserv status</code>
novell-tftp	<code>/etc/init.d/novell-tftp status</code>
novell-zmgprebootpolicy	<code>/etc/init.d/novell-zmgprebootpolicy status</code>

You should not need to change the default configuration of these daemons.

If the server where the Preboot Services components are installed is also a DHCP server, see [“Configuring LAN Environments for Preboot Services” on page 252](#).

## 23.3.2 Deploying Preboot Services In a Network Environment

To implement the network deployment strategies outlined in this section, you must have a solid understanding of the TCP/IP network protocol and specific knowledge of TCP/IP routing and the DHCP discovery process.

Deploying Preboot Services (with PXE) in a single network segment is a relatively simple process. However, Preboot Services deployment in a multi-segment network is far more complex and might require configuration of both the Preboot Services daemons and the network switches and routers that lie between the server and the PXE devices.

Configuring the routers or switches to correctly forward Preboot Services network traffic requires a solid understanding of the DHCP protocol, DHCP relay agents, and IP forwarding. The actual configuration of the switch or router must be performed by a person with detailed knowledge of the hardware.

We strongly recommend that you initially set up Preboot Services in a single segment to ensure that the servers are configured correctly and are operational.



This section includes the following information:

- ♦ [“Server Configuration” on page 249](#)
- ♦ [“Network Configuration” on page 250](#)
- ♦ [“Configuring Filters on Switches and Routers” on page 255](#)
- ♦ [“Spanning Tree Protocol in Switched Environments” on page 255](#)

## Server Configuration

There are three important points about configuring servers for Preboot Services:

- ♦ **DHCP server:** The Preboot Services environment requires a standard DHCP server. It is up to you to install your standard DHCP server.
- ♦ **Preboot Services daemons:** The four Preboot Services daemons (novell-pbserv, novell-tftp, novell-proxydhcp, and novell-zmgprebootpolicy) are all installed on the imaging server when you install ZENworks Linux Management. These daemons must run together on the same server.
- ♦ **Imaging server:** The Preboot Services daemons can be installed and run on the same or different server than DHCP.

The following sections give general information about these services:

- ♦ [“The DHCP Server” on page 249](#)
- ♦ [“The novell-pbserv daemon” on page 249](#)
- ♦ [“The novell-proxydhcp daemon” on page 250](#)
- ♦ [“The novell-tftp daemon” on page 250](#)
- ♦ [“The novell-zmgprebootpolicy daemon” on page 250](#)

It is seldom necessary to make changes to the default configuration of these services. However, if you need more detailed configuration information, see [“Configuring Preboot Services Imaging Servers in Linux” on page 256](#).

### The DHCP Server

The standard DHCP server must be configured with an active scope to allocate IP addresses to the PXE devices. The scope options should also specify the gateway or router that the PXE devices should use.

If Preboot Services (specifically novell-proxydhcp) is installed on the same server as the DHCP server, then the DHCP server must be configured with a special option tag. For more information, see [“Configuring LAN Environments for Preboot Services” on page 252](#).

### The novell-pbserv daemon

The Preboot Services novell-pbserv daemon provides imaging services to devices.

This includes sending and receive image files, discovering assigned Preboot bundles, acting as session master for multicast imaging, and so on.

### The novell-proxydhcp daemon

The Preboot Services Proxy DHCP server runs alongside a standard DHCP server to inform PXE devices of the IP address of the TFTP server, the IP address of the server where novell-zmgprebootpolicy is running, and the name of the network bootstrap program (`nvlnbp.sys`).

### The novell-tftp daemon

The Preboot Services novell-tftp daemon is used by PXE devices to request files that are needed to perform imaging tasks. The TFTP server also provides a central repository for these files.

A PXE device uses one of these servers to download the network bootstrap program (`nvlnbp.sys`).

### The novell-zmgprebootpolicy daemon

PXE devices use novell-zmgprebootpolicy to check if there are any imaging actions that need to be performed on the device. It forwards requests to novell-pbserv on behalf of PXE devices.

If you are using **Intel AMT**, support for it should be enabled in the `novell-zmgprebootpolicy.conf` file.

## Network Configuration

The configuration required to run Preboot Services in your network depends on your network setup. Design your network so that PXE devices can effectively connect to the server where the Preboot Services daemons are running. Make sure you consider the number of PXE devices to be installed on the network and the bandwidth available to service these devices. To understand how the devices and servers need to interact during the Preboot Services process, see [Section 22.4, “The Preboot Services Processes,” on page 224](#).

You can configure Preboot Services where Preboot Services and DHCP are running on the same server or on different servers in both LAN and WAN/VLAN environments:

- ♦ [“Understanding Preboot Services in LAN and WAN/VLAN Environments” on page 250](#)
- ♦ [“Comparing Preboot Services Setups in LAN and WAN/VLAN Environments” on page 251](#)
- ♦ [“Configuring LAN Environments for Preboot Services” on page 252](#)
- ♦ [“Configuring a WAN/VLAN with Preboot Services and DHCP Running on the Same Server” on page 253](#)
- ♦ [“Configuring a WAN/VLAN With Preboot Services and DHCP Running on Separate Servers” on page 253](#)

### Understanding Preboot Services in LAN and WAN/VLAN Environments

Imaging servers should be installed so that PXE devices have access to imaging services within their LAN. A good design ensures that a client does not need to connect to imaging services through a slow WAN link.

While you can have any number of imaging servers, generally only one Proxy DHCP server should be enabled per DHCP server scope.

In a WAN, the PXE device is usually separated from the Proxy DHCP and DHCP servers by one or more routers. The PXE device broadcasts for DHCP information, but by default the router does not forward the broadcast to the servers, causing the Preboot Services session to fail.

In a VLAN (Virtual LAN) environment, the PXE device is logically separated from the Proxy DHCP server and the DHCP server by a switch. At the IP level, this configuration looks very similar to a traditional WAN (routed) environment.

In a typical VLAN environment, the network is divided into a number of subnets by configuring virtual LANs on the switch. Devices in each virtual LAN usually obtain their IP address information from a central DHCP server. In order for this system to work, it is necessary to have Bootp or IP helpers configured on each gateway. These helpers forward DHCP requests from devices in each subnet to the DHCP server, allowing the DHCP server to respond to devices in that subnet.

### Comparing Preboot Services Setups in LAN and WAN/VLAN Environments

The following illustrates the differences for a LAN configuration between installing Preboot Services on the same server as DHCP, or on a separate server. In this case, only the PXE devices on the LAN connect to the Preboot Services imaging server.

**Table 23-3** LAN Configuration Differences Between Same and Separate Servers

Information	On the Same Server	On Separate Servers
Configuration	<p>Because Preboot Services and DHCP are running on the same server, option tag 60 must be set on the DHCP server.</p> <p>For information on setting this tag, see <a href="#">“Configuring LAN Environments for Preboot Services” on page 252</a>.</p>	None required.
Advantages	<ul style="list-style-type: none"> <li>♦ Easy installation and setup.</li> <li>♦ No network configuration is required.</li> </ul>	<ul style="list-style-type: none"> <li>♦ Easiest installation and setup.</li> <li>♦ No network configuration is required.</li> <li>♦ No DHCP server configuration is required.</li> </ul>
Disadvantages	<ul style="list-style-type: none"> <li>♦ DHCP server configuration is required (option tag 60).</li> <li>♦ Limited use, because a single-LAN environment only exists in small lab-type networks.</li> </ul>	<ul style="list-style-type: none"> <li>♦ Limited use, because a single-LAN environment only exists in small lab-type networks.</li> </ul>

The following illustrates the differences for a WAN/VLAN configuration between installing Preboot Services on the same server as DHCP, or on a separate server. In this case, all PXE devices over the entire WAN/VLAN connect to the Preboot Services imaging server.

**Table 23-4** WAN/VLAN Configuration Differences Between Same and Separate Servers

Information	On the Same Server	On Separate Servers
Configuration	<p>The routers/switches have been configured with IP helpers to forward network traffic to the DHCP server.</p> <p>Because Preboot Services and DHCP are running on the same server, option tag 60 is set on the DHCP server.</p> <p>For information on setting this tag, see <a href="#">“Configuring a WAN/VLAN with Preboot Services and DHCP Running on the Same Server” on page 253</a>.</p>	<p>A DHCP relay agent or IP helper is configured on the router/switch serving the subnet that the PXE device belongs to. The helper is configured to forward all DHCP broadcasts that are detected in the subnet to the DHCP and Proxy DHCP servers.</p> <p>This normally requires two helpers to be configured: the first to forward DHCP broadcasts to the DHCP server, and the second to forward the DHCP broadcasts to the Proxy DHCP server.</p>
Advantages	<ul style="list-style-type: none"><li>◆ No network equipment (routers/switches) needs to be configured to forward network traffic to the TFTP server.</li></ul>	<ul style="list-style-type: none"><li>◆ Common network setup.</li><li>◆ Multiple Preboot Services imaging servers can be installed so that each server provides service only for certain subnets.</li></ul>
Disadvantages	<ul style="list-style-type: none"><li>◆ DHCP server configuration required (option tag 60).</li><li>◆ Only one Preboot Services imaging server can be installed because it needs to run on the same server as the DHCP server (and there is usually only one DHCP server).</li></ul>	<ul style="list-style-type: none"><li>◆ The network equipment (routers/switches) must be configured with additional IP helpers. Some network equipment might not function properly when more than one additional IP helper is configured.</li></ul>

## Configuring LAN Environments for Preboot Services

For the case where you have Preboot Services and DHCP running on separate servers, no network configuration is required.

For the case where you have Preboot Services and DHCP are running on the same server, option tag 60 must be set on the DHCP server. Do the following to set up standard DHCP and Proxy DHCP on the same server:

- 1 Stop the DHCP services on the Linux imaging server.
- 2 On this server, open the `dhcp.conf` file in an editor.
- 3 Insert the following line in the file:  
`option vendor-class-identifier "PXEClient";`
- 4 Save the file.
- 5 Restart the DHCP service.

## Configuring a WAN/VLAN with Preboot Services and DHCP Running on the Same Server

You can install ZENworks Linux Management (which includes Preboot Services) on the same server where DHCP is installed and running. However, you must do the following to make it work:

- ♦ Set option tag 60 on the DHCP server so that it can work with the novell-proxydhcp daemon. See the steps in the previous section ([“Configuring LAN Environments for Preboot Services” on page 252](#)).
- ♦ On the Linux server, edit the `/etc/opt/novell/novell-proxydhcp.conf` file and change:

```
LocalDHCPFlag = 0
```

to

```
LocalDHCPFlag = 1
```

Then restart the daemon so that the change is recognized by entering the following command on the Linux server:

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

---

**IMPORTANT:** If the switch is acting as a firewall and limiting the type of traffic on the network, understand that the novell-tftp and novell-zmgprebootpolicy daemons are not firewall or network filter friendly. You should not attempt to run these daemons through a firewall. If users need to pass preboot work through a firewall, then all Preboot Services work needs to be on the outside and merely reference a Web service inside the firewall.

---

## Configuring a WAN/VLAN With Preboot Services and DHCP Running on Separate Servers

You can install ZENworks Linux Management (which includes Preboot Services) on a separate server than where DHCP is installed and running. However, you must configure the network equipment so that it correctly forwards Preboot Services network traffic.

---

**IMPORTANT:** If the switch is acting as a firewall and limiting the type of traffic on the network, understand that the novell-tftp and novell-zmgprebootpolicy daemons are not firewall or network filter friendly. You should not attempt to run these daemons through a firewall. If users need to pass preboot work through a firewall, then all Preboot Services work needs to be on the outside and merely reference a Web service inside the firewall.

---

An example deployment is given below of a WAN/VLAN environment with Preboot Services and DHCP running on the same server. The following sections provide the specific steps required to configure network equipment so that it correctly forwards Preboot Services network traffic.

### Example Deployment

In this example, three VLANs are configured on a Bay Networks Accel 1200 switch running firmware version 2.0.1. One VLAN hosts the Proxy DHCP server, the second VLAN hosts the DHCP server, and the third VLAN hosts the PXE device. The PXE device's DHCP broadcast is forwarded by the switch to both the Proxy DHCP server and the DHCP server. The response from both servers is then routed correctly back to the PXE device, and the PXE device starts the Preboot Services session correctly.

The three VLANs are all 24-bit networks; their subnet mask is 255.255.255.0.

The first VLAN gateway is 10.0.0.1. This VLAN hosts the PXE device that is allocated an IP in the range of 10.0.0.2 to 10.0.0.128. This VLAN is named VLAN1.

The second VLAN gateway is 10.1.1.1. This VLAN hosts the DHCP server with IP 10.1.1.2. This VLAN is named VLAN2.

The third VLAN gateway is 196.10.229.1. This VLAN hosts the server running novell-proxydhcp and novell-zmgprebootpolicy. The server's IP is 196.10.229.2. This VLAN is named VLAN3.

Routing is enabled between all VLANs. Each VLAN must be in its own spanning tree group.

### Configuring Cisco Equipment

- 1 Go to the Global configuration mode.
- 2 Type `ip forward-protocol udp 67`, then press Enter.
- 3 Type `ip forward-protocol udp 68`, then press Enter.
- 4 Go to the LAN interface that serves the PXE device.
- 5 Type `ip helper-address 10.1.1.2`, then press Enter.
- 6 Type `ip helper-address 196.10.229.2`, then press Enter.
- 7 Save the configuration.

### Configuring Nortel Network Equipment

- 1 Connect to the router with Site Manager.
- 2 Ensure that IP is routable.
- 3 Enable the *Bootp* check box on the PXE device subnet/VLAN.
- 4 Select the interface that the PXE devices are connected to.
- 5 Edit the circuit.
- 6 Click *Protocols*.
- 7 Click *Add/Delete*.
- 8 Ensure there is a check mark in the *Bootp* check box.
- 9 Click *OK*.
- 10 Click *Protocols > IP > Bootp > Relay Agent interface table*.  
The interface where Bootp was enabled is visible in the list.
- 11 Click *Preferred server*.
- 12 Change the *Pass through mode* value to Bootp and DHCP.
- 13 Set up the relay agents:
  - 13a Click *Add*.
  - 13b In the *Relay agent IP address* box, type the local LAN IP address.
  - 13c In the *Target server IP address* box, type the DHCP server IP address.
  - 13d Click *OK*.
  - 13e Change the *Pass through mode* value to Bootp and DHCP.
  - 13f Perform **Step 1** to **Step 5** again and specify the Proxy DHCP server IP address at **Step 3**.

**13g** Apply the configuration.

## Configuring Bay Network Equipment

Perform the following steps on the switch:

- 1 Enable DHCP for the client VLAN using the following command lines:

```
# config vlan1 ip
# dhcp enable
```

- 2 Configure IP helpers to forward DHCP requests from the device subnet to the TFTP server, using the following command lines:

```
# config ip dhcp-relay
# create 10.0.0.1 10.1.1.2 mode dhcp state enable
# create 10.0.0.1 196.10.229.2 mode dhcp state enable
```

The create command has the form `create agent server mode dhcp state enable`, where *agent* is the IP address of the gateway that serves the PXE device, and *server* is the IP address of the server that the DHCP frame should be forwarded to.

- 3 Save the configuration.

## Configuring Filters on Switches and Routers

Some network devices filter network traffic that passes through them. Preboot Services makes use of several different types of traffic, and all of these must be able to successfully pass through the router or switch for the Preboot Services session to be successful. The Preboot Services session uses the following destination ports:

**Table 23-5** Destination Ports for Preboot Services

Component	Port
DHCP and Proxy DHCP servers	UDP Port 67, 68, and 4011
TFTP server	UDP Port 69
novell-zmgprebootpolicy	UDP Port 13331

**IMPORTANT:** If the switch is acting as a firewall and limiting the type of traffic on the network, understand that the novell-tftp and novell-zmgprebootpolicy daemons are not firewall or network filter friendly. You should not attempt to run these daemons through a firewall. If users need to pass preboot work through a firewall, then all Preboot Services work needs to be on the outside and merely reference a Web service inside the firewall.

## Spanning Tree Protocol in Switched Environments

The spanning tree protocol (STP) is available on certain switches and is designed to detect loops in the network. When a device (typically a network hub or a device) is patched into a port on the switch, the switch indicates to the device that the link is active, but instead of forwarding frames from the port to the rest of the network, the switch checks each frame for loops and then drops it. The switch can remain in this listening state from 15 to 45 seconds.

The effect of this is to cause the DHCP requests issued by PXE to be dropped by the switch, causing the Preboot Services session to fail.

It is normally possible to see that the STP is in progress by looking at the link light on the switch. When the device is off, the link light on the switch is obviously off. When the device is turned on, the link light changes to amber, and after a period of time changes to a normal green indicator. As long as the link light is amber, STP is in progress.

This problem only affects PXE devices that are patched directly into an Ethernet switch. To correct this problem, perform one of the following:

- ♦ Turn off STP on the switch entirely.
- ♦ Set STP to Port Fast for every port on the network switch where a PXE device is attached.

After the problem is resolved, the link light on the port should change to green almost immediately after a device connected to that port is turned on.

Information about STP and its influence on DHCP can be found at [Using PortFast and Other Commands to Fix End-Station Startup Connectivity Problems \(http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg\\_v1/tr1923.htm#xtocid897350\)](http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/tr1923.htm#xtocid897350).

### 23.3.3 Administering Preboot Services

This section includes information about administering and configuring Preboot Services:

- ♦ “Configuring Preboot Services Imaging Servers in Linux” on page 256
- ♦ “Configuring IP Port Usage” on page 258

#### Configuring Preboot Services Imaging Servers in Linux

In Preboot Services, the daemons do not use switches. Instead, to configure a daemon to do something that is not a default, you need to edit the configuration files.

You can edit configuration files while the daemon is running, because they are only read when the daemon starts. Therefore, after editing the file you must restart the daemon for the changes to take effect.

For more information on the daemon configuration files, see [Section B.7, “Imaging Server,” on page 414](#).

The following sections explain how to configure the following ZENworks Linux Management imaging servers:

- ♦ “Configuring the TFTP Server” on page 257
- ♦ “Configuring the Proxy DHCP Server” on page 257
- ♦ “Configuring the Novell-pbserv Daemon” on page 257
- ♦ “Configuring Novell-zmgprebootpolicy” on page 258
- ♦ “Configuring the DHCP Server” on page 258



## Configuring the TFTP Server

It is seldom necessary to change the default TFTP server configuration values. If you need to change them, use the following procedure:

- 1 Open the following file in an editor:  
`/etc/opt/novell/novell-tftp.conf`
- 2 Edit the configuration settings per instructions within the file.
- 3 Save the changes.
- 4 In a shell console, enter the following command:  
`/etc/init.d/novell-tftp restart`

## Configuring the Proxy DHCP Server

The Proxy DHCP server provides PXE devices with the information that they require to be able to connect to the Preboot Services system.

Use the following steps to modify the settings of novell-proxydhcp:

- 1 Open the following file in an editor:  
`/etc/opt/novell/novell-proxydhcp.conf`
- 2 Edit the configuration settings per instructions within the file.
- 3 Save the changes.
- 4 In a shell console, enter the following command:  
`/etc/init.d/novell-proxydhcp restart`

You can set any of the IP address fields in the configuration utility to 0.0.0.0. The server replaces these entries with the IP address of the first network adapter installed in the server.

## Configuring the Novell-pbserv Daemon

The novell-pbserv daemon provides imaging services to the devices.

Use the following steps to modify the settings of novell-pbserv:

- 1 Open the following file in an editor:  
`/etc/opt/novell/zenworks/preboot/novell-pbserv.conf`
- 2 Edit the configuration settings per instructions within the file.
- 3 Save the changes.
- 4 In a shell console, enter the following command:  
`/etc/init.d/novell-pbserv restart`

## Configuring Novell-zmgprebootpolicy

The novell-zmgprebootpolicy daemon is used to check if there are any imaging actions that need to be performed on the device. It forwards requests to novell-pbserv on behalf of PXE devices.

Use the following steps to modify the settings of novell-zmgprebootpolicy:

- 1 Open the following file in an editor:  
`/etc/opt/novell/zenworks/preboot/novell-zmgprebootpolicy.conf`
- 2 Edit the configuration settings per instructions within the file.
- 3 Save the changes.
- 4 In a shell console, enter the following command:  
`/etc/init.d/novell-zmgprebootpolicy restart`

## Configuring the DHCP Server

The DHCP server needs to have option 60 (decimal) added to the DHCP tags if the Proxy DHCP and DHCP servers are running on the same physical server. This option should be a string type and must contain the letters PXEClient.

For more information, see [“Configuring LAN Environments for Preboot Services” on page 252](#).

## Configuring IP Port Usage

This section describes the network ports used by Preboot Services. Using the information in this section, you can configure routers to correctly forward the network traffic generated by Preboot Services. For further information about configuring routers, see [Section 23.3.2, “Deploying Preboot Services In a Network Environment,” on page 248](#).

Preboot Services uses both well-known and proprietary IP ports.

The well-known IP ports include:

- ♦ **67 decimal:** The Proxy DHCP server listens on this port for PXE information requests. This is the same port used by a standard DHCP server.
- ♦ **68 decimal:** The DHCP/Proxy DHCP server responds to client requests on this port. This is the same port used by a standard DHCP server.
- ♦ **69 decimal:** The TFTP server listens on this port for file requests from PXE devices.
- ♦ **4011 decimal:** When running on the same server as the DHCP daemon, the Proxy DHCP server listens on this port for PXE information requests.

The proprietary IP ports include:

- ♦ **998 decimal:** novell-pbserv client connection port. The novell-pbserv daemon receives all connection requests from the Preboot Services devices on this port.
- ♦ **13331 decimal:** novell-zmgprebootpolicy client connection port. The novell-zmgprebootpolicy daemon receives all connection requests from the PXE devices on this port.

While PXE devices make their initial requests to the novell-tftp and novell-zmgprebootpolicy daemons on the ports listed above, the remainder of the transactions can occur on any available port. For this reason, imaging servers cannot be separated from their clients by a firewall.

---

**IMPORTANT:** The novell-tftp and novell-zmgprebootpolicy daemons are not firewall or network filter friendly. You should not attempt to run these daemons through a firewall. If users need to pass preboot work through a firewall, then all Preboot Services work needs to be on the outside and merely reference a Web service inside the firewall.

---

### 23.3.4 Editing the Preboot Services Menu

Depending on the configuration settings for Preboot Services in the ZENworks Control Center, PXE devices may be able to display the Preboot Services Menu during the boot process. The menu has the following options:

*Start ZENworks Imaging*  
*Start ZENworks Imaging Maintenance*  
*Disable the ZENworks Partition*  
*Enable the ZENworks Partition*  
*Exit*

For more information on configuring whether to display the menu, see [Section 23.4.1, “Configuring Preboot Menu Options,” on page 262](#).

There might be circumstances when you want to modify the options on the Preboot Services Menu. You can customize these options by editing a text file contained on the imaging server. For example, you can:

- ♦ Add, delete, and modify menu options
- ♦ Change the color scheme
- ♦ Change the menu title and screen name

The following procedure should be done on each imaging server where you want to customize the menu.

To edit the Preboot Services Menu:

- 1 In a text editor, open the following file on an imaging server where novell-proxydhcp is running:

`/srv/tftp/pxemenu.txt`

---

**IMPORTANT:** If you want to save the default options for this menu, we recommend that you make a backup copy of `pxemenu.txt`, such as `pxemenu_orig.txt`.

---

A `pxemenu65.txt` file also exists for use by ZENworks 6.5 PXE devices that attach to ZENworks 7 servers through Preboot Services server referrals (see [Section 22.3.6, “Preboot Referral Lists,” on page 222](#)). Its content and format is the same as `pxemenu.txt`, so instructions in this section apply equally to `pxemenu65.txt`, except where data is different for ZENworks 6.5.

The following is the content of the default Preboot Services Menu's pxemenu.txt file:

```
#This file describes a PXEMenu

ScreenName = Novell Preboot Services Menu
ScreenInfo = Version 1.1 July, 2005
MenuTitle = ZENworks Preboot Options

#The screen colors determine the color of the main part of the menu
screen
ScreenColor = bright_white
ScreenBackgroundColor = blue

#The info colors determine the color of the screen information at
the top
#of the menu screen
InfoColor = yellow
InfoBackgroundColor = blue

#The hint colors determine the color of the hint line at the bottom
of the screen
HintColor = lt_cyan
HintBackgroundColor = blue

#The menu colors determine the color of the menu box and menu title
MenuColor = yellow
MenuBackgroundColor = blue

#The option colors determine the color of the menu option
OptionColor = BRIGHT_WHITE
OptionBackgroundColor = BLUE

#The chosen colors determine the color of the high-lighted option
ChosenColor = BRIGHT_WHITE
ChosenBackgroundColor = RED

#Maximum of 9 menu items
MenuOptionCount = 5

option1 = Start ZENworks Imaging
option2 = Start ZENworks Imaging Maintenance
option3 = Disable ZENworks Partition
option4 = Enable ZENworks Partition
option5 = Exit

CFG1 = z_auto.cfg
CFG2 = z_maint.cfg
CFG3 = z_zpdis.cfg
CFG4 = z_zpen.cfg
CFG5 = 0

Hint1 = ZENworks Imaging in Automated Mode
Hint2 = ZENworks Imaging Linux Session in Interactive Mode
Hint3 = Disable Existing ZENworks Partition
```

Hint4 = Re-enable a Disabled ZENworks Partition  
Hint5 = Boot to Local Hard Drive

- 2 To change the appearance of the menu, edit the first seven sections (title and colors).

To change colors, the mnemonics you enter must be selected from the following:

BLACK	RED	GRAY	LT_GREEN
BLUE	MAGENTA	YELLOW	LT_CYAN
GREEN	BROWN	BRIGHT_WHITE	LT_RED
CYAN	WHITE	LT_BLUE	LT_MAGENTA

- 3 To change the menu options, edit the last four sections, beginning with “MenuOptionCount.”

The menu options, their code, and their hint descriptions are correlated by the number (see “#” where used below).

**MenuOptionCount:** This number must match the total number of options defined in the next three sections. The limit is 9 menu options.

**option#:** Displayed in the menu as the option’s text.

**CFG#:** The configuration file that is used upon selecting the menu option.

**Hint#:** Displayed in the bottom of the screen to explain the highlighted menu option’s function. It changes as you highlight a menu option.

---

**IMPORTANT:** If you add or subtract a menu option, make sure that you do the same thing to each of the last three sections. The numbering should be consecutive (such as 1 through 5). Be sure to keep the corresponding items matched in each of the last three sections.

---

- 4 When finished, save the `pxemenu.txt` file.

## 23.4 Configuring Preboot Services Defaults

You can configure Preboot Services default settings for a ZENworks Management Zone. These are settings that apply globally to all devices in the management zone.

Some of these settings enable you to automatically register devices with the ZENworks Linux Management server, and some can be overridden by configurations done for devices or folders containing devices. For more information, see [Section 23.5, “Overriding Preboot Services Defaults,”](#) on page 280.

The following default settings can be configured in the ZENworks Control Center:

- ♦ [Section 23.4.1, “Configuring Preboot Menu Options,”](#) on page 262
- ♦ [Section 23.4.2, “Configuring Image Storage Security,”](#) on page 263
- ♦ [Section 23.4.3, “Configuring Non-registered Device Settings,”](#) on page 265
- ♦ [Section 23.4.4, “Configuring Preboot Work Assignments,”](#) on page 268
- ♦ [Section 23.4.5, “Configuring the Server Referral List,”](#) on page 275
- ♦ [Section 23.4.6, “Configuring Intel Active Management Technology \(AMT\),”](#) on page 276

## 23.4.1 Configuring Preboot Menu Options

To determine whether the Preboot Services Menu should be displayed on your devices when they boot:

- 1 In the ZENworks Control Center, click the *Configuration* tab, which displays the following Management Zone Settings section:

Management Zone Settings			⌵
Category	Description	Is Configured	
<a href="#">System Variables</a>	Configure system variables.	Yes	
<a href="#">Device Refresh Schedule</a>	Configure the device refresh interval.	No	
<a href="#">Device Inventory</a>	Configure inventory settings.	No	
<a href="#">Local Device Logging</a>	Enable and configure local logging of warnings and errors encountered by managed devices.	Yes	
<a href="#">Preboot Services</a>	Configure Preboot Services.	Yes	
<a href="#">Remote Management</a>	Enable and configure remote management.	Yes	
<a href="#">Centralized Message Logging</a>	Configuration of settings related to logging performed by the central server.	Yes	
<a href="#">Content Replication Schedule</a>	Configuration of the refresh schedule used for replicating content between ZENworks servers.	Yes	
<a href="#">Platforms</a>	Configuration of the available target platforms.	Yes	

- 2 In this section, click *Preboot Services* to display the configuration sections.
- 3 Locate the Preboot Menu Options section:

**Preboot Menu Options** ⌵

Determine if the Preboot eXecution Environment (PXE) menu should be displayed when a client boots.

☐ Always show Preboot menu

☐ Never show Preboot menu

☒ Show Preboot menu if CTRL+ALT pressed

- 4 Select one of the following:

*Always Show Preboot Menu*

*Never Show Preboot Menu*

*Show Preboot Menu if CTRL+ALT Pressed*

- 5 Click either *Apply* or *OK* to save the change.

This sets the default Preboot Services Menu display mode for the ZENworks Management Zone. This can be overridden at the folder or device level. For more information, see [Section 23.5, “Overriding Preboot Services Defaults,”](#) on page 280.

---

**IMPORTANT:** PXE must be enabled on the device for the menu to be displayed.

---

The Preboot Services menu provides options for how Preboot Services can be used on your devices. The following options are presented when the menu is displayed:

**Table 23-6** *Preboot Services Menu Options*

Menu Option	Function
<i>Start ZENworks Imaging</i>	Executes the assigned Preboot Services imaging bundles.
<i>Start ZENworks Imaging Maintenance</i>	Displays the bash prompt, where you can execute imaging commands.
<i>Disable ZENworks Partition</i>	Prevents an existing ZENworks partition from being used when booting to execute the assigned Preboot bundles.
<i>Enable ZENworks Partition</i>	Allows an existing ZENworks partition to be used when booting to execute the assigned Preboot bundles.
<i>Exit</i>	Resumes booting of the device without doing any Preboot bundle work.

Generally, if your Preboot Services work is completely automated, you should select to never display the Preboot Menu on the device when it boots. Conversely, if you need to do manual Preboot Services functions for some or all devices, then select to always display the menu. A compromise is where you select to display the menu if Ctrl+Alt is pressed, allowing unattended Preboot Services work while allowing you the opportunity to display the menu when needed.

## 23.4.2 Configuring Image Storage Security

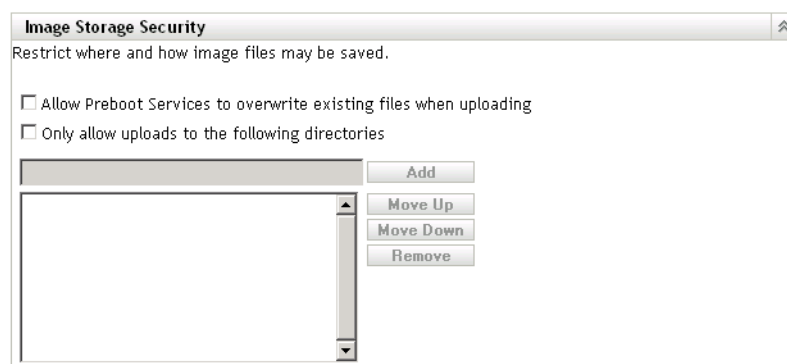
To determine the degree of security you want with respect to saving image files:

- 1 In the ZENworks Control Center, click the *Configuration* tab, which displays the following Management Zone Settings section:

Management Zone Settings		
Category	Description	Is Configured
<a href="#">System Variables</a>	Configure system variables.	Yes
<a href="#">Device Refresh Schedule</a>	Configure the device refresh interval.	No
<a href="#">Device Inventory</a>	Configure inventory settings.	No
<a href="#">Local Device Logging</a>	Enable and configure local logging of warnings and errors encountered by managed devices.	Yes
<a href="#">Preboot Services</a>	Configure Preboot Services.	Yes
<a href="#">Remote Management</a>	Enable and configure remote management.	Yes
<a href="#">Centralized Message Logging</a>	Configuration of settings related to logging performed by the central server.	Yes
<a href="#">Content Replication Schedule</a>	Configuration of the refresh schedule used for replicating content between ZENworks servers.	Yes
<a href="#">Platforms</a>	Configuration of the available target platforms.	Yes

- 2 In this section, click *Preboot Services* to display the configuration sections.

**3** Locate the Image Storage Security section:



**4** Select one or both of the following options:

**Allow Preboot Services to overwrite existing files when uploading:** Select this option only if you want existing image files to be overwritten during imaging.

**Only allow uploads to the following directories:** This option allows you to determine where images can be restored on the imaging server.

Specify a full path to the directory in the *Add* field, then click *Add* to enter it into the list box. These are the directories where images are allowed to be saved on the imaging server. These are the locations that can be selected when configuring where to store image files.

Use *Move up* or *Move down* to rearrange the order of the locations, including the order of the imaging servers that are listed.

To remove a directory path from the listing, select the path and click *Remove*. You can select multiple paths for removing.

**5** Click either *Apply* or *OK* to save the changes.

This sets the default image storage settings for the ZENworks Management Zone.



## 23.4.3 Configuring Non-registered Device Settings

The following configurations can be set after a device is imaged. The settings are applied to devices not registered in the ZENworks Management Zone.

For more information, see [Section 22.3.4, “Non-registered Device Settings,” on page 220](#).

To configure default ID settings for non-registered devices:

- 1 In the ZENworks Control Center, click the *Configuration* tab, which displays the following Management Zone Settings section:

Management Zone Settings			
Category	Description	Is Configured	
<a href="#">System Variables</a>	Configure system variables.	Yes	
<a href="#">Device Refresh Schedule</a>	Configure the device refresh interval.	No	
<a href="#">Device Inventory</a>	Configure inventory settings.	No	
<a href="#">Local Device Logging</a>	Enable and configure local logging of warnings and errors encountered by managed devices.	Yes	
<a href="#">Preboot Services</a>	Configure Preboot Services.	Yes	
<a href="#">Remote Management</a>	Enable and configure remote management.	Yes	
<a href="#">Centralized Message Logging</a>	Configuration of settings related to logging performed by the central server.	Yes	
<a href="#">Content Replication Schedule</a>	Configuration of the refresh schedule used for replicating content between ZENworks servers.	Yes	
<a href="#">Platforms</a>	Configuration of the available target platforms.	Yes	

- 2 In this section, click *Preboot Services* to display the configuration sections.
- 3 Locate the Non-Registered Device Settings section:

Non-Registered Device Settings

Configuration settings to apply to non-registered devices after an image has been restored.

DNS Suffix:

Name Servers:  

Add

Move Up

Move Down

Remove

Device Name:  

☐ Use Prefix:

☐ Use BIOS Asset Tag

☐ Use BIOS Serial Number

☒ Do not automatically assign a name

IP Configuration:  

☐ Use DHCP

☒ Specify Address List:

#### 4 Fill in the fields:

**DNS suffix:** Provides a suffix for all of your device's names.

For example, if you enter "provo.novell.com" and a device's name is "device1," that device's full name becomes "device1.provo.novell.com."

**Name servers:** To control what DNS servers the device uses, specify a DNS name server, then click *Add* to place it into the listing.

So that a booting device can find a name server efficiently, specify multiple DNS name servers.

For optimal availability of a DNS server for a device, you can rearrange the order using *Move up* and *Move down*, one name server entry at a time.

You can delete multiple name servers by selecting them and clicking *Remove*.

**Device name:** You can determine the default device names for non-registered devices. The name is applied after the device is imaged.

This can be useful for when you have multiple devices to be imaged. You can automatically provide unique names for each device (from its BIOS asset tag or its BIOS serial number), as well as group devices by providing the same prefix for their names.

Options:

- ♦ **Use prefix: \_\_\_\_:** This provides a common prefix to the device names, such as Lab1 to distinguish them from the devices in Lab2. This can be useful when doing bulk imaging of certain groups of devices. It is limited to 8 characters.

If this option is used, the prefix you enter here is appended with a random string of letters and numbers to make the device name 15 characters long. Underscores and hyphens are valid in your prefix. The remaining random string uniquely names the device.

For example, if you enter Lab1\_, then ten other characters are randomly generated to complete the name with Lab1 separated from the random characters by the underscore for readability.

- ♦ **Use BIOS asset tag:** This is the asset tag stored in the device's BIOS, which is unique for every device. This can be useful for tracking a device based on its asset tag.
- ♦ **Use BIOS serial number:** This is the serial number stored in the device's BIOS, which is unique for every device. This can be useful for tracking a device based on its serial number.
- ♦ **Do not automatically assign a name:** Select this option if you do not want to use any of the above. This is the default option.

**IP configuration:** You can select either *Use DHCP* or *Specify address List* to identify devices for Preboot Services work.

IP Configuration:

☐ Use DHCP

☒ Specify Address List:

Subnet Mask:

Default Gateway:

IP Addresses Available for Machines:

Start and end of IP Address Range  
(leave end of range field empty for single IP address entry)

to

Add

Move Up

Move Down

Remove

IP Addresses Currently Assigned:

These are the settings that the device is told to use after it is imaged. It uses them for Preboot Services work any time it reboots.

- ♦ **Use DHCP:** Select to use DHCP, which allows the devices to be dynamically assigned IP addresses.
- ♦ **Specify address list:** You can use IP addresses to identify your devices. The addresses you add to the list are available to be used by your devices. This way, you can specify a range of IP addresses or individual IP addresses that you want your devices to use. For example, you can ensure that all of your lab devices use addresses between 10.0.0.5 and 10.0.0.25.

If you select this option, the following fields are displayed:

**Subnet mask:** (Optional) For assigning devices to a specific subnet mask.

**Default gateway:** (Optional) For assigning devices to a specific gateway for access to the Internet or network after the device is imaged and rebooted.

**IP addresses available for machines:** According to the information you provide in this section, this list box displays the available IP addresses for your devices to use.

**Start and end of IP address range:** Do either of the following:

- ♦ Specify one IP address at a time in the first field and click *Add* each time to place it into the list box.
- ♦ Specify a range of IP addresses and click *Add* to place them into the list box. Each IP address in a range is listed independently, allowing you to selectively remove any of them from within the range.

You can select multiple IP addresses for removal.

**IP addresses currently assigned:** This display-only list box shows which IP addresses from the IP Addresses Available for Machines list have been assigned to a device. When they are displayed here, they are no longer displayed in the list box above.

After a device is imaged, IP settings are applied to the device. The IP address that is assigned to the imaged device is no longer in the available list, but is instead listed in this currently assigned list.

- 5 Click either *Apply* or *OK* to save the changes.

This sets the default device ID method for the ZENworks Management Zone.

## 23.4.4 Configuring Preboot Work Assignments

This section allows you to set up Preboot work assignments for your defined bundles for non-registered devices, or registered devices that do not have an effective bundle defined.

In this section of the Preboot Services page, you can set up rules for your Preboot bundles. Work assignment rules are hardware keys used to determine which bundle should be applied to which device. When a device is seeking work to be done, it scans the rules until it finds a rule where all of the rule's filters match the device, then executes the bundle assigned to the rule.

For more information, see [Section 22.3.5, “Preboot Work Assignment Rules,”](#) on page 220.

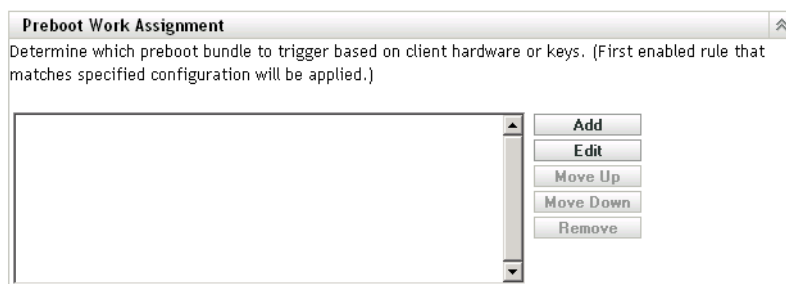
To configure work assignment rules:

- 1 In the ZENworks Control Center, click the *Configuration* tab, which displays the following Management Zone Settings section:

Management Zone Settings			
Category	Description	Is Configured	
<a href="#">System Variables</a>	Configure system variables.	Yes	
<a href="#">Device Refresh Schedule</a>	Configure the device refresh interval.	No	
<a href="#">Device Inventory</a>	Configure inventory settings.	No	
<a href="#">Local Device Logging</a>	Enable and configure local logging of warnings and errors encountered by managed devices.	Yes	
<a href="#">Preboot Services</a>	Configure Preboot Services.	Yes	
<a href="#">Remote Management</a>	Enable and configure remote management.	Yes	
<a href="#">Centralized Message Logging</a>	Configuration of settings related to logging performed by the central server.	Yes	
<a href="#">Content Replication Schedule</a>	Configuration of the refresh schedule used for replicating content between ZENworks servers.	Yes	
<a href="#">Platforms</a>	Configuration of the available target platforms.	Yes	

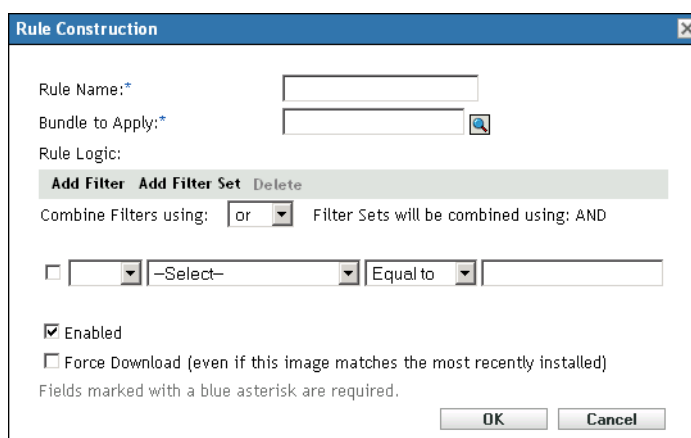
- 2 In this section, click *Preboot Services* to display the configuration sections.

### 3 Locate the Preboot Work Assignment section:



### 4 Click *Add* to configure a rule.

The information configured in the Rule Construction dialog box comprises one rule. You can add multiple rules. The rules are used to determine whether there is a device that should have any preboot work done. If so, it only does the effective preboot work assigned to it.



### 5 In the Rule Construction dialog box, provide a name for the work rule in the *Rule name* field.

This is the name that is displayed in the rules listing on the Preboot Services page in the Preboot Work Assignment section. Make it descriptive enough that you can later remember its purpose.

### 6 In the *Bundle to apply* field, browse for or specify the bundle where you want to apply this rule.

Each rule can be applied to only one bundle. However, you can apply multiple rules to a bundle.

When a device boots and searches the Preboot Work Assignment section for work, if the device meets a rule's criteria, the rule's applicable bundle is applied to the device.

Because the rules, not the bundles, are listed in the Preboot Work Assignment section, you can apply multiple rules to a given bundle. In that case, such a bundle has multiple chances to be selected for preboot work.

When multiple rules are listed, the first rule to have criteria to match a device causes that rule's assigned bundle to be applied to the device.

If no rules match a device, then the effective bundle is not applied to the device.

## 7 Review the following to understand how to configure the work rule logic:

Rule Construction

Rule Name:\*

Bundle to Apply:\*

Rule Logic:

Add Filter Add Filter Set Delete

Combine Filters using: and Filter Sets will be combined using: OR

☐ [ ] -Select- Equal to [ ] and

☐ [ ] -Select- Equal to [ ]

OR

☐ [ ] -Select- Equal to [ ]

OR

☐ [ ] -Select- Equal to [ ] and

☐ [ ] -Select- Equal to [ ] and

☐ [ ] -Select- Equal to [ ]

☒ Enabled

☐ Force Download (even if this image matches the most recently installed)

Fields marked with a blue asterisk are required.

OK Cancel

A rule is made up of one or more filters that are used to determine whether a device complies with the rule. The Rule Construction dialog box begins with one empty filter. A device must match the entire filter list of a rule (as determined by the logical operators that are explained below) for the rule to apply to the device.

A filter is a row of fields providing a condition that must be met by a device in order for the bundle to be applied. For example, you can add a filter to specify that the device must have exactly 512 MB of RAM in order to be accepted by the rule, and you can add another filter to specify that the hard drive be at least 20 GB in size. There is no technical limit to the number of filters that you can add in the rule, but there are practical limits, such as:

- ♦ Designing a rule that is easy to understand
- ♦ Devising the rule so that you do not accidentally create conflicting filters
- ♦ Being able to view the dialog box as it grows in size because of the filters that you add

Filters can be added individually or in sets. Each set contains logical operators within the set. The logical operator OR is displayed by default for the filters within a set in the *Combine filters using* field, which you can change, and AND is displayed in the *Filter sets will be combined using* field, which is display-only. In other words, the logical operator that is used within a set must be opposite the operator that is used between the sets.

You can think of filters and filter sets using algebraic notation parentheses, where filters are contained within parentheses, and sets are separated into a series of parenthetical groups. Logical operators (AND and OR) separate the filters within a the parentheses, and the operators are used to separate the parentheticals.

For example, “(u AND v AND w) OR (x AND y AND z)” means “match either uvw or xyz.” In the Rule Construction dialog box, this looks like:

u AND  
v AND  
w  
OR

x AND  
y AND  
z

Filter sets cannot be nested. You can only enter them in series, and the first filter set to match the device is used to validate using the applied bundle to do preboot work on the device. Therefore, the order they are listed does not matter. You are simply looking for a match to cause the bundle to be applied to the device.

---

**TIP:** You can easily run a test to see how these logical operators work. Access the Rule Construction dialog box, click both the *Add filter* and *Add filter set* options a few times each to create a few filter sets, then switch between AND and OR in the *Combine filters using* field and observe how the operators change. Click *Cancel* to exit the Rule Construction dialog box when you are finished.

---

You can set up the conditions for a rule by adding all of the filters and filter sets that you need to identify the type of device you want to match. You typically do not need to set up complex rules. However, because you can apply multiple rules to a bundle, you can further complicate the use of logical operators, because each rule is considered to be an OR condition for the bundle, causing the bundle to be applied if any one of the rules matches the device. Therefore, keep in mind the OR condition of multiple rules for a bundle when designing your rules.

For example, you could create several rules for the bundle with each rule being a long listing of AND conditions to be met. Therefore, each rule becomes a specific set of criteria for a device to meet, causing the bundle to be applied if one is met. Conversely, if you have that same amount of information in one rule (using filter sets for the AND and OR conditions), it might make the dialog box so long that it becomes unmanageable.

To determine whether you need one filter set with multiple filters, multiple filter sets with only one or a few filters per set, multiple filter sets each with multiple filters, or even multiple rules per bundle, remember that the logical operators for filters within a set are the opposite of the operators between the sets, and all rules for a bundle use the OR condition. For example, when selecting the operator in the *Combine filters using* field:

---

Operator Selected	Within Filter Sets	Between Filter Sets	Multiple Rules Per Bundle
OR	Only one filter in the set needs to apply to the device (OR condition). The first filter that applies is used.	Each filter set must have one filter in it that applies to the device (AND condition).	The first rule that applies is used (OR condition).
AND	All filters within the set must apply to the device (AND condition).	Only one filter in the set must apply to the device (OR condition). The first filter that applies is used.	The first rule that applies is used (OR condition).

---

Obviously, adding filter sets complicates the use of logical operators, and adding multiple rules to the bundle further complicates it. Therefore, carefully plan how to place your information before using this dialog box.

**8** To add or remove filters and filter sets, select from the following:

- ♦ **Add filter:** Adds one filter (a row of fields) after the last filter in this dialog box.

Subsequent clicks of the *Add filter* option add those filters to the end of the current set, which is the last listed filter set when there are multiple filters in the set (see **Add Filter Set** below). You cannot insert a new filter between existing filters.

The order of the filters in a set does not matter, and you cannot reorder the filters after you have created them. What matters in this structure is properly grouping the filters with respect to the selected *OR* and *AND* operator options.

- ♦ **Add filter set:** Adds the next filter as a filter set with either *AND* or *OR* placed between the filter sets, as dictated by your selection in the *Combine filters using* field.

To create filter sets, first click *Add filter set*, then click *Add filter* as many times as necessary to add filters into that set.

You cannot insert filter sets between existing filter sets.

- ♦ **Delete:** Deletes any filters that are selected (see **Check Box** below in **Step 10**).

**9** To determine the filter and filter set logic, select *AND* or *OR* from the *Combine filters using* drop-down list.

The logical operator you select here determines which operator is used within the filter sets. The operator for this field applies to multiple sets.

To provide multiple sets for the rule, indicate whether the sets should all be required (select *AND*) or are all optional (keep *OR*). If *OR*, then the values in only one of the sets need to match the device for the rule to apply. If *AND*, then all values in the entire rule must match the device for the rule to apply.

If you only have one filter set (which could contain several filters), *AND* is the default logical operator within the set, because *OR* defaults in the *Combine filters using* field, which you can change.

*Filter sets will be combined using* is a display-only field. When providing multiple sets for the rule, this field displays the opposite logical operator from the one you select for the *Combine filters using* field.

To require all filters within a filter set, but only one of the filter sets, select *OR* in the *Combine filters using* field. To require all filter sets, but only one of the filters within each set, select *AND* in the *Combine filters using* field.

**10** To configure rule filters, fill in the fields:

- ♦ **Check box:** Selects filters for deletion.
- ♦ **Drop-down list:** If blank, this field means to do as worded in the filter. If you select *NOT*, it means to do the opposite of what the filter says.

For example, if you select *NOT* and the RAM size is configured to be “less than 512 MB,” then the device must have at least 512 MB of RAM for the bundle to be applied. In other words, the filter reads “not less than 512 MB of Ram.” Conversely, if you configured it as “more than 512 MB,” then left the field blank, any computer containing exactly 512 MB of RAM is excluded, which you might not intend. So, be sure that you think the logic through for your filter configurations with respect to whether you use *NOT*.



- ♦ **Device component:** A drop-down list provides the various items available for matching on the device in order to determine whether the work rule applies for the bundle. The options are:

BIOS Asset Tag  
 BIOS Serial Number  
 BIOS Version  
 CPU Chipset  
 Hard Disk Controller  
 Hard Drive Size (in MB)  
 IP Address  
 MAC Address  
 Network Adapter  
 RAM (in MB)  
 Sound Card  
 System Manufacturer  
 Video Adapter

If the drop-down list on the left displays NOT, then the work rule is stating that the device should not match the component as described in the next two fields.

- ♦ **Relationship to:** This defines the relationship for a filter between the *Device component* field listed above and the value provided in the *Value for the component* field.

The possible options for the *Hard drive size* and *RAM* fields are:

< (less than)  
 > (greater than)  
 = (equal to)  
 >= (greater than or equal to)  
 <= (less than or equal to)  
 <> (not equal to)

For all other components, the options are:

Contains  
 Equal To  
 Starts With

If the drop-down list on the left displays NOT, then the work rule is stating that the component does the opposite. For example, does NOT Contain, is NOT Equal To, does NOT Start With, is NOT >, is NOT >=, is NOT =, is NOT <>, and so on.

- ♦ **Value for the component:** Enter the information that exactly describes the device component's value that the device must match to accept the rule. For example, 512 could be entered for the *RAM* field value in *Device component* field, meaning the device must have that amount of RAM, or more or less, depending on the selections you make in the other fields in the filter.

---

**IMPORTANT:** Be aware of the possibility of creating conflicting filters. For example, if the *RAM (in MB)* field is used in multiple filters, make sure the effective logical operators where each is used make sense for the MB values that you enter. You could have one filter requiring exactly 512 MB of RAM and another accepting a device having at least 512 MB

of RAM. If those filters are both required for the device to match the rule (this is with the AND condition existing between them), you'd have a conflict that causes the filter to fail its purpose.

---

- 11** Because you can create multiple rules to be listed here, and the information configured in the Rule Construction dialog box comprises one rule, repeat **Step 8** through **Step 10** as necessary.

- 12** To enable this work rule, select the check box for the *Enabled* field.

After you exit this dialog box, you can see whether the work rule is enabled by viewing the work rules listing on the Preboot Services page.

To enable or disable a rule after creating it, you must edit the work rule from the Preboot Services page.

- 13** To force the image to be reapplied to the device, select the check box for the *Force download* field.

By default, ZENworks imaging does not reimage a machine containing the same image. This option allows you to force the image to be reapplied to the device. For example, you might want to refresh all of your lab machines for the next use of the lab.

---

**IMPORTANT:** Use this option cautiously, because you can create an endless loop when the option remains selected after an image is applied. If you image a device that remains non-registered after it is imaged, it is reimaged with the same image over and over each time it boots. To prevent this, after you have imaged the applicable devices, deselect this option.

---

- 14** After exiting the Rule Construction dialog box, you can manipulate the order and existence of the listed rules:

**Edit:** Opens the Rule Construction dialog box in edit mode.

**Move up/down:** After adding rules, you can change the order in which they are to be executed. You can only move one rule at a time. This order is important because the first rule that is found in the listing to match the device is used to apply the bundle, and the remainder of the rules are ignored.

**Remove:** Removes the selected rules.

- 15** Click either *Apply* or *OK* to save the changes.

## 23.4.5 Configuring the Server Referral List

Referral lists are used to make sure managed devices belonging to other ZENworks Management Zones can access their home zone. For more information, see [Section 22.3.6, “Preboot Referral Lists,” on page 222](#).

To set up referral lists:

- 1 In the ZENworks Control Center, click the *Configuration* tab, which displays the following Management Zone Settings section:

Management Zone Settings		
Category	Description	Is Configured
<a href="#">System Variables</a>	Configure system variables.	Yes
<a href="#">Device Refresh Schedule</a>	Configure the device refresh interval.	No
<a href="#">Device Inventory</a>	Configure inventory settings.	No
<a href="#">Local Device Logging</a>	Enable and configure local logging of warnings and errors encountered by managed devices.	Yes
<a href="#">Preboot Services</a>	Configure Preboot Services.	Yes
<a href="#">Remote Management</a>	Enable and configure remote management.	Yes
<a href="#">Centralized Message Logging</a>	Configuration of settings related to logging performed by the central server.	Yes
<a href="#">Content Replication Schedule</a>	Configuration of the refresh schedule used for replicating content between ZENworks servers.	Yes
<a href="#">Platforms</a>	Configuration of the available target platforms.	Yes

- 2 In this section, click *Preboot Services* to display the configuration sections.
- 3 Locate the Server Referral List section:

**Server Referral List**

List the servers outside the zone that can host preboot operations.

*It is sometimes useful to have multiple servers assigned to handle imaging tasks. For example, one server hosting PXE services, while another is used to store image files. Refer to the documentation for further examples and a full description of this feature.*

List of Server IP Addresses and DNS Names

Add

Move Up

Move Down

Remove

- 4 Specify the ZENworks Linux Management servers:

**List of server IP addresses and DNS names:** Specify the DNS name or IP address of a server that can host Preboot operations, then click *Add* to place the server into the referral list.

**Move up/Move down:** Arranges the order in which the servers are contacted. You can move only one server at a time.

**Remove:** To remove a server from the list, select the server, then click *Remove*.

- 5 Click either *Apply* or *OK* to save the changes.

- 6 Depending on the ZENworks version of the server, do the following to copy the necessary files from the ZENworks Linux Management imaging server to your `\tftp` directory on the servers in your referral list:

ZENworks Version	Files to Copy	Action
ZENworks 6.5	<code>/svr/tftp/z_auto65.cfg</code> <code>/svr/tftp/pxelinux.0</code>	Copy the files.
ZENworks 7 (running on a NetWare or Windows server)	<code>/svr/tftp/z_auto.cfg</code> <sup>1</sup> <code>/svr/tftp/pxelinux.0</code>	Copy both of the files, but rename <code>z_auto.cfg</code> to <code>z_auto65.cfg</code> .

<sup>1</sup> This file may not contain the same information as `/svr/tftp/z_auto65.cfg`, so that when you rename it with the 65, it may have different content than the file used for ZENworks 6.5 servers. Therefore, for ZENworks 7 do not simply copy the `z_auto65.cfg` file instead of renaming the `z_auto.cfg` file.

No files need to be copied for servers running the following ZENworks versions:

ZENworks 7 (running on a Linux server)  
ZENworks 7 Linux Management

## 23.4.6 Configuring Intel Active Management Technology (AMT)

To set up global Intel AMT enterprise names:

- “Downloading and Installing the iAMT Redirection Drivers” on page 276
- “Provisioning the AMT Devices” on page 277
- “Setting Up the Global Intel AMT Enterprise Names” on page 279

### Downloading and Installing the iAMT Redirection Drivers

After a device has had its AMT resources provisioned, those resources can be accessed locally by the ZENworks implementation of AMT. However, before you can provision a device’s resources, you need to install the iAMT Redirection Drivers from Intel. You can do this on one device, then send the result to the other devices that need the drivers, as outlined in the steps below.

The following are required to be installed and operational on the device where you initially install the drivers:

- The Linux kernel source
- GCC (gnu c compiler)

To download and install the device drivers:

- 1 In a Web browser, access [Intel\(R\) PRO/10/100/1000/10GbE Drivers](http://sourceforge.net/projects/e1000/) (<http://sourceforge.net/projects/e1000/>) on the SourceForge Web site.
- 2 Click the green *Download Intel(R) PRO/10/100/1000/10GbE Drivers* option.
- 3 In the *Latest File Releases* section, select the *iAMT Redirection Drivers* option.
- 4 Click the green *Download* option.

- 5 In the *Filename* column under *iAMT Redirection Drivers*, click the *iamt-1.1.8.tar.gz* option (or later version) and save the file to a location on your network.
- 6 Unzip the *.tar.gz* file and decompress the *iamt-1.1.8.tar* (or later version) file.
- 7 To install the drivers, follow the instructions contained in the *Readme* file that is contained in the *.tar* file.  
This creates binaries of the drivers.
- 8 After following the instructions to compile the iAMT Redirect Drivers, make RPMs of the binaries, then distribute the RPMs to the other devices that need the drivers.  
For more information, see [Chapter 16, “Using RPM Bundles,” on page 153](#).

## Provisioning the AMT Devices

You can provision your AMT devices in either of two ways:

- ♦ [“Provisioning in Enterprise Mode” on page 277](#)
- ♦ [“Provisioning in Small Business Mode” on page 277](#)

### Provisioning in Enterprise Mode

If you use another AMT-enabled application that requires the AMT devices to be provisioned in Enterprise mode, do the following:

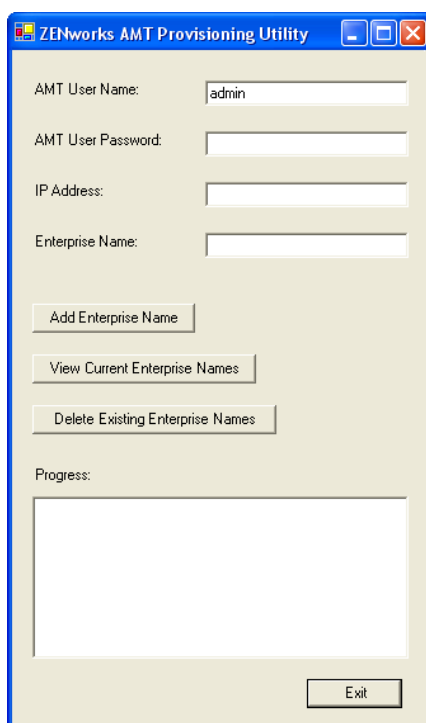
- 1 During the boot process for a device, access the AMT BIOS.  
Refer to your device’s documentation for instructions.
- 2 When prompted, enter the device’s AMT administrator username and password.  
You are required to change the administrator username and password before you can proceed.  
See your computer documentation for instructions on changing the password.
- 3 Set the provisioning mode to “Enterprise.”
- 4 Configure the other settings as appropriate.  
Refer to your device’s or AMT-enabled application’s documentation for instructions.
- 5 Configure the provisioning server supplied with the application to assign at least one enterprise name to the device.  
Refer to your AMT-enabled application’s documentation for instructions.
- 6 Repeat [Step 1](#) through [Step 5](#) for each device to be provisioned with the Enterprise mode.
- 7 To provide the provisioned enterprise names to ZENworks Linux Management, continue with [Section , “Setting Up the Global Intel AMT Enterprise Names,” on page 279](#).

### Provisioning in Small Business Mode

To provision an AMT device in small business mode for use with ZENworks Linux Management, do the following:

- 1 During the boot process for a device, access the AMT BIOS.  
Refer to your device’s documentation for instructions.

- 2** When prompted, enter the device's AMT administrator username and password.  
You are required to change the administrator username and password before you can proceed.  
See your computer documentation for instructions on changing the password.
- 3** Set the provisioning mode to "Small Business."
- 4** Configure the other settings as appropriate.  
Refer to your device's documentation for instructions.
- 5** If you configured the AMT device to use DHCP mode for IP addressing, you might need to boot the device into an operating system to discover a currently valid IP address.  
You can use the ZENworks Linux Management imaging CD or DVD for this, if necessary.  
Boot from the CD or DVD, select the ZENworks Maintenance Mode, then at the bash prompt enter `ifconfig eth0`. This provides the currently assigned IP address.
- 6** Run `/opt/novell/zenworks/zdm/imaging/winutils/smb-provisioning.exe` on a Windows XP workstation running .NET framework to display the following dialog box:



This must be run on a different device than is being provisioned.

- 7** Fill in the fields:
  - 7a** Enter the appropriate administrator account and passwords in their respective fields.  
This is the same as you entered in **Step 2**.
  - 7b** Enter the currently valid IP address for the device.
  - 7c** Enter an enterprise name.  
Intel suggests that the enterprise name be chosen to indicate the device's general location.  
For example, all the devices in the home office may be given an enterprise name of

“Company\_HQ,” and all devices in field offices may be given enterprise names reflecting their geographical locations.

While it is not required, it is assumed that large numbers of devices will have the same enterprise name. Each AMT device itself may have up to four different enterprise names.

You can use the *View Current Enterprise Names* or the *Delete Existing Enterprise Names* to manage the names in the *Progress* list box.

- 8 Select *Add Enterprise Name*, then click *Exit*.

This adds the defined enterprise name into the *Progress* list box and to the device.

- 9 Repeat **Step 1** through **Step 8** for each device to be provisioned with the Small Business mode.
- 10 To provide the provisioned enterprise names to ZENworks Linux Management, continue with **Section , “Setting Up the Global Intel AMT Enterprise Names,” on page 279.**

## Setting Up the Global Intel AMT Enterprise Names

The Intel AMT functionality allows you to accurately identify devices, even if they have had physical drive replacements. This sets up Preboot Services with persistent device identification by providing ZENworks with nonvolatile memory for storing the unique device identity.

For more information, see **Section 22.3.7, “Intel Active Management Technology (AMT),” on page 222.**

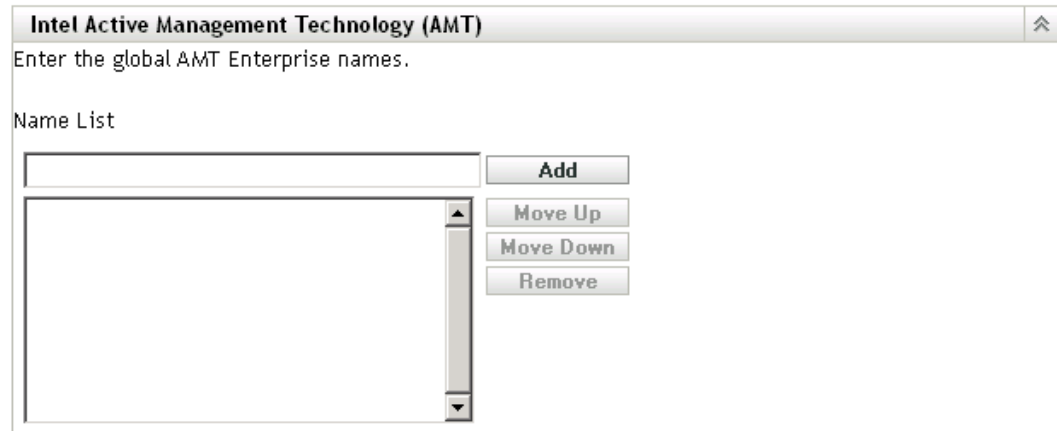
To configure Intel AMT for Preboot Services:

- 1 In the ZENworks Control Center, click the *Configuration* tab, which displays the following Management Zone Settings section:

Management Zone Settings			⌵
Category	Description	Is Configured	
<a href="#">System Variables</a>	Configure system variables.	Yes	
<a href="#">Device Refresh Schedule</a>	Configure the device refresh interval.	No	
<a href="#">Device Inventory</a>	Configure inventory settings.	No	
<a href="#">Local Device Logging</a>	Enable and configure local logging of warnings and errors encountered by managed devices.	Yes	
<a href="#">Preboot Services</a>	Configure Preboot Services.	Yes	
<a href="#">Remote Management</a>	Enable and configure remote management.	Yes	
<a href="#">Centralized Message Logging</a>	Configuration of settings related to logging performed by the central server.	Yes	
<a href="#">Content Replication Schedule</a>	Configuration of the refresh schedule used for replicating content between ZENworks servers.	Yes	
<a href="#">Platforms</a>	Configuration of the available target platforms.	Yes	

- 2 In this section, click *Preboot Services* to display the configuration sections.

- 3 Locate the Intel Active Management Technology (AMT) section:



- 4 Fill in the fields:

**Name list:** Enterprise names are given to AMT devices when they are provisioned. This list should contain at least one valid AMT enterprise name for every AMT device in the ZENworks Management Zone. Click *Add* to place each one into the list box.

**Move up/Move down:** Arranges the order in which the AMT names are listed. You can move only one at a time.

**Remove:** To remove a name from the list, select the name, then click *Remove*.

- 5 Click either *Apply* or *OK* to save the changes

## 23.5 Overriding Preboot Services Defaults

You can determine which Preboot Services Menu displays a configuration to use and whether the menu should be displayed on a device when it boots. By default, the ZENworks Management Zone configuration applies to all folders and devices. You can override this at the folder or device level.

For more information on the Preboot Services Menu options, see [Section 22.3.2, “Preboot Services Menu,” on page 219](#).

The Preboot Services Menu can be customized by editing the `pxemenu.txt` file. For more information, see [Section 23.3.4, “Editing the Preboot Services Menu,” on page 259](#).

To override the default configuration at the folder or device level:

- 1 In the ZENworks Control Center, click the *Devices* tab to display the Devices page:

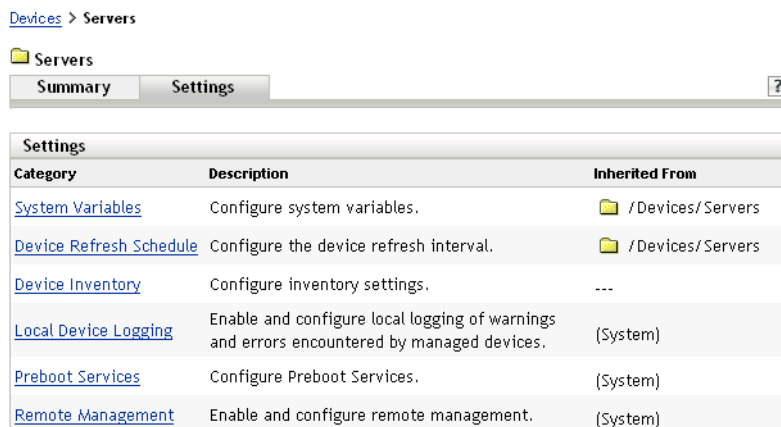




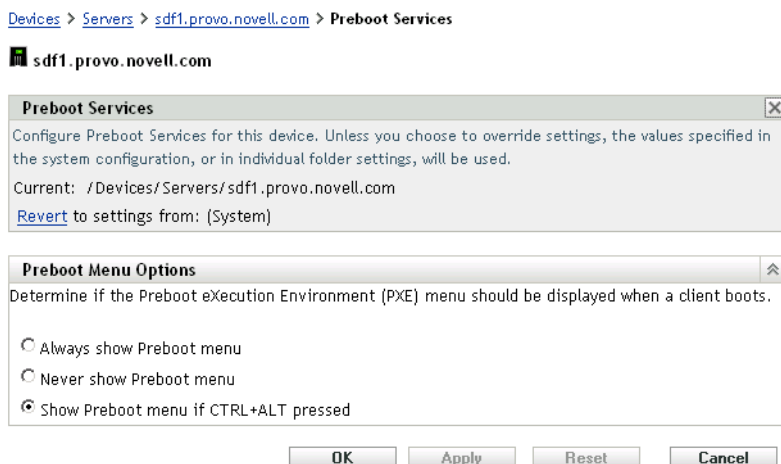
2 Select one of the following on this page:

- ♦ The *Details* option next to the *Servers* or *Workstations* folder
- ♦ The *Servers* folder, then a server contained in the folder
- ♦ The *Workstations* folder, then a workstation contained in the folder

3 On the page that is displayed, click the *Settings* tab to display the Settings section options:



4 Click *Preboot Services* to display the Preboot Services configuration page:



If you have not previously configured for this folder or device, the following is displayed:

Current: (System) (Override settings)

and the Preboot Menu Options section is disabled for editing. The above text varies depending on whether you are at the folder or device level.

5 To configure the settings for the folder or device, click *Override*.

The following is displayed:

Current: /Devices/Servers

Revert to settings from: (System)

and the Preboot Menu Options section is enabled for editing. The above text varies depending on whether you are at the folder or device level.

- 6 Select which option to use:

*Always Show Preboot Menu*

*Never Show Preboot Menu*

*Show Preboot Menu if CTRL+ALT is Pressed*

---

**IMPORTANT:** PXE must be enabled on the device for the menu to be displayed.

---

- 7 Click *Apply* or *OK*.

**OK:** Enables the change and exits the page.

**Apply:** Enables the change and retains focus on the page, so you can click *Revert* to temporarily disable the configuration change.

- 8 To temporarily disable the change, click *Revert* and the ZENworks Management Zone settings for the menu remain in effect.

## 23.6 Enabling PXE on Devices

To image a device using Preboot Services, you need to find out if the device is PXE capable, and then make sure that PXE is enabled.

PXE code is typically delivered with newer devices (PC 99 compliant or later) on the NIC.

This section includes the following information:

- ♦ [Section 23.6.1, “Enabling PXE on a PXE-Capable Device,” on page 282](#)
- ♦ [Section 23.6.2, “Verifying That PXE Is Enabled on a Device,” on page 283](#)

### 23.6.1 Enabling PXE on a PXE-Capable Device

When PXE is enabled, it can lengthen the time of the boot process slightly, so most NICs have PXE turned off by default. To enable PXE on a PXE-capable device:

- 1 Access the computer system BIOS and look at the *Boot Sequence* options.

The PXE activation method for a device varies from one manufacturer to another, but generally one of the following methods is used:

- ♦ Some BIOSs have a separate entry in the BIOS configuration to enable or disable the PXE functionality. In this case, set either the *PXE boot* setting or the *Network boot* setting to Enabled.
- ♦ Some BIOSs extend the entry that allows you to configure boot order. For example, you can specify that the system should try to boot from a diskette before trying to boot from the hard drive. In this case, set the system to try *Network boot* before trying to boot from a diskette or from the hard disk.

- 2 If PXE is not listed in the *Boot Sequence* options and if the NIC is embedded in the motherboard, look at the Integrated Devices section of the BIOS, which might have an option to enable PXE. PXE might be called by another name, such as MBA (Managed Boot Agent) or Pre-Boot Service.

After enabling PXE in the Integrated Devices section, look at the *Boot Sequence* options and move PXE so that it is first in the boot sequence.

- 3 Save any changes you have made and exit the system BIOS.

#### 4 Reboot the device.

If the device does not have the network adapter and PXE integrated into the motherboard, it uses the installed NIC management software to prompt you to start PXE configuration during the boot process.

For example, many network adapters that are PXE-aware prompt you to press Control+S during the boot process to allow you to configure the PXE functionality. Other network adapters might prompt you to press Control+Alt+B or another key combination to configure PXE.

If the computer system does not have an integrated NIC, you might need to use NIC management software to configure your NIC to support PXE. Refer to your NIC documentation for support of PXE.

### 23.6.2 Verifying That PXE Is Enabled on a Device

After you have activated PXE, it becomes available in the Boot section of the BIOS. PXE is correctly enabled on a device when the device attempts to establish a PXE session during the boot process. You can see this happening when the device pauses during the boot process and displays the following on the screen:

```
CLIENT MAC ADDR: 00 E0 29 47 59 64
DHCP...
```

The actual message displayed varies from one manufacturer to another, but you can identify it by the obvious pause in the boot process as the device searches for DHCP.

## 23.7 Setting Up Devices for Imaging

The following sections cover procedures to prepare devices for imaging. The procedures that are applicable to you depend on your imaging deployment strategy. For more information, see [Section 23.3.2, “Deploying Preboot Services In a Network Environment,” on page 248.](#)

If you are using Preboot Services (PXE) as your imaging method, you need to enable PXE on the device. For more information, see [Section 23.2.1, “Using Preboot Services \(PXE\),” on page 240.](#)

If you are using a ZENworks partition as your imaging method, you need to create the partition on the device. For more information, see [“Creating a ZENworks Partition” on page 245.](#)

The following sections contain additional information:

- ♦ [Section 23.7.1, “Device Requirements,” on page 284](#)
- ♦ [Section 23.7.2, “Enabling a Device for Imaging Operations,” on page 284](#)

## 23.7.1 Device Requirements

This section gives the requirements for using a network-connected device.

It is possible (but usually not as convenient) to image a device without connecting to the network. Such operations can't be fully automated.

The following are the requirements for the device:

**Table 23-7** *Device Requirements*

Device Must Have	Because
A supported Ethernet card	The device must connect with the imaging server to store or retrieve the images. This connection is made when the device is under the control of the ZENworks Imaging Engine. Therefore, make sure the device has a supported Ethernet card. For more information, see <a href="#">“Supported Ethernet Cards” on page 455</a> .
Free disk space for a ZENworks partition (optional)	Unless you are using PXE, unattended operations require a ZENworks partition to be installed on the device hard disk, so that the ZENworks Imaging Engine can gain control when booting. The default partition size is 150 MB, and the minimum partition size is 50 MB. This partition is not required if you are performing manual imaging operations using bootable CDs, DVDs, or diskettes. Partition size can be in megabytes of disk space.
Standard hardware architecture	NEC* PC98 architecture is not supported.
PXE enabled	If you are using Preboot Services, PXE must be enabled in the BIOS. For more information, see <a href="#">Section 23.2.1, “Using Preboot Services (PXE),” on page 240</a> .
Supported imaging partition type	The only supported partition types for imaging are the ReiserFS, Ext2, and Ext3 file systems.

**NOTE:** ZENworks Linux Management imaging does not support devices running boot managers, such as System Commander. Boot managers create their own information in the MBR and overwrite the ZENworks boot system, which prevents the device from communicating with the imaging server. If you are using boot managers in your environment, you should disable or remove them before performing imaging operations.

## 23.7.2 Enabling a Device for Imaging Operations

Use one of the following methods to enable a device for auto-imaging operations:

- ♦ [“Using PXE” on page 285](#)
- ♦ [“Using a ZENworks Partition” on page 285](#)
- ♦ [“Using a CD or DVD” on page 285](#)

## Using PXE

You can set up a device to be automatically imaged from Preboot bundles by enabling PXE on the device.

For more information, see [Section 23.6.1, “Enabling PXE on a PXE-Capable Device,” on page 282.](#)

## Using a ZENworks Partition

If you cannot enable PXE on the device, this procedure allows you to perform unattended imaging operations.

For more information, see [“Creating a ZENworks Partition” on page 245.](#)

## Using a CD or DVD

If you cannot use the PXE or ZENworks partition methods to automate imaging of your devices, you can manually image a device using an imaging CD or DVD.

For information, see [Section 24.3.3, “Setting Up Disconnected Imaging Operations,” on page 314.](#)



This section provides instructions on how to use Novell® ZENworks® Linux Management Preboot Services:

- ♦ [Section 24.1, “Configuring AutoYaST or Kickstart Installation Script Bundles,” on page 287](#)
- ♦ [Section 24.2, “Configuring ZENworks Script Bundles,” on page 295](#)
- ♦ [Section 24.3, “Imaging Devices,” on page 298](#)
- ♦ [Section 24.4, “Multicasting Images,” on page 319](#)
- ♦ [Section 24.5, “Assigning Unassigned Preboot Bundles,” on page 330](#)
- ♦ [Section 24.6, “Editing Preboot Services Work,” on page 332](#)

## 24.1 Configuring AutoYaST or Kickstart Installation Script Bundles

The following sections explain how to create, configure, and assign AutoYaST and kickstart bundles:

- ♦ [Section 24.1.1, “Configuring an AutoYaST Bundle,” on page 287](#)
- ♦ [Section 24.1.2, “Configuring a Kickstart Bundle,” on page 292](#)

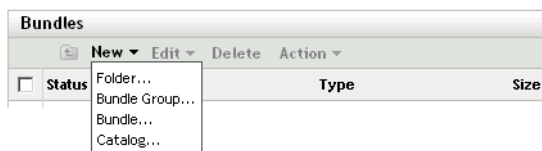
### 24.1.1 Configuring an AutoYaST Bundle

An AutoYaST bundle contains software for installing SUSE® Linux.

Use this wizard to create a new AutoYaST bundle. Using ZENworks Linux Management, you can install software using a bundle. Software included in a bundle that is assigned directly is considered mandatory; the software is installed on all assigned devices (the bundle is directly assigned to the devices, their groups, or their folders).

To configure an AutoYaST bundle and assign devices to the bundle:

- 1 In the ZENworks Control Center, click the *Bundles* tab to display the Bundles page:



- 2 Click *New > Bundle* to start the Create New Bundle Wizard:

[Bundles](#) > [Create New Bundle](#)

Create New Bundle ?

Step 1: Select Bundle type

Select the type of Bundle you wish to create from the list of options.

New Bundle Type:

☐ RPM Package Bundle

☒ Preboot Bundle

<< Back   Next >>   Cancel

- 3 In the Create New Bundle Wizard, select *Preboot bundle*, then click *Next* to display the Select Preboot Bundle Type page:

[Bundles](#) > [Create New Bundle](#)

Create New Bundle ?

Step 2: Select Preboot Bundle Type

Select the type of Preboot Bundle you wish to create from the list of options.

Preboot Bundle Type:

- AutoYaST Bundle
- Kickstart Bundle
- ZENworks Image Bundle
- ZENworks Multicast Bundle
- ZENworks Script Bundle

Type Description:

**AutoYaST Bundle** - Describes the location and access protocol of an AutoYaST script and network install directory for SUSE Linux. This bundle allows you to launch an automated installation of SUSE Linux using Preboot Services.

<< Back   Next >>   Cancel

- 4 On the Select Preboot Bundle Type page, select *AutoYaST bundle*, then click *Next* to display the Set General Information page:

[Bundles](#) > [Create New Bundle](#)

Create New Bundle ?

Step 3: Set General information

Name:

Folder:

/Bundles

Description:

<< Back   Next >>   Cancel

- 5 Fill in the fields:

**Name:** (Required) Although bundles can be identified in ZENworks Control Center by their type of icon, as well as the folder they are listed under, you should develop a naming scheme that differentiates the AutoYaST bundles that are listed together in a folder.



**Folder:** Browse for the location where you want the AutoYaST bundle to be displayed in ZENworks Control Center. The folder must exist. You cannot specify a non-existent folder, because ZENworks does not create them from this wizard.

**Description:** Provide a description to help you later recognize the exact purpose of this AutoYaST bundle.

**6** Click *Next* to display the Set AutoInstall Attributes page:

Bundles > Create New Bundle

Create New Bundle AutoYaST Bundle ?

Step 4: Set AutoInstall Attributes

Describe how to access the Linux boot files. These files should have been copied to the Preboot TFTP server from the CD.

Linux Kernel File:

(Path should be relative to the default directory of the TFTP daemon.  
e.g.: suse/pro9.1/linux)

Initial RAM Drive:

(Path should be relative to the default directory of the TFTP daemon.  
e.g.: suse/pro9.1/initrd)

<< Back Next >> Cancel

**7** Fill in the fields:

**Linux kernel file:** The path should be relative to the default directory of the novell-tftp daemon. For example, you might do the following:

1. Copy the kernel file, which might be located at `/boot/loader/linux` on a SLES 9 SP1 bootable CD.
2. Place the copy in a location on your imaging server. For example, `/srv/tftp/autoyast/linux`.
3. In this field, enter the path that is relative to the daemon. For example, `autoyast/linux`.

**Initial RAM drive:** The path should be relative to the default directory of the novell-tftp daemon. For example, you might do the following:

1. Copy the RAM drive file, which might be located at `/boot/loader/initrd` on a SLES 9 SP1 bootable CD.
2. Place the copy in a location on your imaging server. For example, `/srv/tftp/autoyast/initrd`.
3. In this field, enter the path that is relative to the daemon. For example, `autoyast/initrd`.

- 8 Click *Next* to display the next Set AutoInstall Attributes page:

[Bundles](#) > Create New Bundle

Create New Bundle AutoYaST Bundle ?

Step 5: Set AutoInstall Attributes

Protocol and IP address (or DNS name) required to access the network install directory:

NFS

Path to network install directory (relative to protocol):

(Path should be relative to the default directory of the selected protocol daemon. e.g.: suse/pro9.1)

---

<< Back Next >> Cancel

- 9 Fill in the fields:

**Protocol and IP address (or DNS name) required to access the network installation directory:** Select *NFS*, *FTP*, *HTTP*, or *TFTP* from the drop-down list, then specify the IP address or DNS name of the device containing the network installation directory..

**Path to the network installation directory (relative to protocol):** The path should be relative to the default directory of the selected protocol daemon.

For example, if you specify the HTTP protocol, enter *myserver.provo.novell.com* as the DNS name, and specify the path as */installs/scripts/myscript.cfg*, then the URL to the installation directory is *http://myserver.provo.novell.com/installs/scripts/myscript.cfg*, where */installs/scripts/myscript.cfg* is relative to the protocol and server ID.

- 10 Click *Next* to display the next Set AutoInstall Attributes page:

[Bundles](#) > Create New Bundle

Create New Bundle AutoYaST Bundle ?

Step 6: Set AutoInstall Attributes

Protocol and IP address (or DNS name) required to access the script:

NFS

AutoYaST Script name and path (Relative to protocol default directory):

(e.g.: autoyast.xml)

Additional Kernel Parameters:

---

<< Back Next >> Cancel

- 11 Fill in the fields:

**Protocol and IP address required to access the script:** Select *NFS*, *FTP*, *HTTP*, or *TFTP* from the drop-down list, then specify the IP address or DNS name of the device containing the script.

**AutoYaST script name and path (relative to the protocol default directory):** The path should be relative to the default directory of the selected protocol daemon.

For example, if you select the HTTP protocol, enter *myserver.provo.novell.com* as the DNS name, and enter the path and filename as */scripts/autoyast.xml*, then the URL to the installation directory is *http://myserver.provo.novell.com/scripts/autoyast.xml*, where */scripts/autoyast.xml* is relative to the protocol and server ID.

**Additional kernel parameters:** Specify additional kernel parameters. These are not Preboot Services or ZENworks parameters. They are parameters that your Linux kernel needs. For more information, see your Linux documentation.

**12** Click *Next* to display the Summary page:

[Bundles](#) > Create New Bundle

Create New Bundle	AutoYaST Bundle	?
Step 7: Summary		

Review the following information, and click 'Finish' to create the new Image Bundle.

Name:	AutoYaST Bundle
Preboot Bundle Type:	AutoYaST Bundle
Folder:	Bundles
Description:	AutoYaST Bundle
Linux Kernel File:	suse/pro9.1/linux
Initial RAM Drive:	suse/pro9.1/initrd
Install Directory:	NFS
	192.68.1.203
	suse/pro9.1
Protocol and IP address:	NFS
	192.68.1.203
AutoYaST Script name and path:	autoyast.xml
Additional Kernel Parameters:	

---

<< Back    Next >>    Finish    Cancel

**13** Review the configuration, then click one of the following:

**Back:** Allows you to make changes after reviewing the summary.

**Next:** Allows you to perform the following tasks before creating the bundle:

- ♦ Specify device assignments for this bundle
- ♦ Specify groups for this bundle

Continue with [Section 24.5, “Assigning Unassigned Preboot Bundles,” on page 330](#) to assign the bundle and complete the wizard.

**Finish:** Creates the AutoYaST bundle as configured per the settings listed on this Summary page.

This bundle is not assigned to any device or group after it is created, unless you click *Next* instead of *Finish* to make that assignment.

When any device assigned to the AutoYaST bundle boots, the bundle’s SUSE Linux installation work is performed on the device.

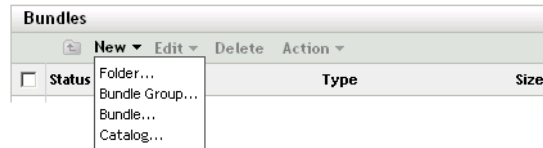
## 24.1.2 Configuring a Kickstart Bundle

A kickstart bundle contains software for installing Red Hat Linux.

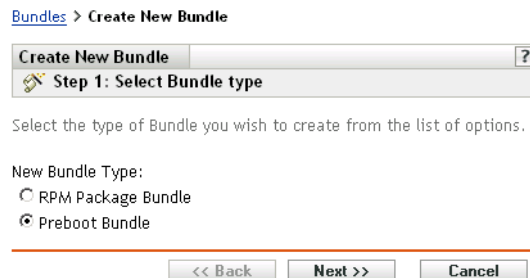
Using ZENworks Linux Management, you can install software using a bundle. Software included in a bundle that is assigned directly is considered mandatory; the software is installed on all assigned devices (the bundle is directly assigned to the devices, their groups, or their folders).

To configure a kickstart bundle and assign devices to the bundle:

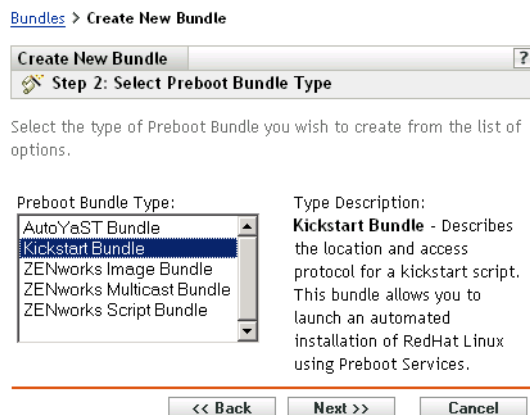
- 1 In the ZENworks Control Center, click the *Bundles* tab.



- 2 Click *New > Bundle* to start the Create New Bundle Wizard:



- 3 In the Create New Bundle Wizard, select *Preboot bundle*, then click *Next*.



- 4 On the Select Preboot Bundle Type page, select *Kickstart bundle*, then click *Next* to display the Set General Information page:

Bundles > Create New Bundle

Create New Bundle ?

Step 3: Set General information

Name:

Folder:

Description:

<< Back   Next >>   Cancel

- 5 Fill in the fields:

**Name:** (Required) Although bundles can be identified in ZENworks Control Center by their type of icon, as well as the folder they are listed under, you should develop a naming scheme that differentiates the kickstart bundles that are listed together in a folder.

**Folder:** Browse for the location where you want the kickstart bundle displayed in ZENworks Control Center. The folder must exist. You cannot specify a non-existent folder, because ZENworks does not create them from this wizard.

**Description:** Provide a description to help you later recognize the exact purpose of this kickstart bundle.

- 6 Click *Next* to display Set AutoInstall Attributes page:

Bundles > Create New Bundle

Create New Bundle ?

Step 4: Set AutoInstall Attributes

Describe how to access the Linux boot files. These files should have been copied to the Preboot TFTP server from the CD.

Linux Kernel File:

(Path should be relative to the default directory of the TFTP daemon.  
e.g.: redhat/8.0/vmlinuz)

Initial RAM Drive:

(Path should be relative to the default directory of the TFTP daemon.  
e.g.: redhat/8.0/initrd.img)

<< Back   Next >>   Cancel

- 7 Fill in the fields:

**Linux kernel file:** The path should be relative to the default directory of the novell-tftp daemon. For example, you might do the following:

1. Copy the kernel file, which might be located at `/isolinux/vmlinuz` on a Red Hat Enterprise Linux 4 bootable CD.

2. Place the copy in a location on your imaging server. For example, `/srv/tftp/kickstart/vmlinuz`.
3. In this field, enter the path that is relative to the daemon. For example, `kickstart/vmlinuz`.

**Initial RAM drive:** The path should be relative to the default directory of the novell-tftp daemon. For example, you might do the following:

1. Copy the RAM drive file, which might be located at `/isolinux/initrd.img` on a Red Hat Enterprise Linux 4 bootable CD.
2. Place the copy in a location on your imaging server. For example, `/srv/tftp/kickstart/initrd.img`.
3. In this field, enter the path that is relative to the daemon. For example, `kickstart/initrd.img`.

8 Click *Next* to display the next Set AutoInstall Attributes page:

Bundles > Create New Bundle

Create New Bundle kickstart Bundle ?

Step 5: Set AutoInstall Attributes

Protocol and IP address (or DNS name) required to access the configuration file:

NFS

Path to the kickstart configuration file (relative to the protocol default directory):

(e.g.: `config/ks.cfg`)

Additional Kernel Parameters:

<< Back Next >> Cancel

9 Fill in the fields:

**Protocol and IP address required to access the script:** Select *NFS* or *HTTP* from the drop-down list, then specify the IP address or DNS name of the device containing the script.

**Kickstart script name and path (relative to the protocol default directory):** The path should be relative to the default directory of the selected protocol daemon.

For example, if you select the HTTP protocol, enter *myserver.provo.novell.com* as the DNS name, and enter the path and filename as `/config/ks.cfg`, then the URL to the installation directory is `http://myserver.provo.novell.com/config/ks.cfg`, where `/config/ks.cfg` is relative to the protocol and server ID.

**Additional kernel parameters:** Specify additional kernel parameters. These are not Preboot Services or ZENworks parameters. They are parameters that your Linux kernel needs. For more information, see your Linux documentation.

10 Click *Next* to display the Summary page:

Bundles > Create New Bundle

Create New Bundle kickstart Bundle ?

Step 6: Summary

Review the following information, and click 'Finish' to create the new Image Bundle.

Name: kickstart Bundle

Preboot Bundle Type: Kickstart Bundle

Folder: Bundles

Description: Kickstart Bundle

Linux Kernel File: redhat/8.0/vmlinuz

Initial RAM Drive: redhat/8.0/initrd.img

Protocol and IP address: NFS

192.68.1.203

Kickstart Configuration File: config/ks.cfg

Additional Kernel Parameters:

<< Back Next >> Finish Cancel

11 Review the configuration, then click one of the following:

**Back:** Allows you to make changes after reviewing the summary.

**Next:** Click to perform the following tasks before creating the bundle:

- ♦ Specify device assignments for this bundle
- ♦ Specify groups for this bundle

Continue with [Section 24.5, “Assigning Unassigned Preboot Bundles,”](#) on page 330 to assign the bundle and complete the wizard.

**Finish:** Creates the kickstart bundle as configured per the settings listed on this Summary page.

This bundle is not assigned to any device or group after it is created, unless you click *Next* instead of *Finish* to make that assignment.

When any device assigned to the kickstart bundle boots, the bundle’s Red Hat installation work is performed on the device.

## 24.2 Configuring ZENworks Script Bundles

A ZENworks Script bundle can contain any ZENworks script.

Using ZENworks Linux Management, you can install software using a bundle. Software included in a bundle that is assigned directly is considered mandatory; the software is installed on all assigned devices (the bundle is directly assigned to the devices, their groups, or their folders).

To configure a ZENworks Script bundle and assign devices to the bundle:

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

Bundles

New Edit Delete Action

Folder... Bundle Group... Bundle... Catalog...

Status	Type	Size
--------	------	------

- 2 Click *New > Bundle* to start the Create New Bundle Wizard:

Bundles > Create New Bundle

Create New Bundle ?

Step 1: Select Bundle type

Select the type of Bundle you wish to create from the list of options.

New Bundle Type:

☐ RPM Package Bundle

☒ Preboot Bundle

<< Back   Next >>   Cancel

- 3 In the Create New Bundle Wizard, select *Preboot bundle*, then click *Next*.

Bundles > Create New Bundle

Create New Bundle ?

Step 2: Select Preboot Bundle Type

Select the type of Preboot Bundle you wish to create from the list of options.

Preboot Bundle Type:	Type Description:
<div>AutoYaST Bundle</div> <div>Kickstart Bundle</div> <div>ZENworks Image Bundle</div> <div>ZENworks Multicast Bundle</div> <div>ZENworks Script Bundle</div>	<b>ZENworks Script Bundle -</b> Allows you to write a custom Linux bash script that will be executed on preboot computers in Linux. This allows fine control over ZENworks imaging operations as well as almost any linux-based task imaginable.

<< Back   Next >>   Cancel


- 4 On the Select Preboot Bundle Type page, select *ZENworks Script bundle*, then click *Next* to display the Set General Information page:

Bundles > Create New Bundle

Create New Bundle ?

Step 3: Set General information

Name:

Folder:  
 

Description:

<< Back   Next >>   Cancel

- 5 Fill in the fields:

**Name:** (Required) Although bundles can be identified in ZENworks Control Center by their type of icon, as well as the folder they are listed under, you should develop a naming scheme that differentiates the ZENworks Script bundles that are listed together in a folder.



**Folder:** Browse for the location where you want the ZENworks Script bundle displayed in ZENworks Control Center. The folder must exist. You cannot specify a non-existent folder, because ZENworks does not create them from this wizard.

**Description:** Provide a description to help you later recognize the exact purpose of this ZENworks Script bundle.

6 Click *Next* to display the Preboot Bundle Creation page:

Bundles > Create New Bundle

Create New Bundle ZENworks Script Bundle ?

Step 4: Preboot Bundle Creation

Configure the preboot information

Script Text:

#!/bin/sh

<< Back Next >> Cancel

7 Fill in the fields:

**Script text:** Specify the text of the ZENworks script. The script is restricted to doing preboot work prior to the device booting.

For information on using this bundle to perform scripted imaging, see [“Imaging a Device Using a Script” on page 304](#).

8 Click *Next* to display the Summary page:

Bundles > Create New Bundle

Create New Bundle ZENworks Script Bundle ?

Step 5: Summary

Review the following information, and click 'Finish' to create the new Image Bundle.

Name: ZENworks Script Bundle

Preboot Bundle Type: ZENworks Script Bundle

Folder: Bundles

Description: ZENworks Script Bundle

Script Text: #!/bin/sh

<< Back Next >> Finish Cancel

9 Review the configuration, then click one of the following:

**Back:** Allows you to make changes after reviewing the summary.

**Next:** Click to perform the following tasks before creating the bundle:

- ◆ Specify device assignments for this bundle
- ◆ Specify groups for this bundle

Continue with [Section 24.5, “Assigning Unassigned Preboot Bundles,” on page 330](#) to assign the bundle and complete the wizard.

**Finish:** Creates the ZENworks Script bundle as configured per the settings listed on this Summary page.

This bundle is not assigned to any device or group after it is created, unless you click *Next* instead of *Finish* to make that assignment.

When a device assigned to the ZENworks Script bundle boots, the bundle's work is performed on the device before its operating system starts.

## 24.3 Imaging Devices

Preboot Services provides tools for creating and compressing images of device hard disks, as well as images of specific add-on applications or file sets. ZENworks Linux Management also provides tools for customizing such images and for making images available to auto-imaging operations.

You can take images of devices, reimage them with those images, and image other devices with the images. In ZENworks 7 Linux Management, the available devices are servers and workstations.

ZENworks Linux Management imaging supports devices that physically connect to the network that meet the minimum requirements for devices. ZENworks Linux Management imaging does not support imaging operations (creating or restoring images) using wireless connectivity.

---

**NOTE:** ZENworks Linux Management imaging does not support devices running boot managers, such as System Commander. Boot managers create their own information in the MBR and overwrite the ZENworks boot system, which prevents the device from communicating with the imaging server. If you are using boot managers in your environment, you should disable or remove them before performing imaging operations.

---

Some imaging tasks can be performed manually on a device, some in the ZENworks Control Center, and some in both:

- ♦ [Section 24.3.1, “Imaging Using the ZENworks Control Center,” on page 298](#)
- ♦ [Section 24.3.2, “Performing Manual Imaging Tasks,” on page 304](#)
- ♦ [Section 24.3.3, “Setting Up Disconnected Imaging Operations,” on page 314](#)

### 24.3.1 Imaging Using the ZENworks Control Center

The following imaging tasks are available in the ZENworks Control Center:

- ♦ [“Taking a Base Image of a Device” on page 298](#)
- ♦ [“Configuring the ZENworks Image Bundle for Automatic Imaging” on page 301](#)
- ♦ [“Imaging a Device Using a Script” on page 304](#)

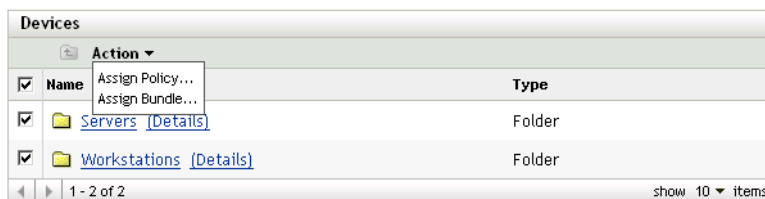
#### Taking a Base Image of a Device

A *base* image is an image of all partitions and data on a source device's hard disks. Normally, such an image is prepared with the intent to completely replace the contents of a target device's hard disks.

You can take an image of an existing device and use to image a similar device, or as a backup image for reimaging the device.

To take a base image of a device:

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



- 2 Click *Servers* or *Workstations*, then select the check box next to a device.

This selects the device for taking the image.

- 3 Click *Actions* > *Take image*.

You can also select the check box next to *Servers* or *Workstations* to start this wizard, then click *Actions* > *Take image*. If you do so, you are asked to select a device from the group. Then the File Information page is displayed.

- 4 Click *Next* to display the File Information page:


[Devices](#) > [Servers](#) > Take an Image

Take an Image sdf1.provo.novell.com ?

Step 1: File Information

Specify the server, path, and compression options for the new image file:

Server and File Path:\*



☒ Use compression:

- ☒ Balanced
- ☐ Optimize for speed
- ☐ Optimize for space

☐ Create an image bundle

Fields marked with a blue asterisk are required.

- 5 Fill in the fields:

**Server and file path:** (Required) Browse for the object, DNS name, or IP address of the server where the image file is to be stored, then specify the path to the storage location. This must be a server where ZENworks Linux Management is installed.

Images can take up a large amount of disk space. Make sure your imaging server has the disk space available before selecting it.

**Use compression:** Compression is required. Choose one of the following:

- ♦ **Balanced:** Automatically balances compression between an average of the reimaging speed and the available disk space for the image file.
- ♦ **Optimize for speed:** Optimizes the compression to allow for the fastest reimaging time. Use this option if CPU speed is an issue.
- ♦ **Optimize for space:** Optimizes the compression to minimize the image file's size to conserve disk space. This can cause reimaging to take longer.

**Create an image bundle:** If you select this option, another wizard page is displayed (see [Step 6](#)) where you can configure the new bundle. Otherwise, the Summary is your next wizard page (skip to [Step 9](#)).

- 6 If you selected to create an image bundle, the New Image Bundle page is displayed:


Devices > Servers > Take an Image

Take an Image sdf1.provo.novell.com ?

Step 2: New Image Bundle

Specify a name and a description for the new image bundle.

Name:

Destination Folder:  
 

Description:

---

<< Back Next >> Cancel

- 7 Fill in the fields:

**Name:** Specify a unique name for the bundle, because many other bundle names might be listed in its folder.

**Destination folder:** Specify a folder where you want to list the new bundle. This is a location in ZENworks Control Center, not a file location on a device.

**Description:** Enter information to help you later recognize the purpose and scope of this image bundle. For example, "Image taken after Linux OS was installed, but before GroupWise was installed."


- 8 Click *Next* to display the Summary page:

Devices > Servers > Take an Image

Take an Image sdf1.provo.novell.com ?

Step 3: Image File and Bundle Summary

Review the information and click 'Finish' to submit this task to the device and create the new image bundle. The image will be taken the next time the device is rebooted and checks for preboot work.

Device:	 /Devices/Servers/sdf1.provo.novell.com
Server and File Path:	192.68.1.203 : /images/image.zmg
Use compression:	Balanced
Name:	Image Bundle 2
Description:	ZENworks Image Bundle #2
Location:	Bundles

---

<< Back Finish Cancel

- 9 Review the configuration, then click one of the following:

**Back:** Allows you to make changes after reviewing the summary.

**Finish:** Click to take the image. If you completed [Step 7](#), the image is assigned to the bundle when it is created.

This base image can be used in [Step 8 on page 302](#) under “Configuring the ZENworks Image Bundle for Automatic Imaging” on page 301.

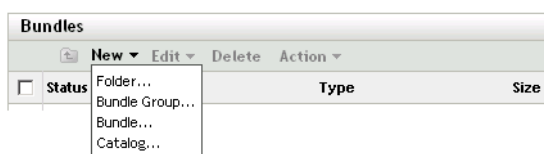
To create an add-on image for use in [Step 8 on page 302](#), see “Creating an Add-On Image” on page 309.

## Configuring the ZENworks Image Bundle for Automatic Imaging

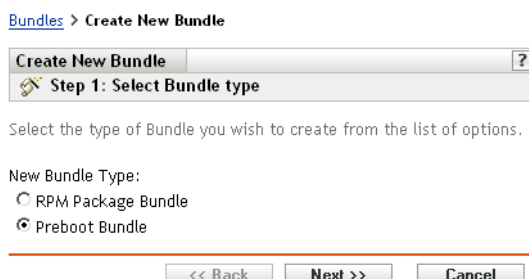
Using ZENworks Linux Management, you can install software using a bundle. Software included in a bundle that is assigned directly is considered mandatory; the software is installed on all assigned devices (the bundle is directly assigned to the devices, their groups, or their folders).

To configure a ZENworks Image bundle and assign devices to the bundle:

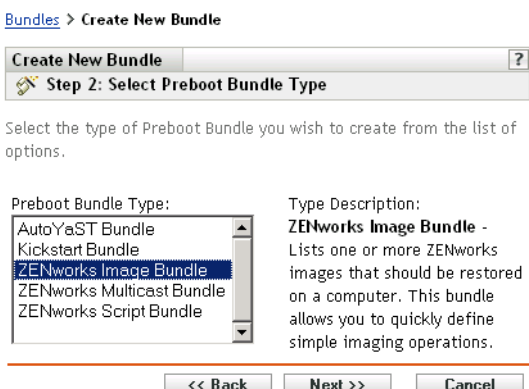
- 1 In the ZENworks Control Center, click the *Bundles* tab.



- 2 Click *New > Bundle* to start the Create New Bundle Wizard:



- 3 In the Create New Bundle Wizard, select *Preboot bundle*, then click *Next*.



- 4 On the Select Preboot Bundle Type page, select *ZENworks Image bundle*.

5 Click *Next* to display the Set General Information page:

The screenshot shows the 'Create New Bundle' wizard at Step 3: Set General information. The breadcrumb path is 'Bundles > Create New Bundle'. The window title is 'Create New Bundle' with a help icon. The step indicator shows a wizard icon and 'Step 3: Set General information'. There are three input fields: 'Name:' with an empty text box, 'Folder:' with a text box containing '/Bundles' and a browse icon, and 'Description:' with a larger empty text box. At the bottom, there are three buttons: '<< Back', 'Next >>', and 'Cancel'.

6 Fill in the fields:

**Name:** (Required) Although bundles can be identified in ZENworks Control Center by their type of icon, as well as the folder they are listed under, you should develop a naming scheme that differentiates the ZENworks Image bundles that are listed together in a folder.

**Folder:** Browse for the location where you want the ZENworks Image bundle displayed in ZENworks Control Center. The folder must exist. You cannot specify a non-existent folder, because ZENworks does not create them from this wizard.

**Description:** Provide a description to help you later recognize the exact purpose of this ZENworks Image bundle.

7 Click *Next* to display the Bundle Configuration page:

The screenshot shows the 'Create New Bundle' wizard at Step 4: Preboot Bundle Creation. The breadcrumb path is 'Bundles > Create New Bundle'. The window title is 'Create New Bundle ZENworks Image Bundle' with a help icon. The step indicator shows a wizard icon and 'Step 4: Preboot Bundle Creation'. Below the step indicator, it says 'Configure the preboot information'. There are two main sections: 'Base Image File:' with a text box, a browse icon, and a 'Clear' button; and 'Add-On Image Files:' with a list box and buttons for 'Add', 'Edit', 'Move Up', 'Move Down', and 'Remove'. At the bottom left, there is a 'File Set:' dropdown menu showing '1'. At the bottom, there are three buttons: '<< Back', 'Next >>', and 'Cancel'.

8 Fill in the fields:

**Base image file:** This is an image file existing on an imaging server. You must provide the full path and filename here. The image filename must end in .zmg. For information on creating a base image, see [“Taking a Base Image of a Device” on page 298](#).

**Add-on image files:** These are existing image files that you can add onto the device after it is reimaged with the base image file. You must provide the full paths and filenames here. The

image filename must end in `.zmg`. For information on creating an add-on image, see [“Creating an Add-On Image” on page 309](#).

**File set:** File sets are assigned to the current ZENworks Image bundle using this *File set* field. File sets are defined on the imaging server from the base image using the **Image Explorer** utility, which can be run on a Windows machine from a Linux server running Samba. The Image Explorer utility is located at `/opt/novel/zenworks/zdm/imaging/winutils/ImgExp.exe` on the Linux server.

When you define a file set using Image Explorer, you specify files and directories to be excluded from the image. Thus, a file set is a subset of the original image that excludes the files you select in Image Explorer. A separate image file is not created for the file set; instead, a file set contains internal attributes representing the excluded information. Therefore, even though a file set does not exist as a separate, physical image file, it is accessed as though it is, placing the image on the receiving device, minus the excluded files.

For example, `devicelimage.zmg` is the image file on your imaging server. You use Image Explorer to determine which data to exclude and assign this to a file set number, such as 2. When a device assigned to this ZENworks Image bundle boots, it is imaged with the smaller version (file set 2) of `devicelimage.zmg`.

File sets provide an advantage because you can create a base image and modify it slightly for various devices, instead of creating separate, somewhat different base images for each device. However, because file sets only concern excluded files, if you add files to the base image using Image Explorer, all file sets will include those additional files. If you don’t want them included in a file set, you must use Image Explorer to exclude these new files from that file set.

There are a maximum of 10 file sets. Each of the ten file set numbers represents the original base image, until you use Image Explorer and assign the results to a file set number.

---

**IMPORTANT:** If you create 10 different file sets, the original image can be lost. If you want to maintain the original image’s information, do not use Image Explorer to assign exclusions to file set 1, which is the default file set if you don’t select a file set when using this wizard.

---

**Add:** Accesses the Server and Path Information dialog box:

- ♦ **Server object, IP, or DNS:** The identity of the imaging server where the Novell ZENworks Linux Management Imaging Agent (**novell-zislnx**) is installed and running, and where the base image file is stored.
- ♦ **File path on server:** The full path to the base image file.

**9** Click *Next* to display the Summary page:

**Create New Bundle** ZENworks Image Bundle ?

Step 5: Summary

Review the following information, and click 'Finish' to create the new Image Bundle.

<b>Name:</b>	ZENworks Image Bundle
<b>Preboot Bundle Type:</b>	ZENworks Image Bundle
<b>Folder:</b>	Bundles
<b>Description:</b>	ZENworks Image Bundle
<b>Base Image File:</b>	192.68.1.203 : /images/image.zmg
<b>Add-On Image Files:</b>	
<b>File Set:</b>	1

<< Back   Next >>   Finish   Cancel

**10** Review the configuration, then click one of the following:

**Back:** Allows you to make changes after reviewing the summary.

**Next:** Click to perform the following tasks before creating the bundle:

- ♦ Specify device assignments for this bundle
- ♦ Specify groups for this bundle

Continue with [Section 24.5, “Assigning Unassigned Preboot Bundles,” on page 330](#) to assign the bundle and complete the wizard.

**Finish:** Creates the ZENworks Script bundle as configured per the settings listed on this Summary page.

This bundle is not assigned to any device or group after it is created, unless you click *Next* instead of *Finish* to make that assignment.

When a device assigned to the ZENworks Image bundle boots, the bundle’s work is performed on the device before its operating system starts.

### Imaging a Device Using a Script

You can perform scripted imaging using the ZENworks Script bundle. Any imaging commands can be entered for the script.

For example, if you want to mount a DVD and restore an image from it, you could enter something similar to the following in the *Script text* field in the Create New Preboot Bundle Wizard when defining a ZENworks Script bundle:

```
echo "Please insert the DVD containing the image into the drive."  
mount /dev/cdrom /mnt/cdrom  
img rl /mnt/cdrom/myimagefile.zmg  
umount /mnt/cdrom  
eject /dev/cdrom
```

This example is a combination of automatic and manual tasks, where you define the bundle in the ZENworks Control Center, assign it to the device, then when the device boots, it runs the bundle’s script, prompting you to insert the DVD containing an image into the device’s DVD drive. The script then runs the commands to restore the image on the device and ejects the DVD when finished.

For information on creating a ZENworks Script bundle, see [Section 24.2, “Configuring ZENworks Script Bundles,” on page 295](#).

## 24.3.2 Performing Manual Imaging Tasks

The following manual imaging tasks are available:

- ♦ [“Manually Taking an Image of a Device” on page 305](#)
- ♦ [“Using Image Explorer to Customize an Image” on page 308](#)
- ♦ [“Creating an Add-On Image” on page 309](#)
- ♦ [“Manually Putting an Image on a Device” on page 309](#)
- ♦ [“Making an Image Available for Automatic Imaging” on page 312](#)

These instructions assume that you have already prepared the imaging server (see [Section 23.1, “Preparing a Preboot Services Server,” on page 239](#)), prepared devices for imaging (see



[Section 23.7, “Setting Up Devices for Imaging,” on page 283](#)), and set up imaging defaults ([Section 23.4, “Configuring Preboot Services Defaults,” on page 261](#)).

ZENworks Linux Management imaging supports devices that physically connect to the network and that meet the minimum requirements for devices. ZENworks Linux Management imaging does not support imaging operations (creating or restoring images) using wireless connectivity.

## Manually Taking an Image of a Device

This section explains how to take an image of a device by booting from an imaging method and entering a particular imaging command. The image is stored on your imaging server.

If you want to store an image locally rather than on an imaging server, see [“Using a CD or DVD for Disconnected Imaging Operations” on page 314](#) and [“Using a Hard Disk for Disconnected Imaging Operations” on page 316](#).

Ensure that your imaging server has enough disk space for the image. Otherwise, you receive a “Failed to write to proxy” error.

The following sections contain additional information:

- ♦ [“Manually Taking an Image of a Device Using the Bash Prompt” on page 305](#)
- ♦ [“Manually Taking an Image of a Device Using the ZENworks Imaging Engine Menu” on page 307](#)

### Manually Taking an Image of a Device Using the Bash Prompt

**1** Boot the device using one of the following methods:

- ♦ If the device is PXE-enabled, boot it from the Preboot Services imaging server. For more information, see [Section 23.2.1, “Using Preboot Services \(PXE\),” on page 240](#).
- ♦ Boot the device using an imaging boot CD or DVD. For more information, see [Section 23.2.2, “Preparing Imaging Boot CDs or DVDs,” on page 240](#).
- ♦ Boot the device from the ZENworks partition. For more information, see [“Creating a ZENworks Partition” on page 245](#).

**2** Enter `manual` at the boot prompt.

or

Select *Start ZENworks imaging maintenance* from the Preboot Services Menu.

**3** (Optional) At the bash prompt, type `img dump`, then press Enter.

This displays a list of the partition slots on the device. For your reference, note the number and type of partitions and which one is active.

**4** Enter a command at the bash prompt using one of the following formats:

- ♦ To create an image and store it on the imaging server, enter:  

```
img makep serverIPaddr_or_DNSname //uncpath/newimg.zmg  
[comp=comp level]
```

The `makep` parameter stands for “make on proxy,” which creates an image and stores it on the imaging (proxy) server.

The IP address or DNS name should be that of your imaging server.

The UNC path specifies the location and filename where the new image is to be stored.

The directories in the path must exist. You can use the following characters in the path and filename:

- ♦ Letters: a through z (uppercase and lowercase)
- ♦ Numbers
- ♦ Special Characters: \$ % ' - \_ @ { } ~ ` ! # ( )

*comp level* is the amount of compression used when creating the image. Specify any number from 0-9. 0 means no compression. 1 is the same as *Optimize for speed* and is used by default if you do not specify this parameter. 6 is the same as *Balanced*. 9 is the same as *Optimize for space*. (*Optimize for speed* takes the least amount of time but creates the largest image file. *Optimize for space* creates the smallest image file but might take a significant amount of time. *Balanced* is a compromise between compression time and image file size.)

For example:

```
img makep 137.65.95.127 //xyz_srv/sys/imgs/cpqnt.zmg comp=6
```

- ♦ To create an image and store it locally, enter:

```
img makel filepath [comp=comp level]
```

The makel parameter stands for “make locally,” which creates an image and stores it on a local hard disk.

---

**NOTE:** Unless you mount a drive before using makel, the image is created in RAM and is lost during a reboot of the device.

---

*filepath* is the image filename, including the .zmg extension and the complete path from the root of the partition.

The directories in the path must exist. You can use the following characters in the path and filename:

- ♦ Letters: a through z (uppercase and lowercase)
- ♦ Numbers
- ♦ Special Characters: \$ % ' - \_ @ { } ~ ` ! # ( )

*comp level* is the amount of compression used when creating the image. Specify any number from 0-9. 0 means no compression. 1 is the same as *Optimize for speed* and is used by default if you do not specify this parameter. 6 is the same as *Balanced*. 9 is the same as *Optimize for space*. (*Optimize for speed* takes the least amount of time but creates the largest image file. *Optimize for space* creates the smallest image file but might take a significant amount of time. *Balanced* is a compromise between compression time and image file size.)

For example:

```
img makel /imgs/dellnt.zmg comp=6
```

---

**IMPORTANT:** Make sure to use *forward slashes* in the UNC path as shown above. Backslashes are not recognized by Linux. However, you can use backslashes and enclose the entire UNC path in quotes. The path you specify must exist on your imaging server.

---

For more information on the parameters you can use and usage examples, see [Section C.3, “Make Mode \(img make\),” on page 427](#).

Depending on the amount of data on the hard disk, the image might take several minutes to create. If the screen goes blank, just press any key. (Linux enters a screen-saving mode after a few minutes.)

- 5 After the image is created and the bash prompt is displayed, remove any diskette from the drive and reboot the device.
- 6 (Optional) Verify that the image file was created on your imaging server. You might also want to check its size.

## Manually Taking an Image of a Device Using the ZENworks Imaging Engine Menu

- 1 Boot the device using one of the following methods:
  - ♦ If the device is PXE-enabled, boot it from the Preboot Services imaging server. For more information, see [Section 23.2.1, “Using Preboot Services \(PXE\),” on page 240.](#)
  - ♦ Boot the device using an imaging boot CD or DVD. For more information, see [Section 23.2.2, “Preparing Imaging Boot CDs or DVDs,” on page 240.](#)
  - ♦ Boot the device from the ZENworks partition. For more information, see [“Creating a ZENworks Partition” on page 245.](#)
- 2 Enter `manual` at the boot prompt.  
or  
Select *Start ZENworks imaging maintenance* from the Preboot Services Menu.
- 3 Enter `img` to display the ZENworks Imaging Engine menu.
- 4 (Optional) Click *System information > Drive information* to display a list of the partition slots on the device.  
  
For your reference, note the number and type of partitions and which one is active.
- 5 Click *Imaging > Make image*.
- 6 In the Make Image Wizard window, specify the destination where the image is stored (Local or Server), then click *Next*.  
  
The directories in the path must exist. You can use the following characters in the path and filename:
  - ♦ Letters: a through z (uppercase and lowercase)
  - ♦ Numbers
  - ♦ Special Characters: \$ % ' - \_ @ { } ~ ` ! # ( )
- 7 Browse to and specify the path to the image archive.
- 8 Select the partitions that you want to include in the image.
- 9 Select a compression option:  
**None:** No compression is used.  
**Speed:** Takes the least amount of time to compress but creates the largest compressed image file. This option is used by default when an image is created.  
**Balanced:** Represents a compromise between compression time and image file size.  
**Size:** Creates the smallest image file but takes longer to compress.
- 10 Click *Next*.

**11** (Optional) Fill in the fields:

**Author:** The name of the person creating this image.

**Computer:** The name of the computer being imaged.

**Image description:** A description of the image.

**Comments:** Any additional comments about the image.

**12** Click *Next*.

Depending on the amount of data on the hard disk, the image might take several minutes to create. If the screen goes blank, just press any key. (Linux enters a screen-saving mode after a few minutes.)

**13** After the image is created, exit from the ZENworks Imaging Engine menu, remove any diskette from the drive, then reboot the device.

**14** (Optional) Verify that the image file was created on your imaging server. You might also want to check its size.

## Using Image Explorer to Customize an Image

After you have created a base or add-on image as explained in the previous sections, you can customize it with the Image Explorer utility. Specifically, you can:

- ♦ **Compress the image:** You can compress an image (including images created by previous versions of ZENworks Linux Management) to 40-60% of the original file size, if you have not done so already during the imaging process. There are three compression options. *Optimize for speed* takes the least amount of time but creates the largest compressed image file. *Optimize for space* creates the smallest image file but might take a significant amount of time. *Balanced* is a compromise between compression time and image file size. This option is used by default when an image is created.

ZENworks Linux Management provides the following compression methods:

- ♦ **Compress:** Use this option to compress an image file that you currently have open in Image Explorer. For more information, see [“Compressing an Open Image” on page 404](#).
- ♦ **QuickCompress:** Use this option to compress an image file without waiting for the file to fully load into Image Explorer. For more information, see [“Compressing Any Image without Waiting for the File to Fully Load into Image Explorer” on page 405](#).
- ♦ **Split the image:** You can specify a device image file that you want to split into separate files so that the entire image can be spanned across several CDs or DVDs. Splitting a device image is helpful for putting down or restoring images in a disconnected environment. For more information, see [Section B.1.15, “Splitting an Image,” on page 405](#).
- ♦ **Resize a partition in an image:** For base images, you can edit the value in the *Original size* text box to allow you to change how big the ZENworks Imaging Engine makes the partition when the image is restored. For more information, see [Section B.1.16, “Resizing a Partition in an Image,” on page 406](#).
- ♦ **Purge deleted files:** Excluded or hidden files and folders can be completely removed from an open image. This saves space in the image if you no longer want to include the files. For more information, see [Section B.1.5, “Excluding a File or Folder from a File Set in the Open Image,” on page 403](#).
- ♦ **Exclude individual files and folders from the image:** In doing this, you create subsets of the image by specifying which of ten possible file sets to exclude a given file or folder from. This

exists merely as internal attributes of the same image archive. For more information, see [Section B.1.7, “Purging Files and Folders Marked for Deletion from the Open Image,” on page 403](#).

---

**IMPORTANT:** Do not exclude BPB files from a base image or the device won’t be able to boot the new operating system after receiving the image.

---

- ♦ **Add files and folders to the image:** By default, any file or folder you add is included in all file sets. To change this, you must explicitly exclude the file or folder from one or more file sets. For more information, see [Section B.1.3, “Adding a File or Folder to an Open Image,” on page 402](#).

For information on starting Image Explorer, see [Section B.1, “Image Explorer \(ImgExp.exe\),” on page 401](#).

## Creating an Add-On Image

An *add-on* image is an archived collection of files to be applied to an existing installation on a target device. This is sometimes referred to as an application overlay. The existing partitions and files on the target device are left intact, except for any files that the add-on image might update.

An add-on image typically corresponds to an application or utility, or simply to a set of data files or configuration settings.

To create an add-on image:

- 1 Run the Image Explorer utility, which is located on the Linux imaging server at:  
`/opt/novell/zenworks/zdm/imaging/winutils/ImgExp.exe`
- 2 Drag files and folders from an existing device into a new image archive.  
For more information, see [Section B.1, “Image Explorer \(ImgExp.exe\),” on page 401](#).
- 3 Save this image with the `.zmg` extension in the same directory on the imaging server where you store base images.

Generally, an add-on image created in this manner doesn’t require any post-processing on the target device. It is simply a set of files that are copied to the appropriate locations on the hard disk, much like what happens when you unzip an archive. For more information, see [“Using Image Explorer to Customize an Image” on page 308](#).

This add-on image can be used in [Step 8 on page 302](#) under [“Configuring the ZENworks Image Bundle for Automatic Imaging” on page 301](#).

## Manually Putting an Image on a Device

The section explains how to put an image on the device by booting from an imaging method and entering a particular imaging command. The image is retrieved from your imaging server.

Ensure that the device receiving a new image has enough disk space for the image. Otherwise, you receive a “Failed to write to proxy” error.

The following sections contain additional information:

- ♦ [“Manually Putting an Image on a Device Using the Bash Prompt” on page 310](#)
- ♦ [“Manually Putting an Image on a Device Using the ZENworks Imaging Engine Menu” on page 311](#)

## Manually Putting an Image on a Device Using the Bash Prompt

- 1 If you haven't already done so, create the image to put on the device, as instructed in [“Manually Taking an Image of a Device” on page 305](#).

Make sure that the image is of the same type of device (same hardware configuration) and is stored on your imaging server. You can use a previous image of the same device.

---

**IMPORTANT:** If you are putting an image on a device without a ZENworks partition, make sure the image was made on a device without a ZENworks partition. Otherwise, the wrong MBR (Master Boot Record) is restored, and the device fails to boot.

---

- 2 (Optional) Boot the device from a Windows startup disk and run FDISK to remove all partitions from the hard disk.

Running FDISK is not required, but it is recommended for purposes of comparing workstation or server partitions before and after the imaging operation.

- 3 Boot the device using one of the following methods:

- ♦ If the device is PXE-enabled, boot it from the Preboot Services imaging server. For more information, see [Section 23.2.1, “Using Preboot Services \(PXE\),” on page 240](#).
- ♦ Boot the device using an imaging boot CD or DVD. For more information, see [Section 23.2.2, “Preparing Imaging Boot CDs or DVDs,” on page 240](#).
- ♦ Boot the device from the ZENworks partition. For more information, see [“Creating a ZENworks Partition” on page 245](#).

- 4 Enter `manual` at the boot prompt.

This step is not the same as in the previous step's manual processes.

- 5 (Optional) At the bash prompt, type `img dump`, then press Enter to display a list of the partition slots on the device.

For your reference, note the number and type of partitions and which one is active. If you removed all partitions using FDISK, each slot should be empty and none should be active.

- 6 Enter a command at the bash prompt using one of the following formats:

- ♦ To restore an image from the imaging server and put it down on a device, enter:

```
img restorep serverIPaddr_or_DNSname //uncpath/newimg.zmg
```

The `restorep` parameter stands for “restore from proxy,” which retrieves an image from the imaging (proxy) server and puts it on this device. The IP address or DNS name should be that of your imaging server, and the UNC path specifies the location and filename where the image is to be retrieved from.

For example:

```
img restorep 137.65.95.127 //xyz_srv/sys/imgs/cpqnt.zmg
```

- ♦ To retrieve an image from a local device and put it down on a device:

```
img restorel filepath
```

The `restorel` parameter stands for “restore from local,” which retrieves an image from a local device and puts it on this device. *Filepath* represents the filename of the image to retrieve, including the `.zmg` extension and the complete path from the root of the partition.

---

**IMPORTANT:** Make sure to use *forward slashes* in the UNC path as shown above. Backslashes aren't recognized by Linux. However, you can use backslashes and enclose the

entire UNC path in quotes. The server portion of the path must be the name of your imaging server.

If you want to manually restore an image from a folder that uses extended or double-byte characters in its name, you should perform an automatic image restoration. For more information, see [Section 22.5.2, “Creating, Installing, and Restoring Standard Images,” on page 233](#) or [Section 22.5.4, “Restoring Lab Devices to a Clean State,” on page 234](#).

---

For more information on the parameters you can use and usage examples, see [Section C.4, “Restore Mode \(img restore\),” on page 429](#).

Depending on the size of the image, it might take several minutes to put the image down. Images usually take slightly longer to put down than they do to take.

- 7 (Optional) After the image is put down and the bash prompt is displayed, type `img dump`, then press Enter.

As before, this displays a list of the partition slots on the device. You should now see information about the new partitions that are created and activated by the image that you just put down.

- 8 At the bash prompt, type `lilo.s`, then press Enter.
- 9 Remove any diskette from the drive and reboot the device.
- 10 Verify that the device boots to the operating system that was installed by the new image.

## Manually Putting an Image on a Device Using the ZENworks Imaging Engine Menu

- 1 If you haven't already done so, create the image to put on the device, as instructed in [“Manually Taking an Image of a Device” on page 305](#).

Make sure that the image is of the same type of device (same hardware configuration) and is stored on your imaging server. You can use a previous image of the same device.

---

**IMPORTANT:** If you are putting an image on a device without a ZENworks partition, make sure the image was made on a device without a ZENworks partition. Otherwise, the wrong MBR (Master Boot Record) is restored, and the device fails to boot.

---

- 2 (Optional) Boot the device from a Windows startup disk and run FDISK to remove all partitions from the hard disk.

Running FDISK is not required, but it is recommended for purposes of comparing the workstation or server partitions before and after the imaging operation.

- 3 Boot the device using one of the following methods:

- ♦ If the device is PXE-enabled, boot it from the Preboot Services imaging server. For more information, see [Section 23.2.1, “Using Preboot Services \(PXE\),” on page 240](#).
- ♦ Boot the device using an imaging boot CD or DVD. For more information, see [Section 23.2.2, “Preparing Imaging Boot CDs or DVDs,” on page 240](#).
- ♦ Boot the device from the ZENworks partition. For more information, see [“Creating a ZENworks Partition” on page 245](#).

- 4 Enter `manual` at the boot prompt.

or

Select *Start ZENworks imaging maintenance* from the Preboot Services Menu.

- 5 Enter `img` to display the ZENworks Imaging Engine menu.



- 6 (Optional) Click *System information > Drive information* to display a list of the partition slots on the device.  
For your reference, note the number and type of partitions and which one is active. If you removed all partitions using FDISK, each slot should be empty and none should be active.
- 7 Click *Imaging > Restore image*.
- 8 In the Restore Image Wizard window, specify the source location of the image (Local or Server), then click *Next*.
- 9 Browse to and specify the path to the image archive.
- 10 (Optional) Specify a file set.
- 11 (Optional) Specify any advanced options, such as *sfileset* or *apartition:ppartition*.  
For details on this and other related img command parameters, see “ZENworks Imaging Engine Commands” on page 425.
- 12 Click *Next*.  
Depending on the size of the image, it might take several minutes to put the image down. Images usually take slightly longer to put down than they do to take.
- 13 (Optional) Click *System information > Drive information* to display a list of the partition slots on the device.  
As before, this displays a list of the partition slots on the device. You should now see information about the new partitions that are created and activated by the image that you just put down.
- 14 Exit the ZENworks Imaging Engine menu.
- 15 Run `lilo.s` from the bash prompt.
- 16 Remove any diskette from the drive and reboot the device.
- 17 Verify that the device boots to the operating system that was installed by the new image.

## Making an Image Available for Automatic Imaging

When you boot a device from an imaging method and allow the boot process to proceed in auto-imaging mode, the imaging operation that is performed on the device is determined by default Preboot Services settings that you define in the ZENworks Control Center.

Creating a Preboot Services bundle also allows you to combine a base image and one or more add-on images into a single entity that can be put down on target devices. You can specify a standard image file to put down, or you can create a script to further customize your imaging operation. You can also specify that a particular file set of an image be used.

The sections that follow give instructions for performing these tasks:

- ♦ “Creating a Base Image” on page 313
- ♦ “Associating an Add-On Image with a Base Image” on page 313
- ♦ “Using a File Set of an Image” on page 314



## Creating a Base Image

- 1 Create the base image using one of the following methods:
  - ♦ **ZENworks Control Center:** See [“Taking a Base Image of a Device” on page 298](#).
  - ♦ **Manually from a bash prompt:** See [“Manually Taking an Image of a Device” on page 305](#).
- 2 After the base image is created, perform one of the following procedures in the ZENworks Control Center:
  - ♦ If you created the image using a Preboot bundle, assign the bundle to the devices to be imaged:
    - 1) In the ZENworks Control Center, click *Bundles*, click the bundle containing the base image that you want to associate the add-on images with, then click *Details*.
    - 2) In the Assignments section, click *Add* to start the Assign Bundle wizard.
    - 3) Click *Add* to open the Select Objects dialog box.
    - 4) Select the devices or groups containing devices, then click *OK*.
    - 5) Click *Next* to display the Summary page, then click *Finish* > *OK* to assign the devices to the bundle and exit the wizard.
  - ♦ If you created the image manually, assign the image to a Preboot Image bundle, then assign that bundle to the devices to be imaged:
    - 1) Follow the instructions in [“Configuring the ZENworks Image Bundle for Automatic Imaging” on page 301](#).
    - 2) In [Step 10 on page 304](#), click *Next* to assign the bundle to the devices.

The next time these devices boot, they are imaged from this Preboot bundle.

## Associating an Add-On Image with a Base Image

- 1 Create the add-on image to associate with the base image. For more information, see [“Creating an Add-On Image” on page 309](#).
- 2 Copy the add-on image file to a ZENworks Linux Management imaging server that is accessible as a server object in your eDirectory tree.

You might want to copy your add-on images to the same location as the base image.
- 3 In the ZENworks Control Center, click *Bundles*, click the bundle containing the base image that you want to associate the add-on images with, then click *Details*.
- 4 For the Add-On Image Files section, click *Add*.
- 5 Browse for and select an add-on image.

You can associate more than one add-on image with a base image. Repeat this step for each add-on image.
- 6 Click *Apply*.

When a device boots that is assigned to this bundle, the add-on images are put down after the base image in the order listed on this page.

## Using a File Set of an Image

As explained in [“Using Image Explorer to Customize an Image” on page 308](#), you can exclude individual files and folders from any of 10 possible file sets of an image.

**Table 24-1** *Image File Set Usages*

Type of imaging operation	How to specify the file set to use
Automatic (Preboot Services based on default settings)	<p>In the Multicast Wizard in the ZENworks Control Center, specify the number of the file set in the <i>File set</i> field. You must create the file set using the Image Explorer utility. For more information, see <a href="#">Section B.1, “Image Explorer (ImgExp.exe),” on page 401</a>.</p> <p>You can create multiple Preboot bundles that point to the same base image, but to different file sets of that image.</p>
Manual (command line or menu)	<p>Use the <code>s</code> parameter on the <code>img restore</code> command. For example, to specify file set number 3:</p> <pre>img restore1 dellnt4.zmg s3</pre> <p>or</p> <p>You can enter <code>img</code> at the bash prompt to display a menu, select <i>Restore an image</i>, then select <i>Local image</i>. Specify <i>sfileset</i> (for example, <code>s3</code>) in the <i>Advanced parameters</i> field.</p> <p>For details, see <a href="#">“ZENworks Imaging Engine Commands” on page 425</a>.</p>

### 24.3.3 Setting Up Disconnected Imaging Operations

Disconnected imaging operations are inherently manual. To perform a disconnected imaging operation on a device, you must have a storage device to hold the image to be created or put down, and that storage device must be locally accessible to the ZENworks Imaging Engine (in Linux) when you boot the device from the imaging boot media.

The following sections explain how to set up and perform disconnected operations:

- ♦ [“Using a CD or DVD for Disconnected Imaging Operations” on page 314](#)
- ♦ [“Using a Hard Disk for Disconnected Imaging Operations” on page 316](#)

#### Using a CD or DVD for Disconnected Imaging Operations

Using ZENworks Linux Management, you can use CDs and DVDs only as the storage medium for an image to put down, not for an image to be created.

You can put down an image from a bootable or non-bootable imaging CD or DVD using either the bash prompt or using the ZENworks Imaging Engine menu.

The following sections contain additional information:

- ♦ [“Putting Down an Image Using the Bash Prompt” on page 315](#)
- ♦ [“Putting Down an Image Using the ZENworks Imaging Engine Menu” on page 315](#)

## Putting Down an Image Using the Bash Prompt

- 1 Use your CD- or DVD-burning software to burn the source image onto a CD or DVD.
- 2 Boot the device using one of the following methods:
  - ♦ If the device is PXE-enabled, boot it from the Preboot Services imaging server. For more information, see [Section 23.2.1, “Using Preboot Services \(PXE\),” on page 240](#).
  - ♦ Boot the device using an imaging boot CD or DVD. For more information, see [Section 23.2.2, “Preparing Imaging Boot CDs or DVDs,” on page 240](#).
  - ♦ Boot the device from the ZENworks partition. For more information, see [“Creating a ZENworks Partition” on page 245](#).
- 3 Enter `manual` from the boot prompt.
- 4 Insert the CD or DVD that contains the source image.
- 5 At the Linux prompt, enter `cdrom.s` to mount the CD or DVD.  
This mounts the CD or DVD to `/mnt/cdrom`.
- 6 Enter a command using the following format:  

```
img restore1 /mnt/cdrom/path/image_name.zmg
```

  
where *path* and *image\_name* are the path and filename of the image relative to the root of the CD or DVD.
- 7 When the imaging is done, remove the imaging boot media (if applicable) and do the following to boot the device with the new image:
  - 7a At the Linux prompt, type `lilo.s`, then press Enter.
  - 7b Press Ctrl+Alt+Delete.  
  
If the device doesn't boot to the new operating system (that is, if the Linux prompt is displayed), enter `lilo.s` again and reboot the device a second time.

## Putting Down an Image Using the ZENworks Imaging Engine Menu

- 1 Use your CD- or DVD-burning software to burn the source image onto a CD or DVD.
- 2 Boot the device using one of the following methods:
  - ♦ If the device is PXE-enabled, boot it from the Preboot Services imaging server. For more information, see [Section 23.2.1, “Using Preboot Services \(PXE\),” on page 240](#).
  - ♦ Boot the device using an imaging boot CD or DVD. For more information, see [Section 23.2.2, “Preparing Imaging Boot CDs or DVDs,” on page 240](#).
  - ♦ Boot the device from the ZENworks partition. For more information, see [“Creating a ZENworks Partition” on page 245](#).
- 3 Enter `manual` from the boot prompt.
- 4 Insert the CD or DVD that contains the source image.
- 5 At the Linux prompt, enter `cdrom.s` to mount the CD or DVD.  
This mounts the CD or DVD to `/mnt/cdrom`.
- 6 Enter `img` to display the ZENworks Imaging Engine menu.
- 7 Click *Imaging*, then click *Restore image*.
- 8 Click *Local*, then click *Next*.
- 9 Browse to and specify the path to the image archive.

- 10** (Optional) Specify a file set.
- 11** (Optional) Specify any advanced options, such as *sfileset* or *apartition:ppartition*.  
For details on this and other related `img` parameters, see [“ZENworks Imaging Engine Commands” on page 425](#).
- 12** Click *Next*.  
Depending on the size of the image, it might take several minutes to put the image down. Images usually take slightly longer to put down than they do to take.
- 13** When the imaging is done, remove the imaging boot media (if applicable) and do the following to boot the device with the new image:
  - 13a** At the Linux prompt, type `lilo.s`, then press Enter.
  - 13b** Press Ctrl+Alt+Delete.  
If the device doesn’t boot to the new operating system (that is, if the Linux prompt is displayed), enter `lilo.s` again and reboot the device a second time.

## Using a Hard Disk for Disconnected Imaging Operations

When you boot a device from a ZENworks Linux Management imaging boot media, you can create an image on, or put down an image from, any primary partition on an IDE or SCSI hard drive. You can also use the local ZENworks partition if one is installed. Any target partition must have sufficient space.

When you create an image, the partition where you store the image is itself excluded from the image. When you put down an image, the source partition is not altered.

You can create or put down an image on a hard disk using either the bash prompt or using the ZENworks Imaging Engine menu.

The following sections contain the instructions:

- ♦ [“Creating an Image Using the Bash Prompt” on page 316](#)
- ♦ [“Creating an Image Using the ZENworks Imaging Engine Menu” on page 317](#)
- ♦ [“Putting Down an Image Using the Bash Prompt” on page 318](#)
- ♦ [“Putting Down an Image Using the ZENworks Imaging Engine Menu” on page 318](#)

### Creating an Image Using the Bash Prompt

- 1** Boot the device using one of the following methods:
  - ♦ If the device is PXE-enabled, boot it from the Preboot Services imaging server. For more information, see [Section 23.2.1, “Using Preboot Services \(PXE\),” on page 240](#).
  - ♦ Boot the device using an imaging boot CD or DVD. For more information, see [Section 23.2.2, “Preparing Imaging Boot CDs or DVDs,” on page 240](#).
  - ♦ Boot the device from the ZENworks partition. For more information, see [“Creating a ZENworks Partition” on page 245](#).
- 2** Enter `manual` from the boot prompt.
- 3** At the Linux prompt, enter `img dump` to view the available partitions.  
Note the number of the partition where you will store the new image.

- 4 Enter a command using the following format:

```
img make1[pNumber] /path/image.zmg [comp=comp_level]
```

where *pNumber* is the number of the partition to store the image in, and *comp\_level* is the amount of compression used when creating the image. Specify any number from 0-9. 0 means no compression. 1 is the same as *Optimize for speed*. 6 is the same as *Balanced* and is used by default if you do not specify this parameter. 9 is the same as *Optimize for space*. (*Optimize for speed* takes the least amount of time but creates the largest image file. *Optimize for space* creates the smallest image file but might take a significant amount of time. *Balanced* is a compromise between compression time and image file size.) *Path* and *image* are the path and filename of the new image relative to the partition root. If you omit the partition number, the local ZENworks partition is used.

For details on other related img command parameters, see “ZENworks Imaging Engine Commands” on page 425.

## Creating an Image Using the ZENworks Imaging Engine Menu

- 1 Boot the device using one of the following methods:

- If the device is PXE-enabled, boot it from the Preboot Services imaging server. For more information, see [Section 23.2.1, “Using Preboot Services \(PXE\),” on page 240](#).
- Boot the device using an imaging boot CD or DVD. For more information, see [Section 23.2.2, “Preparing Imaging Boot CDs or DVDs,” on page 240](#).
- Boot the device from the ZENworks partition. For more information, see [“Creating a ZENworks Partition” on page 245](#).

- 2 Enter `manual` from the boot prompt.

- 3 Enter `img` to display the ZENworks Imaging Engine menu.

- 4 (Optional) Click *System information > Drive information* to display a list of the partition slots on the device.

For your information, note the number of the partition where you will store the new image.

- 5 Click *Imaging > Make image*.

- 6 In the Make Image Wizard window, click *Local > Next*.

- 7 Browse to and specify the path to the image archive.

- 8 Select the partitions that you want to include in the image.

- 9 Select a compression option.

**None:** No compression is used.

**Speed:** Takes the least amount of time to compress but creates the largest compressed image file. This option is used by default when an image is created.

**Balanced:** Represents a compromise between compression time and image file size.

**Size:** Creates the smallest image file but takes longer to compress.

- 10 Click *Next*.

- 11 (Optional) Fill in the fields:

**Author:** The name of the person creating this image.

**Computer:** The name of the computer being imaged.

**Image description:** A description of the image.

**Comments:** Any additional comments about the image.

**12** Click *Next*.

Depending on the amount of data on the hard disk, the image might take several minutes to create.

**13** After the image is created, exit from the ZENworks Imaging Engine menu, remove any diskette from the drive, then reboot the device.

**14** (Optional) Verify that the image file was created. You might also want to check its size.

### Putting Down an Image Using the Bash Prompt

**1** Boot the device using one of the following methods:

- ♦ If the device is PXE-enabled, boot it from the Preboot Services imaging server. For more information, see [Section 23.2.1, “Using Preboot Services \(PXE\),” on page 240](#).
- ♦ Boot the device using an imaging boot CD or DVD. For more information, see [Section 23.2.2, “Preparing Imaging Boot CDs or DVDs,” on page 240](#).
- ♦ Boot the device from the ZENworks partition. For more information, see [“Creating a ZENworks Partition” on page 245](#).

**2** Enter `manual` from the boot prompt.

**3** (Optional) At the Linux prompt, enter `img dump` to view the available partitions.

For your information, note the number of the partition where the source image is stored.

**4** Enter a command using the following format:

```
img restore1[pNumber] /path/image.zmg
```

where *pNumber* is the number of the partition where the source image is stored, and *path* and *image* are the image path and filename relative to the partition root. If you omit the partition number, the local ZENworks partition is used.

For details on other related `img` command parameters, see [“ZENworks Imaging Engine Commands” on page 425](#).

**5** When the imaging is done, remove the imaging boot media (if applicable) and do the following to boot the device with the new image:

**5a** At the Linux prompt, type `lilo.s`, then press Enter.

**5b** Press Ctrl+Alt+Delete.

If the device doesn't boot to the new operating system (that is, if the Linux prompt is displayed), enter `lilo.s` again and reboot the device a second time.

### Putting Down an Image Using the ZENworks Imaging Engine Menu

**1** Boot the device using one of the following methods:

- ♦ If the device is PXE-enabled, boot it from the Preboot Services imaging server. For more information, see [Section 23.2.1, “Using Preboot Services \(PXE\),” on page 240](#).
- ♦ Boot the device using an imaging boot CD or DVD. For more information, see [Section 23.2.2, “Preparing Imaging Boot CDs or DVDs,” on page 240](#).
- ♦ Boot the device from the ZENworks partition. For more information, see [“Creating a ZENworks Partition” on page 245](#).

**2** Enter `manual` from the boot prompt.

- 3 Enter `img` to display the ZENworks Imaging Engine menu.
- 4 (Optional) Click *System information > Drive information* to display a list of the partition slots on the device.

For your reference, note the number of the partition where the source image is stored.

- 5 Click *Imaging > Restore image*.
- 6 Click *Local > Next*.
- 7 Browse to and specify the path to the image archive.
- 8 (Optional) Specify a file set.
- 9 (Optional) Specify any advanced options, such as *sfileset* or *apartition:ppartition*.

For details on this and other related `img` command parameters, see “ZENworks Imaging Engine Commands” on page 425.

- 10 Click *Next*.

Depending on the size of the image, it might take several minutes to put the image down. Images usually take slightly longer to put down than they do to take. If the screen goes blank, just press any key. (Linux enters a screen-saving mode after a few minutes.)

- 11 When the imaging is done, remove the imaging boot media (if applicable) and do the following to boot the device with the new image:

**11a** At the Linux prompt, type `lilo.s`, then press Enter.

**11b** Press Ctrl+Alt+Delete.

If the device doesn't boot to the new operating system (that is, if the Linux prompt is displayed), enter `lilo.s` again and reboot the device a second time.

## 24.4 Multicasting Images

ZENworks Linux Management's Preboot Services includes a multicasting capability for its imaging software. You can perform multicasting of images either in the ZENworks Control Center or manually:

- ♦ [Section 24.4.1, “Multicasting in the ZENworks Control Center,” on page 319](#)
- ♦ [Section 24.4.2, “Multicasting Manually,” on page 325](#)

### 24.4.1 Multicasting in the ZENworks Control Center

- ♦ [“Configuring Multicast Bundles” on page 319](#)
- ♦ [“Enabling a Multicast Session” on page 324](#)

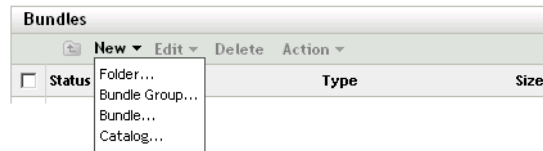
#### Configuring Multicast Bundles

With Preboot Services, multicasting is an automated procedure. As described in “Automatic Multicasting Example” on page 237, you simply define a Multicast bundle and assign it to the devices. The multicast session starts when the trigger event that you configured occurs.

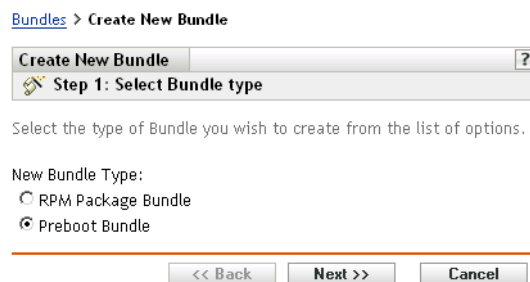
Using ZENworks Linux Management, you can install software using a bundle. Software included in a bundle that is assigned directly is considered mandatory; the software is installed on all assigned devices (the bundle is directly assigned to the devices, their groups, or their folders).

To configure a Multicast bundle and assign devices to the bundle:

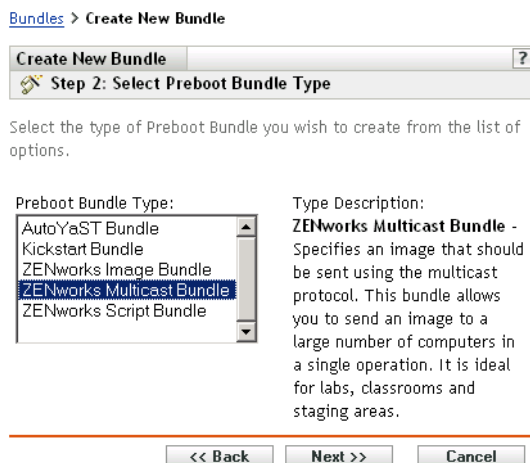
- 1 In the ZENworks Control Center, click the *Bundles* tab.



- 2 Click *New > Bundle* to start the Create New Bundle Wizard:



- 3 In the Create New Bundle Wizard, select *Preboot bundle*, then click *Next* to display the Select Preboot Bundle Type page:





- 4 Select *ZENworks Multicast bundle*, then click *Next* to display the Set General Information page:

The screenshot shows the 'Create New Bundle' wizard at Step 3: Set General information. The breadcrumb path is 'Bundles > Create New Bundle'. The window title is 'Create New Bundle'. Below the title bar, there's a sub-header 'Step 3: Set General information'. The form contains three input fields: 'Name:' (empty), 'Folder:' (containing '/Bundles' with a search icon), and 'Description:' (empty). At the bottom, there are three buttons: '<< Back', 'Next >>', and 'Cancel'.

- 5 Fill in the fields:

**Name:** (Required) Although bundles can be identified in ZENworks Control Center by their type of icon, as well as the folder they are listed under, you should develop a naming scheme that differentiates the ZENworks Multicast bundles that are listed together in a folder.

**Folder:** Browse for the location where you want the ZENworks Multicast bundle displayed in ZENworks Control Center. The folder must exist. You cannot specify a non-existent folder, because ZENworks does not create them from this wizard.

**Description:** Provide a description to help you later recognize the exact purpose of this ZENworks Multicast bundle.

If you are using subsets of an image, be sure to indicate which file set this bundle is configured for.

- 6 Click *Next* to display the Master Image Source page:

The screenshot shows the 'Create New Bundle' wizard at Step 4: Master Image Source. The breadcrumb path is 'Bundles > Create New Bundle'. The window title is 'Create New Bundle'. Below the title bar, there's a sub-header 'Step 4: Master Image Source:'. The form contains a text input field for 'File Path:' with a blue asterisk, a search icon, and a 'Clear' button. Below that is a 'File Set:' dropdown menu with '1' selected. At the bottom, there are three buttons: '<< Back', 'Next >>', and 'Cancel'. A note at the bottom states: 'Fields marked with a blue asterisk are required.'

- 7 Fill in the fields:

ZENworks Multicast bundles use an image that is taken previously from a device and is stored on an imaging server. The image is sent to multiple devices at one time to reimage them, rather than sent one time for each device, thus saving on network bandwidth usage. For example, if you have 10 devices in the multicast session and the image is 3 GB in size, your network

experiences 3 GB of network traffic to image all 10 devices. Without multicasting, the network experiences 30 GB of network traffic.

For multicasting to work properly, all routers and switches on the network must have their multicast features configured. Otherwise, multicast packets might not be routed properly.

**File path:** The location on the imaging server where the image file to be used by the ZENworks Multicast bundle is stored.

**File set:** File sets are assigned to the current ZENworks Image bundle using this *File set* field. File sets are defined on the imaging server from the base image using the **Image Explorer** utility, which can be run on a Windows machine from a Linux server running Samba. The Image Explorer utility is located at `/opt/novel/zenworks/zdm/imaging/winutils/ImgExp.exe` on the Linux server.

When you define a file set using Image Explorer, you specify files and directories to be excluded from the image. Thus, a file set is a subset of the original image that excludes the files you select in Image Explorer. A separate image file is not created for the file set; instead, a file set contains internal attributes representing the excluded information. Therefore, even though a file set does not exist as a separate, physical image file, it is accessed as though it is, placing the image on the receiving device, minus the excluded files.

For example, `deviceimage.zmg` is the image file on your imaging server. You use Image Explorer to determine which data to exclude and assign this to a file set number, such as 2. When a device assigned to this ZENworks Image bundle boots, it is imaged with the smaller version (file set 2) of `deviceimage.zmg`.

The advantage file sets provide is that you can create a base image and modify it slightly for various devices, instead of creating separate, somewhat different base images for each device. However, because file sets only concern excluded files, if you add files to the base image using Image Explorer, all file sets will include those additional files. If you don't want them included in a file set, you must use Image Explorer to exclude these new files from that file set.

There are a maximum of 10 file sets. Each of the ten file set numbers represents the original base image, until you use Image Explorer and assign the results to a file set number.

---

**IMPORTANT:** If you create 10 different file sets, then the original image can be lost. If you want to maintain the original image's information, do not use Image Explorer to assign exclusions to file set 1, which is the default file set if you do not select a file set when using this wizard.

---

**8** Click *Next* to display the Session Start Triggers page:

Bundles > Create New Bundle

Create New Bundle ZENworks Multicast Bundle ?

Step 5: Session Start Triggers

Specify when this session should begin:

Start the session as soon as:

☒ 1 clients have joined, or

☐ 5 minutes have elapsed since a new client has joined

<< Back Next >> Cancel

**9** Fill in the fields:

There are two triggers that you can use to determine when to start the ZENworks Multicast session. The first trigger to be realized starts the session.

A session consists of all clients (devices) that are assigned to the ZENworks Multicast bundle that are booting (joining), but must wait for a start trigger to trip. Therefore, the boot processes for the devices can be held up until one of the triggers is realized, even for as long as you specify in an elapsed time or number of clients entry.

After a session has started, other devices booting that are assigned to this bundle do not become part of this session, but become part of the next session when it triggers.

**Start the session as soon as:** You have two choices:

- ◆ \_\_\_\_ clients have joined

This trigger, if met first, limits the session to the number of clients that you specify. The default is 1.

- ◆ \_\_\_\_ minutes have elapsed since a new client has joined

This trigger, if met first, causes the session to start, regardless of the number of clients that have joined, except that at least one client must have joined (otherwise there is no device to multicast to).

A “new client” means that it is the first device to boot that starts this round of waiting for a trigger to be realized. The default is 5.

These triggers are useful if you want economy of scale in multiple clients joining, but don’t want to stall the session too long from starting.

**10** Click *Next* to display the Summary page:

[Bundles](#) > [Create New Bundle](#)

Create New Bundle

ZENworks Multicast Bundle

?

Step 6: Summary

Review the following information and click 'Finish' to created the new multicast session:

Session Name:	ZENworks Multicast Bundle
Preboot Bundle Type:	ZENworks Multicast Bundle
Description:	ZENworks Multicast Bundle
Master Image Source:	192.68.1.203 : / images/ image.zmg
Session Start Trigger(s):	- When 1 clients have joined - When 5 minutes have elapsed
File Set:	1

<< Back

Next >>

Finish

Cancel

**11** Review the configuration, then click one of the following:

**Back:** Allows you to make changes after reviewing the summary.

**Next:** Click to perform the following tasks before creating the bundle:

- ◆ Specify device assignments for this bundle
- ◆ Specify groups for this bundle

Continue with [Section 24.5, “Assigning Unassigned Preboot Bundles,” on page 330](#) to assign the bundle and complete the wizard.

**Finish:** Creates the Multicast bundle as configured per the settings listed on this Summary page.

This bundle is not assigned to any device or group after it is created, unless you click *Next* instead of *Finish* to make that assignment.

When the Multicast bundle's trigger event occurs (configured in [Step 9](#)), the Multicast session begins.

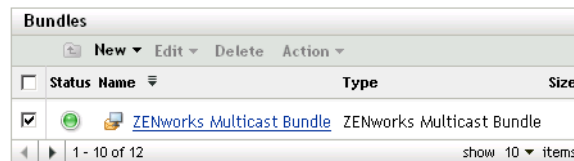
## Enabling a Multicast Session

A wizard allows you to cause each device assigned to the ZENworks Multicast bundle to be enabled for receiving the bundle when it reboots, even if the configuration for the device is to “do nothing” (see [Step 5](#) through [Step 7](#) in [Section 24.6, “Editing Preboot Services Work,”](#) on page 332).

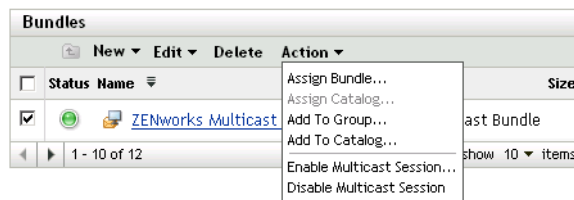
The wizard does not assign a bundle to any device, nor make it the effective bundle for any device. It only sets up a device to do ZENworks Multicast Bundle work for its effective bundle the next time it boots.

To enable a ZENworks Multicast bundle:

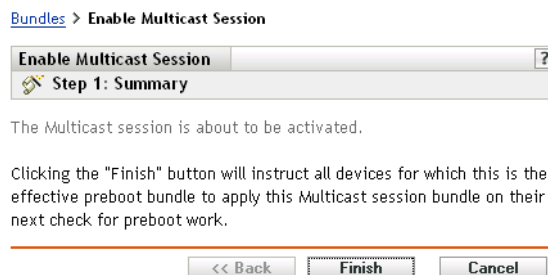
- 1 In the ZENworks Control Center, click the *Bundles* tab to display the Bundles page:



- 2 Select the check box next to a *ZENworks Multicast bundle*.



- 3 Click *Actions > Enable multicast session* to start the Enable Multicast Session wizard:



- 4 Click *Finish* to enable multicasting for the selected device.
- 5 Click *OK* to the message displayed that indicates multicasting is successfully enabled.

The next time a device assigned to the multicast bundle boots, it can become part of that multicast session. For more information, see [Section 24.4, “Multicasting Images,”](#) on page 319.

## 24.4.2 Multicasting Manually

If you want to perform a manual multicast session, you need to start the multicast session from the ZENworks imaging server and physically visit each participating device. Performing a manual multicast session is particularly useful in a lab environment in which a small number of devices participate.

The following sections contain step-by-step information about performing a manual multicast session. To perform a manual multicast session, you must perform the steps in both of the following sections; however, the order in which you perform these tasks does not matter.

- ♦ “Initiating a Multicast Session from the ZENworks Imaging Server” on page 325
- ♦ “Initiating a Multicast Session from Each Client” on page 327

### Initiating a Multicast Session from the ZENworks Imaging Server

On the ZENworks Linux Management imaging server, do the following to initiate the multicast session:

- 1 In the shell console, enter the following command to make sure the imaging software is running:

```
/etc/init.d/novell-pbserv -status
```

If it is not running, then enter:

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

- 2 In the shell console, enter the following command to enable a multicast session:

```
/opt/novell/zenworks/preboot/bin/novell-zmgmcast -mcast arguments
```

where *arguments* represents the following that you can append to the command line:

Argument	Description
<i>session_name</i>	(Required) The session name is any string that uniquely identifies this multicast session from other multicast sessions that might be in progress on the network.
<i>-p path</i>	(Required) The path to the image to be multicast, which is located on the imaging server. This must be the full path.
<i>-i IP_address</i>	(Optional) The IP address of the imaging server.

Argument	Description
<code>-f file_set_number</code>	<p>(Optional) File sets are assigned to the current ZENworks Image bundle using this information. File sets are defined on the imaging server from the base image using the <b>Image Explorer</b> utility, which can be run on a Windows machine from a Linux server running Samba. The Image Explorer utility is located at <code>/opt/novell/zenworks/zdm/imaging/winutils/ImgExp.exe</code> on the Linux server.</p> <p>When you define a file set using Image Explorer, you specify files and directories to be excluded from the image. Thus, a file set is a subset of the original image that excludes the files you select in Image Explorer. A separate image file is not created for the file set; instead, a file set contains internal attributes representing the excluded information. Therefore, even though a file set does not exist as a separate, physical image file, it is accessed as though it is, placing the image on the receiving device, minus the excluded files.</p> <p>For example, <code>deviceimage.zmg</code> is the image file on your imaging server. You use Image Explorer to determine which data to exclude and assign this to a file set number, such as 2. When a device assigned to this ZENworks Image bundle boots, it is imaged with the smaller version (file set 2) of <code>deviceimage.zmg</code>.</p> <p>File sets provide an advantage because you can create a base image and modify it slightly for various devices, instead of creating separate, somewhat different base images for each device. However, because file sets only concern excluded files, if you add files to the base image using Image Explorer, all file sets include those additional files. If you don't want them included in a file set, you must use Image Explorer to exclude these new files from that file set.</p> <p>There are a maximum of 10 file sets. Each of the ten file set numbers represents the original base image, until you use Image Explorer and assign the results to a file set number.</p> <hr/> <p><b>IMPORTANT:</b> If you create 10 different file sets, then the original image can be lost. If you want to maintain the original image's information, do not use Image Explorer to assign exclusions to file set 1, which is the default file set if you don't select a file set when using this wizard.</p> <hr/>
<code>-t time_wait</code>	<p>(Optional) If not enough devices have booted to fulfill the Client Count requirement, the multicast session begins if a participating device boots and a certain amount of time passes without another participating device booting. Specify this amount of time. The default is 5 minutes.</p>
<code>-c client_count</code>	<p>(Optional) The number of participating devices you want to have booted before the multicast session begins. If you do not specify a number, the default is 1.</p>

---

**IMPORTANT:** The image is sent to and put down on each participating device only after you initiate the multicast session from each participating client.

---

**3** To view the status of the multicast session, enter:

```
/opt/novell/zenworks/preboot/bin/novell-zmgmcast -status -i
proxy_IP_address
```

The `-i` argument is optional.

- 4 To view the list of multicast sessions, enter:

```
/opt/novell/zenworks/preboot/bin/novell-zmgmcast -list -i  
proxy_IP_address
```

The `-i` argument is optional.

- 5 To stop a multicast session, enter:

```
/opt/novell/zenworks/preboot/bin/novell-zmgmcast -stop  
session_name -i proxy_IP_address
```

The `session_name` is required and the `-i` argument is optional.

- 6 Continue with [“Initiating a Multicast Session from Each Client” on page 327](#).

## Initiating a Multicast Session from Each Client

You can use the bash prompt or the ZENworks Imaging Engine menu to perform the multicast session as you physically visit each device.

The following sections contain additional information:

- ♦ [“Using the Bash Prompt to Perform the Multicast Session” on page 327](#)
- ♦ [“Using the ZENworks Imaging Engine Menu to Perform the Multicast Session” on page 328](#)

### Using the Bash Prompt to Perform the Multicast Session

- 1 (Optional) Install the Novell ZENworks Linux Management Imaging Agent (`novell-zislnx`) on each of the participating devices.

If you do not install the Imaging Agent on each participating device, the devices have duplicate network identities. For more information, see [“Limitations of Multicasting Images” on page 236](#).

- 2 Create an imaging boot CD or DVD for each person who will assist with the multicast session, or enable PXE on the participating devices.

If you don’t know how to do this, see [Section 23.2, “Setting Up the Preboot Services Methods,” on page 240](#).

- 3 At each device, including the master device (unless you are starting the multicast session from the imaging server), access a Linux prompt by using the imaging boot CD or DVD, or if it is PXE-enabled, boot it.

- 4 Enter `manual` at the boot prompt.

- 5 To identify each participating device in the multicast session, enter the following command at the bash prompt of every device:

```
img session session_name
```

where `session_name` is any string that uniquely identifies this multicast session from other multicast sessions that might be in progress on the network. Use the same session name on each of the participating devices in this multicast session. You can specify any multicast session, including one that originates from the imaging server (as long as you specify the session name used by the imaging server).

Example: `img session mcast01`

The `img session` command can take other parameters that allow you to designate the master device and the imaging start time beforehand. See [“ZENworks Imaging Engine Commands” on page 425](#) for details.

- 6 (Conditional) If you have not already done so, start the multicast session from the master device or from the imaging server.

**Master device:** To start the multicast session from the master device, after all of the other devices have registered as participants, click *Start session*.

If you start the session from the master device, the session master must be a device. If you start the session from the imaging server, the session master must be an imaging server using a previously saved image file.

The ZENworks Imaging Engine begins creating the image of the master device and the image is sent to and put down on each participating device. Any problems are reported and displayed on the master device.

**Imaging server:** To start the multicast session from the imaging server, follow the steps under [“Initiating a Multicast Session from the ZENworks Imaging Server” on page 325](#).

- 7 At each participating device, when the imaging is done, do the following to boot the device with the new operating system:

**7a** At the Linux prompt, type `lilo.s`, then press Enter.

**7b** Press Ctrl+Alt+Delete.

If the device doesn't boot to the new operating system (that is, if the Linux prompt is displayed), enter `lilo.s` again and reboot the device a second time.

### Using the ZENworks Imaging Engine Menu to Perform the Multicast Session

- 1 (Optional) Install the Novell ZENworks Linux Management Imaging Agent ([novell-zislnx](#)) on each of the participating devices.

If you do not install the Imaging Agent on each participating device, the devices have duplicate network identities. For more information, see [“Limitations of Multicasting Images” on page 236](#).

- 2 Create an imaging boot CD or DVD for each person who will assist with the multicast session, or enable PXE on the participating devices.

If you don't know how to do this, see [Section 23.2, “Setting Up the Preboot Services Methods,” on page 240](#).

- 3 At each device, including the master device (unless you are starting the multicast session from the imaging server), access a Linux prompt by using the imaging boot CD or DVD, or if it is PXE-enabled, boot it.

- 4 Enter `manual` at the boot prompt.

or

Select *Start ZENworks Imaging Maintenance* from the Preboot Services Menu.

- 5 To identify each participating device in the multicast session, type `img` at the bash prompt to display the ZENworks Imaging Engine screen.

- 6 Click *Imaging*, then click *Multicast session* (or on the task bar, click *F7 Multicast*) to start the Multicast Wizard.

- 7 Enter a session name.

The session name is any string that uniquely identifies this multicast session from other multicast sessions that might be in progress on the network. Use the same session name on each of the participating devices in this multicast session. You can specify any multicast session,



including one that originates from the imaging server (as long as you specify the session name used by the imaging server).

**8** Select a *Session role* option:

**Master:** Select this option if this is the session master.

**Client:** Select this option if this is a participating device.

**9** (Optional) If you chose Master in **Step 8**, click *Specify additional options*, click *Next*, then fill in the fields:

**Compression level:** Specify the compression level you want to use for this multicast session:

- ♦ **None:** No data compression is used. Data is sent immediately across the network to participating devices. You might use this option if the master device has a slow CPU; the amount of time to compress the data is eliminated and the data is immediately sent across the network. However, this option creates more network traffic than if you selected one of the other compression levels (*Speed*, *Balanced*, or *Size*).
- ♦ **Speed:** Takes the least amount of time to compress the data before the data is sent across the network to participating devices. You might use this option if the master device has a slow CPU; the amount of time to compress the data is reduced before the data is sent across the network. With this option, however, the multicast session creates more network traffic than if you selected either the *Balanced* or *Size* compression level.
- ♦ **Balanced:** Represents a compromise between data compression and the amount of network traffic that the multicast session creates.
- ♦ **Size:** Takes the most amount of time to compress the data before sending it across the network to participating devices. You might use this option if the master device has a fast CPU. Using this option requires the most CPU resources to compress the data but creates less network traffic to transfer the data to the participating devices.

**Automated session:** Click *Enabled* to specify the number of participating devices (clients) that must register before starting the automated multicast session and to specify the amount of time, in minutes, that can expire without the number of participating devices to register before starting the automated multicast session. If you do not click the *Enabled* check box, you must manually start the multicast session.

**10** Click *Next*, then click *Start session*.

You can cancel the session by clicking *Abort session* > *Yes* > *OK* > *Close*.

**11** At each participating device, when the imaging is done, do the following to boot the device with the new operating system:

**11a** At the Linux prompt, type `lilo.s`, then press Enter.

**11b** Press Ctrl+Alt+Delete.

If the device doesn't boot to the new operating system (that is, if the Linux prompt is displayed), enter `lilo.s` again and reboot the device a second time.

## 24.5 Assigning Unassigned Preboot Bundles

- 1 If you click *Next* on the Summary page of a wizard, or if you access this page through the *Devices* or *Bundles* tabs, the Bundle Assignments page is displayed:

[Bundles](#) > Create New Bundle

Create New Bundle Script Bundle X ?

Step 6: Bundle Assignments

Specify the assignments for this bundle:

Add	Remove	
<input type="checkbox"/>		<b>Name</b> <b>In Folder</b>
No items selected, click add to select items		

---

<< Back Next >> Cancel

The wizard's step number depends on where you access the wizard from. The examples in these instructions are based on accessing this wizard when creating a ZENworks Script bundle.

- 2 Click *Add* to display the Select Assignments dialog box:

Select Assignments

Look in: /Devices

Item name: \* Items of type: All Types

Name	Type
Servers	Folder
Workstations	Folder

2 Items 1 - 2 of 2 show 10 items

Select All 0 Items Selected Remove All

OK Cancel

- 3 Browse for and select the devices that you want to be assigned to this bundle, then click *OK*.  
You can select individual devices, or the *Servers* or *Workstations* folders containing such devices, or mixtures of folders and devices.
- 4 Click *Next* to display the Bundle Groups page:

[Bundles](#) > Create New Bundle

Create New Bundle Script Bundle X ?

Step 7: Bundle Groups

Specify the groups for this bundle:

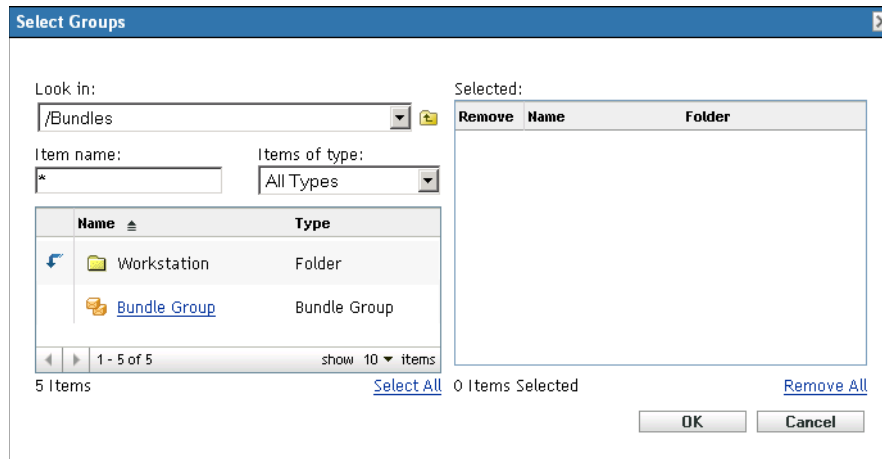
Add	Remove	
<input type="checkbox"/>		<b>Name</b> <b>In Folder</b>
No items selected, click add to select items		

---

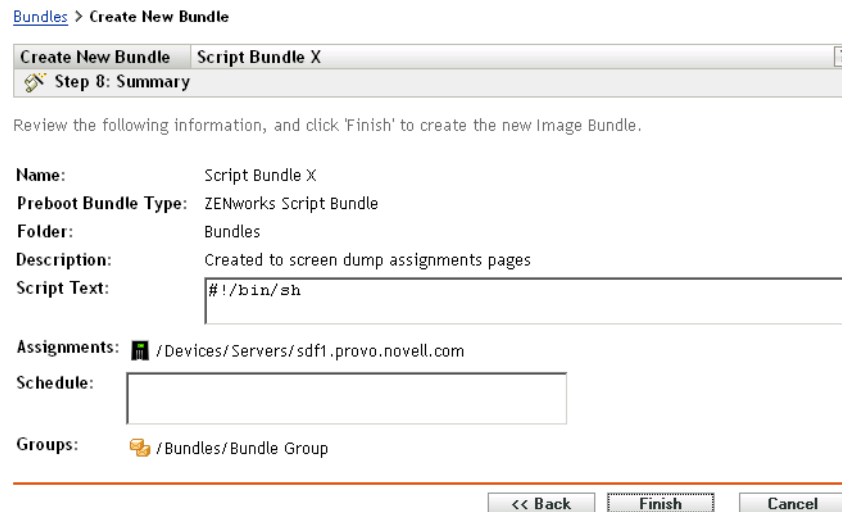
<< Back Next >> Cancel

This is optional. You can click *Next* to display the Summary page without assigning a bundle group. In this case, skip to **Step 8**.

- 5 Click *Add* to display the Select Groups dialog box:



- 6 Browse for and select the groups that you want to be assigned to this bundle, then click *OK*.  
You can select individual groups, including browsing the folders containing groups.
- 7 Click *Next* to display the Summary page:



- 8 Review the configuration, then click one of the following:  
**Back:** If necessary, use this to make changes before finishing.  
**Finish:** Click to create the bundle and assign the devices or groups to the bundle when it is created.

## 24.6 Editing Preboot Services Work

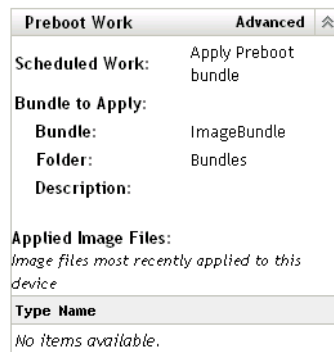
The Edit Preboot Work page allows you to view all images that are recently applied to the selected device, and the image that is currently assigned (known as its “effective” image).

To edit a server’s or workstation’s Preboot Services work:

- 1 In the ZENworks Control Center, click the *Devices* tab to display the Devices page:

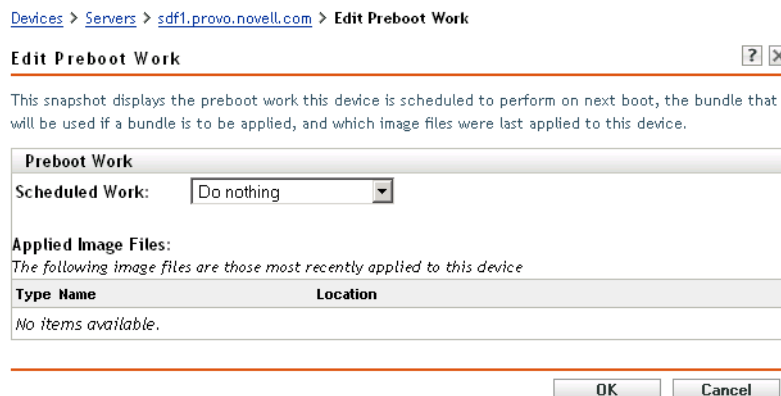


- 2 Click *Servers* or *Workstations*, then select a device to display the page with the Preboot Work section:



- 3 In the Preboot Work section, click *Advanced*.

This starts the Edit Preboot Work Wizard:



- 4 In the Preboot Work section, select one of the following from the drop-down list for the *Scheduled work* field:

**Do nothing:** Continue with **Step 5**.

**Apply Preboot bundle:** Continue with **Step 6**.

**Take an image:** Continue with **Step 7**.

- 5 If you select *Do nothing*, skip to step **Step 8**.

The Applied Image Files section displays the image files most recently applied to this device.

[Devices](#) > [Servers](#) > [sdf1.provo.novell.com](#) > **Edit Preboot Work**

**Edit Preboot Work**



This snapshot displays the preboot work this device is scheduled to perform on next boot, the bundle that will be used if a bundle is to be applied, and which image files were last applied to this device.

Preboot Work	
Scheduled Work:	Apply Preboot bundle
Bundle to Apply:	
Bundle:	ImageBundle
Folder:	Bundles
Description:	
Applied Image Files:	
The following image files are those most recently applied to this device	
Type	Name
Location	
No items available.	

OK

Cancel

- 6 If you select *Apply Preboot bundle*, fill in the field under Bundle to Apply, then skip to **Step 8**:

**Bundle:** Select or specify the bundle. Its bundle name, folder, and description are displayed.

The *Bundle* field displays the currently effective bundle. You can select the bundle to apply from the drop-down list, which changes the effective bundle for the device.

The next time the device boots, or when you manually apply a Preboot bundle (such as from a ZENworks imaging CD or DVD), the selected bundle is applied.

[Devices](#) > [Servers](#) > [sdf1.provo.novell.com](#) > **Edit Preboot Work**

**Edit Preboot Work** ? ✕

This snapshot displays the preboot work this device is scheduled to perform on next boot, the bundle that will be used if a bundle is to be applied, and which image files were last applied to this device.

**Preboot Work**

**Scheduled Work:** Take image ▾

**Server and Path of new image file:\***  🔍 Clear

**Image Compression Options:**  
☒ Use compression:  
☒ Optimize for speed  
☐ Balanced  
☐ Optimize for space

Fields marked with a blue asterisk are required.

**Applied Image Files:**  
*The following image files are those most recently applied to this device*

Type	Name	Location
No items available.		

OK Cancel

**7** If you select *Take an image*, fill in the fields, then skip to step **Step 8:**

The image is taken the next time the device boots, or when you manually apply a Preboot bundle, such as from a ZENworks imaging CD or DVD.

**Server and path of new image file:** Browse for or enter the full path to where you want the image file saved.

**Image compression options:** Select one:

- ♦ **Balanced:** Automatically balances compression between an average of the reimaging speed and the available disk space for the image file.
- ♦ **Optimize for speed:** Optimizes the compression to allow for the fastest reimaging time. Use this option if CPU speed is an issue.
- ♦ **Optimize for space:** Optimizes the compression to minimize the image file's size to conserve disk space. This can cause reimaging to take longer.

**8** Click *OK* to exit the wizard.

Your changes should be displayed in the Preboot Work section for the device.

# Hardware and Software Inventory

# VI

The following chapters provide information on Novell® ZENworks® Linux Management hardware and software inventory features:

- ♦ Chapter 25, “Inventory Overview,” on page 337
- ♦ Chapter 26, “Reviewing Device Inventory,” on page 339
- ♦ Chapter 27, “Rolling Up Hardware Inventory to the ZENworks 7 Server Management or ZENworks 7 Desktop Management Inventory Database,” on page 345





# Inventory Overview

# 25

The Server Inventory component of Novell® ZENworks® Linux Management allows you to collect hardware and software inventory information from local and remote servers or workstations of your enterprise. This inventory information is scanned and stored in a database that can be accessed by the ZENworks administrator.

The Inventory scanning capability of ZENworks Linux Management performs the following tasks:

- ♦ Collects hardware and software inventory information from workstations and servers managed within your enterprise.
- ♦ Stores the inventory information in a database that can be accessed by the ZENworks administrator.
- ♦ Rolls up the hardware inventory data from the database to the ZENworks 7 Server Management or ZENworks 7 Desktop Management Inventory database to view the inventory data at the enterprise level.



# Reviewing Device Inventory

# 26

From the ZENworks Control Center you can view the complete hardware and software inventory of servers and workstations. This chapter discusses the following topics:

- ♦ [Section 26.1, “Accessing the Device Inventory,” on page 339](#)
- ♦ [Section 26.2, “Reviewing Device Inventory Summaries,” on page 339](#)
- ♦ [Section 26.3, “Reviewing Hardware \(General\),” on page 340](#)
- ♦ [Section 26.4, “Reviewing Software \(General\),” on page 340](#)
- ♦ [Section 26.5, “Reviewing Hardware Details,” on page 340](#)

## 26.1 Accessing the Device Inventory

To view a device’s hardware and software inventory:

- 1 In the ZENworks Control Center, click the *Devices* tab.
- 2 Navigate the folder structure to locate the desired device, then click the device to show its details.
- 3 Click the *Inventory* tab.

Refer to the following sections for descriptions of the inventory information:

- ♦ [Section 26.2, “Reviewing Device Inventory Summaries,” on page 339](#)
- ♦ [Section 26.3, “Reviewing Hardware \(General\),” on page 340](#)
- ♦ [Section 26.4, “Reviewing Software \(General\),” on page 340](#)
- ♦ [Section 26.5, “Reviewing Hardware Details,” on page 340](#)

## 26.2 Reviewing Device Inventory Summaries

The Inventory page provides the following inventory information about each device:

**Table 26-1** *Inventory Information for Devices*

Scan Data Item	Description
Last Scan Date	The last time the selected managed device was scanned for inventory information
Alias	The alternative name for the managed device
Host Name	The network name that should resolve to the managed device’s IP address
Mac Address	The hardware address of the managed device’s network interface card
IP Address	The unique address of the managed device on the TCP/IP network
Subnet Mask	The network segment the managed device is on
Location	The server location

## 26.3 Reviewing Hardware (General)

The Inventory page provides the following general information about the device's hardware. For detailed hardware information, see [Section 26.5, “Reviewing Hardware Details,” on page 340](#).

**Table 26-2** *General Information about Device Hardware*

Scan Data Item	Description
Asset Tag	The asset identification number assigned to the machine by the company
Serial Number	A unique number assigned to the machine by the manufacturer
Vendor	The product supplier, such as Compaq or Dell
Operating System	The operating system currently installed on the machine
Code Page	The selected character set of the machine
Visible Memory	Total physical memory available to the operating system
Virtual Memory	Amount of virtual memory assigned

## 26.4 Reviewing Software (General)

The Inventory page provides the following information about the device's software. Click *Bundles* (Details) or *Packages* (Details) for detailed information about each.

**Table 26-3** *General Information about Device Software*

Scan Data Item	Description
Bundles	Software bundled with the server
Packages	Additional software deployed on the server

## 26.5 Reviewing Hardware Details

The following table provides common device information that might be useful for troubleshooting. For detailed information about each device, click the hardware component name in the interface.

**Table 26-4** *Common Device Information*

Inventory Item	Attributes	Description
Batteries	Name	Battery name.
	Manufacturer	Battery manufacturer name.
	Serial Number	Battery serial number.
	Chemistry	The battery chemistry, for example, lithium-ion or nickel metal hydride.

Inventory Item	Attributes	Description
BIOS	Name	BIOS name.
	Manufacturer	BIOS manufacturer name.
	Version	The version or revision level of the BIOS.
Busses	Name	Bus type, such as PCI, ISA, and others.
	Description	Bus description.
CD ROMs	Name	CD-ROM name.
	Manufacturer	CD-ROM manufacturer.
Chassis	Name	Chassis name.
	Manufacturer	Chassis manufacturer.
	Asset Tag	A code for property and product identification.
	Serial Number	Serial number assigned by the manufacturer.
Desktop Monitors	Name	Monitor name. When a monitor is connected through a KVM (keyboard, video, mouse) switch, the system might pass two instances of the desktop monitor. This is because of manufacturing limitations for the device.
	Manufacturer	Monitor manufacturer.
	Model	Identifying information of the monitor.
	Size	Monitor screen size.
Floppy Disks	Name	Floppy disk name.
	Capacity	Floppy disk capacity.
	Description	Floppy disk description.
Keyboards	Name	Keyboard brand name and model.
	Description	Description of the keyboard, such as interface, ergonomics, system requirements, and so on.
Logical Disks	Volume Label	Name of the logical disk volume.
	Filesystem Type	Type of file system, such as File Allocation Table (FAT).
	Filesystem Size	Drive's actual size in MB.
	Available Space	Available space on the logical disk.

Inventory Item	Attributes	Description
Modems	Name	Modem name.
	Manufacturer	Modem manufacturer.
Motherboards	Name	Motherboard name.
	Manufacturer	Motherboard manufacturer name.
	Version	The version of the motherboard.
	Slots	The number of expansion slots in the motherboard for adding more memory, graphic capabilities, and support for special devices.
Network Adapters	Name	Network adapter name.
	Manufacturer	Network adapter manufacturer.
	Maximum Speed	Rate at which the information is transferred over the LAN.
	Mac Address	Short for Media Access Control address, a hardware address that uniquely identifies each node of a network.
Parallel Ports	Name	Port name.
	Description	Port description.
Physical Disks	Name	Disk name.
	Manufacturer	Disk manufacturer.
	Capacity	Capacity of the disk.
	Free Space	Remaining free space on the disk.
Pointing Devices	Name	Pointing device name.
		When a pointing device is connected through a KVM (keyboard, video, mouse) switch, the system might not pass the correct name and configuration of the device, because of manufacturing limitations for the device.
	Buttons	Number of buttons.
	Description	Description of the pointing device.
Power Supplies	Name	Name of the power supply.
	Description	A description of the power supply.
Processors	Name	Processor name.

Inventory Item	Attributes	Description
	Family	The name of the class or group to which the processor belongs, such as Pentium II, Pentium III, and others.
	Speed	The speed at which a microprocessor executes instructions. Every computer contains an internal clock that regulates the rate at which instructions are executed and that synchronizes all the various computer components. Clock speeds are expressed in megahertz (MHz) or gigahertz (GHz).
Serial Ports	Name	Serial port name.
	Description	Serial port description.
Sound Adapters	Name	Sound adapter name.
	Description	A description of the sound adapter.
Video Adapters	Name	Video adapter name.
	Manufacturer	Manufacturer name.





# Rolling Up Hardware Inventory to the ZENworks 7 Server Management or ZENworks 7 Desktop Management Inventory Database

You can roll up the hardware inventory data from the Novell® ZENworks® 7 Linux Management database to the ZENworks 7 Server Management or ZENworks 7 Desktop Management Inventory database to view the inventory data at the enterprise level.

Review the following sections:

- ♦ [Section 27.1, “Preparing to Roll Up Inventory,” on page 345](#)
- ♦ [Section 27.2, “Configuring the Inventory Roll-Up Policy,” on page 345](#)
- ♦ [Section 27.3, “Understanding the Roll-Up Process,” on page 347](#)
- ♦ [Section 27.4, “Understanding the Components Involved in the Inventory Roll-Up,” on page 348](#)
- ♦ [Section 27.5, “Viewing the Inventory Data Stored in the ZENworks 7 Server Management or ZENworks 7 Desktop Management Inventory Database,” on page 349](#)

## 27.1 Preparing to Roll Up Inventory

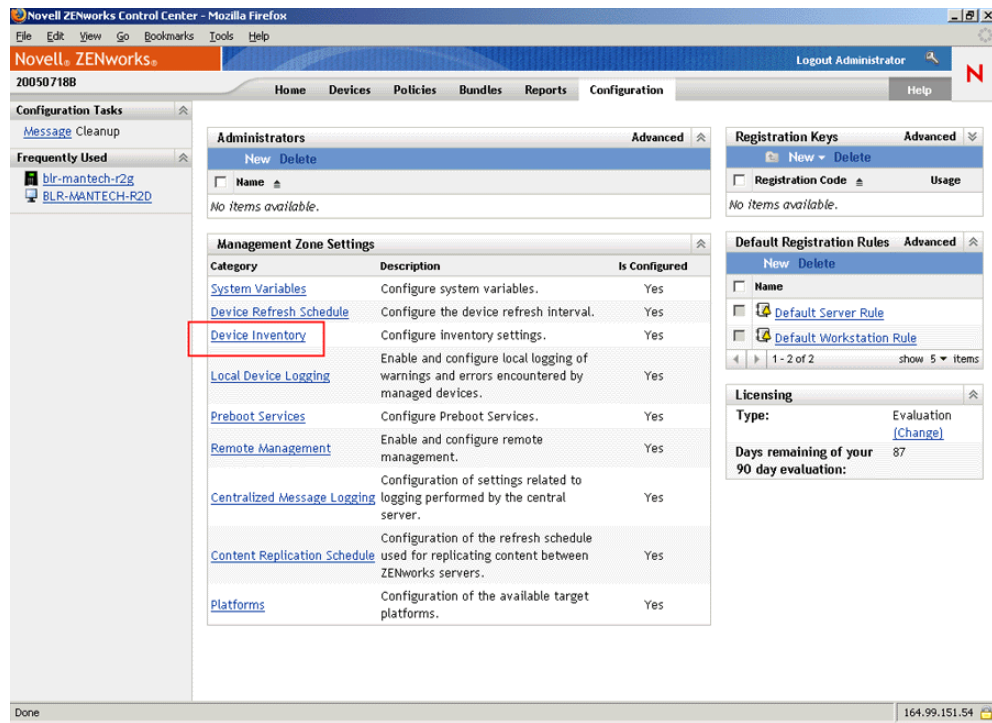
Ensure that the following prerequisites are met:

- ☐ ZENworks 7 Linux Management has been successfully installed.
- ☐ The hardware inventory data has been stored in the ZENworks Linux Management database.
- ☐ The ZEN Loader service is up and running on the ZENworks Linux Management server.
- ☐ The Inventory server and Inventory database components of ZENworks 7 Server Management or ZENworks 7 Desktop Management have been successfully installed and set up.
- ☐ One of the following roles for the ZENworks 7 Inventory server has been configured:
  - ♦ Root Server
  - ♦ Root Server with Workstations
  - ♦ Intermediate Server with Database
  - ♦ Intermediate Server with Database and Workstations
- ☐ The Inventory service is up and running on the ZENworks 7 Server Management or ZENworks 7 Desktop Management Inventory server.

## 27.2 Configuring the Inventory Roll-Up Policy

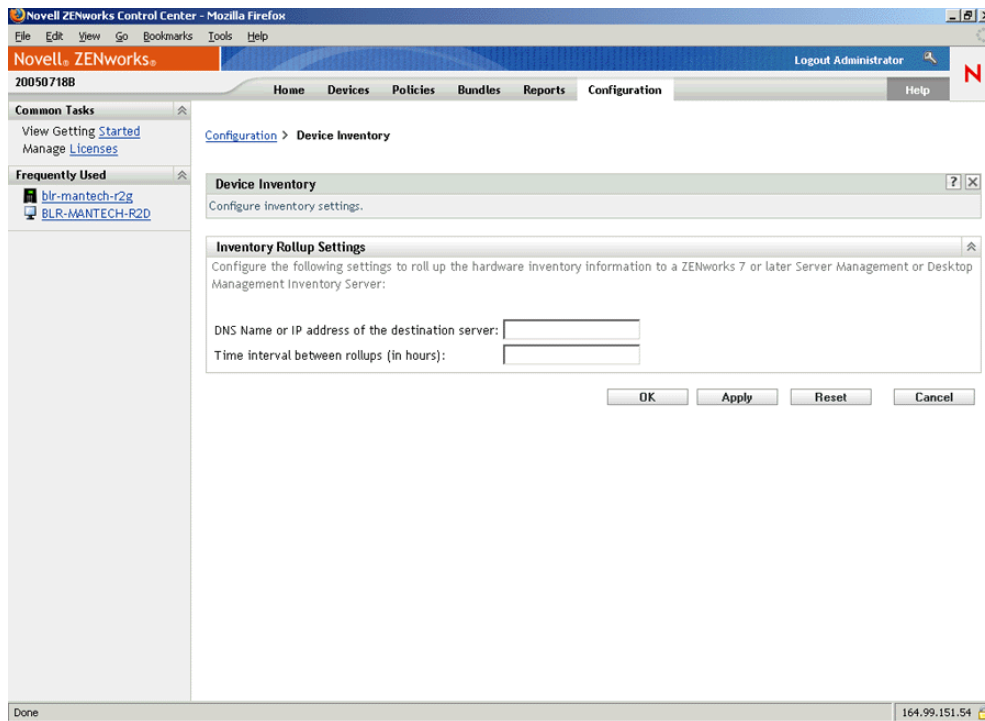
- 1 In the ZENworks Control Center, click *Configuration*.

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



- 3 In the *Inventory Roll-Up Settings* pane, do the following:
- 3a Specify the DNS name or the IP address of the ZENworks 7 Server Management or ZENworks 7 Desktop Management Inventory server to which you want to roll up the hardware inventory data.

**3b** Specify the time interval between roll-ups. By default, the time interval is 168 hrs.



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

## 27.3 Understanding the Roll-Up Process

ZENworks uses the following process to collect inventory and roll it up to the Inventory server

1. The Sender converts the hardware inventory stored in the ZENworks 7 Linux Management database into .str files, and places the files into the `/var/opt/novell/zenworks/inventory/entmerge` directory.
2. The Sender moves the .str files from the `entmergedir` directory to the `entpushdir` directory, and compresses the files as a .zip file.
3. The Sender sends the .zip file from the `entpushdir` directory to the Receiver on the ZENworks 7 Server Management or ZENworks 7 Desktop Management Inventory server.
4. The Receiver places the .zip files in the `/entpushdir/zipdir` directory.
5. The Receiver copies the .zip files to the `/entpushdir` directory and deletes the .zip files from the `entpushdir\zipdir` directory.
6. The Receiver copies the .zip files to the database directory (`dbdir`) if a database is attached to the Inventory server.
7. The Sender-Receiver logs the status in Novell eDirectory™.

## 27.4 Understanding the Components Involved in the Inventory Roll-Up

The Sender on the Inventory servers transfer the scan files from the ZENworks 7 Linux Management Inventory server to the ZENworks 7 Server Management or ZENworks 7 Desktop Management Inventory server. The following sections contain more information:

- [Section 27.4.1, “Understanding the Sender,” on page 348](#)
- [Section 27.4.2, “Understanding the Compressed Scan Data File,” on page 348](#)

### 27.4.1 Understanding the Sender

The Sender is a Java\* component that runs on any ZENworks 7 Linux Management server. The Sender is a service loaded by the ZEN Loader.

The flow of information from the Sender in the roll-up of inventory information is as follows:

1. The ZEN Loader starts the Sender on the Inventory server. At the time specified in the Roll-Up Schedule, the Sender moves the scan data files (.str) from the enterprise merge directory (entmergedir) to the enterprise push directory (entpushdir).

The Sender compresses these .str files in the \entpushdir directory of the Inventory server as a .zip file and then deletes the .str files. This .zip file is again compressed with the .prp file into a .zip file. The .prp file is an internal file containing information about the .zip file.

2. Based on the Discard Scan Data Time in the Inventory Service object properties of the Receiver, the Sender deletes the compressed .zip files in the \entpushdir directory that have been created earlier than the specified discard scan data time. This removes unwanted scan information being sent in the roll-up.
3. The Sender sends the compressed .zip files to the Receiver, with the oldest compressed files sent first.
4. The Sender after transferring the .zip file, deletes the compressed files in the \entpushdir directory.

If the Sender is unable to connect to the Receiver, the Sender retries to connect after 10 seconds. The time interval increases exponentially by a factor of 2. After 14 retries, the Sender stops trying to connect to the Receiver. The Sender retries for approximately 23 hours before it discontinues trying. The Sender does not process any other information while it is establishing the connection.

### 27.4.2 Understanding the Compressed Scan Data File

The Sender compresses the scan data files (.str) into a .zip file. This .zip file is again compressed with the .prp file into a .zip file. The .zip file (containing the .zip files and .prp) is named using the following naming conventions:

*scheduledtime\_inventoryservername\_treename\_storedstatus.zip*

where *scheduledtime* refers to the date and time when the .zip file is created, *inventoryservername* refers to the Inventory server on which the .zip file was compressed, *treename* refers to the unique tree name in which the .zip file is currently located, *storedstatus* refers to the storage status of the .zip file, and *ZIP* is the file extension for the compressed files. The *storedstatus* displays 0, 1, or 2. 0

indicates the .zip file has not yet been stored. 1 indicates the .zip file will be stored for the first time in the Inventory server. 2 indicates the .zip file has already been stored once

The .zip filename changes depending on if the database is attached to the Inventory server.

The .zip file contains the .zip files and a property file. The property file is named using the following conventions:

*scheduledtime\_inventoryservername.prp*

The property file contains the scheduled time, Inventory server name, and signature. The signature helps to authenticate the .zip file.

Each .zip file can contain a maximum of 50 .str files.

## 27.5 Viewing the Inventory Data Stored in the ZENworks 7 Server Management or ZENworks 7 Desktop Management Inventory Database

You can view the inventory data stored in the ZENworks 7 Server Management or ZENworks 7 Desktop Management Inventory database using the following Inventory ConsoleOne® utilities:

- ♦ Inventory Query
- ♦ Inventory Reports

For more information on how to invoke and work with these utilities, see the “[Workstation Inventory](#)” section in the *Novell ZENworks 7 Desktop Management Administration Guide* or the “[Server Inventory](#)” section in the *Novell ZENworks 7 Server Management Administration Guide*.



# Remote Management

# VII

The Remote Management component of Novell® ZENworks® 7 Linux Management gives you the ability to remotely manage devices from the management console. Remote Management allows you to:

- ♦ Remotely control the managed device
- ♦ Remotely view the managed device
- ♦ Remotely login to the managed device
- ♦ View log information about any Remote Management sessions performed on any managed device from anywhere in your network

Remote Management can save you and your organization time and money. For example, you or your organization's help desk can analyze and remotely fix problems on the devices without visiting the user's device, which reduces problem resolution time and increases productivity.

The following sections will help you understand and use Remote Management:

- ♦ [Chapter 28, “Remote Management Overview,” on page 353](#)
- ♦ [Chapter 29, “Setting Up Remote Management,” on page 355](#)





You can use Novell® ZENworks® 7 Linux Management to remotely manage all the supported platforms. To see details on supported platforms, see “[Managed Device Requirements](#)” under “[System Requirements](#)” in the *Novell ZENworks 7 Linux Management Installation Guide*.

The following sections provide information to help you understand the functionality of Remote Management components:

- ♦ [Section 28.1, “Remote Management Terminology,” on page 353](#)
- ♦ [Section 28.2, “Understanding the Remote Management Components,” on page 353](#)

## 28.1 Remote Management Terminology

**Managed device:** A device that you want to remotely manage. To remotely manage a managed device, you must install the ZENworks 7 Linux Management Agent on it.

**Management server:** A server where ZENworks 7 server is installed.

**Management console:** A Windows or Linux device that provides console to manage ZENworks. The management console provides the interface to manage and administer your workstations.

**Administrator:** A person who can perform various Remote Management operations.

**Remote Control Service:** A component that is installed on a managed device, enabling the administrator to remotely control and remote view the managed device. The Remote Control Service starts automatically when the managed device boots up. It verifies whether the administrator is allowed to perform Remote Control operations on the managed device before the Remote Management session proceeds with authentication.

**Remote Login Service:** A component that is installed on a managed device, enabling the administrator to remotely login into the managed device. The Remote Login Service starts automatically when the managed device boots up. It verifies whether the administrator is allowed to perform Remote Login on the managed device before the Remote Management session proceeds with authentication.

**Remote Management Viewer:** A window displaying the desktop session of the managed device.

## 28.2 Understanding the Remote Management Components

The following sections provide information to help you understand the functionality of Remote Management components. You must install the Remote Management Agent on the managed devices to perform the Remote Management operations.

- ♦ [Section 28.2.1, “Understanding Remote Control,” on page 354](#)
- ♦ [Section 28.2.2, “Understanding Remote View,” on page 354](#)
- ♦ [Section 28.2.3, “Understanding Remote Login,” on page 354](#)

## **28.2.1 Understanding Remote Control**

Remote Control lets you control a managed device desktop from the management console so you can provide user assistance and help resolve problems on the devices.

Remote Control establishes a connection between the management console and the managed device. With remote control connections, the administrator can go beyond viewing a managed device to taking control of it.

## **28.2.2 Understanding Remote View**

Remote View lets you view the managed device instead of controlling it. This helps you troubleshoot problems that the user encountered by observing how the user at a managed device performs certain tasks.

## **28.2.3 Understanding Remote Login**

Remote Login lets you login into a managed device from the management console. This helps you to start a new graphical session without disturbing the user on the managed device. The user on the managed device would not be able to view a Remote Login session.

# Setting Up Remote Management

# 29

The following sections provide information on deploying the Remote Management component of Novell® ZENworks® 7 Linux Management in a production environment:

- ♦ [Section 29.1, “Configuring the Remote Management Settings,” on page 355](#)
- ♦ [Section 29.2, “Configuring Remote Management Agent,” on page 358](#)
- ♦ [Section 29.3, “Starting Remote Management Operations Using the ZENworks Control Center,” on page 359](#)
- ♦ [Section 29.4, “Starting Remote Management Operations Using the Native VNCViewer,” on page 362](#)
- ♦ [Section 29.5, “Establishing SSH Tunneling,” on page 363](#)
- ♦ [Section 29.6, “Improving Remote Management Performance,” on page 364](#)

## 29.1 Configuring the Remote Management Settings

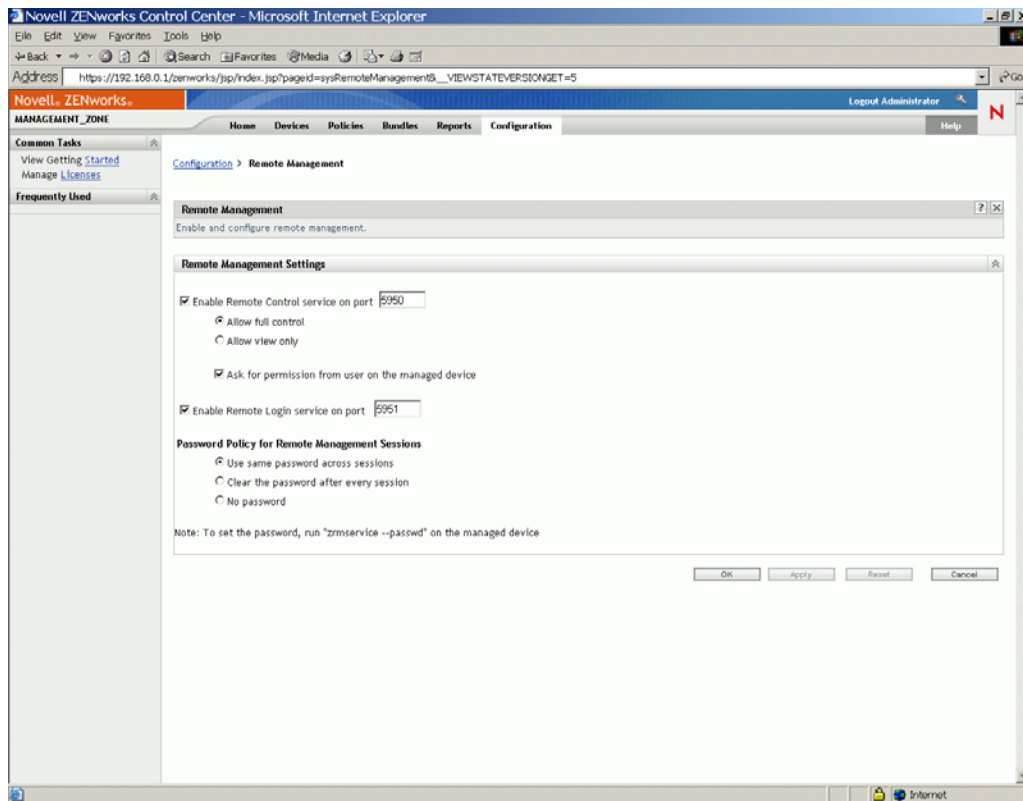
Remote Management Settings allows you to configure the Remote Management settings for the management zone. This includes enable and disable options for remote management operations as well as configurations for custom ports. The Remote Management Settings can be applied at Zone, Folder, and Device levels.

- ♦ [Section 29.1.1, “Configuring Remote Management Settings at the Zone Level,” on page 355](#)
- ♦ [Section 29.1.2, “Configuring Remote Management Settings at the Folder Level,” on page 357](#)
- ♦ [Section 29.1.3, “Configuring Remote Management Settings at the Device Level,” on page 357](#)

### 29.1.1 Configuring Remote Management Settings at the Zone Level

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

2 In the Management Zone Settings section, click *Remote Management*.



3 To enable the Remote Control Service on a particular port, select the *Enable remote control service on port* option.

By default, the Remote Control Service listens on port number 5950.

4 Select *Allow full control* or *Allow view only*.

Select *Allow full control* to enable the user to perform both remote control and remote view operation to a managed device. Select *Allow view only* to enable the user to perform only remote view operations to a managed device. Selecting *Allow view only* disallows the user to perform remote control operation.

5 Select the *Ask for permission from user on the managed device* option to request the permission of a user on the managed device before starting a Remote Control or Remote View session.

6 To enable Remote Login Service on a particular port, select the *Enable remote login service on port* option.

By default, the Remote Login Service listens on port 5951.

7 In the Password Policy for Remote Management Sessions section, select the desired option.

Select *Use same password across sessions* to use the same password across all sessions. By default, this option is selected. Select *Clear the password after every session* to set the password for every session. If you select this option, the password is cleared after every successful or unsuccessful attempt for a Remote Management operation. If you want to launch a Remote Control, Remote Login, or Remote View operation without asking for a password, select *No password*.

---

**NOTE:** We recommend you to use the *No password* option judiciously as it allows access to the managed device without any password.

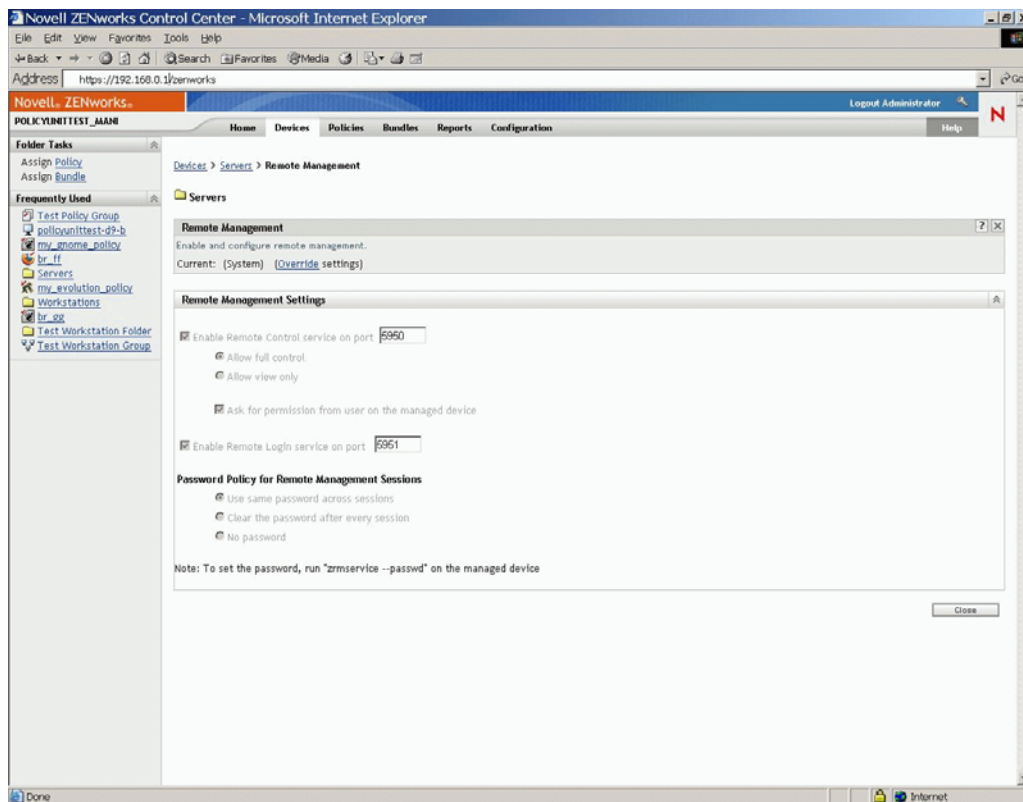
---

- 8 Click *Apply*.

These changes will be effective on the managed devices on their next Settings Refresh Schedule.

## 29.1.2 Configuring Remote Management Settings at the Folder Level

- 1 In the ZENworks Control Center, click *Devices*.
- 2 Click the folder you wish to configure.
- 3 Click *Settings*, then click *Remote Management*.



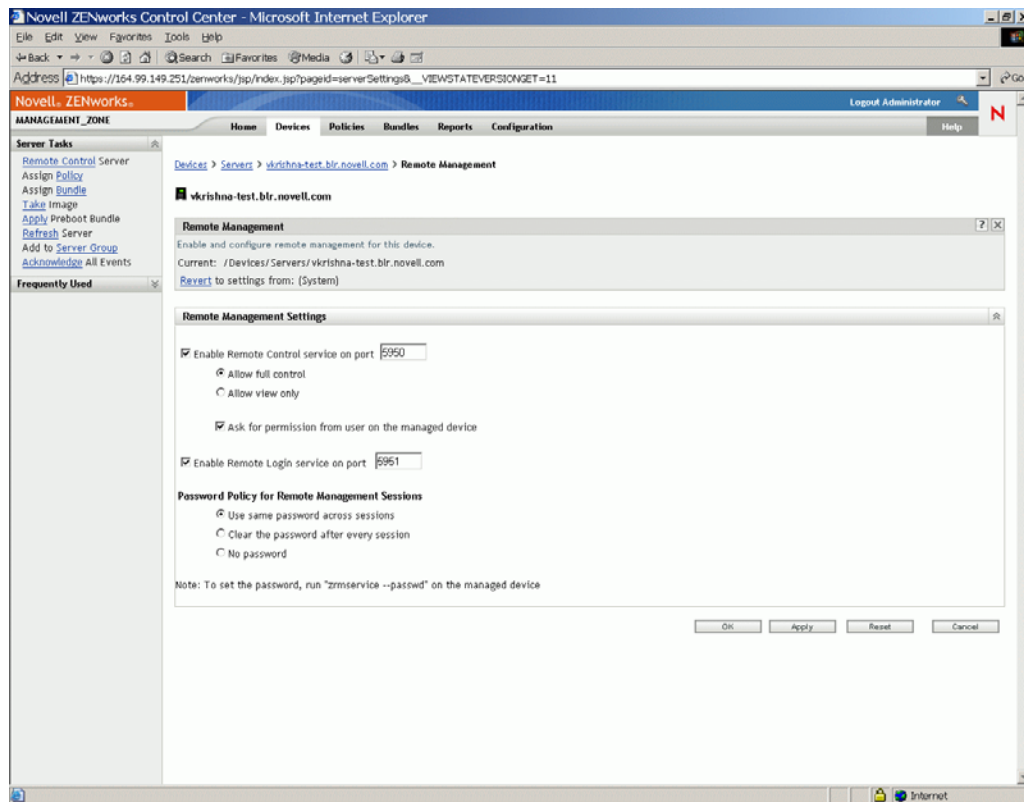
- 4 Click *Override*.
- 5 Edit the Remote Management Settings as required.
- 6 Click *Apply*.

These changes will be effective on the managed devices on their next Settings Refresh Schedule.

## 29.1.3 Configuring Remote Management Settings at the Device Level

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

- 2 Click *Servers* or *Workstations* to display the list of managed devices.
- 3 Click the name of a device for which you want to configure Remote Management.
- 4 Click *Settings*, then click *Remote Management*.



- 5 Click *Override*.
- 6 Edit the Remote Management Settings as per your requirements.
- 7 Click *Apply*.

These changes will be effective on the managed device on its next Settings Refresh Schedule.

## 29.2 Configuring Remote Management Agent

The Remote Management Agent allows you to remotely manage the device and configure the following:

- ◆ Section 29.2.1, “Setting Up the Remote Management Agent Password on the Managed Device,” on page 359
- ◆ Section 29.2.2, “Clearing the Remote Management Agent Password,” on page 359
- ◆ Section 29.2.3, “Clearing Remote Management Agent Log Files,” on page 359

## 29.2.1 Setting Up the Remote Management Agent Password on the Managed Device

The user on the managed device must set a Remote Management Agent password and communicate the password to the administrator.

To set the Agent password on the managed device, enter the following command at the shell prompt:

```
# /opt/novell/zenworks/sbin/zrmservice --passwd
```

The password is case-sensitive and should be between three to eight characters in length.

---

**NOTE:** This step is not necessary if the Password Policy is configured to *No password*.

---

## 29.2.2 Clearing the Remote Management Agent Password

To clear the Agent password on the managed device, enter the following command at the shell prompt:

```
# /opt/novell/zenworks/sbin/zrmservice --clrpasswd
```

## 29.2.3 Clearing Remote Management Agent Log Files

To clear the Agent log files on the managed device, enter the following command at the shell prompt:

```
# /opt/novell/zenworks/sbin/zrmservice --clearlog
```

# 29.3 Starting Remote Management Operations Using the ZENworks Control Center

The ZENworks Control Center is the comprehensive web-based control interface for ZENworks 7 Linux Management. It provides an intuitive and task-driven console to manage various ZENworks components including Remote Management.

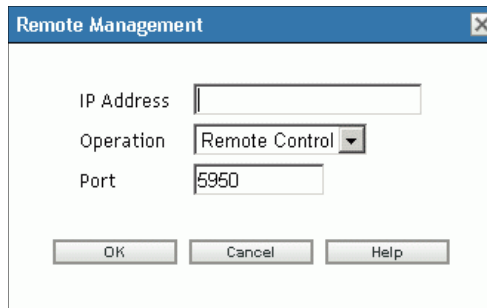
You can initiate various Remote Management operations from the following locations:

- ♦ [Section 29.3.1, “Initiating a Remote Management Session from Common Tasks,” on page 359](#)
- ♦ [Section 29.3.2, “Initiating a Remote Management Session from the Device Context,” on page 360](#)

## 29.3.1 Initiating a Remote Management Session from Common Tasks

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

- 2 In Device Tasks in the left pane, click *Remote Control Device* to open the following dialog box:

A screenshot of a 'Remote Management' dialog box. It has a title bar with 'Remote Management' and a close button. Inside, there are three fields: 'IP Address' with an empty text box, 'Operation' with a dropdown menu showing 'Remote Control', and 'Port' with a text box containing '5950'. At the bottom are three buttons: 'OK', 'Cancel', and 'Help'.

- 3 In the *IP address* field, specify the IP address or DNS name of the device you want to remotely control.
- 4 Select the Remote Management operation to be performed on the device. The available options are *Remote control*, *Remote view*, and *Remote login*.

The following table lists and explains all the operations you can select from the drop-down list:

Option	Description
Remote control	Allows you to take control of the managed device.
Remote view	Allows you to view the managed device.
Remote login	Allows you to remotely log in to a new desktop session on the managed device. This desktop cannot be viewed by the users on the managed device.

- 5 Specify the port number configured for the selected operation.  
The auto-populated port numbers are those which are configured in the Remote Management Settings at Zone Level.
- 6 Click *OK*.
- 7 Read the Java Security message and click *Yes* to accept the Certificate of the Signed Applet. To avoid the message to be displayed again, select *Always*.
- 8 If the *Ask for permission from user on the managed device* setting is enabled, click *Yes* in the permission change dialog-box on the managed device.
- 9 Specify the password at the management console, then click *OK*.

---

**IMPORTANT:** We recommend you to use Java plug-in 1.4.x in the browser of the Management Console.

---

## 29.3.2 Initiating a Remote Management Session from the Device Context

You can perform Remote Management operations on a specific device.

- 1 In the ZENworks Control Center home page, click *Devices*.
- 2 Click *Servers* or *Workstations*.

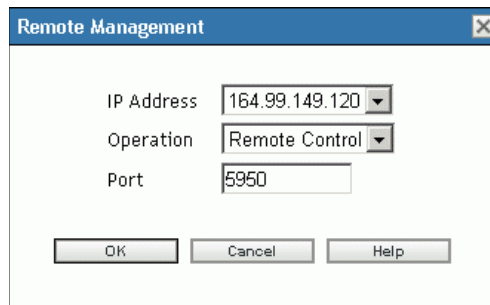


- 3 Select the device you want to remotely control.

or

Click the device name, then click *Remote Control* in Server Tasks (if you have selected Server) or *Workstation Tasks* (if you have selected Workstation) in left pane.

- 4 If you have selected the device in step 3, click *Remote control* in the *Action* menu to open the Remote Management dialog box:

The image shows a 'Remote Management' dialog box. It has a title bar with the text 'Remote Management' and a close button (X). Inside the dialog, there are three fields: 'IP Address' with a dropdown menu showing '164.99.149.120', 'Operation' with a dropdown menu showing 'Remote Control', and 'Port' with a text box containing '5950'. At the bottom of the dialog, there are three buttons: 'OK', 'Cancel', and 'Help'.

- 5 Select the IP address of the device.
- 6 Select the Remote Management operation to be performed on the device.

The drop-down list of operations is based on the effective Remote Management Settings for the managed device. The available options are *Remote control*, *Remote view*, and *Remote login*.

The following table lists and explains all the operations you can select from the drop-down list:

Option	Description
Remote Control	Allows you to take control of the managed device.
Remote View	Allows you to view the managed device.
Remote Login	Allows you to remotely login to a new desktop session on the managed device. This desktop cannot be viewed by the users on the managed device.

- 7 Specify the port number configure for the selected operation.

The auto-populated port numbers are those which are configured in the effective Remote Management Settings for the selected device.

- 8 Click *OK*.
- 9 Read the Java Security message and click *Yes* to accept the Certificate of the Signed Applet. To avoid the message to be displayed again, select *Always*.
- 10 If the *Ask for permission from user on the managed device* setting is enabled, click *Yes* on the permission change dialog-box on the managed device.
- 11 Specify the password at the management console, then click *OK*.

## 29.4 Starting Remote Management Operations Using the Native VNCViewer

The following sections contain additional information:

- [Section 29.4.1, “Starting Remote Management Operations Using the Windows VNC Viewer,” on page 362](#)
- [Section 29.4.2, “Starting Remote Management Operations Using the Linux VNC Viewer,” on page 363](#)

### 29.4.1 Starting Remote Management Operations Using the Windows VNC Viewer

- 1 Download the latest stable version of the native VNC Viewer from the [TightVNC web site](http://www.tightvnc.com/download.html) (<http://www.tightvnc.com/download.html>).
- 2 Install Tight VNC from the executable you have downloaded.
- 3 Launch the Tight VNC Viewer from *Start > Programs > Tight VNC > Tight VNC Viewer*.

---

**IMPORTANT:** We recommend using Tight VNC Viewer (Fast Compression) over fast links and Tight VNC Viewer (Best Compression) over slow links.

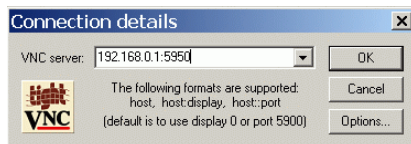
---

- 4 In *Connection details*, specify the IP address with a port number as configured, then click *OK*.

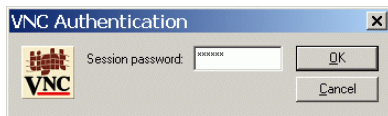
You can specify the port number after the IP address with a doublecolon (::) preceding it. For example, if the IP address of the managed device is 192.168.0.1, and the Remote Control Service port number is 5950, specify as 192.168.0.1::5950.

You can specify the display number after the IP address with a singlecolon (:) preceding it. For example, if the IP address of the managed device is 192.168.0.1, and the Remote Control Service port number is 5950, specify the IP address as 192.168.0.1:50.

You can also specify a DNS name instead of an IP address.



- 5 In *VNC authentication*, specify the correct password, then click *OK*.



Now, you will have an access to the desktop of the managed device you have specified.

## 29.4.2 Starting Remote Management Operations Using the Linux VNC Viewer

- 1 Download the latest stable version of native VNC Viewer from the TightVNC Web site at [TightVNC web site \(http://www.tightvnc.com/download.html\)](http://www.tightvnc.com/download.html).
- 2 Install Tight VNC from the RPM Package you have downloaded.
- 3 Launch Tight VNC Viewer by specifying the following command at the Shell prompt:  

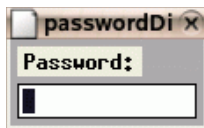
```
$ vncviewer
```
- 4 In serverDialog, specify the IP address with a port number as configured, then click *OK*.



You can specify the port number after the IP address with a doublecolon (::) preceding it. For example, if the IP address of the managed device is 192.168.0.1, and the Remote Control Service port number is 5950, specify the IP address as 192.168.0.1::5950.

You can specify the display number after the IP address with a singlecolon (:) preceding it. For example, if the IP address of the managed device is 192.168.0.1, and the Remote Control Service port number is 5950, specify as 192.168.0.1:50.

- 5 In passwordDialog, specify the correct session password, then click *OK*.



Now, you will have an access to the desktop of the IP address you have specified.

## 29.5 Establishing SSH Tunneling

The VNC protocol and data are unencrypted between the management console and the managed device. If you perform Remote Management operations over an insecure network like Internet, you should tunnel the VNC protocol using SSH for secure communication.

- 1 Establish SSH tunneling to use VNC between management console and managed device.  
  
For more information on establishing VNC through an SSH tunnel between the console and managed device, see [Section F.1, “SSH Tunneling between a Linux Management Console and a Linux Managed Device,” on page 457](#).
- 2 Launch the Remote Control session from Device Tasks at the top left of the ZENworks Control Center on the Devices page.
- 3 Specify the IP address and port of the configured SSH tunnel.
- 4 Select the desired operation from drop-down list.
- 5 Click *OK*.

## 29.6 Improving Remote Management Performance

The performance during a Remote Management session over a slow link or a fast link varies depending on the network traffic. For better response time, try one or more of the following strategies:

### On the Management Console

On the Remote Management viewer window at the console, click *Options* and set the following values:

- ♦ Set the Encoding value to Tight
- ♦ Adjust the Compression level and JPEG image quality depending on the quality of the image required.
- ♦ Set Cursor Shape Updates to No.
- ♦ Set the CopyRect option to Yes.
- ♦ Use 8 bit color mode by setting Restricted Colors to Yes.

### On the Managed Device

- ♦ The speed of the Remote Management session depends upon the processing power of the managed device. We recommend that you use Pentium\* III, 500MHz (or later) with 64 MB RAM or higher.
- ♦ Disable the wallpaper.
- ♦ Configure the following settings at the managed device:
  - ♦ Reduce the screen resolution.
  - ♦ Reduce the depth of color pixels.

### More Performance Tuning Tips

For additional information on performance tuning tips, refer to the following Web sites for specific components:

- ♦ [www.tightvnc.com](http://www.tightvnc.com) (<http://www.tightvnc.com>)
- ♦ [www.realvnc.com](http://www.realvnc.com) (<http://www.realvnc.com>)
- ♦ [FAQs on x11VNC](http://www.karlrunde.com/x11vnc) (<http://www.karlrunde.com/x11vnc>)

# Event Monitoring

# VIII

Novell® ZENworks® 7 Linux Management includes a Message Logger component that tracks and logs significant system events. Administrators can use this information to monitor events related to devices, policies, and bundles. Specifically, event monitoring allows you to

- ♦ Monitor problems associated with devices, policies, and bundles
- ♦ Track successful events
- ♦ Log events and run reports
- ♦ View a summary of problems on a hot list

This section contains the following topics:

- ♦ [Chapter 30, “Event Monitoring Overview,” on page 367](#)
- ♦ [Chapter 31, “Working with Event Logs,” on page 371](#)
- ♦ [Chapter 32, “Message Logger,” on page 377](#)
- ♦ [Chapter 33, “Configuring Message Logger Settings,” on page 379](#)



Event monitoring allows you to manage your environment by taking messages from the Message Logger and displaying them in various event logs, making it easy to track errors, problems, and successful events for your devices, policies, and bundles.

You can capture and store specific events related to devices, policies, and bundles that you or your organization's help desk can analyze and use to monitor problems without visiting the server or workstation, which can reduce problem resolution times and increase productivity. The captured information includes a description, time stamp, severity status, and message ID.

To keep your environment running at its maximum efficiency, you can use the event logs to stay abreast of critical errors and help you to troubleshoot and fine-tune your environment.

The following sections provide additional information:

- ♦ [Section 30.1, “Event Monitoring Terminology,” on page 367](#)
- ♦ [Section 30.2, “Monitoring Device Events,” on page 367](#)
- ♦ [Section 30.3, “Monitoring Policy Events,” on page 368](#)
- ♦ [Section 30.4, “Monitoring Bundle Events,” on page 368](#)
- ♦ [Section 30.5, “Using the Hot List,” on page 368](#)

## 30.1 Event Monitoring Terminology

**Event:** Something that happens, such as a successful installation, that triggers a message to be created and sent.

**Local Log:** A list of the event messages generated by the ZENworks Agent that resides on the server or workstation.

**System Log:** A list of event messages displayed only for servers that are functioning as primary or secondary ZENworks Servers. The log lists the system event messages generated by the ZENworks Server for activities that it performs on behalf of all managed devices in its Management Zone.

**Message:** A detailed description of an event. A message explains an exception such as an error or warning, provides information to a user, or includes a debug statement used for debugging the module.

**Community String:** The protocol password for SNMP. Applications use community strings for access control. You can use the trap receiver console to define the set of community strings to accept the trap. The agent, in turn, accepts or rejects the operation. When none of the community string matches, the trap is discarded.

## 30.2 Monitoring Device Events

When you use Novell® ZENworks® Linux Management to remotely install applications, you need feedback on the success and failure of certain events so you can keep your systems working at an optimal level. With event monitoring, you can track things such as software installation on client





To view the Hot List, click *Home* on the toolbar. This page shows the System Summary and the Hot List. The System Summary page shows the various categories-servers, workstations, policies, and bundles-and their respective status counts. In this example, there are four policies and none have had a warning or critical event; one server that has not had any warning or critical events; and seven bundles that haven't had any warnings or critical events. In the workstation category, one workstation has had at least one critical event. You can click the workstation name to view a summary, which includes details of the problem events.



# Working with Event Logs

# 31




Event logs are automatically created for important events, such as successful installations or critical errors.

The following sections provide additional information:



- ♦ [Section 31.1, “The Event Log Page,” on page 371](#)
- ♦ [Section 31.2, “Working with the Log Pages,” on page 372](#)

## 31.1 The Event Log Page



The Event Log page gives you an overview of the recorded events. The Event Log lists the event messages generated by the ZENworks® Agent that resides on the server or workstation. The list is ordered by date, with the latest date first. Each event listed includes the following information:

- ♦ **Status:** An indication of the event’s severity:
  - ♦ The  icon indicates an event has executed successfully.
  - ♦ The  icon indicates an exception condition that might cause problems but that might not need immediate attention.
  - ♦ The  icon indicates that an action could not be completed because of a user or system error, and it needs immediate attention.
- ♦ **Event:** Something that happens, such as a successful installation, that triggers a message to be created and sent. Click the event message to display additional details. You can use the message details window to acknowledge the message, which causes the message to be cleared from the event log.
- ♦ **Data:** The date and time the event occurred.
- ♦ **Advanced:** A page showing you both acknowledged and unacknowledged events. You can sort events by status, date, or whether an event has been acknowledged or not. You can also acknowledge events from this page.

**Figure 31-1** Event Logs

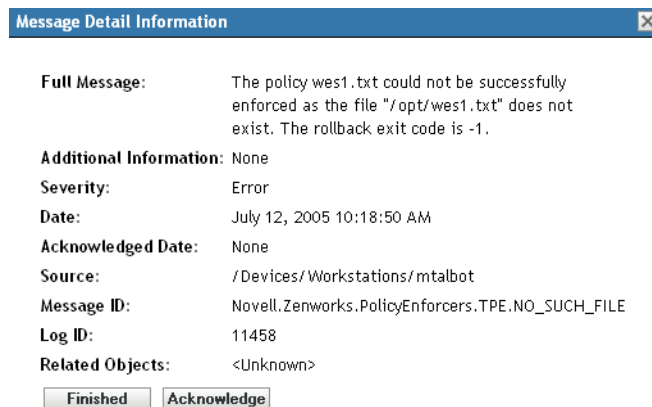
Event Log		Advanced	⌵
Status	Event	Date	
	<a href="#">The IP address of destination Inventory server has</a>	7/7/05 10:58:53 AM	
	<a href="#">The IP address of destination Inventory server has</a>	7/7/05 10:58:53 AM	
	<a href="#">The IP address of destination Inventory server has</a>	7/7/05 10:58:33 AM	
1 - 3 of 3		show 10 ▾ items	

System Event Log		Advanced	⌵
Status	Event	Date	
	<a href="#">Device mtalbot was successfully updated</a>	7/14/05 8:20:41 AM	
	<a href="#">Device sdf1.provo.novell.com was successfully upd:</a>	7/14/05 7:37:48 AM	
	<a href="#">Device veritech was successfully updated</a>	7/14/05 7:34:20 AM	
	<a href="#">Device linux was successfully updated</a>	7/14/05 7:07:41 AM	
	<a href="#">Device mtalbot was successfully updated</a>	7/14/05 6:20:32 AM	
1 - 5 of 248		show 5 ▾ items	

When you click the description of an event, the following page appears:

**Figure 31-2** Detailed Information Concerning the Event



This page can be used to acknowledge the event. Acknowledging an event removes it from the main event log, but you can still see it in the Advanced page. Clicking *Finished* closes the window.

There are two log lists, the Event Log and the System Event Log. The Event Log lists the event messages generated by the ZENworks Agent that resides on the server or workstation; the System Event Log is displayed only for servers that are functioning as primary or secondary ZENworks Servers. The System Event Log lists the system event messages generated by the ZENworks Server for activities that it performs on behalf of all managed devices in its management zone.

## 31.2 Working with the Log Pages

After an event has been logged, you can view and acknowledge it.

The following sections provide additional information:

- ♦ [Section 31.2.1, “Viewing an Event Log,” on page 372](#)
- ♦ [Section 31.2.2, “Acknowledging an Event,” on page 373](#)
- ♦ [Section 31.2.3, “Using the Advanced Page,” on page 375](#)
- ♦ [Section 31.2.4, “Clearing the Event Log,” on page 375](#)

### 31.2.1 Viewing an Event Log

You can view event logs for devices, policies, and bundles. To view an event log, start with the appropriate tab in the ZENworks Control Center: Devices, Policies, or Bundles. For example, to view the event log for a server, do the following:

- 1 Click the *Devices* tab on the ZENworks Control Center page to display a list of managed devices.
- 2 Click *Servers* to display a list of servers.

- 3 Click the server you want to check. A summary page appears that includes the event logs. To view additional details, click the event.

**Novell ZENworks SDF1**

Home Devices Policies Bundles Reports Configuration

Server Tasks: Remote Control Server, Assign Policy, Assign Bundle, Take Image, Apply Preboot Bundle, Refresh Server, Add to Server Group, Acknowledge All Events

Frequently Used: sdf1.provo.novell.com, linux, Prebootbundle, Script Bundle, ZENworks Image Bundle 1, epiphany, mtalbot, PolicyFolder, Bundle\_1, Bundle Delivery Failures

Devices > Servers > sdf1.provo.novell.com

**sdf1.provo.novell.com**

Summary Inventory Settings

**General**

Alias:	sdf1.provo.novell.com
Host Name:	sdf1
IP Address:	137.65.79.62
ZENworks Agent Status:	
Operating System:	SUSE Linux Enterprise Server 9
Number of errors not acknowledged:	0
Number of warnings not acknowledged:	0
GUID:	58c4e62b344cd73bd3a85cb42f849d18

**Effective Bundles** Advanced

Status	Name	Type
No items available.		

**Effective Policies** Advanced

Status	Name	Type
No items available.		

**Event Log** Advanced

Status	Event	Date
	<a href="#">The IP address of destination Inventory server has</a>	7/7/05 10:58:53 AM
	<a href="#">The IP address of destination Inventory server has</a>	7/7/05 10:58:53 AM
	<a href="#">The IP address of destination Inventory server has</a>	7/7/05 10:58:33 AM

1 - 3 of 3 show 10 items

**System Event Log** Advanced

Status	Event	Date
	<a href="#">Device sdf1.provo.novell.com was successfully up</a>	7/18/05 2:01:47 PM
	<a href="#">Device veritech was successfully updated</a>	7/18/05 1:34:16 PM
	<a href="#">Device mtalbot was successfully updated</a>	7/18/05 12:31:37 PM

## 31.2.2 Acknowledging an Event

After you view the logs and identify a problem, you can acknowledge it. To acknowledge an event means you've seen it and either fixed it or decided to take care of the problem later. When you acknowledge an event, it is removed from the event and system log lists but kept in the database and on the Advanced page. You can view acknowledged events either by running a report or using the Advanced page.

There are three ways to acknowledge an event. You can acknowledge a single event, acknowledge multiple events, or acknowledge all events.

To acknowledge a single event:

- 1 Open the Summary page. (For information, see [Section 31.2.1, “Viewing an Event Log,” on page 372.](#))
- 2 Click the event you want to acknowledge.

Message Detail Information

Full Message:

The policy wes1.txt could not be successfully enforced as the file "/opt/wes1.txt" does not exist. The rollback exit code is -1.

Additional Information:

None

Severity:

Error

Date:

July 12, 2005 10:18:50 AM

Acknowledged Date:

None

Source:

/Devices/Workstations/mtalbot

Message ID:

Novell.Zenworks.PolicyEnforcers.TPE.NO\_SUCH\_FILE

Log ID:

11458

Related Objects:

<Unknown>

Finished

Acknowledge

- 3 Click *Acknowledge*.

The event disappears from the list but remains in the database and is listed on the Advanced page.

To acknowledge several events:

- 1 Open the Summary page. (For information, see [Section 31.2.1, “Viewing an Event Log,” on page 372.](#))
- 2 Click *Advanced* on the toolbar in the Event Log section.

HomeDevicesPoliciesBundlesReportsConfiguration

Devices > Servers > sdf1.provo.novell.com > Edit System Event Log

Edit System Event Log

Events logged from this device are displayed in this list.

System Event Log

Acknowledge

<input type="checkbox"/>	Status	Event	Date	✓
<input type="checkbox"/>	✓	<a href="#">Device sdf1.provo.novell.com was</a>	7/18/05 2:01:47 PM	
<input type="checkbox"/>	✓	<a href="#">Device veritech was successfully updated</a>	7/18/05 1:34:16 PM	
<input type="checkbox"/>	✓	<a href="#">Device mtalbot was successfully updated</a>	7/18/05 12:31:37 PM	
<input type="checkbox"/>	✓	<a href="#">Device sdf1.provo.novell.com was</a>	7/18/05 12:01:19 PM	
<input type="checkbox"/>	✓	<a href="#">Device veritech was successfully updated</a>	7/18/05 11:34:16 AM	

1 - 5 of 426

show 5 items

- 3 Select the check box for each message you want to acknowledge.
- 4 Click *Acknowledge*.

To acknowledge all events:

- 1 Open the Summary page.
- 2 Click *Acknowledge All Events* in the upper-left corner.

Clicking *Acknowledge All Events* acknowledges *all* system events, not just those in a single category.

### 31.2.3 Using the Advanced Page

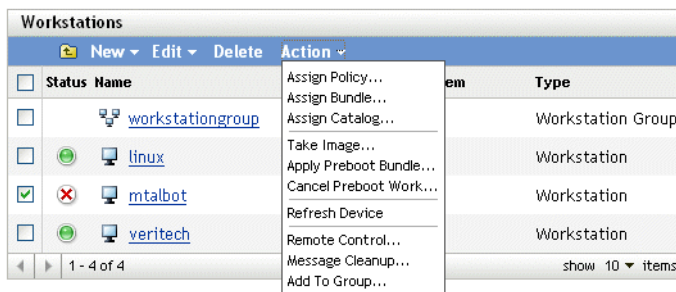
You can open the Advanced page by clicking *Advanced* in the upper-right corner of the event log part of the page. In the Advanced page, you can acknowledge events, view acknowledged events, and click the description of an event for more details.

### 31.2.4 Clearing the Event Log

After you acknowledge an event, you have two options for cleaning up the logs. You can clear the events, which deletes the events from all the lists, including the Advanced window. Once cleared, the event is only available through reports. You can also permanently delete the event, which deletes the event from both the logs and the database. You can clear events associated with servers, workstations, policies, and bundles. For each, the process is the same.

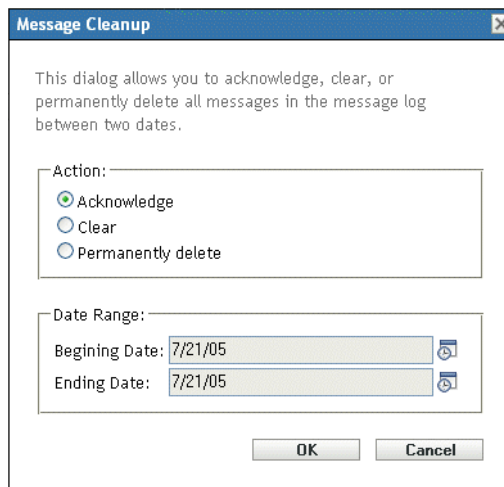
To clear the event log for a workstation:

- 1 Open the Devices page, then click *Workstations*.
- 2 Click the check box of the workstation you want cleared of events.



- 3 Click *Action* on the toolbar.

#### 4 Click *Message Cleanup*.



From here you can do the following:

- ♦ Acknowledge all event messages for the device. This acknowledges all events within a specified date range and deletes them from the Hot List, event log, and system event log.
  - ♦ Clear all event messages. This clears all events within a specified date range from the event log, system event log, advanced event log, and advanced system event log.
  - ♦ Permanently delete all event messages. This deletes all events within a specified date range from all the log lists and the database.
- 5 When you have selected the option you want and set a date range, click *OK* to clear the messages.



You can use the Message Logger component of Novell® ZENworks® 7 Linux Management to log the messages on managed devices and servers.

The following sections provide information to help you understand the functionality of the Message Logger component:

- ♦ [Section 32.1, “What Is Message Logger?,” on page 377](#)
- ♦ [Section 32.2, “Message Severity,” on page 377](#)
- ♦ [Section 32.3, “Message Format,” on page 377](#)

## 32.1 What Is Message Logger?

Message Logger is the component responsible for logging the messages to different output targets. Several components of ZENworks 7 Linux Management use Message Logger to log messages, including zenloader and webservices on the server and the ZENworks management daemon (ZMD), Remote Management, and Policy Enforcers on the client. For more information about ZENworks services, see [Section 3.1, “ZENworks Services,” on page 23](#).

Message Logger logs the messages in different output targets, such as e-mails, SNMP traps, writes to the database, local and system log files, and the central log file.

## 32.2 Message Severity

Messages are classified in the following three categories:

**Error:** Indicates that an action cannot be completed because of a user or system error. These messages require immediate attention from an administrator.

**Warning:** Calls attention to an exception condition. These messages might not be an error but can cause problems if not resolved. These messages do not require immediate attention from an administrator.

**Information:** Provides feedback about something that happened in the product or system that is important and informative for an administrator.

## 32.3 Message Format

Messages are logged on the managed device and primary server in the following format:

```
Severity: [time] Component_Name Message_ID Message_String  
Additional_Info:Value_for_Additional_Info
```

For example, ERROR: [3/15/05 3:28:45 PM] PolicyEnforcers  
Novell.Zenworks.PolicyEnforcers.EPE.NO\_SUCH\_FILE The Text File policy could not be  
successfully enforced as the file abc.txt does not exist.

Additional Info: PolicyEnforcer Exception: file does not exist.



# Configuring Message Logger Settings

# 33

You can perform the following activities by configuring Message Logger settings:

- ♦ Write messages to a local log file
- ♦ Write messages to a system log file
- ♦ Send messages as SNMP traps
- ♦ Send messages as SMTP mail
- ♦ Purge the database entries

---

**NOTE:** The Message Logger does not log the messages with severity levels other than error, warning, information, and debug.

---

There are two ways to configure Message Logger settings:

- ♦ [Section 33.1, “Configuring Message Logger Settings for the Primary Server,” on page 379](#)
- ♦ [Section 33.2, “Configuring Message Logger Settings for a Managed Device,” on page 382](#)

## 33.1 Configuring Message Logger Settings for the Primary Server


The following settings of the Message Logger can be configured to log messages on the primary server:

- ♦ [Section 33.1.1, “Configuring Database Maintenance Settings,” on page 379](#)
- ♦ [Section 33.1.2, “Configuring Centralized Log Settings,” on page 380](#)
- ♦ [Section 33.1.3, “Configuring SMTP Settings,” on page 380](#)
- ♦ [Section 33.1.4, “Configuring SNMP Settings,” on page 381](#)

### 33.1.1 Configuring Database Maintenance Settings

These settings allow you to configure the database maintenance settings for purging the database log messages.

- 1 In the ZENworks® Control Center, click *Configuration*.
- 2 In *Management Zone Settings*, click *Centralized Message Logging*.
- 3 Under *Central Server*, specify the name of the server that is responsible for purging message log entries from the database.

You can also select a server by clicking .

The ZENworks servers that are displayed here are the ones that are registered with Novell® ZENworks Linux Management Server.

- 4 In the *Purge Log Entries After* field, select a value from the drop-down list. The available options are 30, 60, and 90.  
Log entries older than the selected number of days are purged. Purging is done every midnight and 5 minutes after zenloader starts.
- 5 Click *OK* or *Apply*.

### 33.1.2 Configuring Centralized Log Settings

These settings allow you to use a log file to log the messages of a server and all the managed devices that are connected to this server. The name of this log file is `central-message.log`, and it is located in `/var/opt/novell/log/zenworks`.

- 1 In the ZENworks Control Center, click *Configuration*.
- 2 In *Management Zone Settings*, click *Centralized Message Logging*.
- 3 Under *Centralized File Log*, select the *Log Message to a Centralized File if Severity Is* check box to enable the settings.
- 4 In the *Log Message to a Centralized File if Severity Is* field, select a value from the drop-down list.
  - ♦ Select *Error* to store the messages that have an Error severity.
  - ♦ Select *Warning and Above* to store the messages that have a severity of Warning and Error.
  - ♦ Select *Information and Above* to store the messages that have a severity of Information, Warning, and Error.
- 5 In the *Limit File Size To* field, specify the size of a file in KB or MB.  
The message file is backed up after reaching the specified size.
- 6 In the *Number of Backup Files* field, specify the number of backup files to take.  
The maximum number of backup files is 99. The most recent backup file is named `central-message.log.1`, the second most recent file has the number 2, and so on. When the maximum file size is reached, the oldest file is deleted.
- 7 Click *Apply* or *OK*.

### 33.1.3 Configuring SMTP Settings

These settings allow you to send error messages through e-mail by configuring SMTP settings.

- 1 In the ZENworks Control Center, click *Configuration*.
- 2 In *Management Zone Settings*, click *Centralized Message Logging*.
- 3 Under *E-mail Notification*, select the *Send Log Message via E-mail If Severity Is* check box to enable the settings.
- 4 In the *SMTP Server Address* field, specify the SMTP server address.  
You can specify a DNS name or IP address as a server address.
- 5 Select *SMTP Server Requires Authentication* to authenticate to the SMTP server.
- 6 Specify the username to use to authenticate to the SMTP server.
- 7 Specify the password to use to authenticate to the SMTP server.

---

**IMPORTANT:** For security considerations, you should create a separate e-mail account and password to send ZENworks messages.

---

**8** In the *Message Settings* section, specify the sender's e-mail address in the *From* field. The error messages are sent from this e-mail address.

**9** In the *To* field, specify the e-mail address of the recipients.

You can specify more than one e-mail address by separating the addresses with commas.

**10** Specify a subject for the e-mail.

The following table describes how you can customize the subject field:

Format Specifiers	Value
%s	Severity of the message
%c	Component name
%d	Device ID
%t	Time when the message is generated
%a	Alias name of the device on which the message is generated.

Format specifiers are a special set of characters that are replaced with their associated values.

For example, if you want the subject line to be displayed as "ERROR occurred on device TestDevice at 4/7/05 5:31:01 PM," then in the subject line you should specify "%s occurred on device %a at %t."

**11** Click *OK* or *Apply*.

### 33.1.4 Configuring SNMP Settings

These settings allow you to send messages as SNMP traps. The location of the MIB file is `/opt/novell/zenworks/share/loggermodule/messageloger.mib`.

---

**NOTE:** The MIB file should not be modified or deleted, or sending of traps does not work.

---

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

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

**3** Under *SNMP Traps*, select the *Log to SNMP Trap if Severity Is* check box to enable all the fields.

**4** In the *Log to SNMP Trap if Severity Is* field, select a value from the drop-down list.

- ♦ Select *Error* to forward on as traps the messages that have Error, Information, Warning, and Debug severity.
- ♦ Select *Warning and Above* to forward on as traps the messages with a severity of Warning and Error.
- ♦ Select *Information and Above* to forward on as traps the messages that have a severity of Information, Warning, and Error.

**5** Specify a trap target.

You can specify the IP address or DNS name of the management console as a trap target.

**6** Specify the port number of the SNMP server.

By default, the port number is 162.

**7** Specify the community string of the SNMP trap that is to be sent.

The default value of the community string is Public.

**8** Click *OK* or *Apply*.

## 33.2 Configuring Message Logger Settings for a Managed Device

The following settings of the Message Logger can be configured to log the messages on a managed device:

- ♦ [Section 33.2.1, “Configuring Local Log Settings,” on page 382](#)
- ♦ [Section 33.2.2, “Configuring System Log Settings,” on page 383](#)

### 33.2.1 Configuring Local Log Settings

These settings allow you to write messages into a local file. The name of the log file for ZMD logging is `zmd-message.log`; for ZENloader logging it is `loader-message.log`; and for ZEN server logging it is `services-message.log`. The path of the local log files is `/var/opt/novell/log/zenworks`.

- 1** In the ZENworks Control Center, click *Configuration*.
- 2** In *Management Zone Settings*, click *Local Device Logging*.
- 3** Under *Local File*, select the *Log Message to a Local File if Severity Is* check box to enable the fields.
- 4** In the *Log Message to a Local File if Severity Is* field, select a value from the drop-down list.
  - ♦ Select *Error* to store the messages that have Error, Information, Warning, and Debug severity.
  - ♦ Select *Warning and Above* to store the messages with a severity of Warning and Error.
  - ♦ Select *Information and Above* to store the messages that have a severity of Information, Warning, and Error.
  - ♦ Select *Debug and Above* to store the messages that have a severity of Debug, Information, Warning, and Error
- 5** In the *Limit File Size To* field, specify the size of the file in MB or KB.

The messages are backed up after reaching the specified size and the file is reset.
- 6** In the *Number of Backup Files* field, specify the number of backup files to take.

The maximum number of backup files is 99. The most recent backup file is named `central-message.log.1`, the second most recent file has the number 2 and so on. When the maximum file size is reached, the oldest file is deleted.
- 7** Click *OK* or *Apply*.

## 33.2.2 Configuring System Log Settings

These settings allow you to insert messages into the system file. The path of the system log file is `/var/log/messages`.

- 1** In the ZENworks Control Center, click *Configuration*.
- 2** In *Management Zone Settings*, click *Local Device Logging*.
- 3** Under *System Log*, select the *Send Message to Local System Log if Severity Is* check box to enable the fields.
- 4** In the *Send Message to Local System Log if Severity Is* field, select a value from the drop-down list.
  - ♦ Select *Error* to store the messages with Error, Information, Warning, and Debug severity.
  - ♦ Select *Warning and Above* to store the messages with a severity of Warning and Error.
  - ♦ Select *Information and Above* to store the messages with a severity of Information, Warning, and Error.
- 5** Click *OK* or *Apply*.





# Reports



The following chapters provide information on Novell® ZENworks® Linux Management reporting features:

- ♦ Chapter 34, “Reports Overview,” on page 387
- ♦ Chapter 35, “Generating ZENworks Reports,” on page 389



Reports can contain details from a large volume of inventory, packaging, and other device or bundle information. You can create new reports, edit existing reports, delete reports, or generate one or multiple reports simultaneously. You can create folders to organize and store reports based on your own criteria.

The Reports page, accessed from the ZENworks Control Center, displays reports and folders. A number of standard bundle and device reports are included with ZENworks, and you can easily modify these and define your own. Reports are generated in HTML. After a report is generated, it can be printed, saved, or exported to XML or comma-separated values (CSV) format. When you create reports, the system stores them as objects in Novell eDirectory™. You can generate up to 25,000 records per report.

The following reports are provided with ZENworks:

- ♦ [Section 34.1, “Bundle Reports,” on page 387](#)
- ♦ [Section 34.2, “Device Reports,” on page 387](#)

## 34.1 Bundle Reports

The following bundle reports are provided with ZENworks Linux Management:

**Table 34-1** *Bundle Reports*

Report Name	Description
Bundle Delivery Failure	Lists bundle delivery failures per device.
Bundle Delivery in the Past 24 Hours	Displays the previous day's bundle deliveries.
Bundle Delivery Information per Device	Lists information consisting of error, warning, and success counts, as well as the last bundle delivery message and status.
Last Bundle Delivery per Device	Displays the last bundle delivery that took place per device.

## 34.2 Device Reports

The following device reports are provided with ZENworks Linux Management:

**Table 34-2** *Device Reports*

Report Name	Description
Device Errors in the Past 24 Hours	Lists all device errors in the past 24 hours.
Device Errors in the Past Week	Lists all device errors in the past week.

Report Name	Description
Device Disk Usage	Lists disk usage for all devices.
Devices Registered in the Past 24 Hours	Lists all devices registered in the past 24 hours.
Devices Registered in the Past Week	Lists all devices registered in the past week.

This chapter includes the following topics:

- ♦ Section 35.1, “Creating a Folder,” on page 389
- ♦ Section 35.2, “Creating a Report,” on page 390
- ♦ Section 35.3, “Organizing Reports and Folders,” on page 392
- ♦ Section 35.4, “Modifying Report Details,” on page 393
- ♦ Section 35.5, “Generating Reports,” on page 393
- ♦ Section 35.6, “Resetting Default Reports,” on page 394

## 35.1 Creating a Folder

You create folders to store ZENworks reports.

- 1 In the ZENworks Control Center, click the *Reports* tab.
- 2 Click *New > Folder*.
- 3 Specify the name and folder location.

You can browse to select an existing folder in which to store the new folder.

- 4 Enter a report description, if necessary, then click *OK*.

**New Folder**

Name: \*  
Hard Disk Reports

Folder: \*  
/Reports

Description:  
Contains reports for hard disk inventory.

Fields marked with a blue asterisk are required.

OK Cancel

The system displays the new folder on the Reports page, as follows:

Reports	
New Edit Delete Generate	
<input type="checkbox"/> Name	Type
<input type="checkbox"/> <a href="#">Bundle Reports</a> <a href="#">[Details]</a>	Folder
<input type="checkbox"/> <a href="#">Device Reports</a> <a href="#">[Details]</a>	Folder
<input type="checkbox"/> <a href="#">Hard Disk Reports</a> <a href="#">[Details]</a>	Folder
1 - 3 of 3	
show 10 items	

## 35.2 Creating a Report

Use this wizard to create a new report. ZENworks allows you to define the devices for which the system generates report data, and to customize how the information is displayed. After you create the report, you can generate the report and view or print it in formats such as XML, HTML, or CSV (comma-separated values). You can also create new folders to store multiple reports that you can run simultaneously.

- 1 In the ZENworks Control Center, click the *Reports* tab.
- 2 Click *New > Report*.

[Reports](#) > [Create New Report](#)

Create New Report

Help


Step 1: Report Information

Specify the name, and description of the new report:

Report Name: \*

Folder: \*

Report Description:

Fields marked with a blue asterisk are required.

<< Back

Next >>

Cancel

- 3 Use the Report Information page to specify the following information:
  - Report name:** Specify a report name.
  - Folder:** Specify the folder name, or browse to locate the folder in which you want to store the report. When you browse to locate a folder, the system displays the Select Folder dialog box. After you locate the desired folder, click the *Select* icon to select the folder, then click *OK*.
  - Report description:** Specify a report description. The system displays this description beneath the report name in the generated report.
- 4 Click *Next*.

- 5 Use the Columns page to add and sort the columns that you want to display on the report.

Device Alias	Bundle Delivery Error Count	Bundle Delivery Warning Count	Bundle Delivery Informational Count	Bundle Delivery Last Status	Bundle Delivery Last Action Time
--------------	-----------------------------	-------------------------------	-------------------------------------	-----------------------------	----------------------------------

Primary Sort: Device Alias Ascending Secondary Sort: None Ascending

**Columns:** Select a column, then click *Add*. You can select a group of items by holding the Shift key and clicking the first and last items in the group, or you can select several items by holding the Ctrl key and clicking each item. The system displays the items as you add them. Use the ZENworks interface to sort or remove the columns.

**Primary and secondary sort:** Use the drop-down menus to specify a primary and secondary sort, if needed. You can sort by a column in ascending or descending order.

- 6 Click *Next*.

Reports > Create New Report

Create New Report Physical Disks ?

Step 3: Filters

Create filter rule(s) to limit data showing in this report:

Add Filter Add Filter Set Delete

Combine Filters using: or Filter Sets will be combined using: AND

Show data matching the filter rules:

☐ -Select- Equal to

<< Back Next >> Cancel

Use the Filters page to create filter rules to manipulate the amount of queried data you want to display on the report. Filter sets enable you to create sets of individual filters, and evaluate them with another set of individual filters. The system uses Boolean logic (And, Or, and Not operators) that determines how to process filters and filter sets. Individual filters can be grouped by And or Or based on how you select the conjunction operator. If you select And to combine filters within filter sets, then the filter sets will be Or, and vice versa. Filter sets can be grouped using Or or And. If you have multiple conditions that must be met, group them using individual filter sets with an And condition.

For example, you can add a filter to report inventory data for a particular BIOS Serial Number if the number is equal to or contains a specific value, then add a second filter to further limit (or expand) the results, such as whether the BIOS Install Date is before, after, or relative to the date you specify in the second filter. You then might add another filter and use the Not operator to eliminate a certain BIOS Release Date value from the search.

- 7 Click *Add Filter* to create a filter.

Use the drop-down menu to specify whether to combine filters using And or Or. This selection also controls how the system combines filter sets. Depending on the item you select for the filter, ZENworks provides a variety of filtering criteria, such as:

- ♦ Alphanumeric (equal to / contains)
- ♦ Date and time (before, after, relative, non-existent)
- ♦ Size (<, >, =, and so on)

- ♦ True/false
- ♦ Has/doesn't have

For example, the following filter sets return all devices with 10 GB hard disk drives containing less than 2 GB of free space:

☐  Physical Disk Free Size(bytes)  <  2147483648
 ☐  Physical Disk Capacity(bytes)  <  10737418240

- 8 Click *Add Filter Set* to create a new set of filters, then click *Add Filter* to add filters to the new set.

For example, the following filter set returns all devices with more than 2 GB of free space that are not made by the specified manufacturer:

☐  Physical Disk Free Size(bytes)  <  2147483648  
 AND  
☐ NOT  Physical Disk Manufacturer  =  Disk Maker

New filters are always added to the newest filter set.

To delete a filter, select a filter's check box, then click *Delete*.

- 9 Click *Next*.

Use the Summary page to review the report information.

- 10 Click *Finish* to create the new report, then click *OK* on the Results page to return to the Reports page.

Novell recommends that you use the *Message From This Type Object* column only in conjunction with other message and device columns and filters. If you add other types of columns or filters, the message displayed in this column may be inaccurate. Known exceptions of device columns and filters that also cause this inaccuracy are:

- ♦ Device Code Page
- ♦ Device Virtual Memory
- ♦ Device Visible Memory

## 35.3 Organizing Reports and Folders

You can simplify report management and generation by organizing the report list and storing reports in separate folders.

- ♦ [Section 35.3.1, "Editing the Reports List," on page 392](#)
- ♦ [Section 35.3.2, "Deleting a Report or Folder," on page 393](#)

### 35.3.1 Editing the Reports List

To edit the reports list, select the report or folder check box, then click *Reports > Edit*.

The following table describes each task:



**Table 35-1** *Editing Options*

Task	Description
Rename	Displays the Rename Report or the Rename Folder dialog box. Specify a new name for the object.
Copy	Displays the Copy Report dialog box. You can specify a new name for the copied report. You cannot copy folders.
Move	Displays the Move Report dialog box. Select the folder to which the report should be moved.

### 35.3.2 Deleting a Report or Folder

To delete a report or folder, click *Reports > Delete*. This permanently removes the report from the database.

## 35.4 Modifying Report Details

- 1 In the ZENworks Control Center, click the *Reports* tab.
- 2 Select a report.
- 3 To modify the settings of an existing report, complete any of the following fields or options:

Field	Description
General	Revise the report description.
Columns	Add, delete, or change the column layout and sorting details of the report. See <a href="#">Section 35.2, "Creating a Report," on page 390</a> for more information about adding columns to a report.
Filters	Revise, add, or delete the report filters. See <a href="#">Section 35.2, "Creating a Report," on page 390</a> for more information about naming, formatting, and filtering.
Generate	Runs the report based on the settings displayed on the page. See <a href="#">Section 35.5, "Generating Reports," on page 393</a> for more information.
Apply	Saves the new settings.
Reset	Resets the report to its original settings.

- 4 To generate the report, click *Generate*.

## 35.5 Generating Reports

You can generate an existing report, or generate multiple reports simultaneously. After the system displays the report, you can print the information or export and view the data in XML, CSV, or HTML formats.

- 1 In the ZENworks Control Center, click the *Reports* tab.
- 2 To generate a report, select the report's check box, then click *Generate*.

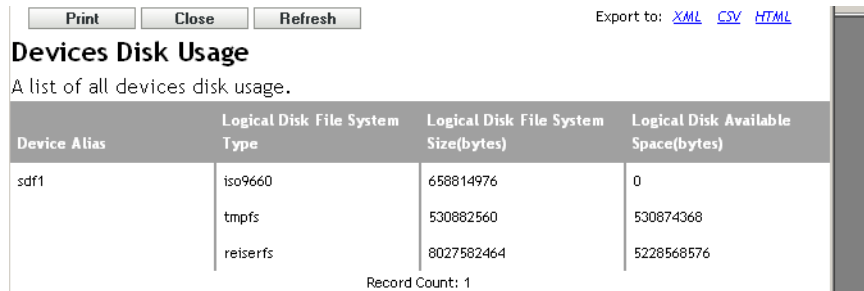
or

- 3 To generate a batch of reports, select the report folder's check box, then click *Generate*.

You can also select individual reports and run them simultaneously.

The following graphic is a sample of a generated ZENworks report.

**Figure 35-1** Report Generation Page



The screenshot shows a web interface for report generation. At the top, there are buttons for 'Print', 'Close', and 'Refresh', and a link to 'Export to: XML CSV HTML'. Below this is the title 'Devices Disk Usage' and a subtitle 'A list of all devices disk usage.' A table displays disk usage data for device 'sdf1'. The table has four columns: 'Device Alias', 'Logical Disk File System Type', 'Logical Disk File System Size(bytes)', and 'Logical Disk Available Space(bytes)'. The data shows three file systems: iso9660, tmpfs, and reiserfs. Below the table, it says 'Record Count: 1'.

Device Alias	Logical Disk File System Type	Logical Disk File System Size(bytes)	Logical Disk Available Space(bytes)
sdf1	iso9660	658814976	0
	tmpfs	530882560	530874368
	reiserfs	8027582464	5228568576

Record Count: 1

**Table 35-2** Output Types

Output Type	Description
XML	When you view a report in XML, the system displays the information using rows, rather than in table format. You can view this data in any application that can display XML.
CSV	The system displays the information as CSV (comma-separated values), allowing you to view the report data in a spreadsheet.
HTML	The system displays the report data in the default browser. However, you can choose another program to open this document, if needed. The HTML styles are embedded in the report output.

## 35.6 Resetting Default Reports

Click Reset Default Reports to reset the default reports to their original settings when you installed ZENworks. The default reports are the bundle and device reports that come with the installed software.

# Appendixes



The following appendixes are accessed from other sections of the *Novell® ZENworks® 7 Linux Management Administration Guide*:

- ♦ [Appendix A, “Bundle and Policy Schedules,” on page 397](#)
- ♦ [Appendix B, “Imaging Utilities and Components,” on page 401](#)
- ♦ [Appendix C, “ZENworks Imaging Engine Commands,” on page 425](#)
- ♦ [Appendix D, “Updating ZENworks Imaging Resource Files,” on page 441](#)
- ♦ [Appendix E, “Supported Ethernet Cards,” on page 455](#)
- ♦ [Appendix F, “Establishing SSH Tunneling,” on page 457](#)
- ♦ [Appendix G, “Limited Support for SLES10 and SLED10 Managed Devices,” on page 461](#)
- ♦ [Appendix H, “License Agreement for libacl and libgconf,” on page 463](#)
- ♦ [Appendix I, “Documentation Updates,” on page 469](#)



# Bundle and Policy Schedules

# A

Using Novell® ZENworks® Linux Management, you can schedule when bundles are deployed to or installed on assigned devices. You can also schedule when policies are applied to assigned devices.

The following scheduling options are available:

- ♦ [Section A.1, “No Schedule,” on page 397](#)
- ♦ [Section A.2, “Date Specific,” on page 397](#)
- ♦ [Section A.3, “Day of the Week Specific,” on page 398](#)
- ♦ [Section A.4, “Event,” on page 399](#)
- ♦ [Section A.5, “Monthly,” on page 399](#)
- ♦ [Section A.6, “Relative to Refresh,” on page 400](#)

## A.1 No Schedule

Use this option to indicate no schedule; no action occurs.

## A.2 Date Specific

Select one or more dates on which to run the scheduled event and set other restrictions that might apply.

**Start Dates(s):** Click the plus (+) symbol to display a calendar from which you can select dates to run the event on. Click the arrows next to the month to display the previous or next month’s calendar; click the arrows next to the year to display the previous or next year’s calendar.

**Run Event Every Year:** Select this option to run the event every year on the dates that you selected in the *Start date(s)* field.

**Select When Schedule Execution Should Start:** Select one of the following options:

- ♦ **Start Immediately at Start Time:** The scheduled event runs immediately at the time that you specify in the *Start Time* box.
- ♦ **Start at a Random Time between Start Time and End Time:** This option randomly spreads out the scheduled event times so the scheduled event does not run at the same time on multiple devices. You can use this option to avoid possible network overload. For example, if you want to distribute or install a bundle to 100 users, you could use the *Start at a random time between start time and end time* option to specify a one-hour block of time (starting at the scheduled start time) in which to randomly deploy or install the bundle to the various devices.

**StartTime\End Time:** Use the down-arrows to select the start and end times of the scheduled event.

---

**IMPORTANT:** Be aware that ZENworks Linux Management uses the *End Time* as the “expiration time.” If a bundle or policy is in the middle of being executed, execution will stop at the specified time.

---

**Use Greenwich Mean Time (GMT):** Usually, a schedule is based on the device's local time zone. If your network spans different time zones and you schedule an application to run at 1:00 p.m., it runs at 1:00 p.m. in each time zone. This option lets you specify a single time across the globe.

You can, for example, select this option to have bundles deployed or installed on devices at the same time regardless of their time zones.

## A.3 Day of the Week Specific

Select one or more days of the week to run the scheduled event on and set other restrictions that might apply.

**Select the Days of the Week to Run the Scheduled Event:** Select one or more days, Sunday to Saturday, on which you want to run the scheduled event. By default, no days are selected; a day is selected when the check box is checked.

**Restrict Schedule Execution to the Following Date Range:** Use the *Start date* and *End date* fields to restrict the scheduled event to the dates between the start and end dates. Click the *Calendar* icon to display a calendar from which you can select the respective dates.

**Select When Schedule Execution Should Start:** Select one of the following options:

- ♦ **Start Immediately at Start Time:** The scheduled event runs immediately at the time that you specify in the *Start Time* box.
- ♦ **Start at a Random Time between Start Time and End Time:** This option randomly spreads out the scheduled event times so the scheduled event does not run at the same time on all devices. You can use this option to avoid possible network overload. For example, if you want to distribute or install a bundle to 100 users, you could use the *Start at a random time between start time and end time* option to specify a one-hour block of time (starting at the scheduled start time) in which to randomly deploy or install the bundle to the various devices.
- ♦ **Start Immediately at Start Time, and then Repeat until End Time Every:** Use the *Hours* and *Minutes* fields to specify how often you want the scheduled event repeated until deployment or installment of the bundle is successful.

**Start Time\End Time:** Use the down-arrows to select the start and end times of the scheduled event.

---

**IMPORTANT:** Be aware that ZENworks Linux Management uses the *End Time* as the “expiration time.” If a bundle or policy is in the middle of being executed, execution will stop at the specified time.

---

**Use Greenwich Mean Time (GMT):** Usually, a schedule is based on the device's local time zone. If your network spans different time zones and you schedule an application to run at 1:00 p.m., it runs at 1:00 p.m. in each time zone. This option lets you specify a single time across the globe.

You can, for example, select this option to have bundles deployed or installed on devices at the same time regardless of their time zones.

**Set the “Black Out” Time Ranges when Execution Should Not Occur:** Click *Add* to display the Specify Black-Out Time Period dialog box. Use the *Start/End date* and the *Start/End time* options to specify the time period in which you do not want the scheduled event run. You can use this option to minimize network traffic during a certain time period.

## A.4 Event

Select the event that this schedule should be triggered on:

- ♦ **Runlevel Change:** The Linux operating system has different modes of operation, or runlevels, the operating system can run in. These runlevels are similar to the safe mode or command-prompt-only mode in Microsoft\* Windows. The *Runlevel change* option lets you trigger the event schedule when a user or administrator changes the runlevel on the device.
- ♦ **User Login:** The *User login* option lets you trigger the event schedule when the user logs in to the device.

## A.5 Monthly

Select the day of the month to run the scheduled event on and set other restrictions that might apply.

**Day of the Month:** Select one of the following options:

- ♦ **Start the Scheduled Event on a Specific Day of the Month:** Specify the day of the month on which to run the scheduled event.
- ♦ **Start the Scheduled Event on the Last Day of the Month:** Select this option to run the scheduled event on the last day of the month. For example, for the month of February, the event runs on the 28th (except for leap years, in which case it runs on the 29th); for the month of December, the event runs on the 31st.

**Select When Schedule Execution Should Start:** Select one of the following options:

- ♦ **Start Immediately at Start Time:** The scheduled event runs immediately at the time that you specify in the *Start Time* box.
- ♦ **Start at a Random Time between Start Time and End Time:** This option randomly spreads out the scheduled event times so the event is not run at the same time on all devices. You can use this option to avoid possible network overload. For example, if you want to distribute or install a bundle to 100 users, you could use the *Start at a random time between start time and end time* option to specify a one-hour block of time (starting at the scheduled start time) in which to randomly deploy or install the bundle to the various devices.

**Start Time\End Time:** Use the down-arrows to select the start and end times of the scheduled event.

---

**IMPORTANT:** Be aware that ZENworks Linux Management uses the *End Time* as the “expiration time.” If a bundle or policy is in the middle of being executed, execution will stop at the specified time.

---

**Use Greenwich Mean Time (GMT):** Usually, a schedule is based on the device’s local time zone. If your network spans different time zones and you schedule an application to run at 1:00 p.m., it runs at 1:00 p.m. in each time zone. This option lets you specify a single time across the globe.

You can, for example, select this option to have bundles deployed or installed on devices at the same time regardless of their time zones.

**Set the “Black Out” Time Ranges when Execution Should Not Occur:** Click *Add* to display the Specify Black-Out Time Period dialog box. Use the *Start/End date* and the *Start/End time* options to

specify the time period in which you do not want the scheduled event run. You can use this option to minimize network traffic during a certain time period.

## A.6 Relative to Refresh

Select the initial delay and repeat frequency to run the scheduled event and set other restrictions that might apply.

**Schedule Execution:** Select one of the following options:

- ♦ **Start Immediately on Refresh:** Select this option to run the scheduled event when the device refreshes (looks for new bundles, policies, and so forth).
- ♦ **Delay Execution after Refresh:** Select this option to run the scheduled event for a specified number of days, hours, or minutes after the device refreshes (looks for new bundles, policies, and so forth).

**After Executing, Repeat Every:** Select this option and specify the number of days, hours, and minutes after which you want to repeat execution of the scheduled event after a successful execution.

**Set the “Black Out” Time Ranges when Execution Should Not Occur:** Click *Add* to display the Specify Black-Out Time Period dialog box. Use the *Start/End date* and the *Start/End time* options to specify the time period in which you do not want the scheduled event run. You can use this option to minimize network traffic during a certain time period.



# Imaging Utilities and Components

# B

The following sections provide reference information on Novell® ZENworks® Linux Management imaging utilities, commands, and configuration settings.

- ♦ [Section B.1, “Image Explorer \(ImgExp.exe\),” on page 401](#)
- ♦ [Section B.2, “Novell ZENworks Linux Management Imaging Agent \(novell-zislnx\),” on page 406](#)
- ♦ [Section B.3, “Image-Safe Data Viewer and Editor \(zisview and zisedit\),” on page 407](#)
- ♦ [Section B.4, “ZENworks Imaging Floppy Boot Disk Creator \(zimgboot.exe\),” on page 411](#)
- ♦ [Section B.5, “Imaging Configuration Parameters \(settings.txt\),” on page 411](#)
- ♦ [Section B.6, “Imaging Boot Parameter for PCMCIA Cards,” on page 414](#)
- ♦ [Section B.7, “Imaging Server,” on page 414](#)

## B.1 Image Explorer (ImgExp.exe)

Although ZENworks Imaging Explorer looks, and in most situations, functions like Microsoft Windows Explorer, some functionality differences exist between the two programs. The following describes the key differences between how ZENworks Image Explorer and Microsoft Windows Explorer function:

- ♦ **Replacing Files in an Image:** During the lifecycle of an image, files might be deleted or updated using Image Explorer. When you replace an existing file in an image using Image Explorer, the original file is not deleted from the image. Image Explorer purges only deleted files; it does not purge files that have been updated.

When files are added to an image where the file already exists, Image Explorer appends the entry to the end of the image. When images are restored, all files that have been previously updated are sequentially restored.

To avoid performance problems, you should manually delete and purge each instance of a duplicate file in order to have the duplicates purged from the image. In Windows Explorer, replaced files are automatically deleted.

- ♦ **Dragging Files from Image Explorer:** You cannot drag files from Image Explorer in order to extract them, which you can do in Windows Explorer. However, you can drag and drop files and folders into an image using Image Explorer.

---

**IMPORTANT:** When editing a base image, do not exclude BPB files from it or the device won't be able to boot the new operating system after receiving the image.

---

The following sections describe the tasks that you can perform using the Image Explorer:

- ♦ [Section B.1.1, “Opening Image Explorer \(Imgexp.exe\),” on page 402](#)
- ♦ [Section B.1.2, “Opening an Image,” on page 402](#)
- ♦ [Section B.1.3, “Adding a File or Folder to an Open Image,” on page 402](#)
- ♦ [Section B.1.4, “Creating a Folder in an Open Image,” on page 402](#)

- ◆ Section B.1.5, “Excluding a File or Folder from a File Set in the Open Image,” on page 403
- ◆ Section B.1.6, “Marking a File or Folder for Deletion in the Open Image,” on page 403
- ◆ Section B.1.7, “Purging Files and Folders Marked for Deletion from the Open Image,” on page 403
- ◆ Section B.1.8, “Extracting a File or Directory from the Open Image to a Folder,” on page 403
- ◆ Section B.1.9, “Extracting a File or Directory from the Open Image as an Add-On Image,” on page 403
- ◆ Section B.1.10, “Viewing a File from the Open Image in its Associated Application,” on page 404
- ◆ Section B.1.11, “Saving Your Changes to the Open Image,” on page 404
- ◆ Section B.1.12, “Creating an Add-On Image,” on page 404
- ◆ Section B.1.13, “Adding a Partition to a New Add-On Image,” on page 404
- ◆ Section B.1.14, “Compressing an Image,” on page 404
- ◆ Section B.1.15, “Splitting an Image,” on page 405
- ◆ Section B.1.16, “Resizing a Partition in an Image,” on page 406

## B.1.1 Opening Image Explorer (Imgexp.exe)


Run the ZENworks Image Explorer utility to view or modify device images, create add-on images, compress image files, and split images.

The Image Explorer utility must be run on a Windows machine. You need Samba running on the Linux imaging server where the utility file is located in order for the Windows machine to have access to it.



There are no command line parameters for the Image Explorer utility.

- 1 To start Image Explorer, run the following file:  
`/opt/novell/zenworks/zdm/imaging/winutils/ImgExp.exe`

## B.1.2 Opening an Image


- 1 Start Image Explorer.
- 2 Click  on the toolbar, browse for the image (.zmg) file, then click *Open*.  
 Large image files might take a few moments to open.

## B.1.3 Adding a File or Folder to an Open Image

- 1 Start Image Explorer.
- 2 In the left pane, browse to the partition or folder where you want to add the file or folder.
- 3 Click  or  on the toolbar, browse to the file or folder, then click *Add* or *OK*.

## B.1.4 Creating a Folder in an Open Image

- 1 Start Image Explorer.

- 
- 2 In the left pane, browse to the partition or folder where you want to create the folder, click , type the name of the folder, then click *OK*.

## B.1.5 Excluding a File or Folder from a File Set in the Open Image

- 1 Start Image Explorer.
- 2 Select the file or folder, click *Edit*, click *File sets*, then select the file sets that you want the file or folder to be excluded from.

This image has 10 possible file sets, labeled Set 1, Set 2, and so on. The files and/or folders that you selected in the main window will be excluded only from the file sets that you select in this dialog box.

## B.1.6 Marking a File or Folder for Deletion in the Open Image

- 1 Start Image Explorer.
- 2 Select the file or folder, click *Image*, then click *Delete*.

---

**IMPORTANT:** Deleting a file in the Image Explorer merely marks it for deletion, it can still be retrieved. A file marked as deleted is not removed from the image until the image is purged; files and folders marked as deleted are not restored during imaging.

---

## B.1.7 Purging Files and Folders Marked for Deletion from the Open Image

- 1 Start Image Explorer.
- 2 Ensure that the open image has been saved, click *File*, then click *Purge deleted files*.
- 3 Browse to the image filename or specify a new image filename, then click *Save*.

## B.1.8 Extracting a File or Directory from the Open Image to a Folder

- 1 Start Image Explorer.
- 2 Click the file or directory, click *File > Extract > As files*, browse to and select a folder, then click *OK*.


## B.1.9 Extracting a File or Directory from the Open Image as an Add-On Image

- 1 Start Image Explorer.
- 2 Click the file or directory, click *Extract > As add-on image*, type the name of the new add-on image, then click *OK*.


### B.1.10 Viewing a File from the Open Image in its Associated Application

- 1 Start Image Explorer.
- 2 Click the file, click *File > Extract and view*.


### B.1.11 Saving Your Changes to the Open Image

- 1 Start Image Explorer.
- 2 Click  on the toolbar.

### B.1.12 Creating an Add-On Image

- 1 Start Image Explorer.
- 2 Click  on the toolbar, open Windows Explorer, browse to the files and folders you want the add-on image to contain, drag the files and folders into the right pane from Windows Explorer, then click *Save*.

### B.1.13 Adding a Partition to a New Add-On Image

- 1 Start Image Explorer.
- 2 Click  on the toolbar, click the root of the image, click *Image*, then click *Create partition*.  
You cannot add a partition to an existing add-on image or to any base image.

### B.1.14 Compressing an Image

You can set compression options so that it takes less time to restore the image file and less space to store the file on your imaging server. You can compress an uncompressed image (including images created by previous versions of ZENworks) by 40 to 60 percent of the original file size.

The ZENworks Linux Management Image Explorer provides the following types of image compression:

- ♦ “Compressing an Open Image” on page 404
- ♦ “Compressing Any Image without Waiting for the File to Fully Load into Image Explorer” on page 405

#### Compressing an Open Image

- 1 Start Image Explorer.
- 2 Browse for the image (.zmg) file, then click *Open*.  
Large image files might take a few moments to open.
- 3 Click *File > Compress image*.
- 4 Browse to a folder, specify a new image filename, then select a compression option:  
**Optimize for Speed:** Takes the least amount of time to compress, but creates the largest compressed image file.

**Balanced (Recommended):** Represents a compromise between compression time and image file size. This option is used by default when an image is created.

**Optimize for Space:** Creates the smallest image file, but takes longer to compress.

**5** Click *Compress*.

Files marked for deletion in the image will be removed during the compression operation.

## Compressing Any Image without Waiting for the File to Fully Load into Image Explorer

You can set compression options to quickly compress an image file without waiting for the file to fully load into Image Explorer.

To use QuickCompress:

**1** Start Image Explorer.

**2** Click *Tools* > click *QuickCompress*.

**3** Browse to the image file, browse to a folder, specify a new image filename, then select a compression option:

**Optimize for Speed:** Takes the least amount of time to compress, but creates the largest compressed image file.

**Balanced (Recommended):** Represents a compromise between compression time and image file size. This option is used by default when an image is created.

**Optimize for Space:** Creates the smallest image file, but will take longer to compress.

**4** Click *Compress*.

Files marked for deletion in the image will be removed during the compression operation.

## B.1.15 Splitting an Image

You can split an image file into separate files so that you can span the entire image across several CDs or DVDs.

When you split a device image and span it across several CDs or DVDs, you are essentially creating a base image on the first CD or DVD. The remaining CDs or DVDs are add-on images.

To restore a device image that has been spanned across several CDs or DVDs you should restore the first CD or DVD before restoring the remaining CDs or DVDs containing the add-on images. For more information, see [“Manually Putting an Image on a Device” on page 309](#).

Restoring split Images is a manual task and can only be automated using scripted imaging. For more information, see [“Imaging a Device Using a Script” on page 304](#).

To split an image:

**1** Start Image Explorer.

**2** Click *Tools* > *Image split*.

**3** Specify an existing base image file to split, specify the directory in which to store the split images, then specify the maximum file size of each split-image file.

Because images are split by placing individual files into different images, an image cannot be split if it contains any single file that is larger than the specified maximum file size.

- 4 Click *Split*.

## B.1.16 Resizing a Partition in an Image

For base images, you can edit the value in the *Original size* field to allow you to change how big the ZENworks Imaging Engine will make the partition when the image is restored.

For example, suppose you create a base image of a device with a 20 GB hard drive and you want to then put that image on a new device with a 60 GB hard drive. If you do not increase the size of the partition, the partition will be 20 GB, thus making the remaining 40 GB unusable.

However, if you increase the number in the *Original size* field to match the size of the new hard drive, the ZENworks Imaging Engine will expand the partition when the image is restored so that you will be able to use the entire drive.

To resize a partition:

- 1 Start Image Explorer.
- 2 Right-click a partition in the left frame, then click *Properties*.
- 3 Increase or decrease the value in the *Original size* field.

You cannot decrease the number in the *Original size* field to a smaller value than what is in the *Minimum size* field.

The *Original size* field is not applicable for add-on images and cannot be modified.

## B.2 Novell ZENworks Linux Management Imaging Agent (novell-zislrx)

The Novell ZENworks Linux Management client (which includes novell-zislrx) should be installed on devices where you want to apply images. For information on installing the client on your devices, see “[Setting Up Managed Devices](#)” in the *Novell ZENworks 7 Linux Management Installation Guide*.

Installing the Linux Management client automatically installs the Novell ZENworks Linux Management Imaging Agent (novell-zislrx). The Imaging Agent’s purpose is to save certain device-unique data (such as IP addresses, host name, etc.) to an area on the hard disk that is safe from imaging. The Imaging Agent records this information when you install it on the device. Then the agent restores this information from the **image-safe area** after the device has been imaged. This allows the device to use the same network identity as before.

The Imaging Agent is installed on your imaging server by default when you install ZENworks Linux Management.

If a device is new and does not contain a unique network identity, when you image the device using a Preboot Services Imaging bundle, the default settings that you have configured for the ZENworks Management Zone are applied.

The data that the Imaging Agent saves to (or restores from) the image-safe area includes the following:

- ♦ Whether a static IP address or DHCP is used

- ♦ If a static IP address is used:
  - ♦ IP address
  - ♦ Subnet mask
  - ♦ Default gateway (router)
- ♦ DNS settings
  - ♦ DNS suffix
  - ♦ DNS hostname
  - ♦ DNS servers

The `novell-zislnx` daemon is generally run automatically. However, if you want to run it manually, for the command line arguments that can be used with the Imaging Agent, see “[Understanding Script Arguments](#)” on page 422.

## B.3 Image-Safe Data Viewer and Editor (`zisview` and `zisedit`)

After booting a device from an imaging boot media (PXE, CD, DVD, or ZENworks partition), you can enter `zisedit` and `zisview` at the Linux bash prompt to edit and view the image-safe data for that device.

The following sections contain additional information:

- ♦ [Section B.3.1, “Information Displayed by the Image-Safe Data Viewer,” on page 407](#)
- ♦ [Section B.3.2, “Using the Image-Safe Data Viewer,” on page 409](#)
- ♦ [Section B.3.3, “Using the Image-Safe Data Editor,” on page 410](#)

### B.3.1 Information Displayed by the Image-Safe Data Viewer

After booting a device from an imaging boot media, enter `zisview` at the Linux bash prompt to view the image-safe data for that device.

The image-safe data viewer (`zisview`) displays the following information about the device:

**Table B-1** *zisview Information*

Category	Information
Image-safe Data	<ul style="list-style-type: none"> <li>♦ <b>Version:</b> The version number of the Novell ZENworks Linux Management Imaging Agent (<b>novell-zislnx</b>).</li> <li>♦ <b>Just Imaged Flag:</b> If this is set to False, the Imaging Agent reads data from Linux and writes it to the image-safe data store. If this is set to True, the Imaging Agent reads data from the image-safe data store and writes it to Linux.</li> <li>♦ <b>Scripted Image Flag:</b> If this option is set to True, the last imaging operation was a scripted image. If this option is set to False, the last imaging operation was not a scripted image.</li> <li>♦ <b>Last Base Image:</b> The last base image that was restored to the device.</li> <li>♦ <b>Last Base Image Time:</b> The time stamp of the last base image that was restored to the device.</li> <li>♦ <b>Last Base Image Size:</b> The size of the last base image that was restored to the device.</li> <li>♦ <b>Last Base Image Address:</b> The IP address of the last base image that was restored to the device.</li> <li>♦ <b>Script Checksum:</b> Displays the checksum value representing the last script run. The ZENworks Imaging Engine uses the checksum to prevent the same script from re-running on the device unless you specify in the ZENworks Control Center that you want to rerun the same script.</li> </ul>
Device Identity Information	<ul style="list-style-type: none"> <li>♦ <b>Zone GUID:</b> The ZENworks Management Zone that contains the device, if it has been imported.</li> <li>♦ <b>Device GUID:</b> The Globally Unique Identifier of this computer's device.</li> <li>♦ <b>Device Index:</b> The device identification number.</li> <li>♦ <b>Computer Name:</b> The computer name for the device. <sup>1</sup></li> <li>♦ <b>Windows Workgroup:</b> The Microsoft network workgroup of the device. <sup>1</sup></li> <li>♦ <b>Windows SID:</b> The Windows Security ID of the device, a unique number that identifies this device in Windows. <sup>1</sup></li> </ul>



Category	Information
Network Information	<ul style="list-style-type: none"> <li>♦ <b>DHCP:</b> Displays whether this device uses DHCP to obtain its IP address.</li> <li>♦ <b>IP Address:</b> Displays the static IP address that this device uses.</li> <li>♦ <b>Gateway:</b> Displays the gateway that this device uses.</li> <li>♦ <b>Subnet Mask:</b> Displays the subnet mask that this device uses.</li> <li>♦ <b>DNS Servers:</b> The number of DNS nameservers used for DNS name resolution.</li> <li>♦ <b>DNS Server [0]:</b> The IP address of the DNS server. This line is repeated, numbering from 0, 1, 2, 3, and so on for each DNS name server. For example, if the DNS Servers number is 3, there will be three of these lines, numbered from 0 through 2.</li> <li>♦ <b>DNS Suffix:</b> The DNS context of the device.</li> <li>♦ <b>DNS Hostname:</b> The DNS local hostname of the device.</li> </ul>

<sup>1</sup> The *Computer name*, *Windows workgroup*, and *Windows SID* device identity information fields are only present to make ZENworks Linux Management imaging compatible with ZENworks Desktop Management. These fields are not relevant for Linux devices.

## B.3.2 Using the Image-Safe Data Viewer

To use `zisview`, enter any of the following commands at the Linux bash prompt:

Command	Explanation
<code>zisview</code>	Displays all image-safe data.
<code>zisview -z <i>field</i></code>	<p>Displays information about a specific field or fields. <i>field</i> is one or more field names separated by a space. <i>field</i> is not case-sensitive.</p> <p>All of the following are valid field names (the corresponding minimum names that can also be entered on the command line follow each field name in parenthesis):</p> <ul style="list-style-type: none"> <li>JustImaged (J)</li> <li>ScriptedImage (SC)</li> <li>LastBaseImage (L)</li> <li>Zone GUID (T)</li> <li>Device GUID (ObjectDN)</li> <li>Device Index (N)</li> <li>Windows WorkGroup (WorkG)</li> <li>Windows SID (SI)</li> <li>WorkstationID (Works)</li> <li>DHCP (DH)</li> <li>IP (I)</li> <li>Gateway (Gateway)</li> <li>Mask (M)</li> <li>DNSServerCount (DNSServerC)</li> <li>DNSServer (DNSServer)</li> <li>DNSSuffix (DNSSu)</li> <li>DNSHostName (DNSH)</li> </ul>

Command	Explanation
<code>zisview -s</code>	Creates a script that can be used to generate environment variables that contain all of the image-safe data fields.
<code>zisview -h</code>	Displays help for <code>zisview</code> .

### B.3.3 Using the Image-Safe Data Editor

After booting a device from an imaging boot media, you can enter `zisedit` at the Linux bash prompt to change, clear, or remove information the image-safe data for that device.

To use `zisedit`, enter any of the following commands at the Linux bash prompt:

**Table B-2** *zisedit Commands*

Command	Explanation
<code>zisedit</code>	This displays a screen showing all of the image-safe data fields. You can add or change any of the information in the fields.
<code>zisedit field=new_information</code>	<p>You can change the information for one field using this syntax, where <i>field</i> is any valid field name and <i>new_information</i> is the information you want this field to contain. <i>field</i> is not case sensitive.</p> <p>For example, enter <code>zisedit Mask=255.255.252.0</code> to enter this information in the <i>subnet mask</i> field.</p> <p>All of the following are valid field names (the corresponding minimum names that can also be entered on the command line are shown in parenthesis after each field name):</p> <ul style="list-style-type: none"> <li>JustImaged (J)</li> <li>ScriptedImage (SC)</li> <li>LastBaseImage (L)</li> <li>Zone GUID (T)</li> <li>Device GUID (ObjectDN)</li> <li>Device Index (N)</li> <li>Windows WorkGroup (WorkG)</li> <li>Windows SID (SI)</li> <li>WorkstationID (Works)</li> <li>DHCP (DH)</li> <li>IP (I)</li> <li>Gateway (Gateway)</li> <li>Mask (M)</li> <li>DNSServerCount (DNSServerC)</li> <li>DNSServer1 (DNSServer1)</li> <li>DNSSuffix (DNSSu)</li> <li>DNSHostName (DNSH)</li> <li>PXEWorkRevision (PXEWorkR)</li> <li>PXEWorkObject (PXEWorkO)</li> <li>PXETaskID (PXETaskI)</li> <li>PXETaskState (PXETaskS)</li> <li>PXETaskRetCode (PXETaskR)</li> </ul>

Command	Explanation
<code>zisedit -c</code>	Clears all image-safe data fields.
<code>zisedit -r</code>	Removes the image-safe data store.
<code>zisedit -h</code>	Displays help for zisedit.

## B.4 ZENworks Imaging Floppy Boot Disk Creator (`zimgboot.exe`)

You can use this utility to do the following:

- ♦ Create a floppy boot diskette to help devices that cannot boot from their CD or DVD to do so
- ♦ Manage the `settings.txt` file

The ZENworks Imaging Floppy Boot Disk Creator utility must be run on a Windows machine. You need Samba running on the Linux imaging server in order for the Windows machine to have access to the utility.

The `zimgboot.exe` file is located at `/opt/novell/zenworks/zdm/imaging/winutils/zimgboot.exe` on your ZENworks Linux Management imaging server.

For instructions on using the utility, see [Section 23.2.3, “Using the ZENworks Imaging Floppy Boot Disk Creator,” on page 242](#).

## B.5 Imaging Configuration Parameters (`settings.txt`)

The `settings.txt` file contains parameters that control how the imaging boot process occurs. A copy is located in the `/opt/novell/zenworks/zdm/imaging/winutils` directory on the imaging server where ZENworks Linux Management is installed. You should maintain the working copy of `settings.txt` at the root of the imaging boot device (CD or DVD, or ZENworks partition).

`Settings.txt` is a plain text file that contains various parameters, each on a separate line. Each parameter has the general format of `PARAMETER=value`. Lines that begin with a pound sign (`#`) signify comments and are ignored during the imaging boot process.

You can edit this file manually in a text editor, or by making configuration changes in the `zimgboot.exe` utility (see [Section B.4, “ZENworks Imaging Floppy Boot Disk Creator \(`zimgboot.exe`\),” on page 411](#)).

The format and function of each parameter in the `settings.txt` file are described in [Table B-3](#):

**Table B-3** *Setting.txt File Parameters*

Parameter	Specifies
PROMPT	<p>Specifies whether to prompt for each configuration setting when you boot a device from the imaging boot media.</p> <p>If you leave this parameter commented out or set it to No, the device boots using the configuration settings specified in settings.txt and you can't override the settings when booting, unless you type <code>config</code> at the boot prompt before the Linux operating system begins to load.</p> <p>If you set this parameter to Yes, you are automatically prompted for each configuration setting when booting.</p>
MANUALREBOOT	<p>Specifies whether you must reboot a device manually after it was booted from the imaging boot media in automatic mode. If the device was booted from the imaging boot media in manual mode, you must always reboot the device manually.</p> <p>If you boot a device from the imaging boot media and you let the boot process proceed in automatic mode, the ZENworks Imaging Engine starts and checks the imaging server to see if an imaging operation should be performed on the device. If so, it performs the imaging operation and quits. If not, it quits without doing anything.</p> <p>What happens next depends on how you set this parameter:</p> <ul style="list-style-type: none"><li>♦ If you leave it commented out or set it to No, you are prompted to remove the imaging boot media (if necessary) and press any key to reboot the device to the native operating system.</li><li>♦ If you set this parameter to Yes, the device doesn't reboot automatically, but instead displays the Linux bash prompt, allowing you to perform additional imaging-related tasks using the Linux menu or at the command line. This is helpful if you want to do things such as check the current partition information or the image-safe data before booting to the native operating system.</li></ul> <p>Example: <code>MANUALREBOOT=YES</code></p>
PARTITIONSIZE	<p>Specifies the number of megabytes to allocate to the ZENworks partition if you choose to create one locally on a device when you boot the device from the imaging boot media.</p> <p>The default size is 150 MB. The minimum partition size is 50 MB. The maximum size allowed is 2048 MB (2 GB).</p> <p>If you plan to store an image in the ZENworks partition, such as to enable the device to be restored to a certain state without connecting to the network, you might want to specify a larger size on this parameter.</p> <p>Example: <code>PARTITIONSIZE=500</code></p>
netsetup	<p>If you are using DHCP, keep this option enabled. If you are using a specific IP address, replace "dhcp" with "1" and uncomment and configure the other three IP address lines (HostIP, NETMASK, and GATEWAY).</p> <p>Example: <code>netsetup=dhcp</code></p>

Parameter	Specifies
HostIP	<p>The IP address used by a device to communicate on the network when you boot the device from the imaging boot media, if a static IP address is needed.</p> <p>Example: HostIP=137.65.95.126</p> <p>If you want DHCP to be used, leave this and the next two parameters commented out.</p>
NETMASK	<p>Specifies the subnet mask to be used by the device, if the device is using a static IP address.</p> <p>Example: NETMASK=255.255.252.0</p> <p>If DHCP is being used, leave this parameter commented out.</p>
GATEWAY	<p>Specifies the IP address of the gateway (router) to be used by the device, if the device is using a static IP address.</p> <p>Example: GATEWAY=137.65.95.254</p> <p>If DHCP is being used, leave this parameter commented out.</p>
NAMESERVER	<p>Specifies the list of DNS name servers, by IP address, to use for resolving DNS domain names used on this device. Use a space to separate entries.</p> <p>Example: NAMESERVER=123.45.6.7 123.45.6.9</p> <p>If DHCP is being used, leave this parameter commented out.</p>
DOMAIN	<p>Specifies the list of DNS domain suffixes to be used to identify connections used by this device. Use a space to separate entries. For example:</p> <p>DOMAIN=example.novell.com example.xyz.org</p> <p>If DHCP is being used, leave this parameter commented out.</p>
PROXYADDR	<p>Specifies the IP address or full DNS name of the imaging (proxy) server to connect to when you boot a device from the imaging boot media in auto-imaging mode.</p> <p>Examples:</p> <p>PROXYADDR=137.65.95.127</p> <p>PROXYADDR=imaging.xyz.com</p> <p>This parameter is used to set the PROXYADDR environment variable in Linux when the device is booted from an imaging boot media (other than PXE). The ZENworks Imaging Engine then reads this variable to determine which server to contact if it is running in automatic mode. Whether it is running in automatic or manual mode, the ZENworks Imaging Engine attempts to log the imaging results to the server specified in this variable.</p> <p><b>IMPORTANT:</b> This parameter is set automatically when booting PXE and normally should not be specified in <code>/srv/tftp/boot/settings.txt</code>, which is the copy of <code>settings.txt</code> that is used by PXE.</p>

Parameter	Specifies
<code>/bin/setleds -D +num &lt; /dev/tty1</code>	Turns on NUMLOCK upon booting.
<code>export PS1="\`pwd \`#"</code>	Configures the string used by the bash shell. You can change the string by editing the text after the = symbol. The ' character is not a single quote mark, but is from the ~ key.
<code>export IMGCMD</code>	Use to alter the behavior of automated imaging. If this variable is defined as a script (or a series of commands), then that script (or those commands) are executed instead of the usual <code>img auto</code> command (see <code>/bin/imaging.s</code> ).
<code>export ENTERPRISE_NAME=name</code>	<p>This should be a valid Enterprise Name for an AMT device, such as <code>entZENworks</code>. It allows imaging utilities to access image-safe data in AMT NVRAM when AMT devices are disconnected from the ZENworks Management Zone.</p> <p>If you do not use this parameter for disconnected AMT devices, the imaging utilities might not be able to keep the image-safe data up to date.</p>
<code>netdevice=eth0</code>	Selects a specific network adapter. If necessary, replace <code>eth0</code> with the correct interface.
<code>noshell=1</code>	Suppresses a secondary terminal program from displaying.

If you have problems obtaining an IP address for a device running dual NICs, put the following line in the `settings.txt` file:

```
export VALIDATE_NIC=$PROXYADDR
```

This line in the `settings.txt` file validates the NICs; however, you might notice a small performance decrease in the time it takes to obtain an IP address for the device.

## B.6 Imaging Boot Parameter for PCMCIA Cards

When performing imaging work using CDs or DVDs, some computers (particularly laptops) with PCMCIA cards can hang during the boot process. By default, ZENworks Linux Management allows the loading of a PCMCIA driver when a device boots for imaging work. While loading this driver does not normally cause problems, you can use a command line parameter to prevent it from loading.

To prevent the PCMCIA card manager from starting, enter the following at the bash prompt when booting from a CD or DVD:

```
manual NoPCMCIA=1
```

## B.7 Imaging Server

The imaging server is a software component of the Linux Management server. It enables imaging clients to connect with the network to receive imaging services, including:

- ♦ Storage or retrieval of an image on a server
- ♦ Automatic imaging based on settings created in the ZENworks Control Center
- ♦ Logging of the results of an imaging operation

- ♦ A multicast imaging session

Use the imaging server software to do the following:

- ♦ [Section B.7.1, “Initiating the Imaging Processes,” on page 415](#)
- ♦ [Section B.7.2, “Viewing Information About Imaging Requests,” on page 423](#)
- ♦ [Section B.7.3, “Starting a Manual Multicast Session,” on page 423](#)

## B.7.1 Initiating the Imaging Processes

An imaging server daemon is initiated by running the script at the Linux terminal program command line, which in turn calls the executable and uses the configuration set in the corresponding `.conf` file. Because the scripts do not normally accept parameters, but only arguments (such as `start`), you can configure parameters in their corresponding `.conf` files.

The following Linux daemons run the imaging server processes:

- ♦ [“novell-pbserv” on page 415](#)
- ♦ [“novell-proxydhcp” on page 416](#)
- ♦ [“novell-tftp” on page 418](#)
- ♦ [“novell-zmgprebootpolicy” on page 420](#)
- ♦ [“Understanding Script Arguments” on page 422](#)

### novell-pbserv

The novell-pbserv daemon provides imaging services to devices.

This daemon is started automatically when installing ZENworks Linux Management, or when rebooting the server.

- ♦ [“Understanding the novell-pbserv Components” on page 415](#)
- ♦ [“Configuring novell-pbserv” on page 415](#)

### Understanding the novell-pbserv Components

To initiate the novell-pbserv daemon, enter the following command listed for Script Location on the Linux command line in a terminal program:

---

Script Location:	<code>/etc/init.d/novell-pbserv</code>
Script Arguments:	<code>start, stop, restart, force-reload, status, showpid</code> <sup>1</sup>
Executable:	<code>/opt/novell/zenworks/preboot/bin/novell-pbservd</code>
Configuration File:	<code>/etc/opt/novell/zenworks/preboot/novell-pbserv.conf</code>

---

<sup>1</sup> For descriptions of these arguments, see [“Understanding Script Arguments” on page 422](#).

### Configuring novell-pbserv

The novell-pbserv configuration file (`novell-pbserv.conf`), contains the following parameters:

Parameter	Description
EnableLogging=YES	<p>If YES, a log file is created for debug messages. This is the default.</p> <p>If NO, no log file is created for debug messages.</p> <p>The <code>novell-pbserv.log</code> file is created in the <code>/var/opt/novell/log/zenworks/preboot</code> directory.</p>
IPAddress=	<p>The IP address to be used by imaging for all communications. If nothing is entered, novell-pbserv attempts to detect an IP address.</p> <p>Can be used in a clustering environment to specify the IP address of the virtual server.</p> <p>Can also be used in a multiple-NIC environment to bind the imaging server to a specific IP address.</p> <p>By default, this is commented out.</p>
LIBRARY_NAME=	<p>Full path of the library to be loaded by the ZENWorks Imaging Service. If the library name is not specified, then by default <code>libzenimgweb.so</code> is loaded from the <code>/opt/novell/zenworks/preboot/lib</code> directory.</p> <p>By default, this is commented out.</p>

## novell-proxydhcp

The novell-proxydhcp daemon provides PXE devices with the information that they require to be able to connect to the ZENworks Preboot Services system.

This daemon is not started automatically when installing ZENworks Linux Management.

- ♦ [“Understanding the novell-proxydhcp Components” on page 416](#)
- ♦ [“Configuring novell-proxydhcp” on page 416](#)

### Understanding the novell-proxydhcp Components

To initiate the novell-proxydhcp daemon, enter the following command listed for Script Location on the Linux command line in a terminal program:

Script Location:	<code>/etc/init.d/novell-proxydhcp</code>
Script Arguments:	<code>start, stop, restart, force-reload, status, showpid, install</code> <sup>1</sup>
Executable:	<code>/opt/novell/bin/novell-proxydhcpd</code>
Configuration File:	<code>/etc/opt/novell/novell-proxydhcp.conf</code>

<sup>1</sup> For descriptions of these arguments, see [“Understanding Script Arguments” on page 422](#).

### Configuring novell-proxydhcp

The novell-proxydhcp configuration file (`novell-proxydhcp.conf`), contains the following parameters:



Parameter	Description
LocalDHCPFlag = 0	<p>Indicates whether the DHCP server for this subnet resides on the same server as novell-proxydhcp.</p> <p>0 (the default) means novell-proxydhcp is not running on the same server as the DHCP service. 1 means they are running on the same server.</p> <p>The Proxy DHCP server needs to behave slightly differently if it is loaded on the same server as the DHCP service.</p>
LocalInterface = 10.0.0.1	<p>Indicates the IP address to be used by the Proxy DHCP server. This setting is intended only for use on servers with multiple LAN interfaces. The IP address must be valid on the server.</p> <p>By default, this parameter is commented out.</p>
NovellPolicyEngine = 10.0.0.1	<p>The IP address of the server where a Novell Preboot policy engine is running. Most often, this is a ZENworks imaging daemon. If no value is specified, the Proxy DHCP assumes that the daemon is running on the same server.</p> <p>By default, this parameter is commented out.</p>
NBPx86 = nvlntp.sys	<p>The name of the boot file this service will suggest for all x86 computers, such as nvlntp.sys.</p>
MenuTimeout = 2	<p>The number of seconds the F8 menu is displayed before automatically choosing the first option, which is always this server and its default NBP. The default is 2 seconds.</p>
ProxyLogLevel = 2	<p>The value assigned here determines which events are entered in <code>novell-proxydhcp.log</code>. Specifying a high level in an active system can quickly fill the log. Valid values are: 0, 1, 2, 3, and 4. The default is 2.</p> <p>Each message from the Proxy DHCP server is assigned a priority level. If <i>ProxyLogLevel</i> is set to a value equal to or greater than a message's priority level, that message is entered in <code>novell-proxydhcp.log</code>. All other messages are ignored.</p> <p>Priority meaning:</p> <ul style="list-style-type: none"> <li><b>0:</b> Critical information. Service start, stop, and critical events are logged.</li> <li><b>1:</b> Warning information. Additionally, warning information is logged.</li> <li><b>2:</b> Transaction information. All completed client transaction are logged.</li> <li><b>3:</b> Request information. All client requests and Proxy DHCP requests received are logged, including ignored requests. If a request is ignored, the reason for ignoring it is also logged.</li> <li><b>4:</b> Debugging information. All DHCP packets received and accepted are decoded and logged.</li> </ul>
ProxyLogFile = /var/opt/novell/log/novell-proxydhcp.log	<p>The file where all log file entries are placed. It is located at <code>/var/opt/novell/log/novell-proxydhcp.log</code>.</p> <p>By default, this parameter is commented out.</p>

Parameter	Description
ProxyLogFileSize = 15	<p>The size of the <i>ProxyLogFile</i> file is controlled by the value of <i>ProxyLogFileSize</i>, where 15 is the default (in MB).</p> <p>When the log file exceeds the <i>ProxyLogFileSize</i> value, it is deleted and restarted.</p>

Parameters that are not commented out, but contain no values, are given a default value.

The novell-proxydhcp daemon is compliant with the following RFCs:

RFC 2131 - Dynamic Host Configuration Protocol

RFC 2132 - DHCP Options and BOOTP Vendor Extensions

The novell-proxydhcp daemon is compliant with the Preboot eXecution Environment (PXE) Specification v2.1 industry specification, published by Intel.

## novell-tftp

The novell-tftp daemon provides TFTP services to imaging clients.

This daemon is started automatically when installing ZENworks Linux Management, or when rebooting the server.

- ♦ [“Understanding the novell-tftp Components” on page 418](#)
- ♦ [“Configuring novell-tftp” on page 418](#)

## Understanding the novell-tftp Components

To initiate the novell-tftp daemon, enter the following command (listed under Script Location) on the Linux command line in a terminal program:

Script Location:	/etc/init.d/novell-tftp
Script Arguments:	start, stop, restart, force-reload, status, showpid <sup>1</sup>
Executable:	/opt/novell/bin/novell-tftpd
Configuration File:	/etc/opt/novell/novell-tftp.conf

<sup>1</sup> For descriptions of these arguments, see [“Understanding Script Arguments” on page 422](#).

## Configuring novell-tftp

The novell-tftp configuration file (*novell-tftp.conf*), contains the following parameters for the Novell TFTP server:

Parameter	Description
TFTPInterface = 10.0.0.1	<p>The IP address that is used for all TFTP communications. If a value is not given here, the service tries to detect one.</p> <p>This value is most useful for multi-homed servers.</p> <p>By default, this parameter is commented out.</p>

Parameter	Description
TransferBlockSize = 1428	<p>This value determines the size of the data block used by the TFTP server to transmit and receive data to and from a client. Valid values are between 512 and 4428.</p> <p>For ethernet networks, this value should be 1428.</p> <p>For token ring networks, this value can be 4428, but only if you are sure there are no ethernet segments; otherwise, use 1428.</p> <p>Older TFTP clients might be restricted to 512 bytes, the original transfer block size before the adoption of RFC 2348. The Novell TFTP server is compatible with these clients.</p> <p>By default, this parameter is commented out.</p>
TimeoutInterval = 1	<p>This is the amount of time (in seconds) that the TFTP server waits for a client to acknowledge before resending a packet. However, because the TFTP server uses an adaptive algorithm to calculate the actual timeout interval, this value is only used as an initial value. It may increase or decrease, depending on the performance of the network.</p> <p>This value is only a default. It may be changed at the request of a client. See RFC 2349.</p> <p>Valid values are 1 through 60.</p> <p>By default, this parameter is commented out.</p>
Linux -- TFTPDirectory = /srv/tftp	<p><i>TFTPDirectory</i> is the directory where the TFTP server can store and retrieve files. All paths submitted to the TFTP server by clients are assumed to be relative to this directory.</p> <p>Because TFTP has no security, it is suggested that you not place files with sensitive information in this directory, and that you place a space quota on it.</p> <p>The TFTP server does not load if this directory does not exist.</p> <p>By default, this parameter is commented out.</p>
TFTPAllowWrites = 0	<p>This tells the TFTP server whether to allow users to place new files on the server. Setting this variable to 0 makes the TFTP server more secure by not allowing users to place new files on the server. The other option is 1 (the default), which allows users to place new files on the server.</p>
AllowOverwrites = 0	<p>This tells the TFTP server whether to allow users to overwrite existing files on the server. Setting this variable to 0 makes the TFTP server more secure by not allowing users to overwrite files on the server. The other option is 1 (the default), which allows users to overwrite files on the server.</p> <p>TFTPAllowWrites must be set to 1 in order for the AllowOverwrites parameter to be recognized.</p>

Parameter	Description
TFTPLogLevel = 2	<p>The value assigned here determines which events are entered in <code>novell-tftp.log</code>. Specifying a high level in an active system can quickly fill the log. Valid values are: 0, 1, 2, 3, and 4. The default is 2.</p> <p>Each message from the TFTP server is assigned a priority level. If <i>TFTPLogLevel</i> is set to a value equal to or greater than a message's priority level, that message is entered in <code>novell-tftp.log</code>. All other messages are ignored.</p> <p>Priority meaning:</p> <p><b>0:</b> Critical information. Service start, stop, and critical events are logged.</p> <p><b>1:</b> Warning information. Only failed client transactions are logged.</p> <p><b>2:</b> Transaction information. All completed client transaction are logged.</p> <p><b>3:</b> Request information. All client requests and TFTP options are logged.</p> <p><b>4:</b> Debugging information. All server events, including each packet received, are logged.</p> <p>By default, this parameter is commented out.</p>
TFTPLogFile = /var/opt/novell/log/novell-tftp.log	<p>The file where all log file entries are placed.</p> <p>By default, this parameter is commented out.</p>
TFTPLogFileSize = 15	<p>The size of the log file is controlled by the value of <i>TFTPLogFileSize</i>, where 15 is the default (in MB).</p> <p>When the log file exceeds the <i>TFTPLogFileSize</i> value, it is deleted and restarted.</p> <p>By default, this parameter is commented out.</p>

Parameters that are not commented out, but contain no values, are given a default value.

The novell-tftp daemon is compliant with the following RFCs:

- RFC 1350 -- THE TFTP PROTOCOL (REVISION2)
- RFC 2347 - TFTP Option Extension
- RFC 2348 - TFTP Blocksize Option
- RFC 2349 - TFTP Timeout Interval and Transfer Size Options

### **novell-zmgprebootpolicy**

The novell-zmgprebootpolicy daemon allows PXE devices to query the ZENworks Linux Management system for work to do and for Preboot Menu policies.

This daemon is started automatically when installing ZENworks Linux Management, or when rebooting the server.

- ◆ [“Understanding the novell-zmgprebootpolicy Components” on page 421](#)
- ◆ [“Configuring novell-zmgprebootpolicy” on page 421](#)

## Understanding the novell-zmgprebootpolicy Components

To initiate the novell-zmgprebootpolicy daemon, enter the following command (listed under Script Location) on the Linux command line in a terminal program:

Script Location:	/etc/init.d/novell-zmgprebootpolicy
Script Arguments:	start, stop, restart, force-reload, status, showpid <sup>1</sup>
Executable:	/opt/novell/zenworks/preboot/bin/novell-zmgprebootpolicyd
Configuration File:	/etc/opt/novell/zenworks/preboot/novell-zmgprebootpolicy.conf

<sup>1</sup> For descriptions of these arguments, see [“Understanding Script Arguments” on page 422](#).

## Configuring novell-zmgprebootpolicy

The novell-zmgprebootpolicy configuration file (novell-zmgprebootpolicy.conf), contains the following parameters:

Parameter	Description
LocalInterface = 10.0.0.1	<p>The IP address that is used by the Policy server.</p> <p>This setting is intended only for use on servers with multiple LAN interfaces. The address must be valid on the server.</p> <p>By default, this parameter is commented out.</p>
PolicyLogLevel = 1	<p>The value assigned here determines which events are entered in <code>novell-zenprebootpolicy.log</code>. Specifying a high level in an active system can quickly fill the log. Valid values are: 0, 1, 2, 3, and 4. The default is 2.</p> <p>Each message from the novell-zmgprebootpolicy server is assigned a priority level. If <i>PolicyLogLevel</i> is set to a value equal to or greater than a message's priority level, that message is entered in <code>novell-zenprebootpolicy.log</code>. All other messages are ignored.</p> <p>Priority meaning:</p> <ul style="list-style-type: none"><li><b>0:</b> Critical information. Service start, stop, and critical events are logged.</li><li><b>1:</b> Warning information. Only failed client transactions are logged.</li><li><b>2:</b> Transaction information. All completed client transaction are logged.</li><li><b>3:</b> Request information. All client requests are logged.</li><li><b>4:</b> Debugging information. All server events, including each packet received, are logged.</li></ul> <p>By default, this parameter is commented out.</p>
PolicyLogFile = /var/opt/novell/log/zenworks/preboot/novell-zenprebootpolicy.log	<p>The file where all log file entries are placed.</p> <p>By default, this parameter is commented out.</p>

Parameter	Description
PolicyLogFileSize = 15	<p>The size of the log file is controlled by the value of <i>PolicyLogFileSize</i>, where 15 is the default (in MB).</p> <p>When the log file exceeds the <i>PolicyLogFileSize</i> value, it is deleted and restarted.</p>
PrebootServer = 10.0.0.5	<p>This field contains the address of the imaging server that should be used to resolve policies.</p> <p>By default, this parameter is commented out.</p>
EnableAMTSupport = Yes	<p>This field enables or disables support for Intel's AMT technology.</p> <p>By default, this support is disabled by commenting out the parameter.</p>

Parameters that are not commented out, but contain no values, are given a default value.

## Understanding Script Arguments

The following arguments are available for each of the Preboot Services daemons described above:

Argument	Function
start	<p>Starts the daemon.</p> <p>Because novell-proxydhcp is optional, use this argument to start this daemon. However, this daemon does not automatically start when the server reboots. (See <a href="#">install</a> below.)</p>
start setjustimagedflag	For novell-zislnx only, it sets the Just Imaged flag so that a device can be imaged using its existing Image Safe Data.
stop	Stops the daemon.
restart	Stops and restarts the daemon if it is already running.
force-reload	Causes the daemon's configuration file to be reloaded.
status	<p>Displays the current status of the daemon.</p> <p>For example, if you enter <code>/etc/inid.d/novell-pbserv status</code>, information similar to the following is returned:</p> <pre>Novell ZENworks Imaging Service running</pre>
showpid	<p>Displays the daemon's process ID.</p> <p>For example, if you enter <code>/etc/inid.d/novell-pbserv showpid</code>, information similar to the following is returned:</p> <pre>Novell ZENworks Imaging Service running 10211</pre>
install	For novell-proxydhcp only, it causes the daemon to be automatically loaded when the server boots.

## B.7.2 Viewing Information About Imaging Requests

After the imaging server has started, you can view information about the status and results of the imaging requests that it has received from imaging clients. A statistical summary of these requests is shown on the server's terminal program command line using either of the following commands:

- ♦ For the local server:  
`/opt/novell/zenworks/preboot/bin/novell-zmgmcast -status`
- ♦ For a remote server:  
`/opt/novell/zenworks/preboot/bin/novell-zmgmcast -status -i  
remote_server_ID`  
where *remote\_server\_ID* is the IP address or DNS of the remote server.

All statistics are reset to zero if you restart the imaging server.

The statistics shown on this screen are explained below.

**Table B-4** *Imaging Request Statistics*

Statistic	Specifies
Update Requests	The number of imaging requests of any kind that have been received by the imaging server since it was started. This includes requests that failed, were denied, or were referred to other imaging servers (see <a href="#">Client Referrals</a> below). Information about each of these requests, such as the source, type, date/time, and results, is logged on the imaging server.
Images Sent	The number of images that the imaging server has sent to imaging clients since the imaging server was started. This includes only images that were retrieved from this imaging server. See <a href="#">Client Referrals</a> below for more information.
Images Received	The number of new images that have been received and stored on the imaging server since it was started. This includes images that were received through client referrals (see <a href="#">Client Referrals</a> below).
Client Referrals	<p>The number of client requests that have been referred (redirected) by the imaging server to other imaging servers since this imaging server was started. Such referrals are made only when the client is running in auto-imaging mode and the imaging server determines that the image to be created or retrieved is on a different imaging server.</p> <p><b>IMPORTANT:</b> If a client is running in manual imaging mode and it requests to store or retrieve an image on a different imaging server, the request is denied and an error is returned to the client. Referrals are currently supported only when the client is running in auto-imaging mode.</p>

## B.7.3 Starting a Manual Multicast Session

On the the bash prompt, you can start a manual multicast session, see any sessions in progress, and delete sessions. For more information, see [“Initiating a Multicast Session from Each Client” on page 327](#).





# ZENworks Imaging Engine Commands

# C

After booting a device from an imaging boot media, you can use the `img` command at the Linux bash prompt or the ZENworks® Imaging Engine menu to do any of the following:

- ♦ Take an image of the device's hard disks
- ♦ Put down an image on the device's hard disks
- ♦ View or manipulate the device's hard disk partitions
- ♦ View the device's hardware configuration or image-safe data
- ♦ Display a menu from which you can also perform all of these tasks

The ZENworks Imaging Engine is installed to the `/bin` directory on the imaging boot device. If the imaging boot device is a diskette, a CD, or DVD, the `/bin` directory is actually archived in the root file, which is expanded during the imaging boot process. If the imaging boot method is Preboot Services, the ZENworks Imaging Engine is downloaded to the device when booting.

Because the ZENworks Imaging Engine is a Linux application, the command syntax is case-sensitive. The overall syntax is:

```
img [mode]
```

where *mode* is any of the modes described in the following sections:

- ♦ [Section C.1, “Help Mode \(img help\),” on page 425](#)
- ♦ [Section C.2, “Automatic Mode \(img auto\),” on page 426](#)
- ♦ [Section C.3, “Make Mode \(img make\),” on page 427](#)
- ♦ [Section C.4, “Restore Mode \(img restore\),” on page 429](#)
- ♦ [Section C.5, “Session \(Multicast\) Mode \(img session\),” on page 433](#)
- ♦ [Section C.6, “Partition Mode \(img part\),” on page 435](#)
- ♦ [Section C.7, “ZENworks Partition Mode \(img zenPartition\),” on page 436](#)
- ♦ [Section C.8, “Dump Mode \(img dump\),” on page 437](#)
- ♦ [Section C.9, “Information Mode \(img info\),” on page 438](#)

Each mode can be abbreviated to the first letter of its name. For example, `img dump` can be abbreviated as `img d`.

To access the ZENworks Imaging Engine menu from which to perform all of these tasks, enter `img` with no parameters.

## C.1 Help Mode (img help)

Use Help mode to get information about the `img` command if you don't have this documentation available.

To use the Help mode:

**1** Do the one of following:

- ♦ Enter:

```
img [help [mode]]
```

where *mode* is the mode whose command syntax you want help with.

Examples:

Example	Explanation
img help	Displays a short description of each mode.
img help m	Displays information on how to use the Make mode.
img help p	Displays information on how to use the Partition mode.

- ♦ Enter `img` to display the ZENworks Imaging Engine menu, click *Help*, then select a mode name.

## C.2 Automatic Mode (img auto)

Use automatic mode to image the device automatically, based on any applicable Preboot Services default settings. The ZENworks Imaging Engine runs in this mode if you let the imaging boot process proceed without interruption, or if you type the command below at the Linux prompt.

To use the automatic mode, do any of the following:

- ♦ At the bash prompt, enter:  
`img auto`
- ♦ At the bash prompt, to display the ZENworks Imaging Engine menu, enter:  
`img`  
and on the menu bar click *Imaging*, then click *Query for work*.
- ♦ At the bash prompt, to display the ZENworks Imaging Engine menu, enter:  
`img`  
then click on *F9 Query for work* on the task bar.
- ♦ At the bash prompt, to display the ZENworks Imaging Engine menu, enter:  
`img`  
then press *F9*.

In this mode, the ZENworks Imaging Engine queries the imaging server specified in the `PROXYADDR` environment variable for any work to do. The imaging server checks the relevant Preboot Services default settings to determine what imaging tasks should be performed (if any), such as taking or putting down an image. It then instructs the ZENworks Imaging Engine to perform those tasks. If any tasks involve storing or retrieving images on other imaging servers, the imaging server refers the ZENworks Imaging Engine to those servers to complete those tasks. After the ZENworks Imaging Engine has completed its work, it communicates the results to the original imaging server, and the results are logged on that server.

For information on configuring the settings that control what happens in this mode, see [Section 23.4, “Configuring Preboot Services Defaults,”](#) on page 261.

## C.3 Make Mode (img make)

Use the Make mode to take an image of the device and store it in a specified location. Normally, all partitions on the local hard disks are included in the image, but there are some exceptions noted below.

You can take an image of a device using either the bash prompt or using the ZENworks Imaging Engine menu. For step-by-step instructions, see [“Manually Taking an Image of a Device”](#) on page 305. You can also use the Make Locally mode to take an image of the device and store it in a partition on a local hard disk. For step-by-step instructions, see [Section 24.3.3, “Setting Up Disconnected Imaging Operations,”](#) on page 314.

The image size corresponds to roughly half the size of the data in all of the device’s partitions, except that the ZENworks partition and Compaq or Dell configuration partitions are always excluded.

The syntax of this mode depends on whether you will store the image locally or on an imaging (proxy) server.

The following sections contain additional information:

- ♦ [Section C.3.1, “Make Locally \(img makel\),”](#) on page 427
- ♦ [Section C.3.2, “Make to Proxy \(img makep\),”](#) on page 428

### C.3.1 Make Locally (img makel)

Using the bash prompt, the following example explains the syntax and available parameters that you can use with the `makel` “make locally” parameter:

```
img makel[pNumber] filepath [comp=comp level] [xpartition]
```

#### Commands

**Table C-1** *makel* Commands

Parameter	Specifies
<code>makel[pNumber]</code>	<p>The partition number (as displayed by <code>img dump</code>) of the local partition for where to store the image. It must be a primary partition. This partition is excluded from the image that’s created.</p> <p>If you omit the partition number from this parameter, the image is stored in the local ZENworks partition.</p>
<code>filepath</code>	<p>The image filename, including a <code>.zmg</code> extension and the complete path from the root of the partition. The directories in the path must exist. If the file already exists, it is overwritten. However, you are prompted to verify whether to overwrite.</p>

Parameter	Specifies
[ <i>comp=comp level</i> ]	<i>comp level</i> is the amount of compression used when creating the image. Specify any number from 0-9. 0 means no compression. 1 is the same as <i>Optimize for Speed</i> and is used by default if you do not specify this parameter. 6 is the same as <i>Balanced</i> . 9 is the same as <i>Optimize for Space</i> .
<i>xpartition</i>	The partition number (as displayed by <code>img dump</code> ) of a local partition to exclude from the image. You can repeat this parameter as needed to exclude multiple partitions.  If you omit this parameter, all partitions are included in the image except the one where the image will be stored.

## Examples

**Table C-2** *makel Examples*

Example	Explanation
<code>img makel8 /imgs/dellnt.zmg</code>	Takes an image of all partitions except the one in slot 8 and saves the image to <code>imgs/dellnt.zmg</code> in the partition in slot 8. (Assumes slot 8 contains a primary partition.)
<code>img makel /imgs/dellnt.zmg</code>	Takes an image of all partitions and saves it to <code>imgs/dellnt.zmg</code> in the ZENworks partition. (Assumes partition has been installed.)
<code>img makel /imgs/dellnt.zmg x2 x3</code>	Takes an image of all partitions except those in slots 2 and 3 and saves the image to <code>imgs/dellnt.zmg</code> in the ZENworks partition. (Assumes the partition has been installed.)

## C.3.2 Make to Proxy (img makep)

Using the bash prompt, the following example explains the syntax and available parameters that you can use with the `makep` “make to proxy” parameter:

```
img makep address filepath [comp=comp level] [xpartition]
```

## Commands

**Table C-3** *makep Commands*

Parameter	Specifies
<i>address</i>	The IP address or DNS name of the imaging server to store the image on.

Parameter	Specifies
<i>filepath</i>	The image filename, including a <code>.zmg</code> extension and the complete path in UNC style. The directories in the path must exist. If the file already exists, the imaging server won't overwrite it unless you enable this behavior in the ZENworks Control Center. If no folders are specified in the path, the image is created at the root of the volume or drive where the ZENworks Linux Management imaging server software is installed.  <b>IMPORTANT:</b> Because Linux doesn't recognize backslashes, you must use forward slashes in the UNC path, or enclose the entire path in quotes.
[ <i>comp=comp level</i> ]	<i>comp level</i> is the amount of compression used when creating the image. Specify any number from 0-9. 0 means no compression. 1 is the same as <i>Optimize for Speed</i> and is used by default if you do not specify this parameter. 6 is the same as <i>Balanced</i> . 9 is the same as <i>Optimize for Space</i> .
<i>xpartition</i>	The partition number (as displayed by <code>img dump</code> ) of a local partition to exclude from the image. You can repeat this parameter as needed to exclude multiple partitions.  If you omit this parameter, all partitions are included in the image.

## Examples

**Table C-4** *makep* Examples

Example	Explanation
<code>img makep 137.65.95.127 //xyz_server/sys/imgs/dellnt.zmg</code>	Takes an image of all partitions and saves it to <code>sys/imgs/dellnt.zmg</code> on <code>xyz_server</code> . (Assumes 137.65.95.127 is the IP address of <code>xyz_server</code> .)
<code>img makep img.xyz.com //xyz_server/sys/imgs/dellnt.zmg x2 x3</code>	Takes an image of all partitions except those in slots 2 and 3 and saves the image to <code>sys/imgs/dellnt.zmg</code> on <code>xyz_server</code> . (Assumes <code>img.xyz.com</code> is the DNS name of <code>xyz_server</code> .)

## C.4 Restore Mode (`img restore`)

Use the Restore mode to retrieve an image from a specified location and put it down on a device.

You can restore an image of a device using either the bash prompt or using the ZENworks Imaging Engine menu. For step-by-step instructions, see [“Manually Taking an Image of a Device” on page 305](#). You can also use the Restore mode to restore an image from a partition on a local hard disk. For step-by-step instructions, see [Section 24.3.3, “Setting Up Disconnected Imaging Operations,” on page 314](#).

Normally, if the image to be put down is a base image (one created previously by the ZENworks Imaging Engine), all existing partitions except the ZENworks partition and Dell or Compaq configuration partitions are removed from all local hard disks before the new image is put down. When the image is put down, the sizes of the original partitions from which the image was taken are preserved, if possible. If there's insufficient space, the last partition is shrunk to fit, unless this would result in data loss, in which case the ZENworks Imaging Engine denies the requested operation. If

there is extra space left after all partitions in the image have been restored to their original sizes, that space is left unpartitioned.

If the image to be put down is an **add-on image**, or if it's a base image and you specify the `apartition:ppartition` parameter, none of the existing physical partitions are removed. Instead, the appropriate partitions are merely updated with the files from the image, overwriting any existing file of the same name and location.

Restoring add-on images over 4 GB in size is not supported by Linux Management imaging.

The syntax of this mode depends on whether you will retrieve the image from a local device or from an imaging (proxy) server, as explained in the subsections below:

- ♦ **Section C.4.1, “Restore from Local (img restore),” on page 430**
- ♦ **Section C.4.2, “Restore from Proxy (img restorep),” on page 432**

## C.4.1 Restore from Local (img restore)

Use the Restore from Local mode to retrieve an image from a local device and put it down on the device. For more information, see **Section 24.3.3, “Setting Up Disconnected Imaging Operations,” on page 314.**

Using the bash prompt, the following example explains the syntax and available parameters that you can use with the `restorel` “restore from local” parameter:

```
img restorel[pNumber] filepath [sfileset] [apartition:ppartition]
```

### Commands

**Table C-5** *restorel* Commands

Parameter	Specifies
<code>restorel[pNumber]</code>	<p>The partition number (as displayed by <code>img dump</code>) of the local partition to retrieve the image from. It must be a primary partition. This partition will not be changed by the imaging operation.</p> <p>If you omit the partition number from this parameter, the image is retrieved from the local ZENworks partition.</p>
<code>filepath</code>	<p>The filename of the image to retrieve, including the <code>.zmg</code> extension and the complete path from the root of the partition.</p>
<code>sfileset</code>	<p>The number of the image file set to put down. Valid values are 1 through 10. For information on creating file sets of an image, see <b>Section 22.5.2, “Creating, Installing, and Restoring Standard Images,” on page 233.</b></p> <p>If you omit this parameter, file set 1 is used.</p>

Parameter	Specifies
<i>apartition:ppartition</i>	<p>A mapping between a partition in the image archive (<i>apartition</i>) and a target physical partition on the local machine (<i>ppartition</i>). Use this parameter to selectively restore a specific part of the image to a specific local partition.</p> <hr/> <p><b>IMPORTANT:</b> If you use this parameter, none of the existing local partitions are removed, and only the target local partition is updated. The update process does not remove any existing files; however, any existing files of the same names are overwritten. If you want to remove all existing files from the target partition before updating it, first use the <b>Partition Mode (img part)</b> to delete and recreate the partition.</p> <hr/> <p>For <i>apartition</i>, use the partition number displayed for the source partition in the <b>Image Explorer (ImgExp.exe)</b> utility. For <i>ppartition</i>, use the partition number displayed by img dump for the target partition. The target partition must be a partition of a supported file system. You can repeat this parameter as needed to request multiple selective restorations in a single operation. In doing so, you can apply multiple parts of the image to a single local partition, but you can't apply the same part of an image to multiple local partitions in a single operation.</p>

## Examples

**Table C-6** *restore Examples*

Example	Explanation
<code>img restore18 /imgs/dellnt.zmg</code>	Removes all existing local partitions except the one in slot 8, retrieves the image from imgs/dellnt.zmg in slot 8, and puts down the partitions and contents of that image on the available local writable devices. (Assumes there's sufficient local space and that slot 8 contains a primary partition.)
<code>img restore1 /imgs/dellnt.zmg</code>	Removes all existing local partitions, retrieves the image from imgs/dellnt.zmg in the ZENworks partition, and puts down the partitions and contents of that image on the available local writable devices (assuming there's sufficient space).
<code>img restore1 /imgs/dellnt.zmg s2</code>	Removes all existing local partitions, retrieves the image from imgs/dellnt.zmg in the ZENworks partition, and puts down the partitions and contents of file set 2 of that image on the available local writable devices (assuming there's sufficient space).
<code>img restore1 /imgs/dellnt.zmg a2:p1 a3:p1</code>	Retrieves the image from imgs/dellnt.zmg in the ZENworks partition, updates local partition 1 with the data from partitions 2 and 3 of that image, and leaves the other local partitions unchanged. (Assumes there's sufficient space in local partition 1.)

## C.4.2 Restore from Proxy (img restorep)

Use the Restore from Proxy mode to retrieve an image from an imaging (proxy) server and put it down on the device. For more information, see [“Manually Putting an Image on a Device” on page 309](#).

Using the bash prompt, the following example explains the syntax and available parameters that you can use with the `restorep` “restore from proxy” parameter:

```
img restorep address filepath [sfileset] [apartition:ppartition]
```

### Commands

**Table C-7** *restorep* Commands

Parameter	Specifies
<i>address</i>	The IP address or DNS name of the imaging server to retrieve the image from.
<i>filepath</i>	<p>The filename of the image to retrieve, including the <code>.zimg</code> extension and the complete path in UNC style.</p> <p><b>IMPORTANT:</b> Because Linux doesn’t recognize backslashes, you must use forward slashes in the UNC path or enclose the entire path in quotes.</p>
<i>sfileset</i>	<p>The number of the image file set to put down. Valid values are 1 through 10. For information on creating file sets of an image, see <a href="#">Section 22.5.2, “Creating, Installing, and Restoring Standard Images,” on page 233</a>.</p> <p>If you omit this parameter, file set 1 is used.</p>
<i>apartition:ppartition</i>	<p>A mapping between a partition in the image archive (<i>apartition</i>) and a target physical partition on the local machine (<i>ppartition</i>). Use this parameter to selectively restore a specific part of the image to a specific local partition.</p> <p><b>IMPORTANT:</b> If you use this parameter, none of the existing local partitions are removed, and only the target local partition is updated. The update process does not remove any existing files or overwrite any existing files of the same names if they are newer. If you want to remove all existing files from the target partition before updating it, first use the <a href="#">Partition Mode (img part)</a> to delete and recreate the partition.</p> <p>For <i>apartition</i>, use the partition number displayed for the source partition in the <a href="#">Image Explorer (ImgExp.exe)</a> utility. For <i>ppartition</i>, use the partition number displayed by <code>img dump</code> for the target partition. The target partition must be a partition of a supported file system. You can repeat this parameter as needed to request multiple selective restorations in a single operation. In doing so, you can apply multiple parts of the image to a single local partition, but you can’t apply the same part of an image to multiple local partitions in a single operation.</p>



## Examples

**Table C-8** *restorep Examples*

Example	Explanation
<pre>img restorep 137.65.95.127 // xyz_server/sys/imgs/dellnt.zmg</pre>	Removes all existing local partitions, retrieves the image from <code>sys/imgs/dellnt.zmg</code> on <code>xyz_server</code> , and puts down the partitions and contents of that image on the available local writable devices. (Assumes there's sufficient local space and that 137.65.95.127 is the IP address of <code>xyz_server</code> .)
<pre>img restorep img.xyz.com // xyz_server/sys/imgs/dellnt.zmg s2</pre>	Removes all existing local partitions, retrieves the image from <code>sys/imgs/dellnt.zmg</code> on <code>xyz_server</code> , and puts down the partitions and contents of file set 2 of that image on the available local writable devices. (Assumes there's sufficient local space and that <code>img.xyz.com</code> is the DNS name of <code>xyz_server</code> .)
<pre>img restorep img.xyz.com // xyz_server/sys/imgs/dellnt.zmg a2:p1</pre>	Retrieves the image from <code>sys/imgs/dellnt.zmg</code> on <code>xyz_server</code> , updates local partition 1 with the data from partition 2 of that image, and leaves the other local partitions unchanged. (Assumes there's sufficient space in local partition 1 and that <code>img.xyz.com</code> is the DNS name of <code>xyz_server</code> .)

## C.5 Session (Multicast) Mode (img session)

Use the Session (Multicast) mode to take an image of one device and put it down on multiple other devices simultaneously over the network in a single operation.

**IMPORTANT:** For multicasting to work properly, the routers and switches on the network must have multicast features configured. Otherwise, multicast packets might not be routed properly.

For multicasting to work, each participating device must boot from an imaging boot media and run the ZENworks Imaging Engine in this mode, as explained below. The device from which the image is taken is called the *master*, and the devices that receive the image are called *participants*.

You can start the multicast session from the imaging server. If you start the session this way, you specify an image file for multicasting rather than a device as the session master. Otherwise, if you start the session from a client device, you can specify one of the session participants as the session master. In that case, an image of the session master's hard drive is sent to the session participants. For more information, see [“Initiating a Multicast Session from Each Client” on page 327](#).

Using the bash prompt, the following example explains the syntax and available parameters that you can use with the `session` parameter:

```
img session name [master|client] [clients=count] [t=minutes]
```

## Commands

**Table C-9** *session Commands*

Parameter	Specifies
<i>name</i>	<p>The name of the multicast session. Each device joining the session uses the same value for this parameter.</p> <p><b>IMPORTANT:</b> The name must be unique among concurrent multicast sessions. It is hashed by the ZENworks Imaging Engine to produce a Class D IP address for the multicast session. To facilitate troubleshooting (wire sniffing), all Linux Management imaging multicast addresses start with 231. For example, the session name <code>mcast01</code> can produce the multicast address 231.139.79.72.</p>
<i>master client</i>	<p>Specifies that this device is the session master or a session client.</p> <p>If you omit this parameter, the ZENworks Imaging Engine waits for the user at the master device to press <code>m</code> to designate that device as the master, or it waits for another device to be declared master for the imaging session to be started from the imaging server by selecting <i>Manually start multicast</i>, providing the required information, then selecting <i>Yes</i>.</p>
<i>clients=count</i>	<p>The number of participating devices that must register with the master before imaging begins. This option only applies to session masters.</p> <p>If you omit this parameter, the ZENworks Imaging Engine waits for the user at the master device to press <code>g</code>. After imaging has begun, any participating devices attempting to register are denied.</p>
<i>time=minutes</i>	<p>The number of minutes the master device waits for the next participant to register before starting the imaging process without reaching <i>count</i> registered participants. This option only applies to session masters.</p> <p>If you omit this parameter, the imaging process does not start until <i>count</i> is reached, or the user at the master device presses <code>g</code>. After that, any participants attempting to register are denied and queued for the next multicast session.</p>

## Examples

**Table C-10** *session Examples*

Example	Explanation
<code>img session mcast01</code>	<p>Starts a multicast session named <code>mcast01</code>. Each successive device that issues this same command before the imaging begins joins the session. Imaging doesn't start until one of the users presses <code>m</code> to designate himself as master and presses <code>g</code> to start the imaging, or the imaging session is started from the imaging server by selecting <i>Manually start multicast</i>, providing the required information, then selecting <i>Yes</i>.</p>

Example	Explanation
<code>img session mcast01 m</code>	Starts a multicast session named <code>mcast01</code> and designates this device as the master. Each successive device that issues <code>img session mcast01</code> before the imaging begins joins the session as a participant. Imaging doesn't start until the master user presses <code>g</code> .
<code>img session mcast01 master clients=5</code>	Starts a multicast session named <code>mcast01</code> . Each successive device that issues <code>img session mcast01</code> before the imaging begins joins the session. Imaging doesn't start until one of the users presses <code>m</code> to designate himself as master, or until the imaging session is started from the imaging server by selecting <i>Manually Start Multicast</i> , providing the required information, then selecting <i>Yes</i> . Five other devices must also register as participants before the session begins.
<code>img session mcast01 master clients=5 time=20</code>	Starts a multicast session named <code>mcast01</code> . Each successive device that issues <code>img session mcast01</code> before the imaging begins joins the session. Imaging doesn't start until one of the users presses <code>m</code> to designate himself as master, or until the imaging session is started from the imaging server by selecting <i>Manually Start Multicast</i> , providing the required information, then selecting <i>Yes</i> . Either five other devices must register as participants or more than 20 minutes must elapse between any consecutive participant registrations, whichever occurs first, and then the session begins.

## C.6 Partition Mode (img part)

Use the Partition mode to activate (make bootable), add, or delete a partition on the device.

You can activate, add, or delete a partition using either ZENworks Imaging Engine menu or the bash prompt.

The Partition mode can be used in two ways:

- ♦ [Section C.6.1, “Using the ZENworks Imaging Engine Menu,” on page 435](#)
- ♦ [Section C.6.2, “Using the Bash Prompt,” on page 436](#)

### C.6.1 Using the ZENworks Imaging Engine Menu

- 1 Enter `img` to display the ZENworks Imaging Engine menu, then click *Partitioning*.
- 2 Click *Modify partitions*, then click an option:

**Active:** Select a partition that you want to activate (make bootable), then click *Active*.

**Add:** Opens the Create New Partition window. Click a partition type, partition size, and cluster size, then click *OK*.

**Delete:** Select a partition, then click *Delete*.

For more information, see the table in [Section C.6.2, “Using the Bash Prompt,” on page 436](#).

## C.6.2 Using the Bash Prompt

1 From the bash prompt, enter:

```
img poperation
```

where *operation* is one of the following:

Operation	Specifies to
<code>pcpNumber type</code> <code>[size]</code> <code>[cluster=clusterSize]</code>	<p>Create a new partition, where:</p> <ul style="list-style-type: none"><li>♦ <i>pNumber</i> is the number of the partition slot (as displayed by <code>img dump</code>) in which to create the partition</li><li>♦ <i>type</i> is a keyword, a partition name, Extended, or a numerical value for the partition type, for example 0x0C (hexadecimal) or 11 (decimal)  If you are creating an extended partition, you can create a logical drive inside of the extended partition. (See the next table for an example.)</li><li>♦ <i>size</i> is a valid size for the partition type in MB or a percentage  If you omit this parameter, the largest valid size for the partition type is used, given the available unpartitioned space on the drive.  If you give a percentage, include the % symbol; otherwise, the value is considered the size in MB.</li></ul> <p>The new partition is recognizable by other operating systems, but must be formatted or have a base image restored to it before you can store files in it.</p>
<code>pdpNumber</code>	Delete the partition from slot number <i>pNumber</i> . Use <code>img dump</code> to get the slot number.
<code>pd-all</code>	Deletes all non-protected partitions.
<code>papNumber</code>	Activate (make bootable) the partition in slot number <i>pNumber</i> . Use <code>img dump</code> to get the slot number.

The following are examples:

Example	Explanation
<code>img pc1 ext2</code>	Creates the ext2 partition in slot 1 using all of the available unpartitioned space on the drive.
<code>img pc5 reiser 5671</code>	Creates a reiser partition in slot 5 using 5,671 MB on the drive.
<code>img pd3</code>	Deletes the partition from slot 3.
<code>img pc2 extended 2500</code>	Creates an extended partition with a 2500 ext2 logical drive and a 500 MB reiser logical drive.
<code>img pc2 reiser 500</code>	

## C.7 ZENworks Partition Mode (img zenPartition)

Use the ZENPartition mode to enable, disable, or remove the installed ZENworks partition.

To use the ZENPartition mode:

**1** Do one of the following:

- ♦ From the bash prompt, enter the following:

```
img zenPartition operation
```

where *operation* is enable, disable, or remove.

- ♦ Enter `img` to display the ZENworks Imaging Engine menu, click *Partitioning*, then click one of the following:

*Disable ZENworks partition*

*Enable ZENworks partition*

*Remove ZENworks partition*

**2** Enter `lilo.s` to make this change effective.

---

**IMPORTANT:** If you remove an installed ZENworks partition, you must immediately restore a base image with a valid non-LILO MBR (Master Boot Record). If you do not, the device will not be able to boot properly.

---

## C.8 Dump Mode (img dump)

Use the Dump mode to view information about the hard drives and partitions on the device.

To use the Dump mode:

**1** Do one of the following:

- ♦ Enter `img` to display the ZENworks Imaging Engine menu, click *System information*, then click *Drive information*.

- ♦ Enter the following:

```
img dump [geo]
```

where:

Parameter	Specifies to
dump	List the existing partitions on all local hard drives. For each partition, the type, size, and slot number of the partition are given.  The ZENworks partition and Dell or Compaq configuration partitions are not listed.
geo	Display additional information about the geometry (cylinders, heads, and sectors) and capacity of each hard drive.

Examples:

Example	Explanation
<code>img dump</code>	Lists the current partitions on all local writable devices.

Example	Explanation
<code>img dump geo</code>	Lists all hard drives, their geometry and capacity, and the current partitions on the writable devices.

## C.9 Information Mode (img info)

Use the Information mode to view the following:

- ♦ The data currently stored in the image-safe area on the device

This data is saved by the Novell ZENworks Linux Management Imaging Agent (**novell-zislnx**) during each device's session to ensure that it can be restored after the device is reimaged. If the device is new and doesn't have an operating system yet, an initial set of data is supplied from the default configuration for the ZENworks Management Zone, such as IP addresses.

- ♦ Information about the hardware devices on the device

This information is detected during the imaging boot process. If the ZENworks Imaging Engine runs in auto-imaging mode, this information is sent to the imaging server to help determine which image to put on the device, if necessary.

- ♦ Name of the base image that was last put down on the device

To use the Information mode:

- 1 Enter `img` to display the ZENworks Imaging Engine menu, click *System information*, then click *Image-safe data* or *Detected hardware*. (See **Table C-11** for details.)

or

Enter the following from the bash prompt:

```
img info [zisd]
```

## Commands

**Table C-11** *Information Mode Parameters*

Menu item or parameter	Specifies to
System Information > Detected Hardware  or  info (from the bash prompt)	List the detected hardware devices on the device, including: <ul style="list-style-type: none"><li>♦ CPU chipset</li><li>♦ BIOS asset tag</li><li>♦ BIOS serial number</li><li>♦ Video adapter</li><li>♦ Network adapter</li><li>♦ MAC address</li><li>♦ Sound card</li><li>♦ Hard drive controller</li><li>♦ Hard disk capacity</li><li>♦ Detected RAM</li><li>♦ Boot media</li></ul>
System Information > Image Safe Data  or  img info zisd (from the bash prompt)	List the data currently stored in the image-safe area on the device. The items that comprise this data are listed in <a href="#">Section B.3, “Image-Safe Data Viewer and Editor (zisview and zisedit),” on page 407</a> .  In addition to the image-safe data, the last base image that was put down on the device is also listed.

## Examples

Example	Explanation
img info	Lists the detected hardware devices on the device.
img info zisd	Lists the Linux Management image-safe data currently stored on the device and the last base image that was put down.





# Updating ZENworks Imaging Resource Files

# D

In Novell® ZENworks® 7 Server Management, you can manually update ZENworks imaging resource files.

The following sections provide concepts on how the boot process works with ZENworks imaging, and instructions for updating imaging resource files:

- ♦ [Section D.1, “The Linux Distribution for Imaging,” on page 441](#)
- ♦ [Section D.2, “Understanding Device Boot Processes in a ZENworks Imaging Environment,” on page 442](#)
- ♦ [Section D.3, “Understanding ZENworks Partitions and Command Line Parameters,” on page 443](#)
- ♦ [Section D.4, “Modifying ZENworks Imaging Resource Files,” on page 444](#)
- ♦ [Section D.5, “Adding or Updating LAN Drivers,” on page 449](#)
- ♦ [Section D.6, “Using Uname,” on page 451](#)
- ♦ [Section D.7, “Variables and Parameters,” on page 452](#)
- ♦ [Section D.8, “Troubleshooting Linux Driver Problems,” on page 454](#)

## D.1 The Linux Distribution for Imaging

ZENworks Imaging uses a small Linux distribution on the client device to perform imaging operations. The distribution shipping with ZENworks 7 is based on the SUSE® installation system, where SUSE Linux or SUSE Linux Enterprise Server (SLES) boot to a small distribution to perform a YaST installation. ZENworks Imaging uses the same installation system found in SLES, but instead of starting a YaST installation, it starts a ZENworks Imaging session.

In ZENworks 6.5 SP1 and earlier, Linux kernel 2.4.x is used in the customized distribution; in ZENworks 6.5 SP2 the kernel is updated to 2.6 and is a SLES-based distribution.

Using a stable Linux distribution based on SLES gives customers a distribution with the broadest range of stable drivers available. The hardware industry is continually introducing new and updated network and disk drivers, so it's not always possible to provide the latest drivers in its software releases.

This section covers how to update Linux drivers using the new distribution. It deals with the imaging resource files that are based on the SLES distribution and ZENworks Preboot Services processing.

## D.2 Understanding Device Boot Processes in a ZENworks Imaging Environment

The following provides a high-level overview of a Linux boot process and how ZENworks 7 imaging affects it:

1. A boot loader program loads the Linux kernel and `initrd` (initial RAM drive) into memory.

The SLES-based imaging distribution uses `isolinux` as the boot loader for imaging CDs, a modified `pxelinux` for booting using PXE, or `linld.com` when using a single diskette with the CD. If you have a ZENworks partition installed, it uses the `lilo` program to boot alternately between the ZENworks partition and the installed operating system.

Following are the filenames and paths:

Files	When booting from a CD	When booting from PXE
Preboot Loader	<code>isolinux</code>	<code>linld.com</code>
Linux Kernel Name	<code>/boot/loader/linux</code>	<code>/srv/tftp/boot/linux</code>
Initrd Filename	<code>/boot/loader/initrd</code>	<code>/srv/tftp/boot/initrd</code>

2. The Linux kernel starts running, does some device driver setup, then mounts the `initrd` file system.  
Regardless of which boot loader method is used, the main purpose is to set up the `initrd` file as a RAM drive, load the Linux kernel into memory, then turn control over to it with an indication to the Linux kernel of where to find `initrd`.
3. The Linux kernel turns control over to `linuxrc`, for performing initial hardware detection. When finished, control is returned to the Linux kernel.
4. The Linux kernel starts a background process (`/sbin/init`).

After control is passed to the `linuxrc` program, control is never returned to the Linux kernel or passed on to the `init` process.

For more information on `linuxrc` and `zenworks.s`, review the following sections:

- ♦ [Section D.2.1, “linuxrc,” on page 442](#)
- ♦ [Section D.2.2, “zenworks.s,” on page 443](#)

### D.2.1 linuxrc

When control is turned over to `linuxrc`, there are several processes it performs to get the system ready for the imaging process. `Linuxrc` is initially configured from the `/linuxrc.config` file, which is located in the `initrd` file system. Additional configuration information for `linuxrc` can be placed in the `/info` file (located in the `initrd` file system), but ZENworks does not normally use this information.

`Linuxrc` also loads a `root` file system, which is combined with the `initrd` file system that is set up by the boot loader. The `root` file system is located on an imaging CD as the file `/boot/root`. For PXE booting, the `root` file system is stored on the ZENworks imaging server as `/srv/tftp/boot/root`.

Linuxrc attempts to locate and load the `settings.txt` file, either on the root of the imaging CD, or on the ZENworks imaging server in the `/srv/tftp` directory. From `settings.txt`, linuxrc reads and processes any parameters that pertain to itself, then copies `settings.txt` to the root ( `/` ) of the file system.

Linuxrc then also attempts to locate and load a file named `driverupdate`. It is usually located in the same directory as `root`. This file is used to update drivers and other files in the imaging distribution.

The `driverupdate` file is based on standard SUSE technology during a PXE boot. Because the network must be operating normally in order to obtain `driverupdate`, this file cannot update drivers for the active network device. However, other files and drivers can be updated by using the `driverupdate` file. For more information, see [Section D.4.3, “Using the Driverupdate File Method,” on page 447](#).

## D.2.2 zenworks.s

A normal SUSE installation for SUSE Linux or SLES boots to a small distribution to perform a YaST installation. ZENworks Imaging boots with the same installation system, but instead of starting a YaST installation, it starts the ZENworks Imaging process. Control is turned over to the ZENworks script `/bin/zenworks.s`, which is the main script file for ZENworks imaging processing. The script performs a certain number of setup tasks, then gives control to the appropriate script for the selected imaging process. For more information on the imaging process, see [Chapter 22, “Understanding Preboot Services in ZENworks Linux Management,” on page 215](#).

One of the setup tasks is to apply any update files. When booting from a CD, `zenworks.s` copies the `/addfiles` directory structure to the Linux file system. For more information, see [Section D.4.1, “Adding Files to an Imaging Boot CD,” on page 445](#).

## D.3 Understanding ZENworks Partitions and Command Line Parameters

The following sections provide an understanding of the ZENworks partition and imaging commands that are used when updating Linux drivers:

- ♦ [Section D.3.1, “The ZENworks Partition,” on page 443](#)
- ♦ [Section D.3.2, “Command Line Parameters and Variables,” on page 444](#)

### D.3.1 The ZENworks Partition

The ZENworks partition is used to store the files required to load Linux into RAM, making the result similar to using a CD or PXE boot method. The ZENworks partition has a similar boot media layout as an imaging CD. It has a minimum size of 150 MB.

The files stored on the ZENworks partition are `/boot/loader/linux`, `/boot/loader/initrd`, and `/boot/root`, which are the same directories as on the imaging CD. In ZENworks 7, the boot loader continues to be lilo, which loads Linux as described under [Section D.2, “Understanding Device Boot Processes in a ZENworks Imaging Environment,” on page 442](#). The `driverupdate` and `settings.txt` files are searched for and loaded from the ZENworks partition.

If you need to modify the Linux files, you must modify the `initrd` or `root` file sets the same way as you would for other boot methods. For information, see [Section D.4.2, “Adding Files to the Initrd or Root File Systems,”](#) on page 446.

## D.3.2 Command Line Parameters and Variables

There are four types of command line parameters that can be used with the ZENworks imaging process. They are entered manually on the command line when booting from a CD or they can be placed in the `isolinux.cfg` file located in the `/boot/loader` directory. The commands are also located in the `*.cfg` files for PXE and are located in the `/srv/tftp` directory on the ZENworks imaging server.

- ♦ **Kernel parameters:** The valid parameters for the Linux kernel are found in the `/Documentation/kernel-parameters.txt` file that is installed with the kernel source.

Some devices have a faulty BIOS, where you must turn off ACPI processing for the kernel to load properly. To do this, use the kernel parameter `acpi=off`. For more information, see [Novell Support \(http://support.novell.com/techcenter/search/Docs/SuSE/SuSE\\_SDB/en/2002/10/81\\_acpi.html\)](http://support.novell.com/techcenter/search/Docs/SuSE/SuSE_SDB/en/2002/10/81_acpi.html).

- ♦ **Linuxrc parameters:** These parameters affect the way `linuxrc` detects hardware or sets hardware settings. They are described briefly in the `/usr/share/doc/packages/linuxrc/linuxrc.html` file in a Linux system.

`Linuxrc` parameters can be found in the `/linuxrc.config` or `/info` files that reside in the `initrd` file system. Some parameters can be placed in the `settings.txt` file that is located on the root of the imaging CD or ZENworks partition, or in the `/srv/tftp/boot` file for PXE booting.

Parameters that can be placed in the `settings.txt` file (the easiest file to edit) are limited. During PXE booting, parameters that affect the network are not processed from `settings.txt`, because by the time `linuxrc` loads the `settings.txt` file, the network is already set up. Network settings can be placed in the `settings.txt` file when booting from an imaging CD, because it is loaded early enough in the process to take effect.

- ♦ **ZENworks variables:** Some environment variables affect the way imaging performs. They can be configured in any file, but should normally be configured in the `settings.txt` file.

If you add variables to the `settings.txt` file that were not originally defined there, you must export the variable. For example, in the `settings.txt` file, enter:

```
export IMGCMD="myscript"
```

A list of all image engine or script variables is listed under [Section D.7, “Variables and Parameters,”](#) on page 452.

- ♦ **Other variables:** Environment variables that you might want in your script can be added in the same manner as described for the ZENworks variables.

## D.4 Modifying ZENworks Imaging Resource Files

From time to time you might want to modify an imaging distribution by adding your own files. These can be additional programs, scripts, data files, or updated Linux drivers.

You can use the following methods to update imaging resource files:

- ♦ The easiest method is to edit the `settings.txt` file, which is located on the root of the imaging CD or in `/srv/tftp/boot` on the ZENworks imaging server for PXE booting.
- ♦ Where you are using a ZENworks partition, you can boot to the manual or maintenance mode, mount the ZENworks partition, then copy the modified `settings.txt` and the files in `initrd` or `root` to the mounted ZENworks partition.
- ♦ Another easy method is to edit the `.cfg` files located in `/srv/tftp` on the ZENworks imaging server for PXE booting.
- ♦ You can modify files in the `initrd` or `root` file systems, but you need a Linux environment for performing the modification process. Files required during the initial setup (during linuxrc processing time), such as LAN drivers, must be placed in the `initrd` file system. Other files that are not needed until the `zenworks.s` script file takes control can be placed in the `root` file system (for example, an imaging script), or you can use the `driverupdate` file.

This method is discussed in this section.

The following sections provide various methods for modifying imaging resource files:

- ♦ [Section D.4.1, “Adding Files to an Imaging Boot CD,” on page 445](#)
- ♦ [Section D.4.2, “Adding Files to the Initrd or Root File Systems,” on page 446](#)
- ♦ [Section D.4.3, “Using the Driverupdate File Method,” on page 447](#)

## D.4.1 Adding Files to an Imaging Boot CD

If you have files to add to an imaging boot CD so they can be available for use when you get to the actual imaging process (such as scripts, but normally not driver modules), you can copy the files to the `/addfiles` directory on the imaging CD. This is an easy way to insert your script or other files into the distribution without **modifying the `initrd` or `root` file systems**. However, these files are not available during the boot and module loading phases.

The imaging boot CD has a directory named `/addfiles` where you can add files. They should be placed below this directory in their proper directory names. They are then available in this directory structure during the imaging process.

An example of how you can add files:

- 1 If you want to execute your own script instead of the normal imaging process, create a script file named `myscript.s` and place it on the boot CD. For example, `/addfiles/bin/myscript.s`.

---

**IMPORTANT:** The script file must have proper LF line terminators that Linux requires, not the DOS CR and LF end-of-line characters. In other words, you cannot use `Notepad.exe` to create the script; you must use a text editor compatible with Linux or UNIX, such as `TextPad`.

---

- 2 To place the following line in the `settings.txt` file, enter:

```
export IMGCMD=/bin/myscript.s
```

When imaging is run, it runs `/bin/myscript.s` instead of using the normal `img auto` command.

## D.4.2 Adding Files to the Initrd or Root File Systems

This is the preferred method for updating imaging resource files, and must be performed in a Linux environment.

Before performing the procedure given below, make sure you have created backup copies of any files you plan to change, specifically the `/srv/tftp/boot/initrd` file. If you want to change the files on an imaging CD, you need an ISO editor or some other process for extracting and replacing the file in the `bootcd.iso` image file.

---

**IMPORTANT:** When updating or adding files and Linux drivers in the `initrd` or `root` file systems, document the changes you make. When you receive updated resource files from Novell, they do not contain your customized changes. If the kernel version has changed with the newer resource files from Novell, previously added drivers must be updated either by obtaining a new version from the manufacturer or recompiling the driver using the correct Linux kernel version source.

---

You can use the following procedure for the `root` file system by simply replacing “`initrd`” with “`root`” in the steps. However, Linux drivers should always be placed in the `initrd` file system, not the `root` file system.

To add files to the `root` file system, you can also use the `driverupdate` file method described in [Section D.4.3, “Using the Driverupdate File Method,” on page 447](#).

To modify the `initrd` or `root` file system:

- 1 Using a Linux machine, create a working directory and change to that directory.
- 2 To copy `initrd` from the PXE server or the boot CD to the new working directory:
  - ♦ For PXE, copy `\tftp\boot\initrd` to the Linux workstation’s working directory.
  - ♦ For the CD, extract `initrd` from the `\boot\loader` directory on the boot CD, then copy the extracted `initrd` to the Linux workstation’s working directory.
- 3 To rename `initrd` to `initrd.gz`, enter:

```
mv initrd initrd.gz
```
- 4 To unzip the `initrd.gz` file, enter:

```
gunzip initrd.gz
```
- 5 To create another working directory for use as a mount point in the subsequent steps, enter:

```
mkdir work
```
- 6 To mount the `initrd` file system to the `/work` directory, enter:

```
mount -o loop initrd work
```
- 7 To copy your files or updated driver to the mounted `initrd` file system, enter:

```
cp /your_path/module.ko work/lib/modules/2.6.5-override-default/initrd
```

where `your_path` is the path to the `module.ko` file and `module` is the name of the module.  
Other files to be included in the `initrd` file system should be copied to the appropriate directory.
- 8 To unmount the `initrd` file system, enter:

```
umount work
```
- 9 To zip the new `initrd` file, enter:

```
gzip -v9c initrd > initrd.gz
```

**10** To rename `initrd.gz` back to `initrd`, enter:

```
mv initrd.gz initrd
```

**11** To copy the file back:

- ♦ For PXE, copy the updated `initrd` file to the `\tftp\boot` directory on the PXE server.
- ♦ For the CD, copy the updated `initrd` file to the `\boot\loader` directory on the boot CD.

## D.4.3 Using the Driverupdate File Method

Another way to customize the imaging distribution is to utilize the driver update mechanism that is built into all SUSE distributions. This entails modifying a file named `driverupdate` that is located in the `/srv/tftp/boot` directory on your imaging server or on the root (`/`) of an imaging boot CD.

This method is a little less intrusive than modifying the `initrd` or `root` file systems. You simply create an additional file that is incorporated into the imaging operating system during boot time.

There are three types of driver update operations that can be performed:

- ♦ Install the kernel modules or hardware drivers
- ♦ Install files and execute a script
- ♦ Simply place files into the operating system

This section describes the second method. For more information on the other methods, see “[Tech Talk #3 - Spittin’ Image](http://www.novell.com/connectionmagazine/2005/11/tech_talk_3.html)” ([http://www.novell.com/connectionmagazine/2005/11/tech\\_talk\\_3.html](http://www.novell.com/connectionmagazine/2005/11/tech_talk_3.html)) in the *Novell Connection Magazine*.

The example in this section takes the program “tree” that is not currently available in the imaging distribution and installs it at boot time.

The driver update mechanism seeks the `driverupdate` file, which contains a directory structure that mimics the directory structure in the operating system after a device has booted with the ZENworks distribution. If it is present, `linuxrc` downloads it during booting and incorporates it into the operating system dynamically.

The `driverupdate` file is a file system file that can be of any file system type, such as EXT3 or REISER. For simplicity, we’ll use the CRAMFS file system in our example.

To place the tree program into the `driverupdate` file:

- 1** Create a working directory on your imaging server, such as `/work`.
- 2** (Conditional) If you are using the `driverupdate` file, download the `driverupdate.tgz` file into the `/work` directory, then untar it by entering:

```
mkdir work
cd work
wget http://www.novell.com/connectionmagazine/2005/11/download/
driverupdate.tgz
tar -xzvf driverupdate.tgz
```

The `driverupdate.tgz` file contains the same directory structure as is created in [Step 3](#).

- 3** (Conditional) If you are manually creating the directories, create the following directory structure under the /work directory:

```
-- dirstruct
  -- linux
    -- suse
      -- i386-9.2
        -- dud.config
        -- inst-sys
          -- lib
          -- bin
        -- adddir.s
```

The contents of the `dud.config` file should contain lines similar to those listed below. You should maintain the keywords by supplying your own data. However, you can use the listed values:

```
UpdateName:      ZENworks 7 Patch 1
UpdateID:         a37f92556e4dd99e
UpdatePriority: 100
```

The `adddir.s` file should be an executable script that contains the following lines:

```
echo "Processing: adddir.s" > /dev/tty3 2>&1
# driver update: add files to inst-sys
for i in /update/[0-9]*/inst-sys ; do
    [ -d "$i" ] && adddir "$i" /
done
# driver update: run update.pre scripts
for i in /update/[0?9]*/install/update.pre ; do
    echo "Processing: $i" > /dev/tty3 2>&1
    [ -x "$i" ] && "$i"
done
```

- 4** To copy the tree program into the /bin directory, enter:

```
cp /usr/bin/tree dirstruct/linux/suse/i386-9.2/inst-sys/bin/
```

- 5** To create the CRAMFS file, enter:

```
mkfs.cramfs dirstruct/ driverupdate
```

- 6** To copy the driverupdate file into /srv/tftp/boot, enter:

```
cp driverupdate /srv/tftp/boot
```

- 7** Add the following lines to the end of the /srv/tftp/boot/settings.txt file:

```
# SUSE driver update
for i in /update/[0?9]*/install/adddir.s ; do
    [ -x "$i" ] && "$i"
    rm $i
done
```

This causes the `adddir.s` script to run, which creates soft links to all of the new files being copied.

These lines might already be present in the `settings.txt` file.

- 8** Reboot the PXE-enabled device.

You should see the text “ZENworks 7 Patch 1” at the bash prompt after the operating system has booted.

- 9** Execute the tree program.



All of the files you put into the `driverupdate` file are now located under the `/update` directory in the operating system after booting. Then, the `adddir.s` script (or the code that you added to the `settings.txt` file in [Step 7](#)) creates soft links under the `root` file system that point to the corresponding files under the `/update` directory structure. You can verify this by running:

```
/# which tree
/bin/tree
/# ll /bin/tree
lrwxrwxrwx 1 root root 29 Aug 31 21:45 /bin/tree -> /update/000/inst-
sys/bin/tree
```

If you want to simply include a new hardware driver or kernel module in the imaging operating system, an easier process might be to copy the `.ko` file into the `/dirstruct/linux/suse/i386-9.2/modules/` directory. Then, the imaging operating system automatically loads any `.ko` files that are in this directory.

## D.5 Adding or Updating LAN Drivers

As LAN card manufacturers develop and release new LAN adapters, they usually release new or updated drivers as well. Sometimes the new LAN card functions properly with an earlier driver, and sometimes the earlier driver does not recognize the new LAN card and refuses to load. Occasionally, the older driver does load, but the LAN card exhibits serious performance problems. To obtain the full performance capabilities of a new LAN card, you should use the new driver.

The following sections explain how to obtain or compile drivers:

- ♦ [Section D.5.1, “Obtaining Drivers,” on page 449](#)
- ♦ [Section D.5.2, “Building Drivers,” on page 449](#)

If you need to load your drivers with specific parameters, see [Section D.5.3, “Loading Drivers with Parameters,” on page 451](#).

### D.5.1 Obtaining Drivers

New LAN drivers should be obtained from the manufacturer. Most LAN card manufacturers have drivers available for free downloading from their Web site. Some drivers are available from [www.scyld.com/network](http://www.scyld.com/network), and the source to the Broadcom BCM5700 driver can be downloaded from <http://www.broadcom.com/drivers/downloaddrivers.php>.

If a manufacturer has a binary driver compiled specifically for the kernel version used by ZENworks, you can obtain the driver and use one of the update methods to add the driver. ZENworks 7 is based on SLES 9 SP2, kernel version 2.6.5-7.191. If the driver is not for this specific version, you must obtain the source and compile it for this version. For more information, see [Section D.5.2, “Building Drivers,” on page 449](#).

### D.5.2 Building Drivers

Nearly all Linux drivers are distributed in source code form and need to be compiled before they can be used. Follow the manufacturer’s instructions included with the new driver to build the driver module. Many drivers can be built in such a way that they are built into the kernel itself; however, we recommend that LAN drivers be built as external kernel modules.

When building your LAN drivers, make sure that your build machine uses the same kernel as the imaging environment. If you have a LAN driver that doesn't load in your imaging environment, it usually means that you have a mismatch between your build environment and the imaging environment.

You can find the current kernel version of your Linux environment using the following command:

```
uname -r
```

However, you might need to modify the results from the `uname` command to get your kernel versions to match. For more information, see [Section D.6, "Using Uname," on page 451](#).

To build your drivers:

- ♦ ["Obtaining the Linux Source Code Tree" on page 450](#)
- ♦ ["Compiling the Module" on page 450](#)

## Obtaining the Linux Source Code Tree

To compile a module, you need the Linux source code tree that contains the configuration matching the ZENworks kernel. To obtain the necessary source code, download the [zenimgk2657244.tgz](http://download.novell.com/zenimgk2657244.tgz) Linux source code tree file (<http://download.novell.com/Download?buildid=LGijevX8zdA>).

To use the Linux source code tree:

- 1 Unzip the file and install the source code tree in the `/usr/src` directory.

For example, the tar file creates the following directories:

```
/usr/src/linux-2.6.5-7.244
/usr/src/linux-2.6.5-7.244-obj
```

- 2 Obtain the proper configuration file from one of the following locations:
  - ♦ A running ZENworks imaging distribution file (`/proc/config.gz`).
  - ♦ [zenimgk2657244.tgz](http://download.novell.com/zenimgk2657244.tgz) (<http://download.novell.com/Download?buildid=LGijevX8zdA>)

- 3 Copy this configuration file to the directory created in [Step 1](#).

For example, `/usr/src/linux-2.6.5-7.244`.

- 4 To create a link to the source tree:

- 4a To change to the `/usr/src` directory, enter:

```
cd /usr/src
```

- 4b If there is a Linux soft link in the directory, delete it.

- 4c Create the Linux soft link, such as:

```
ln -s linux-2.6.5-7.244 linux
```

You now have the Linux kernel source tree and soft link ready for compiling the module. Continue with ["Compiling the Module" on page 450](#).

## Compiling the Module

To manually compile the module:

- 1 Install the source.

Follow the supplied instructions from the manufacturer to install the source.

Normally, the module source is in a directory under `/usr/src`. Module source files usually come in the form of a gzipped tar file (`.tar.gz` or `.tgz`). The file might also be a bzipped file (`.bz2`).

**2** To compile the source:

**2a** Change directories to the source.

**2b** If you **modified** `uname` to change to the proper kernel version, issue a `make` command.

**3** When you have your module compiled for ZENworks, take the generated `.ko` module file (make sure you select the proper module name and not a work `.ko` file) and install it by using the **driver update method** or **placing it in the `initrd` file system**.

## D.5.3 Loading Drivers with Parameters

If there is a module that you want to load during the `linuxrc` processing time, and if `linuxrc` does not recognize that it needs to be loaded or you want to specify the load parameters, you can enter a line in the `linuxrc.config` or `/info` file. This file then needs to be updated in the `initrd` file system.

You might need to load a LAN driver module with specific parameters. You can do this with a line like:

```
insmod="moduleName parm=xxx"
```

This type of line is most commonly used to load a LAN driver with specific parameters, such as full duplex or specific speed.

## D.6 Using Uname

The `uname` command enables you to find the current kernel version of your Linux environment. However, you might need to modify the results from the `uname` command to get your kernel versions to match.

The following steps modify the `uname` command to provide the value you need:

**1** To obtain your current kernel version, enter:

```
uname -r
```

Write down the version number so you can use it in **Step 4**. This example uses version 2.6.13-15-smp from a SLES 9 SP2 installation.

**2** To create a new directory, enter:

```
mkdir /bin/orig
```

**3** To move the `uname` binary to the `/bin/orig` directory that you just created, enter:

```
mv /bin/uname /bin/orig/uname
```

**4** Use a Linux editor (such as `vi`) to create the `/bin/uname` file that contains the following lines:

```
#!/bin/sh
#uname
if [ $KRNVERSION"a" = "a" ] ; then
    if [ $(/bin/orig/uname -r) = "2.6.13-15-smp" ] ; then
        export KRNVERSION=2.6.13-15-smp
```

```

else
    export KRNLVERSION=2.4.31
fi
fi
if [ $1"a" = "-ra" ] ; then
    echo $KRNLVERSION
else
    /bin/orig/uname $*
fi

```

---

**IMPORTANT:** Replace the strings “2.6.13-15-smp” with the version you found in Step 1.

---

- 5** To make the new `uname` command script executable, enter:

```
chmod +x /bin/uname
```

- 6** Enter the following to cause the `uname -r` command to return a specific version, such as when compiling a module:

```
export KRNLVERSION="2.6.5-7.191"
```

- 7** Following the manufacturer’s directions, compile the module using the appropriate `make` command.

- 8** Reset `uname` so that it returns actual values:

```
unset KRNLVERSION
```

## D.7 Variables and Parameters

The following sections describe the variables and parameters used in updating resource files:

- ♦ [Section D.7.1, “Imaging Script Variables,” on page 452](#)
- ♦ [Section D.7.2, “Linuxrc Parameters Specified in Settings.txt,” on page 453](#)
- ♦ [Section D.7.3, “Image Engine Variables,” on page 453](#)

### D.7.1 Imaging Script Variables

The following environment variables are used in imaging scripts and must not be modified:

**Table D-1** *Imaging Script Variables*

Variable	Definition
ACTIVEPARTITION	Device of the active OS partition.
CDBOOT	YES = Booted from a CD.
DISABLEZEN	1 = Disable the ZENworks partition.
ENABLEZEN	1 = Re-enable the ZENworks partition.
ZENDEVICE	Device name of the ZENworks partition.
ZENPARTBOOT	YES = Booted from ZENworks partition.

The following environment variables can be modified or set in the `settings.txt` file:

**Table D-2** *Environment Variables*

Variable	Definition
HDPARM	NO = Do not set hdparm parameters.
IMGCMD	Imaging command to run instead of the <code>img a</code> command.
MANUALREBOOT	YES = Do not automatically reboot.
PARTITIONSIZE	Size in MB to create the ZENworks partition.
PROXYADDR	IP/DNS address of the Imaging server.
PROMPT	Go to the bash prompt after imaging is complete.

## D.7.2 Linuxrc Parameters Specified in Settings.txt

**Table D-3** *Linuxrc Parameters*

Variable	Definition
netsetup	dhcp = Use DHCP. 1 = Static IP.
HostIP	Static IP address to use.
NetMask	Network mask.
Gateway	Network gateway.
HostName	Host name to assign.
Nameserver	DNS name server.
Domain	Domain suffix.
NetDevice	ethx = Define which network device to configure.

## D.7.3 Image Engine Variables

**Table D-4** *Image Engine Variables*

Variable	Definition
DEVELOPER_LOG	"A" creates a verbose <code>imglog</code> debug file.
ZENIMGLOG	"A" creates a less verbose <code>imglog</code> debug file.
ZEN_IGNORE_GEO_MISMATCH	Ignore geometry device mismatches when restoring raw image formats.
NOABORTBUTTON	If defined, do not display the Abort button during imaging.

## D.8 Troubleshooting Linux Driver Problems

- ♦ [Section D.8.1, “Troubleshooting During the Boot Process,” on page 454](#)
- ♦ [Section D.8.2, “Troubleshooting at the Bash Prompt,” on page 454](#)

### D.8.1 Troubleshooting During the Boot Process

While booting ZENworks imaging, there are several things that you can do to help troubleshoot if there is a problem:

- ♦ Press Esc to see the kernel messages. Usually, messages are shown for failures.
- ♦ Screen 3 (press Alt+F3) is used to show the progress of the linuxrc process. It lists progress results, what linuxrc is doing, which modules are loaded, and so on.
- ♦ Screen 4 (press Alt+F4) is used to show output from the modules during the linuxrc process.
- ♦ Screens 1 (press Alt+F1), 3, and 4 can be used to help determine which part of the process is failing or causing a problem.
- ♦ Screens 3 and 4 indicate which drivers are loaded.
- ♦ If a drive is loaded properly but fails in some way, view screen 4 to see if there is an outdated driver.

If the boot process fails, the first command line parameter to use is `acpi=off`.

### D.8.2 Troubleshooting at the Bash Prompt

When the bash prompt is displayed, there are a few tools that you can use to gather information about the hardware:

- ♦ **hwinfo:** This utility is used by linuxrc to load hardware. You can use `hwinfo -pci` to determine exactly what hardware was recognized.

Pipe to “less,” because `hwinfo` can create a lot of output. For example, `hwinfo -pci | less`.

If you need to contact Novell Support for help, you should capture the output from `hwinfo -pci` to a file for their use. You can gather the most information with this command:

```
hwinfo -pci -log /logfile
```

where *logfile* is the name of the file that you should send.

You can then mount a device, such as a Thumb drive or other USB device, and save the output file for later use. You might also be able to use FTP to save the file where it can be available.

- ♦ **ethtool:** This is a valuable tool (contained in a ZENworks distribution) that can be used to change the configuration on most Ethernet network devices.

# Supported Ethernet Cards



Novell® ZENworks® Linux Management provides the Ethernet card drivers contained in the Linux kernel (2.6) that ships with ZENworks 7.

To determine which Linux kernel you are using, enter `uname -r` at the bash prompt.

If your device or laptop computer uses a different card that is not supported, you must supply your own Ethernet driver.





# Establishing SSH Tunneling

# F

If you are using Remote Management over a network that is not secure, the data between the Remote Management Viewer running on the management console and the Remote Management Agent on the managed device is unencrypted and could be viewed by someone with access to the intervening network. You should tunnel your Remote Management sessions through a secure channel such as SSH.

- ♦ Section F.1, “SSH Tunneling between a Linux Management Console and a Linux Managed Device,” on page 457
- ♦ Section F.2, “SSH Tunneling between a Windows Management Console and a Linux Managed Device,” on page 458
- ♦ Section F.3, “Compression,” on page 459

## F.1 SSH Tunneling between a Linux Management Console and a Linux Managed Device

If you are using Linux, SSH clients and servers are freely available on the internet. The SSH client and server RPMs can be downloaded from the [OpenSSH site](http://www.openssh.com). (<http://www.openssh.com>).

### F.1.1 Basic Use

SSH provides you with a “Secure SHell” to the remote device. All traffic is encrypted between the two devices using public key encryption techniques, making it really very difficult for anyone else to spy on it. When SSH is installed, you could connect to a managed device from elsewhere simply by running the SSH client. For example, if you want to connect to a managed device called “work.” you use the following command:

```
ssh work
```

You are then prompted for the password of your account on the managed device and you are logged in, just like a telnet session, but safer. You can also request that it listens on a particular port on your local management console and forwards that down the secure connection to a port on a managed device at the other end. To do this, use the following command:

```
ssh -L x:work:y work
```

This starts an SSH connection to a device named “work” and also listen on port x on the local management console, and forwards any connections there to port y on “work.”

Remote Management uses two ports on the managed device. By default, the Remote Control service listens on port 5950 and the Remote Login service listens on port 5951. If you want to enable SSH tunneling for Remote Control, you need to forward Remote Management data from a port on your local management console to 5950 of managed device.

Similarly, you should forward data to 5951 if you want to tunnel Remote Login:

- ♦ If you are running Remote Control service on “work” on 5950 and you want a secure connection to it from your local management console, you can start the SSH session using:

```
ssh -L 5952:work:5950 work
```

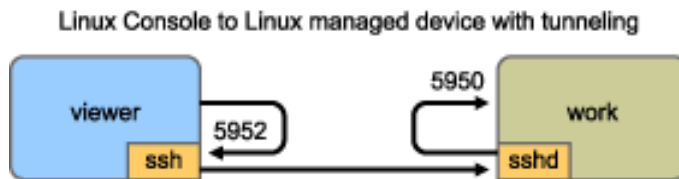
- ♦ Any connections to port 5952 on your local management console would actually connect to 5950 on “work,” so instead of running a vnc viewer as:

```
vncviewer work:50
```

run it as follows:

```
vncviewer localhost:52
```

**Figure F-1** Linux Console to Linux Managed Device with Tunneling



---

**NOTE:** If you are using the Linux VNC viewer to connect via SSH, by default when the viewer connects to a server on the local management console, by default it uses VNC's pixel encoding because this generally gives better performance for local access. If this server is actually an SSHD redirecting the data for another workstation, you can override this using the `-tight` option to the viewer or you can send a lot more data over the network.

---

## F.2 SSH Tunneling between a Windows Management Console and a Linux Managed Device

SSH clients are also available for Windows, Macintosh, and other platforms, but if you want servers on these platforms you may need to use a commercial version or route your connection via a Linux machine.

There are several scenarios for using SSH tunneling between a Windows management console and a Linux managed device. For the sake of simplicity, the following procedure uses a scenario in which you are using a Windows laptop "viewer" in a non-secure Wide Area Network to remotely control your Linux managed device "work" installed inside your secure Local Area Network. Another Linux Machine called "gateway" is in your secure local area network and runs the SSH daemon. The following steps explain how you can use the PuTTY SSH client to configure an SSH tunnel so that the Remote Management data is encrypted when it travels between "viewer" and "gateway" and is then forwarded to "work" inside the secure network.

---

**NOTE:** The PuTTY SSH client is available at the [PuTTY site \(http://www.chiark.greenend.org.uk/~sgtatham/putty\)](http://www.chiark.greenend.org.uk/~sgtatham/putty), if you are using other SSH client software, use the appropriate commands for that software.

---

- 1 Enter the following command in the shell prompt:

```
putty -L 5952:work:5950 gateway
```

The first argument is the local forwarding option, which says that the local fake port 5952 should be created and connected to the genuine port work:5950. The second argument is the

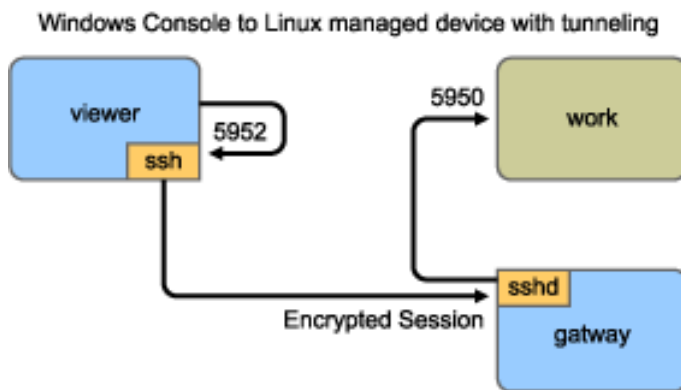
main non-option parameter to SSH, which tells it to connect to the machine that runs the SSH daemon.

- 2 In the PuTTY Security Alert dialog box, verify that the key matches with that of the “gateway” device, then click *Yes*.
- 3 To establish the SSH tunnel between “viewer” and “gateway,” you need to require authentication to “gateway.” Specify a valid username and password of the “gateway” device in the PuTTY dialog box, then click *Yes*.
- 4 Any connections to port 5952 on your local management console would actually connect to 5950 on “work,” so instead of running a vnc viewer as

```
vncviewer work:50
```

run it as follows

```
vncviewer localhost:52
```



---

**NOTE:** If you are using the Linux VNC viewer to connect via SSH, by default when the viewer connects to a server on the local management console, by default it uses VNC's pixel encoding because this generally gives better performance for local access. If this server is actually an SSHD redirecting the data for another workstation, you can override this using the `-tight` option to the viewer or you can send more data over the network.

---

## F.3 Compression

SSH can also compress the data. This is particularly useful if the link between your management console and the managed device is a slow one, such as a modem, but even on a faster network it can be helpful, because encryption takes a certain amount of time and so can slow the link down a little. To add simple compression, use the `-C` option. For more control, set it up in your SSH configuration files. To see how much your data is being compressed, use the `-v` option.



# Limited Support for SLES10 and SLED10 Managed Devices



ZENworks® Linux Management offers limited support for SUSE® Linux Enterprise Server 10 (SLES10) and SUSE Linux Enterprise Desktop (SLED10) managed devices.

Using ZENworks Linux Management, you can use the `zlmirror` utility to mirror updates to your ZENworks Linux server and then use catalogs to distribute the updates to your SLES10 and SLED10 managed devices. At this time, you cannot use ZENworks Linux Management to apply policies, distribute bundles, apply images, inventory managed devices, remotely control devices, and so forth. These capabilities will be added in an upcoming release.

For detailed information and step-by-step information about obtaining and distributing updates to SLES10 and SLED10 managed devices, see the following Technical Information Documents (TIDs):

- ♦ TID 3480922 in the [Novell Support Knowledgebase \(http://www.novell.com/support/supportcentral/supportcentral.do?id=m1\)](http://www.novell.com/support/supportcentral/supportcentral.do?id=m1).
- ♦ TID 3860200 in the [Novell Support Knowledgebase \(http://www.novell.com/support/supportcentral/supportcentral.do?id=m1\)](http://www.novell.com/support/supportcentral/supportcentral.do?id=m1).

---

**NOTE:** Ensure that you select the Search by TID ID box before clicking Search.

---

For more information about using the `zlmirror` utility, see [Chapter 19, “Mirroring Software,” on page 199](#). For more information about using catalogs, see [Chapter 17, “Using Catalogs,” on page 187](#).



# License Agreement for libacl and libgconf



The following is the licence agreement for the libacl and libgconf library that is used in the ZENworks 7 Linux Management Policy Handler/Enforcer software:

## H.1 Library GNU Public License

This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

- ♦ You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

- ♦ You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
  - ♦ The modified work must itself be a software library.
  - ♦ You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

- ♦ You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
- ♦ If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

- ♦ You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

- ♦ You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

- ♦ A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.



However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

- ♦ As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

- ♦ Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)
- ♦ Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.
- ♦ Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.
- ♦ If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.
- ♦ Verify that the user has already received a copy of these materials or that you have already sent this user a copy.
- ♦ For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a

special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

- ♦ It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.
- ♦ You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:
  - ♦ Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.
  - ♦ Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.
- ♦ You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
- ♦ You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.
- ♦ Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.
- ♦ If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting

the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

- ♦ If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
- ♦ The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

- ♦ If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.
- ♦ NO WARRANTY
- ♦ BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
- ♦ IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.



# Documentation Updates

This section contains information on documentation content changes that have been made in the *Administration Guide* after the initial release of Novell® ZENworks® 7 Linux Management. The information will help you to keep current on updates to the documentation.

All changes that are noted in this section were 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 were published. Within a dated section, the changes are alphabetically listed by the names of the main table of contents sections for ZENworks 7 Linux Management.

If you need to know whether a copy of the PDF documentation you are using is the most recent, the PDF document contains the date it was published on the front title page or in the Legal Notices section immediately following the title page.

The documentation was updated on the following dates:

- ♦ Section I.1, “March 23, 2007,” on page 469
- ♦ Section I.2, “January 2, 2007,” on page 470
- ♦ Section I.3, “September 29, 2006,” on page 470
- ♦ Section I.4, “August 18, 2006,” on page 470
- ♦ Section I.5, “July 18, 2006,” on page 471
- ♦ Section I.6, “June 29, 2006,” on page 471
- ♦ Section I.7, “Interim Release 1,” on page 472
- ♦ Section I.8, “December 23, 2005,” on page 473
- ♦ Section I.9, “December 9, 2005,” on page 473

## I.1 March 23, 2007

Updates were made to the following sections:

Location	Change
“Uninstalling a Secondary ZENworks Server Using zlm-config” on page 26	Added entire section.
Section B.7.2, “Viewing Information About Imaging Requests,” on page 423	Updated this section with the Linux command line entry for viewing the server’s status.

Location	Change
"Obtaining the Linux Source Code Tree" on page 450	Updated the URL to the Linux source code tree file.

## I.2 January 2, 2007

Updates were made to the following sections:

Location	Change
Section 29.5, "Establishing SSH Tunneling," on page 363	Updated a cross reference to information about establishing VNC through an SSH tunnel between the console and a managed device.

## I.3 September 29, 2006

Updates were made to the following sections:

Location	Change
Appendix G, "Limited Support for SLES10 and SLED10 Managed Devices," on page 461	Added entire appendix.

## I.4 August 18, 2006

Updates were made to the following sections:

Location	Change
Section 16.11.1, "Bundle Version Deployment Behavior (ZENworks Control Center vs. the zlman Utility)," on page 181	Added entire section to explain the differences between modifying bundles using the ZENworks Control Center and the <code>zlman</code> utility with regards to the new version being deployed.
Section 23.2.2, "Preparing Imaging Boot CDs or DVDs," on page 240	Updated this section by splitting it into two subsections to cover the issues for creating boot CDs/DVDs with or without other files than the imaging boot ISO provided with ZENworks.

Location	Change
Section D.4.2, "Adding Files to the Initrd or Root File Systems," on page 446	Replaced the <code>cp</code> command with <code>mv</code> in <a href="#">Step 3</a> and <a href="#">Step 10</a> because the files should be renamed, not copied.
"Obtaining the Linux Source Code Tree" on page 450	Updated the method for obtaining the necessary source code and <code>config.gz</code> file to a URL where the <code>.tgz</code> file can be downloaded.

## I.5 July 18, 2006

Updates were made to the following sections:

Location	Change
"About This Guide" on page 15	Updated information about ZENworks 7 Linux Management Interim Release 1 (IR1).
"Configuring a WAN/VLAN with Preboot Services and DHCP Running on the Same Server" on page 253	Updated this section with the additional requirement to edit the <code>novell-proxydhcp.conf</code> file.
"Downloading and Installing the iAMT Redirection Drivers" on page 276	Added this section, which explains how to download and install the device drivers for Intel Active Management Technology (AMT) that are needed for provisioning AMT devices.

## I.6 June 29, 2006

Updates were made to the following sections:

Location	Change
Section 19.4, "Deploying Red Hat Network Updates," on page 204	Replaced the text in this section with newer information.

## I.7 Interim Release 1

Updates were made to the following sections:

Location	Change
Technical Information Document (TID) 9183.	A master Technical Information Document (TID) contains download and installation instructions and a list of the updates to Novell ZENworks 7 Linux Management since its initial release. For more information, see TID 3009183 in the <a href="http://www.novell.com/support/supportcentral/supportcentral.do?id=m1">Novell Support site (http://www.novell.com/support/supportcentral/supportcentral.do?id=m1)</a> . Ensure that you click the <i>Search by TID ID</i> check box before performing the search.
"rug" on page 21	Lock rules are now enforced on all transactions, including <code>rug in</code> , <code>rug rm</code> , and all bundle operations, including directly assigned bundles. For more information, see the <a href="http://www.novell.com/documentation/zenworks7/reference/rug.html">HTML version of the rug manpage (http://www.novell.com/documentation/zenworks7/reference/rug.html)</a> .
Section 4.2, "ZENworks Agent (zmd) Cache Settings," on page 29	Added entire section. As the ZENworks Agent (zmd) performs its duties, it maintains a cache that stores the content of bundles that are downloaded for installation on that managed device.
Section 16.12, "Using a Remote Execute Policy to Remove Bundles and Packages from Devices," on page 181	Added information to the table after <a href="#">Step 9 on page 182</a> explaining the <code>rug rm bundle --allow-removals</code> flag. This flag has also been added the HTML version of the rug manpage.
Chapter 19, "Mirroring Software," on page 199	<p>Added the following paragraph to the <a href="#">Chapter 19, "Mirroring Software," on page 199</a> section giving information about new mirroring functionality added to the product since its original release:</p> <p>ZENworks 7 Linux Management automatically looks for SUSE Linux Enterprise Server (SLES) Service Packs and creates Bundle Groups to contain them. Because of this new functionality, you can now mirror SLES Service Packs.</p>
"RemoteServer" on page 200	Added information about STATIC mirroring to the RemoteServer section.
Section 22.3.7, "Intel Active Management Technology (AMT)," on page 222	Updated this section.
Section 23.4.6, "Configuring Intel Active Management Technology (AMT)," on page 276	Added new AMT provisioning steps.
"Understanding Script Arguments" on page 422	<p>Added the following description for a new table row titled "start setjustimagedflag":</p> <p>For novell-zislnx only, it sets the Just Imaged flag so that a device can be imaged using its existing Image Safe Data.</p>



Location	Change
<a href="#">“ZENworks Database Maintenance” on page 37</a>	Added Important note referencing the <a href="#">“Disaster Recovery”</a> section in the <i>ZENworks 7 Linux Management Troubleshooting Guide</i> .

## I.8 December 23, 2005

Updates were made to the following sections:

Location	Change
<a href="#">Part V, “Preboot Services,” on page 209</a>	Made minor updates in some sections.
<a href="#">Part X, “Appendixes,” on page 395</a>	Made minor updates to the Imaging sections.

## I.9 December 9, 2005

Page design reformatted to comply with revised Novell documentation standards.

Updates were made to the following sections:

- ◆ [Section I.9.1, “Device Registration,” on page 473](#)
- ◆ [Section I.9.2, “Establishing SSH Tunneling,” on page 474](#)
- ◆ [Section I.9.3, “General Management,” on page 474](#)
- ◆ [Section I.9.4, “Packages,” on page 474](#)

### I.9.1 Device Registration

The following changes were made in this section:

Location	Change
<a href="#">Chapter 9, “Managing Registration Keys and Rules,” on page 53</a>	Combined the Managing Registration Keys and the Managing Registration Rules sections and added information at the beginning of the new section to explain the differences between registration keys and rules and the advantages of each.

## I.9.2 Establishing SSH Tunneling

The following changes were made in this section:

Location	Change
Appendix F, "Establishing SSH Tunneling," on page 457	Added new Appendix.

## I.9.3 General Management

The following changes were made in this section:

Location	Change
Section 6.2.1, "Understanding Automated Database Maintenance," on page 38	Added new section explaining daily and monthly automated maintenance tasks performed on a PostgreSQL database.

## I.9.4 Packages

The following changes were made in this section:

Location	Change
Section 19.1, "zlmmirror," on page 199	Changed the location of the zlmmirror executable from  <code>/opt/novell/zenworks/bin/zlmmirror</code>  to  <code>/opt/novell/zenworks/bin/</code>
"LocalServer" on page 201	Reworded the Base element description under LocalServer.
Chapter 19, "Mirroring Software," on page 199	Added following text:  <b>NOTE:</b> To mirror from a ZENworks 6.6.x Linux Management server to a ZENworks 7 Linux Management server, the 6.6.x server must also be a YaST Online Update (YOU) server.