

Novell Training Services

Novell® ZENworks 11.2 Configuration Management Administration Manual

Course 3118
Version 1
Volume 2

100-005300-001 Rev A

www.novell.com



Novell ZENworks 11.2 Configuration Manager Administration Manual

3118

Novell Training Services

www.novell.com

AUTHORIZED COURSEWARE

Volume 2

Novell.

Legal Notices

5/4/2012

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. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](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 © 2012 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.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the [Novell Documentation Web page \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Novell Trademarks

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

Third-Party Materials

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

Configure Content Management

Novell.

Objectives

- Describe Satellite Servers
- Perform Content Management Tasks
- Manage Location Awareness

In this section, you learn manage ZENworks content through the use of Satellites and Location Awareness.

Describe Satellite Servers

Describe Satellite Servers

- Describe Satellite Roles
- Add and Configure Satellite Servers
- Manage Satellite Servers
- Specify Content to be Hosted
- Move a Satellite from One Primary to Another

A Satellite is a managed device that can perform some of the roles that a ZENworks Primary Server normally performs, including authentication, information collection, content distribution, and imaging. A Satellite can be any managed Windows or Linux device (server or workstation), but not a Primary Server.

NOTE: For more information, see “System Requirements” in the *ZENworks 11 SP2 Installation Guide* and “Deploying the ZENworks Adaptive Agent” in the *ZENworks 11 SP2 Discovery, Deployment, and Retirement Reference*.

When you configure a Satellite, you specify which roles it performs (Authentication, Collection, Content, or Imaging). A Satellite can also perform roles that might be added by third-party products that are snap-ins to the ZENworks 11.2 framework.

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

Describe Satellite Roles

- **Authentication Role**
 - Speeds up the authentication process by spreading the workload among various devices
- **Collection Role**
 - Minimize network traffic for inventory information by enabling the Collection role
- **Content Role**
 - Improve content access without creating another Primary Server
- **Imaging Role**
 - Used to achieve load balancing for the Primary Server

A Satellite is a device that can perform some of the roles that a ZENworks Primary Server normally performs, including authentication, information collection, content distribution, and imaging.

- **Authentication Role**

When users logged in to previous versions of ZENworks, they were authenticated to the Management Zone by contacting the ZENworks Primary Server, which in turn contacted the user source that contains the users.

Satellite devices with the Authentication role can now speed the authentication process by spreading the workload among various devices and by performing authentication locally to managed devices. You can have multiple Satellite devices with the Authentication role. In addition, each Satellite with the Authentication role can have multiple user sources configured and each Satellite can have multiple connections to each user source to provide failover.

When a managed device uses a Satellite for authentication, the Satellite issues an authentication token to the managed device so that it can authenticate to the Management Zone using SSL.

On the managed device, the Authentication module is inactive until you promote the managed device to be a Satellite with the Authentication role or until the Authentication role is added to an existing Satellite.

NOTE: If a Satellite device performing the Authentication role is a member of a domain, all managed devices authenticating to that Satellite must be members of the same domain.

- **Collection Role**

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

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

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

A Satellite with the Collection role collects inventory information, messages (errors, warning, informational, and so forth), and policy and bundle statuses, then rolls that information up to its parent Primary Server, which in turn either writes to the database directly or passes the information to its parent Primary Server, which does the database writing. The role includes a roll-up schedule that you can edit.

On the managed device, the Collection module is inactive until you promote the managed device to be a Satellite with the Collection role or until the Collection role is added to an existing Satellite.

- **Content Role**

Content consists of bundles, policies, system updates (ZENworks Server and Adaptive Agent), and patches.

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

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

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

On the managed device, the Content module is inactive until you promote the managed device to be a Satellite with the Content role or until the Content role is added to an existing Satellite.

- **Imaging Role**

The Imaging role installs the Imaging services and adds the Imaging role to the device. With this role, the device can be used as an Imaging server to perform all Imaging operations, such as taking an image and applying an image within or across subnets by using unicast or multicast imaging.

The Imaging role can be used to achieve load balancing for the Primary Server, and also to support cross-subnet imaging. The Satellite uses ZENworks Control Center to communicate with the Primary Server for Imaging operations in the Auto mode.

On the managed device, the Imaging module is inactive until you promote the managed device to be a Satellite with the Imaging role or until the Imaging role is added to an existing Satellite. This activates the Imaging services on the device, and enables you to perform the Imaging operations in auto and

maintenance mode. The Imaging services installed on the device include TFTP, Preboot policy, pbserv, and proxy DHCP. All services, except for proxy DHCP, are automatically started. You can manually start or stop the proxy DHCP service from ZENworks Control Center.

Add and Configure Satellite Servers

1. Select the Primary Server to be the parent
2. Select the Device to become the Satellite server
3. Select the Satellite server roles
4. Configure replication schedules

You can create a new Satellite device or configure an existing Satellite with the Authentication, Content, Imaging, and Collection roles, change its default port, and adjust the schedules for the roles. You can also remove roles from an existing Satellite.

Before promoting a managed device as Satellite, be sure to review the following guidelines:

- The ZENworks version installed on the managed device must be same as that of the Primary Server.
- You cannot promote the following devices as a Satellite:
 - A managed device that has a previous version of ZENworks Adaptive Agent (version 10.2.x or 10.3.x) installed.
 - A ZENworks 11 test device.
- You cannot change the Satellite roles and settings for the existing 10.2.x or 10.3.x Satellites.

Select the Primary Server to be the Parent

To add a new Satellite into the Server Hierarchy panel, in ZENworks Control Center, select the **Configuration** tab. In the Server Hierarchy panel, select the check box next to the desired **Primary Server**, select **Action**, then select **Add Satellite Server**.

To configure an existing Satellite from the Server Hierarchy panel, in ZENworks Control Center, select the Configuration tab. In the Server Hierarchy panel, select the check box next to the **Satellite** that you want to configure, select Action, then select Configure Satellite Server.

You can only configure one Satellite at a time.

Select the Device to Become the Satellite Server

Select the **Search** icon, then browse to and select the *managed device* you want to designate as the Satellite server.

Select the Satellite Server Roles

Select the check box next to each role you want assigned to a Satellite server. Normally, you would assign one role to a Satellite server. You can also select the **Configure** link to configure the role.

Manage Satellite Servers

- Refresh a Satellite
 - Pending actions take place immediately
- Remove Roles from a Satellite Server
 - Roles can be added and removed from Satellites
 - One role must be configured for a Satellite to remain a Satellite
 - Removing all roles demotes Satellite to a managed device
- Remove a Satellite Server from the Server Hierarchy
 - Devices can be removed if the Satellite is no longer needed
 - Device Remains in the zone as a managed device

- **Refresh a Satellite**

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

- **Remove Roles from a Satellite**

You can choose to remove one or more roles from a Satellite. However, the Satellite must have at least one role configured for it to continue to perform the Satellite function. If you remove all the roles, the Satellite is demoted to be only managed device.

Removing a Satellite role does not remove the device from any of the non-default Closest Server rules. The device is removed from the non-default Closest Server rules only when it is no longer a Satellite.

NOTE: If your Management Zone consists of ZENworks 11 Primary Server and ZENworks Configuration Management 10.2.x/10.3.x Satellites, you cannot remove individual roles from the Satellites. You can only demote the Satellite to a managed device.

- **Remove a Satellite from the Server Hierarchy**

You can remove a Satellite from the Server Hierarchy listing when that device is no longer needed to perform Satellite functions. The Satellite can have any version of the ZENworks Adaptive Agent installed. The device's object isn't removed from ZENworks; it is just removed from the Server Hierarchy listing. The device is still a managed device in your ZENworks Management Zone. However, it will not contain the replicated content, imaging services and data, or the rolled-up collection-information.

When you remove a Satellite, the managed devices that used it must be reconfigured

to use another server for content and collection purposes.

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

Specify Content to be Hosted

- A Satellite Server with a Content Roles retrieves content from its parent Primary Server
 - Any content you want hosted on the Satellite must also be located on the parent Primary Server
- Content can manually be moved from Primary to Satellite
 - Use **zman** commands to export content from Primary
 - Use **zac** Commands to import content to Satellite
 - Content cannot be moved from Primary to Primary

Because Content role devices retrieve their content from their parent Primary Servers, any content that you want hosted on a Satellite must also be hosted on its parent Primary Server.

When you create relationships between content and content servers (ZENworks Primary Servers and Satellites) by using the Select Content to Update Wizard, these relationships adds to any existing relationships. The selected content is hosted on the content server in addition to the content already existing on the server.

Consider the content for Bundle A and Policy B is hosted on Server 1 and not on Server 2. Select Bundle A and Policy B, then use the Select Content to Update Wizard to include the content on Server 2. During the next scheduled replication, Bundle A and Policy B are added to Server 2.

Depending on the relationships created, the content is replicated to or removed from content servers during the next scheduled replication.

Manually Replicating Content from a Primary Server to Satellite Devices

You can export content from a ZENworks Primary Server's content repository and then manually import that content into a Satellite device's content repository. This process is sometimes called offline content replication.

After you export the content, you can copy it to a network drive or to a storage device and then manually import the content into the Satellite device's content repository.

You cannot manually export content from one ZENworks Primary Server and then import that content into another Primary Server.

Move a Satellite from One Primary to Another

- A Satellite Server can be moved from one Primary Server to another

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

Any content (bundles, policies, and patches) you want hosted on a Satellite with the Content role must also be hosted on its parent Primary Server. If the content is not hosted on the new Primary Server, it is added.

Perform Content Management Tasks

Perform Content Management Tasks

- Describe ZENworks Content
- Describe the Content Repository
- Replicate Content to a New Content Server
- Manually Replicate Content from a Primary Server to a Satellite Server
- Configure Content Replication at the Management Zone Level
- Copy a Bundle Group to a Content Server

Describe ZENworks Content

- ZENworks replicates and distributes content among Primary Servers, Satellite Servers, and managed devices
- Content includes
 - Bundles
 - Policies
 - Patches
 - System Updates

ZENworks replicates and distributes content among Primary Servers, Satellites, and managed devices. This includes the following content:

- **Bundles.** The files, configuration settings, installation instructions, and so forth required to deploy and manage an application or files on a device. Used in ZENworks Configuration Management and ZENworks Patch Management.
- **Policies.** The set of rules that control a range of hardware and software configuration settings on managed devices. Used in ZENworks Configuration Management.
- **Patches.** The files and instructions required to update existing software on a managed device. Used in ZENworks Patch Management.
- **System Updates.** The software updates for ZENworks system components. Used in ZENworks Configuration Management, ZENworks Asset Management, and ZENworks Patch Management.

Describe the Content Repository

- Each ZENworks server contains a Content Repository
 - Stores all Bundle and Policy content that has been replicated
 - Stores any images that have been captured and stored
- Each Server must have its own Content Repository
- Content Repository is self maintaining
 - When content is added the content is replicated based on settings
- Location of a Content Repository can be changed
 - **Example:** Move to an external drive or SAN

Each ZENworks Server contains a content repository. The content repository stores all bundle and policy content that has been replicated to the server and any images that have been captured and stored to the server.

ZENworks 11 supports any filesystem to host the content repository, although each filesystem has advantages and limitations. For example, the XFS filesystem handles very large files, which can be an advantage, depending on the nature of the content in the repository.

A single content repository cannot be shared by multiple Primary Servers. Each server must use its own content repository.

The content repository is self-maintaining. Whenever you add a bundle or policy, the bundle or policy content is added to the appropriate content repositories based upon the replication settings. Whenever you remove a bundle or policy or change which servers host its content, the bundle or policy content is also removed from the appropriate servers.

If necessary, you can move the content repository to a different location.

Replicate Content to a New Content Server

- By default all content is replicated to a new content server when it is added to the zone
- Can be changed at the following levels:
 - Zone
 - Device
 - Bundle Folder
 - Bundle
 - Policy Folder
 - Policy

When you add a bundle or policy that contains files, the files are uploaded to the content repository on the ZENworks Server. In addition, the ZENworks database is updated to reflect the addition of the bundle or policy and its content.

ZENworks Servers and Satellite devices, collectively referred to as content servers, periodically read the ZENworks database to discover new bundles and policies. Each content server that does not have the bundle or policy content retrieves it from the content server where it resides.

There are a variety of settings you can use to control how content is replicated among content servers in your zone.

Content Replication settings can be inherited from the following locations:

- **(System).** The bundle is inheriting the setting established for the Management Zone (Configuration tab > Management Zone Settings > Content > Content Replication).
- **Folder.** The bundle is inheriting the setting established for one of its parent folders.
- **Bundle.** The bundle is not inheriting the setting, but the setting is configured directly on the bundle.
- **---** The bundle is not inheriting the setting and the setting is not configured directly on the bundle. In other words, the setting is not configured at the system level, the folder level, or the bundle level.

If the settings are configured at the system or folder level, select Override settings to enable you to configure the setting at the bundle, policy, or folder level.

If you are configuring settings on a bundle folder or policy folder, you can select Force Inheritance in the Folder Task list in the left navigation pane to ensure that all children (all subfolders as well as individual bundles and policies) inherit the settings.

Content replication settings let you:

- Specify whether content is replicated to new content servers by default.
- Manually include content on or exclude content from content servers.
- Schedule how often replication occurs.
- Set a limit, or throttle, on the maximum amount of content that is replicated per second from one content server to another.
- Specify whether you want the ZENworks Agent on managed devices or Satellite devices to use checksum comparison to help ensure that no errors were introduced during content replication and that the content was not altered.

Manually Replicate Content from a Primary Server to a Satellite Server

- You can export content from a Primary Server and then import the content to a Satellite Server
 - To export, use **zman satellite-server-export-content** (ssec)
 - To import, use **zac cdp-import-content** (cic)

You can export content from a ZENworks Primary Server's content repository and then manually import that content into a Satellite device's content repository. This process is sometimes called offline content replication.

For more information about exporting content from the content repository, see the **zman satellite-server-export-content** (ssec) command under "Satellite Commands" in the *ZENworks 11 SP2 Command Line Utilities Reference*. After you export the content, you can copy it to a network drive or to a storage device and then manually import the content into the Satellite device's content repository.

For more information about importing the content into a Satellite device's content repository, see the **zac cdp-import-content** (cic) command under "Content Distribution Commands" in the *ZENworks 11 SP2 Command Line Utilities Reference*.

NOTE: You cannot manually export content from one ZENworks Primary Server and then import that content into another Primary Server.

Configure Content Replication at the Management Zone Level

- Content replication settings let you
 - Specify whether content is replicated to new content servers by default
 - Manually include content on or exclude content from content servers
 - Schedule how often replication occurs
 - Set a limit, or throttle, on the maximum amount of content that is replicated per second from one content server to another
 - Specify whether you want the Agent to use a checksum comparison

The default replication setting determines whether content is automatically replicated to new content servers. You configure the setting for each bundle, policy, or folder. If you choose to include a bundle's or policy's content on new content servers, it is replicated to all new servers; likewise, if you choose to exclude the content, it is not replicated to any new servers.

In some cases, the default replication settings might not give you the desired replication scope for your content, or the scope might change. If this occurs, you can manually include content on or exclude it from specific content servers. There are four ways to do this:

- Manage a single piece of content on multiple Content Servers
- Manage content on the Folder level
- Manage multiple pieces of content on a single Content Server
- Manage multiple pieces of content on multiple Content Servers

Content replication settings let you:

- Specify whether content is replicated to new content servers by default.
- Manually include content on or exclude content from content servers.
- Schedule how often replication occurs.
- Set a limit, or throttle, on the maximum amount of content that is replicated per second from one content server to another.
- Specify whether you want the ZENworks Agent on managed devices or Satellite devices to use checksum comparison to help ensure that no errors were introduced during content replication and that the content was not altered.

Copy a Bundle Group to a Content Server

- Default Action: bundle is copied to all content servers
 - Primary and Satellite servers
- Bundles are not copied to content servers that do not have a content role
- Bundles can be assigned to specific content servers and excluded from others manually

NOTE: By default, a bundle is copied to each content server. If you specify certain content servers as hosts, the bundle is hosted on only those content servers; it is not copied to all content servers.

Exercise 6-1

Set Up a Satellite Server and Configure ZENworks Content

In this exercise, you configure the XP-Admin workstation to function as a satellite server by doing the following:

- Configure XP-Admin as a Satellite Server
- Assign Windows Bundles to the XP-Admin Satellite Server

Manage Location Awareness

Manage Location Awareness

- Location Awareness Overview
- Closest Server Rule Changes
- Security Locations vs. Configuration Locations
- Define Locations
- Agent Throttling

Location Awareness Overview

Problem and Solution

• Pre-ZCM 11 Problem

- ZAA passed information to Primary which was then used to determine the device's closet server
- The ZAA would receive this information and cache it locally
- Physically moving the device after the closest server rule information was cached caused the user to suffer extremely long login times.
- The ZAA used the cached information that was no longer valid because the device was on a different subnet or network

• ZCM 11 Solution (Location Awareness)

- Location awareness capability of the ZESM Standalone Agent now built into the ZAA of ZCM 11
- The ZAA now determines the device's location not the Primary Server

21

© Novell, Inc. All rights reserved.

Whether a user is a mobile employee who travels frequently, a corporate office employee, or a work-from-home employee, you want to ensure that the user is connecting to the right ZENworks server, that the correct applications are available, and that the appropriate security policies are being applied to protect the device in its current network environment. ZENworks 11.2 Configuration Management allows you to create locations that are used by ZENworks Adaptive Agent to determine what should be available or enforced on a managed device.

A location can represent a specific place, such as Corporate Office Building A, or a type of place, such as Office, depending on your configuration and security needs. A location is a collection of network environments. Each network environment definition identifies a set of conditions (gateways, DNS servers, wireless access points, and so on) that, when matched by a device's current network environment, associates the device to the location.

For example, assume that you have an office in New York and an office in Tokyo. Both offices have the same security requirements. You create an Office location and associate it with two network environments: New York Office Network and Tokyo Office Network. Each of these environments is explicitly defined by a set of wireless access point MAC addresses. Whenever the device determines that its current environment matches the New York Office Network or Tokyo Office Network, it sets its location to Office and applies the configuration and security settings associated with that location.

Location Awareness Overview

How it Works

- Lets you define unique network environments and group them into locations
 - Network environments and locations can then be used in the following ways
 - To define closest servers for devices
 - To define a throttling rate between managed devices and Primary Servers (or Satellites)
 - As a system requirement for bundles or policies
 - As a Security Location specified in a Location Assignment Policy
- Ordering is used to resolve conflicts
- Evaluated by the ZESM agent on Windows which is now part of Core ZCM
 - Available on Linux but implemented natively in the Xplat agent

Network environment definitions are the building blocks for locations. You can define a network environment while you are creating a location, but we recommend that you define network environments first and then add them as you are creating locations.

Closest Server Rule Changes

- Specific locations or network environments can now be defined as having no closest servers
 - When this location is detected the device operates fully disconnected from cache
- Always make sure that there is at least one fall back
 - If you end up with only a disconnected location, you can use the **zac cc** command
 - Agent will fall back to using the server specified in the initial-webservice file
- Locations / Network Environments are zone wide

When a ZENworks Management Zone includes more than one ZENworks Primary Server or Satellite (collectively referred to as servers), devices need to know which servers to contact for collection, content, configuration, and authentication purposes. These servers are referred to as closest servers.

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

NOTE: The Closest Server Rule changes only apply if you are coming from ZCM 10 to 11 (not from ZENworks 7 to ZCM 11).

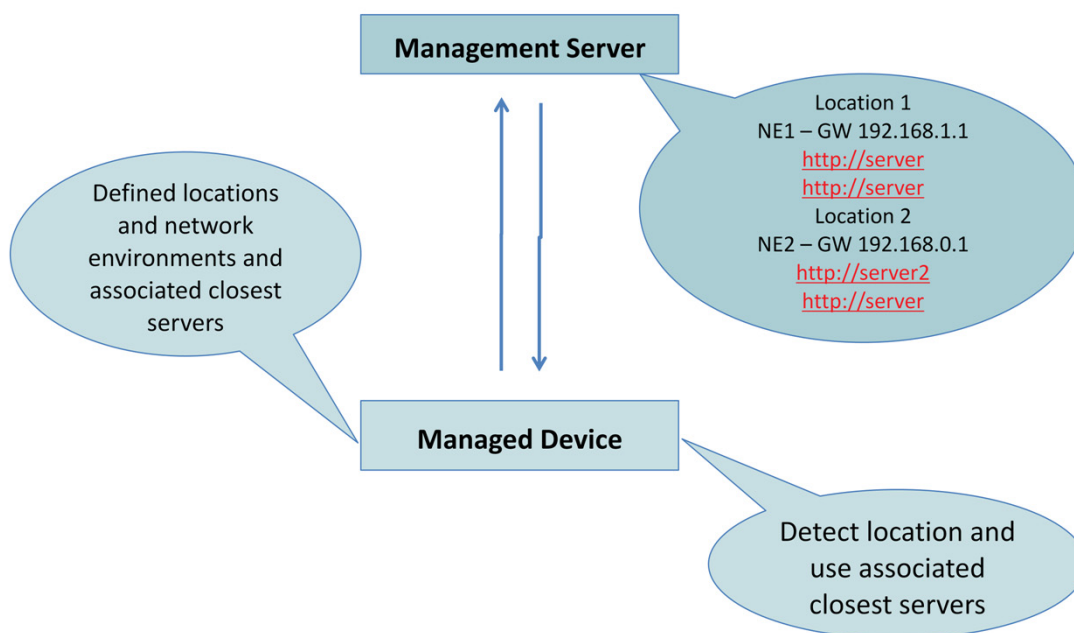
Closest Server Rule Changes

(continued)

- Configuration network environments and locations are evaluated by all clients
- Depending on customer use case we may introduce new filtering capabilities going forward
- Agent now determines closest servers using the latest cached copy of location response

Closest Server Rule Changes

(continued)



Closest servers can be configured on locations, network environments, and in the Closest Server Default Rule. The Closest servers for network environment override the Closest servers for locations.

When a managed device requests its list of closest server, the ZENworks system combines the server lists from the location and default rule (in that order) or network environment and default rule (in that order), and passes the combined list to the device. The managed device contacts the first server in the list and continues down the list until it is able to connect. All of the Closest Server rules are received by the managed device and are cached locally. If the location of a managed device changes, the settings and closest servers rules associated with the new location are applied to the device.

For example, assume that the device detects that it is in NetworkEnvironment1, which is associated with Location1. The closest authentication servers for each of these are defined as follows:

- NetworkEnvironment1: Server4, Server5
- Location: Server4, Server3
- Default Rule: Server1, Server2, Server6

For authentication purposes, a device would receive the following server list. It would attempt to connect to the first one in the list, then the second, and so on until it successfully connected.

- Server4 (network environment)
- Server5 (network environment)
- Server1 (default rule)

- Server2 (default rule)
- Server6 (default rule)

Security Locations vs. Configuration Locations

• Configuration Locations

- Used for Closest Server Default Rule
- Used for Closest Server Rules for those 10.2 or 10.3 managed devices before the ZCM 11 zone is baselined
- Used for bandwidth throttling between the ZAA and the Primary when no satellite is used

• Security Locations:

- Used by the Location Decider component of the ZAA to determine where the device is physically located
- Based on this decision the appropriate Endpoint Security Policies will be applied to the device
- Only those Administrator-defined Locations and Network Environments selected in a Location Assignment Policy are considered for the purposes of security
- All Locations and Network Environments defined in the zone are evaluated by Location Decider to determine the device's security location

A device uses its current network environment to determine both its Configuration location and its Security location.

• Configuration Locations

The Configuration location is determined from the device's current network environment and cannot be changed. You can use this location to determine closest ZENworks servers and control availability of bundles and Configuration policies. The Configuration location applies to both Windows and Linux devices.

• Security Locations

This location is used only with ZENworks 11 SP2 Endpoint Security Management. Like the Configuration location, it is automatically assigned to a device based on the network environment discovered by the device's ZENworks Adaptive Agent. You can use this location to determine availability of Security policies, Configuration policies, and Windows bundles. If you are using ZENworks Configuration Management, the Security location, like the Configuration location, can be used to control availability of bundles and policies.

However, whereas the Configuration location is determined from all defined locations (in ZENworks Control Center), the Security location is determined from a subset of those locations made available to the device through a Location Assignment policy. The security location is the location where the end point security component of the agent has determined you are. Because not all users may be allowed in all locations, the Security Location is determined by looking at a subset of all available locations configured in a Location Assignment Policy.

The intent of the Security policy is to allow ZENworks Endpoint Security Policies,

Windows Bundles, and ZENworks Configuration Policies to be enforced or made available only when the user is determined to be in allowed location. Security Location is currently calculated on Windows devices with the Endpoint Security Management agent components enabled.

Security Locations --- only available when ZESM is installed.

Define Locations

- When defining Locations there are several criteria that can be set
 - Limit to Adapter Type
 - Wired – Wireless
 - Dial Up – All
 - Matching Conditions to determine Location
 - Gateways – Adapters
 - DNS Servers – Access Points
 - DHCP Servers – Client IP Address
 - WINS Servers – Client DNS Settings
 - Dial-up Connections

- **Adapter Type**

By default, the network services you define on this page are evaluated against a device's wired, wireless, and dial-up network adapters. If you want to limit the evaluation to a specific adapter type, select **Wired**, **Wireless**, or **Dial Up**.

- **Matching Conditions**

You specify the minimum number of defined network services that must be matched in order to select this network environment.

For example, if you define one gateway address, three DNS servers, and one DHCP server, you have a total of five services. You can specify that at least three of those services must match in order to select this network environment.

When specifying a minimum match number, keep the following in mind:

- The number cannot be less than the number of services marked as Must Match.
- The number should not exceed the total number of defined services. If so, the minimum match would never be reached, resulting in the network environment never being selected.

Define Locations

Matching Conditions

- When defining multiple conditions to determine network location you can
 - Define Minimum Match
 - One Match
 - Define Multiple Matches
 - Match Required
 - Set Conditions that must be matched to determine location

Network Environment Settings

Limit to Adapter Type: All

Minimum Match: 1

Criteria Conditions

Operator	IP Address	MAC Address	Match Required
=	172.17.0.1		<input checked="" type="checkbox"/>

1 - 1 of 1

show 5 items

Agent Throttling

- Agent throttle can be set at the Location or Network Environment
- When the agent detects that location it automatically asks any Primary server it is requesting content from to throttle the response
- Can be overridden on an individual bundle basis or at a bundle folder

Throttle rate lets you specify the bandwidth throttle rate for distributing content to devices located in this network environment. To maximize performance of your ZENworks Servers and network system, high bandwidth environments can use one set of throttle rates and low bandwidth environments a different set of throttle rates.

For every location or network environment an effective throttle rate can be set. Content that is being downloaded to a particular location should be downloaded with the set throttle rate.

However, if content is being delivered to an end point from a content distribution satellite, the throttling rate set on the location or network environment is ineffective. The full bandwidth is being used for downloading the content.

The throttle rate can be overridden in a bundle so that high-priority patch and bundle content can be deployed quickly. If you do not specify a throttle rate, the network environment inherits the throttle rate assigned to the location.

Exercise 6-2

Implement Location Awareness

In this exercise, you implement Location Awareness by performing the following tasks:

- Define Location Awareness
- Test Location Awareness

Configure ZENworks Configuration Management Policies

Novell.

ZENworks 11.2 Configuration Management lets you configure and enforce settings on managed devices using Policy Management.

In this section you learn about the various policies available in the ZENworks 11.2 Configuration Management product and how to configure these policies using the ZENworks Control Center.

Objectives

- Describe Policies
- Manage Folders
- Create Windows Configuration Policies
- Manage Policies

This section covers basic policy administration concepts and tasks. For additional details on implementing policies, see the *ZENworks 11 SP2 Configuration Policies Reference*.

NOTE: Most of the Policy features available are the same as those available with Bundles.



Describe Policies

Describe Policies

- What is a Policy?
- What is a Policy Group?
- Policy Types
- Policy Features

Novell ZENworks 11.2 Configuration Management provides policies to configure operating system settings and select application settings. By applying a policy to multiple devices, you can ensure that all of the devices have the same configuration.

What is a Policy?

- Rules that control a range of hardware and software configuration settings on a managed device

A policy is a rule that controls a range of hardware and software configuration settings on the managed devices. For example, an administrator can create policies to control browser bookmarks available in the browser, printers to access, and security and system configuration settings on the managed devices.

You can use the policies to create a set of configurations that can be assigned to any number of managed devices. It helps you to provide the devices with a uniform configuration, and it eliminates the need to configure each device separately.

You can assign a policy directly to a device or a user. You can also assign the policy to a folder or group where the user or device is a member. Assigning a policy to device groups rather than device folders is the preferred way, because a device can be a member of multiple device groups, but it can be a member of only one device folder.

On managed devices, each policy type is enforced by a Policy Handler or Enforcer, which makes all the configuration changes necessary to enforce or unenforce the settings in a given policy.

What is a Policy Group?

- A collection of one or more policies
- Eases the administration efforts

A policy group is a collection of one or more policies. Creating policy groups eases the administration efforts in managing policies. You can create policy groups and assign them to managed devices the same way you would assign individual policies.

Because the policy inherits the group's assignments, managing a policy group is easier than managing individual policies. For example, if multiple policies are included in a policy group and the policy group is assigned to a device or a device group, then all the policies included in the policy group are automatically assigned to the device or device group at the same time. You need not individually assign each policy to a device or a device group.

Policy Types

Policy Category	Policy Types
Linux Configuration Management Policies	<ul style="list-style-type: none"> • External Services Policy • Puppet Policy
Windows Configuration Policies	<ul style="list-style-type: none"> • Browser Bookmarks Policy • Dynamic Local User Policy • Local File Rights Policy • Printer Policy • Power Management Policy • Remote Management Policy • Roaming Profile Policy • SNMP Policy • Windows Group Policy • ZENworks Explorer Config Policy
Windows Endpoint Security Policies	NOTE: Available only if licensed for Endpoint Security
Windows Full Disk Encryption Policies	<ul style="list-style-type: none"> • Encrypt entire disk volumes for Windows devices

ZENworks 11.2 Configuration Management lets you create the following policy types:

- **Linux Configuration Policies**

Let you configure policies supplied by ZENworks Configuration Management that are used to manage configuration settings for Linux devices. The following policies are located in this category:

- External Services policy
- Puppet policy

- **Windows Configuration Policies**

Lets you configure policies supplied by ZENworks Configuration Management that are used to manage configuration settings for Windows devices. The following policies are located in this category:

- Browser Bookmarks policy
- Dynamic Local User policy
- Local File Rights policy
- Power Management policy
- Printer policy
- Remote Management policy
- Roaming Profile policy
- SNMP policy
- Windows Group policy

- ZENworks Explorer Configuration policy
- **Windows Endpoint Security Policies**

Lets you configure policies supplied by ZENworks Endpoint Security Management that are used to manage security settings for Windows devices. The following policies are located in this category:

- Application Control policy
- Communication Hardware policy
- Data Encryption policy
- Firewall policy
- Location Assignment policy
- Security Settings policy
- Storage Device Control policy
- USB Connectivity policy
- VPN Enforcement policy
- Wireless policy

Policy Features

Category	Features
Associations	<ul style="list-style-type: none"> A policy is applied to a device/user only if the policy is directly or indirectly associated to that device/user A policy can be associated with groups and containers A policy can be associated with query groups
Hierarchy	<ul style="list-style-type: none"> Policies are chronologically ordered by default Policies have precedence configured to determine the policy that is effective for a device or a user
Other	<ul style="list-style-type: none"> Policies support management by exception Policies support system requirements Singular and Plural policies supported Policies can be disabled ZCM lets you resolve policy conflicts

- Associations**

- A policy is applied to a device or a user only if the policy is directly or indirectly associated to that device or user.

The Browser Bookmarks policy, Dynamic Local User policy, Printer policy, Remote Management policy, Windows Group policy, and ZENworks Explorer Configuration policy can be applied to a device or a user.

The Local File Rights and SNMP policies can be applied only to a device.

The Roaming Profile policy can be applied only to a user.

- A policy can be associated to groups and containers.

In ZENworks Control Center, devices and users can be organized by using containers and groups. A device or user can be a member of multiple groups. The containers can be nested within other containers. If a policy is associated to a group of users, it applies to all users in that group. If a policy is associated to a user container, it applies to all users in the entire subtree rooted at that container. The same behavior applies to device groups and containers.

- A policy can be associated to query groups.

In ZENworks Control Center, the devices can also be members of query groups. Query groups are similar to ordinary groups except that the membership is determined by a query defined by the administrator. All devices that satisfy the query become members of that device group. The query is evaluated periodically and the membership is updated with the results. An administrator can configure the periodicity of the evaluation. An administrator can also force an immediate refresh of a query group. Query groups act just like other groups where policies

are concerned.

- **Hierarchy**

- Policies are chronologically ordered by default.

When multiple policies are associated to a device, user, group, or container, the associations are chronologically ordered by default. The administrator can change the ordering.

If a device or user belongs to multiple groups, the groups are ordered. Consequently, the policies associated to those groups are also ordered. The administrator can change the ordering of groups for a device or user at any time.

In addition, the policies in a policy group are ordered.

- Policies have a precedence configured to determine the policy that is effective for a device or a user.

Many policies of the same type can be applied to a user or a device through direct association and inheritance. For example, if a Browser Bookmark policy is associated to a user and another Browser Bookmark policy is associated to a container containing that user, the policy directly associated to that user overrides the policy associated to the container.

- **Other**

- Policies support management by exception.

You can define a global policy for your enterprise and associate it to the top-level container containing all your user objects. You can then override configuration items in the global policy by defining a new policy and associating it to specific users or user groups. These users receive their configuration from the new policy. All other users receive their configuration from the global policy.

- Policies support system requirements.

You can specify the system requirements of a device or user in a policy. The policy is applied to a device or user only if the device or user meets the system requirements.

For example, the SNMP policy is applied by default on all devices having the SNMP service installed.

- ZENworks Configuration Management supports singular and plural policies.

Singular Policy. If multiple policies of the same policy type are assigned to a device or a user and the policy type is a Singular policy, then only the nearest associated policy meeting the system requirements is applied. If the policy type is associated to both user and device, then two different policies can be assigned to user and device.

The SNMP policy, Dynamic Local User policy, Remote Management policy, Roaming Profile policy, and ZENworks Explorer Configuration policy are singular policies.

Plural Policy. If multiple policies of the same policy type are assigned to a device or a user and the policy type is a Plural type, then all policies meeting the associated system requirement are applied.

The Browser Bookmarks policy, Local File Rights policy, Windows Group policy, and Printer policy are plural policies. However, the security settings in the Windows Group policy are not plural.

- Policies can be disabled.

When you create a policy in ZENworks Configuration Management, the policy is enabled by default. You can disable it if you do not want to apply it on a user or a device.

- ZENworks Configuration Management allows you to resolve policy conflicts.

The set of effective policies is a subset of the set of assigned policies. The set of effective policies for a device or user is calculated by applying precedence rules, multiplicity rules, and system requirements filters on the set of assigned policies. Effective policies are calculated separately for devices and users. The Policy Conflict Resolution setting determines how user and device policies

interact for a specific user and device combination.

Effective policies are calculated separately for devices and users. When a user logs in to a device, policies associated to both the user and the device must be applied. Policy Conflict Resolution settings are used only when policies of the same type are associated to both the device and the user. This setting determines the precedence order among the policies associated to the user and those associated to the device. The Policy Conflict Resolution settings are applied after the effective policies are calculated.

Policy Conflict Resolution settings are defined when associating a policy to a device. The settings cannot be defined for associations to users. For each policy type, the Policy Conflict Resolution setting defined in the closest effective policy of that type is applied for all policies of that type.

Manage Folders

A folder is an organizational object. You can use folders to structure your policies and policy groups into a manageable hierarchy for your ZENworks system. For example, you might want a folder for each type of policy (Browser Bookmarks policy, Dynamic Local User policy, and so forth), or, if applications are department-specific, you might want a folder for each department (Accounting Department folder, Payroll Department folder, and so forth).

Manage Folders

- Create Folders
 - Name
 - Description
- Rename or Move Folders
 - Select **folder**
 - Select **Edit**
- Delete a Folder
 - Select **folder**
 - Select **Delete**

- **Create Folders**

You must provide a unique name for your folder. This is a required field.

When you name an object in ZENworks Control Center (folders, policies, policy groups, and so forth), ensure that the name adheres to the naming conventions; not all characters are supported. For more information on naming conventions, see “Naming Conventions in ZENworks Control Center” in *ZENworks 11 SP2 System Administration Reference*.

- **Rename or Move Folders**

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 selecting 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 Policy object, you can rename, copy, and move the policy. If you select a Folder object, you can rename or move the Folder 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.

- **Delete a Folder**

Deleting a folder also deletes all of its contents (policies, policy groups, and subfolders).

Create Windows Configuration Policies

Novell ZENworks 11.2 Configuration Management lets you create policies by using ZENworks Control Center or by using the zman command line utility.

Create Policies

- Browser Bookmarks Policy
- Dynamic Local User Policy
- Local File Rights Policy
- Power Management Policy
- Printer Policy
- Remote Management Policy
- Roaming Profile Policy
- SNMP Policy
- Windows Group Policy
- ZENworks Explorer Configuration Policy

Browser Bookmarks Policy

- Lets you configure Browsers favorites for Windows devices and users
 - Internet Explorer 8.x/9.x
 - Mozilla Firefox 3.x
 - Mozilla Firefox 4.x

The Browser Bookmarks policy lets you configure Internet Explorer favorites for Windows devices and users.

The Define Details page fill allows you to fill in the following fields:

- **Policy Name.** Provide a name for the policy. The policy name must be different than the name of any other item (group, folder, and so forth) that resides in the same folder. The name you provide displays in ZENworks Control Center.
- **Folder.** Type the name or browse to and select the ZENworks Control Center folder where you want the policy to reside. The default is /policies, but you can create additional folders to organize your policies.
- **Administrator Notes.** Provide a short description of the policy's content. This description displays in ZENworks Control Center.

You can create a browser bookmarks tree by importing a previously exported file or manually entering the data. Before you import a book marks file ensure that it is in UTF-8 format. To manually convert the bookmark file into UTF-8 format, use a text editor

The following list contains browser-specific information to create the exported file:

- **Internet Explorer 8.x/9. x.** In the browser window, click **File > Import and Export**. Follow the instructions given in the Import/Export Wizard to create the bookmark.htm file.
- **Mozilla Firefox 3.x.** In the browser window, select **Bookmarks > Organize Bookmarks, then select Import and Backup > Export HTML** to create the bookmarks.html file.
- **Mozilla Firefox 4.x.** In the browser window, click **Bookmarks > Show All Bookmarks** to open the library. From the toolbar on the library, click **Import and**

Backup > Export Bookmarks to HTML to create the bookmarks.html file.

Dynamic Local User Policy

- Lets you create new users and manage existing users on the following:
 - Windows XP
 - Windows Vista
 - Windows 7
- Does not require the Novell Client to be installed on the workstation

The Dynamic Local User policy lets you create new users and manage existing users on the managed device after they have successfully authenticated to user source.

The Define Details page allows you to fill in the following fields:

- **Policy Name.** Provide a name for the policy. The policy name must be different than the name of any other item (group, folder, and so forth) that resides in the same folder. The name you provide displays in ZENworks Control Center.
- **Folder.** Type the name or browse to the ZENworks Control Center folder where you want the policy to reside. The default is /policies, but you can create additional folders to organize your policies.
- **Administrator Notes.** Provide a short description of the policy's content. This description displays in ZENworks Control Center.

The Dynamic Local User policy can be associated to either a user or device. If the policy is associated to a user object, workstations can be included or excluded from the list.

Dynamic Local User Policy rules for workstations include:

- By default, all workstations are included.
- For an indirect association, if an object is in both lists, the closeness of the association is considered. A direct association is closer than a group association, which in turn is closer than a folder.
- If the closeness is the same, a workstation is directly added to Group A and Group B, and the Included List takes precedence.

Dynamic Local User Policy rules for users include:

- By default, all users are included.

- For an indirect association, if an object is in both the lists, the closeness of the association is considered. A direct association is closer than a group association, which in turn is closer than a folder.
- If the closeness is the same, a user is directly added to Group A and Group B, and the Included List takes precedence.

For instructions on implementing a Dynamic Local User Policy without the Novell Client, see “Section 3.2.3: Implementing the Dynamic Local user Policy Without the Novell Client” in the *ZENworks 11 SP2 Configuration Policies Reference*.

Local File Rights Policy

- Lets you configure rights for files or folders that exist on NTFS file systems

The Local File Rights policy allows you to configure rights for files or folders that exist on the NTFS file systems.

In the **Define Details** page in the wizard you fill in the following fields:

- **Policy Name.** Provide a name for the policy. The policy name must be different than the name of any other item (group, folder, and so forth) that resides in the same folder. The name you provide displays in ZENworks Control Center.
- **Folder.** Type the name or browse to and select the ZENworks Control Center folder where you want the policy to reside. The default is /policies, but you can create additional folders to organize your policies.
- **Administrator Notes.** Provide a short description of the policy's content. This description displays in ZENworks Control Center.

The **Configure Basic Properties** page in the wizard lets you configure the attributes. The page allows you to configure permissions for only one file or folder. If you want to assign permissions to multiple files or folders, then configure them in the Details page after creating the policy.

The **Configure Permissions** page in the wizard lets you configure permissions for selected users or groups.

Power Management Policy

- Configure the AC Power Management settings of the managed device by creating a power scheme
 - Plugged in and Battery power management settings can be configured
 - Can be assigned to a device or a user
 - Currently cannot manage the DC power management settings

The Power Management policy allows you to configure the AC Power Management settings on the managed devices by creating a power scheme. It lets you configure the AC plugged in and battery power management settings and assign them to a device or a user. It does not currently allow you to manage the DC power management settings for a device or user.

In the **Define Details** page in the wizard you fill in the following fields:

- **Policy Name.** Provide a name for the policy. The policy name must be different than the name of any other item (group, folder, and so forth) that resides in the same folder. The name you provide displays in ZENworks Control Center.
- **Folder.** Type the name or browse to and select the ZENworks Control Center folder where you want the policy to reside. The default is /policies, but you can create additional folders to organize your policies.
- **Administrator Notes.** Provide a short description of the policy's content. This description displays in ZENworks Control Center.

The **Add Power Scheme Settings** page in the wizard allows you to fill in the following fields:

- **Scheme Name.** The policy name specified on the Define Details page is automatically displayed. You can either retain the policy name for the scheme or specify a new scheme name. ZENworks 11 SP1 creates a scheme with the specified name on the managed device.
- **Scheme Description.** Provide a description for the power scheme. The description is displayed as a tooltip for the power scheme on the managed device.
- **AC Power Settings.** The following are the power scheme settings you can add to a

device or user:

- Turn Off Monitor
- Turn Off Hard Disks
- System Standby
- Enable System Hibernation

Printer Policy

- Lets you configure Local, SMB, HTTP and iPrint printers on a Windows device

The Printer policy allows you to configure Local, SMB, HTTP, and iPrint printers on a Windows device.

In the **Define Details** page in the wizard you fill in the following fields:

- **Policy Name.** Provide a name for the policy. The policy name must be different than the name of any other item (group, folder, and so forth) that resides in the same folder. The name you provide displays in ZENworks Control Center.
- **Folder.** Type the name or browse to and select the ZENworks Control Center folder where you want the policy to reside. The default is /policies, but you can create additional folders to organize your policies.
- **Administrator Notes.** Provide a short description of the policy's content. This description displays in ZENworks Control Center.

The **Printer Identification** page in the wizard allows you to select the type of printer to be installed on the managed device.

- Local Printer
- Network Printer
- iPrint Printer

On Windows Vista devices, you need to install the Novell iPrint client 5.04 or later.

Remote Management Policy

- Lets you configure the behavior or execution of a Remote Management session on the managed device
- Allows for the following:
 - Remote Control
 - Remote View
 - Remote Execute
 - Remote Diagnostics
 - File Transfer

The Remote Management policy lets you configure the behavior or execution of a Remote Management session on the managed device. The policy includes properties such as Remote Management operations and security.

By default, a secure Remote Management policy is created on the managed device when the ZENworks Adaptive Agent is deployed with the Remote Management component on the device. You can use the default policy to remotely manage a device. To override the default policy, you can explicitly create a Remote Management policy for the device.

For information on creating the Remote Management policy, see “Creating the Remote Management Policy” in the *ZENworks 11 SP2 Remote Management Reference*.

Roaming Profile Policy

- Lets you create a user profile that is stored in a network path
- Configuration options include
 - Store User Profile in User's Home Directory
 - User Profile Page
 - Override Terminal Server Profile

The Roaming Profile policy allows you to create a user profile that is stored in a network path. An administrator can either use the roaming profile stored in the user's home directory or the profile stored in the network directory location.

IMPORTANT: Because of the security settings in Microsoft Vista, administrators must manually add the appropriate security rights to the user registry hive to enable roaming profiles.

In the **Define Details** page in the wizard you fill in the following fields:

- **Policy Name.** Provide a name for the policy. The policy name must be different than the name of any other item (group, folder, and so forth) that resides in the same folder. The name you provide displays in ZENworks Control Center.
- **Folder.** Type the name or browse to and select the ZENworks Control Center folder where you want the policy to reside. The default is /policies, but you can create additional folders to organize your policies.
- **Administrator Notes.** Provide a short description of the policy's content. This description displays in ZENworks Control Center.

Other configuration options include:

- **Store User Profile in User's Home Directory**

Select this option to load and save a user's profile from the user's home directory as specified in eDirectory.

This option is applicable only if the user object is in eDirectory. However, it is currently not supported in Domain Services for Windows environment.

- **User Profile Path**

Select a UNC path to a user's roaming profile. If you want to administer the policy on more than one user object, use %USERNAME% as the environment variable. In this case, the environment variable is resolved with the logged-on username and the user profile is loaded from the specified path.

- **Override Terminal Server Profile**

If a user is accessing a terminal server that has its own profile, enable this option to override the terminal server's profile.

SNMP Policy

- Lets you configure SNMP parameters on the managed devices

If a user is accessing a terminal server that has its own profile, enable this option to override the terminal server's profile.

In the **Define Details** page in the wizard you fill in the following fields:

- **Policy Name.** Provide a name for the policy. The policy name must be different than the name of any other item (group, folder, and so forth) that resides in the same folder. The name you provide displays in ZENworks Control Center.
- **Folder.** Type the name or browse to and select the ZENworks Control Center folder where you want the policy to reside. The default is /policies, but you can create additional folders to organize your policies.
- **Administrator Notes.** Provide a short description of the policy's content. This description displays in ZENworks Control Center.

The SNMP Community Strings page in the wizard allows you to fill in the following information:

- Add a Community String
- Community String
- Community Rights
- Remove All SNMP Community Strings not specified by ZENworks SNMP Policies
- Send SNMP Authentication Trap

You are allowed to add only one community string to the policy. If you want to add multiple community strings, then configure them in the Details page after creating the policy.

Windows Group Policy

- Lets you configure Group policy for Windows devices
 - User Policies
 - Computer Policies
 - Security Policies

The Windows Group Policy allows you to configure a Group Policy for Windows devices.

In the **Define Details** page in the wizard you fill in the following fields:

- **Policy Name.** Provide a name for the policy. The policy name must be different than the name of any other item (group, folder, and so forth) that resides in the same folder. The name you provide displays in ZENworks Control Center.
- **Folder.** Type the name or browse to and select the ZENworks Control Center folder where you want the policy to reside. The default is /policies, but you can create additional folders to organize your policies.
- **Administrator Notes.** Provide a short description of the policy's content. This description displays in ZENworks Control Center.

Other configuration options include:

- **Select the Type of Group Policy to Manage**

With the Windows Group Policy, you can manage either a Local group or an Active Directory group policy.

Before you can configure the Group Policy, you need to install a helper application. Select **Install the Group Policy Helper** to install the novell-zenworks-grouppolicyhelper-10.x.x.x.msi, which is a Windows installer package. This installation needs to be done only once. After the helper is installed, selecting **Configure** launches the helper, which you then use to configure or import a policy.

- **Select the Configuration Settings to Be Applied On the Managed Device**

After you have adjusted the policy settings as you prefer, you can select how to apply

the settings to the managed device.

- **Computer Configuration.** Select this option to apply the computer configuration settings to the managed device.
- **User Configuration.** Select this option to apply the user configuration settings to the managed device.

ZENworks Explorer Configuration Policy

- Lets you administer and centrally manage the behavior and features of ZENworks Explorer

The ZENworks Explorer Configuration Policy allows you to administer and centrally manage the behavior and features of ZENworks Explorer.

In the **Define Details** page in the wizard you fill in the following fields:

- **Policy Name.** Provide a name for the policy. The policy name must be different than the name of any other item (group, folder, and so forth) that resides in the same folder. The name you provide displays in ZENworks Control Center.
- **Folder.** Type the name or browse to and select the ZENworks Control Center folder where you want the policy to reside. The default is /policies, but you can create additional folders to organize your policies.
- **Administrator Notes.** Provide a short description of the policy's content. This description displays in ZENworks Control Center.

Other configuration options include

- **Enable Folder View**

Use this option to display a folder list in the application window.

The values are Yes, No, and Unconfigured. If you select the value as Unconfigured, the default value Yes is set on the managed device.

- **Expand the Entire Folder Tree**

Use this option to expand the entire folder tree when the application window is opened.

The values are Yes, No, and Unconfigured. If you select the value as Unconfigured, the default value No is set on the managed device.

- **Display Application in Windows Explorer**

Use this option to display the application list in Windows Explorer.

The values are Yes, No, and Unconfigured. If you select the value as Unconfigured, the default value Yes is set on the managed device.

- **Name of Root Folder**

Use this option to change the name of the root folder.

- **Hide the Zicon in the taskbar**

Use this option to hide the ZENworks icon in the taskbar.

The values are Yes, No, and Unconfigured. If you select the value as Unconfigured, the default value No is set on the managed device.

- **Enable Manual Refresh**

Use this option to specify whether manual refresh of applications is enabled after starting ZENworks Explorer.

The values are Yes, No, and Unconfigured. If you select the value as Unconfigured, the default value Yes is set on the managed device.

- **Allow Logout/Login as a New User**

Use this option to enable the user to log out and log in as a new user.

The values are Yes, No, and Unconfigured. If you select the value as Unconfigured, the default value Yes is set on the managed device.

- **Show Progress**

Use this option to specify whether the progress of the bundle operations should be displayed.

The values are Yes, No, and Unconfigured. If you select the value as Unconfigured, the default value Yes is set on the managed device.

- **Show Default Notifications**

Use this option to specify whether the default notification should be displayed. The notification is displayed when the content associated with a policy or a bundle is downloaded on the device. For example, during the enforcement of the Printer policy on a device, the following message is displayed in the notification area of the device:

Downloading Files for Printer Policy

The values are Yes, No, and Unconfigured. If you select the value as Unconfigured, the default value Yes is set on the managed device.

- **Start the ZENworks Explorer with the {All} Folder Displayed**

Use this option to specify whether the [All] folder should be displayed when ZENworks Explorer starts.

The values are Yes, No, and Unconfigured. If you select the value as Unconfigured, the default value Yes is set on the managed device.



Manage Policies

Manage Policies

- View the Policy Summary Page
- Edit a Policy
- Publish a Policy
- Delete a Policy
- Disable a Policy
- Assign Policies to Devices or Users
- Create a Policy Group
- Add System Requirements to a Policy
- Copy a Policy to a Content Server
- Review the Status of Policies on a Managed Device

Novell ZENworks 11.2 Configuration Management lets you use effectively manage software and content in your ZENworks system. In addition to editing and deleting existing objects, you can create new objects and perform various tasks on the objects.

You can use ZENworks Control Center or the `zman` command line utility to manage policies. This section explains how to perform this task by using ZENworks Control Center. If you prefer the `zman` command line utility, see “Policy Commands” in the *ZENworks 11 SP2 Command Line Utilities Reference*.

View the Policy Summary Page

- The Summary page of a policy displays the following panels
 - General
 - Contains general information on the policy including size, version, enabled etc.
 - Policy Status
 - Displays a summary of the policies assignment and enforcement status
 - Message Log
 - Displays all unacknowledged messages generated for the policy

The Summary page of a policy displays the following panels:

- **General**

The General panel provides a summary of the policy's general settings, including the following:

- Policy Type
- Size
- Version
- Enabled
- Number of Errors Not Acknowledged
- Number of Warnings Not Acknowledged
- GUID
- Administrator Notes

- **Policy Status**

The Policy Status panel displays a summary of the policy's assignment and enforcement status. The User row displays the status of the policy through assignment to users; the Device row displays the status of the policy through assignment to devices. A policy can be directly assigned or assigned through membership in a folder or group. You can select an underlined link in any column to view the status of the individual users and devices to which the policy is assigned, retry a failed policy, or export the data to a CSV file.

A policy's status is calculated using the status of many events. The numbers in the

various columns represent an overall view of the policy's status.

The policy status information is separated into the following groups, which are independent of each other. For example, it is possible for an installation to be successful, but the launch to be unsuccessful.

- Assignment Status
- Enforcement Status

- **Message Log**

The Message Log panel displays all unacknowledged messages generated for the object. An unacknowledged message is one that you have not yet reviewed and marked as acknowledged.

- **Status**

Displays an icon indicating the type of message: Description: Critical Status icon critical, Description: Warning Status icon warning, and Description: Normal Status icon normal.

- **Message**

Displays a brief description of the event that occurred.

- **Date**

Displays the date and time the event occurred.

NOTE: The Message Log panel on the policy's sandbox or the older versions page does not display any messages. However, the Message Log panel on the policy's published version page displays the messages of the policy's published version, sandbox, and the older versions.

A message remains in the Message Log list until you acknowledge it. You can acknowledge individual messages, acknowledge all messages at one time, or view more information about both acknowledged and unacknowledged messages.-

Edit a Policy

- You can
 - Edit the content of a policy
 - Rename a policy
 - Create a copy of the policy
 - Move a policy to a different folder
 - Copy the system requirements of one policy to another policy

The following lists the tasks you can perform for a policy:

- **Edit the content of a policy**
 1. Select the policy whose content you want to edit.
 2. Select the **Details** tab, then edit the settings according to your requirements.
 3. Select **Apply**.
 4. Select the **Summary** page.
 5. Increment the version of the policy to enforce the changes made to the policy on the managed device.
- **Rename a policy**
 1. Select the check box next to the policy.
 2. Select **Edit > Rename**, then specify the new name.
 3. (Conditional) Select **Publish changed display name immediately**.
 4. Select **OK**.

If more than one check box is selected, the Rename option is not available in the Edit menu.

If a sandbox exists, the policy is updated to a sandbox.

If a sandbox does not exist, you can choose to publish the policy as a new version or update to a sandbox.
- **Create a copy of the policy**
 1. Select the check box next to the policy.

2. Select **Edit > Copy**, then specify a new name.

If more than one check box is selected, the Copy option is not available in the Edit menu.

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.

- **Move a policy to a different folder**

1. Select the check box next to the policy (or policies).
2. Select **Edit > Move**, then select the target folder.

- **Copy the system requirements of one policy to another**

1. Select the check box next to the policy.
2. Select **Edit > Copy System Requirements**.
3. Select **Policies**, then select **Add** to select the policies to which you want to copy the selected policy's system requirements.

If more than one check box is selected, the Copy System Requirements option is not available in the Edit menu.

Publish a Policy

- Like Bundles change management exists for policies
- Publishing a policy increments the version
 - Publish as a new version
 - Publish as a new policy
- Editing a published policy creates a Sandbox version
 - Sandbox versions are only deployed/enforced on test devices/users

The Publish Policy(s) option allows you to publish the sandbox as a new version of the policy or as a different policy.

- **Publish as a New Version**

Lets you create a new version of the policy that has the version number incremented by one from the latest available version of the policy.

Select the **Include policies from subfolders** option to enable all the policies that are within the subfolders of the selected folders to be published.

- **Publish as a New Policy**

Lets you create a new policy.

- **Name.** Provide a name for the policy. The policy name must be different from the names of any other items (policy, group, folder, and so forth) that reside in the same folder. The name you provide displays in ZENworks Control Center and the ZENworks Adaptive Agent (on managed devices).
- **Folder.** Specify the name or browse to the ZENworks Control Center folder where you want the policy to reside. The default is /Policies, but you can create additional folders to organize your policies.
- **Create as Sandbox.** Select the Create as Sandbox check box to enforce the policy as a sandbox version. A sandbox version of a policy enables you to try it in a test environment before actually implementing it on your device.
- **Select Groups.** Lists all the available policy groups. Select the policy groups that the new policy should be a member of.

Delete a Policy

- Deleting a policy
 - Removes the policy content from the ZENworks content servers
 - *Does not* uninstall it from devices where it has already been installed

In ZENworks Control Center, you can select a ***Policy*** (or Policies) and select **Delete**.

Disable a Policy

- A disabled policy
 - Is not deployed to new managed devices or content servers
 - Remains on any devices and content servers to which it has already been deployed

When you create a policy in ZENworks Configuration Management, the policy is enabled by default. Policies can be disabled by an administrator. If a policy is disabled, it is not considered for enforcement on any of the devices and users that it applies to.

In ZENworks Control Center, under the Policies tab, you can select the check box next to the policy (or policies) to Enable or Disable a policy.

Assign Policies to Devices or Users

- Policies are created without assigning devices or users to it or specifying distribution schedules
- You can assign a policy to a Device
 - Specify Conflict Resolution
 - User Last
 - Device Last
 - Device Only
 - User Only
- You can assign a policy to a User

- **Assign a Policy to a Device**

The following points are applicable when you assign a policy to a device:

- If you assign a DLU policy to a device on which a user has logged in, the user is prompted to log in to the device again. Unless the user logs in to the device again, no new policies are enforced on the device.
- When you assign a ZENworks Explorer Configuration Policy to a device, the settings configured in the policy are not immediately reflected on the device. For example, even if Hide the Z icon in the taskbar is enabled in the policy, the ZENworks icon is displayed for a few seconds on the device after the policy is assigned to the device.
- If both user-associated and device-associated policies are effective for a device, only the policy that takes precedence according to the Policy Conflict Resolution settings is applied on the device. However, the Effective status for both policies is displayed as Success in the ZENworks Adaptive Agent icon
- User settings of a device associated Group policy cannot be enforced in console sessions of a Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2 device.
- On a managed device, if you launch a published application that is installed on a Citrix server having iPrint policy configured, it might take considerable time for the policy to be enforced on the server. During this period, the iPrint functionality is not available for the application.

The iPrint policy is not enforced on the device if you set the ZENUserDaemon and the DisableUserDaemonHealing registry keys on the device to enable the user

configuration settings configured in the Group policy to be applied in terminal sessions of Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2 devices.

- **Assign a Policy to Users**

Certain key points that you must be aware of before you assign a policy to a user are as follows:

- There are two types of users: users in the corporate directory and local users on managed devices. Policies can be associated to users in the corporate directory. ZENworks assumes that a mapping exists between users in the corporate directory and users on a device. When a user logs in to the corporate directory, ZENworks obtains the policies for the corporate user and caches them on the device.
- If a mapping exists between a corporate user and a local user, ZENworks also associates the cached policies with the local user. When a user logs in to the device, the previously cached policies are enforced for the local user. When the user also logs in to the corporate directory, the policies for the corporate user are refreshed, then enforced.
- The set of policies, both directly assigned and inherited, is called as a set of assigned policies for a device or a user. When calculating the set of assigned policies, filters such as multiplicity or system requirements are not applied. Groups and containers also have assigned policies. Policies that are disabled are not included in the set of assigned policies.
- Before assigning a Roaming Profile policy to a user on a Windows Vista device or Windows Server 2008 device, make sure a user profile with correct registry hive permissions is available on the device.

The following points are applicable when you assign a policy to a user:

- When you assign a ZENworks Explorer Configuration Policy to a user, the settings configured in the policy are not immediately reflected on the device on which the user logs on. For example, even if Hide the Z icon in the taskbar is enabled in the policy, the ZENworks icon is displayed for a few seconds on the device after the policy is assigned to the user.
- User assigned policies are not enforced in the console sessions of Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2 device.
- If you launch a published application from a Citrix server on to the device, it might take some considerable time for the list of the iPrint printers to be displayed on the device.
- If you launch a published application installed on a Citrix server that has iPrint printer policy configured, it might take some considerable time for the policy to be enforced on the server. During this period, the iPrint functionality is not available for the application.

Create a Policy Group

- Groups consist of two or more policies
 - Groups can be created with a singular policy and then additional policies can be added as they are created
- Lets you assign the group, rather than each individual policy, to devices and users
- Policies can be added
 - To a policy group that already exists
 - As part of creating a new policy group

A policy group consists of two or more policies. Creating policy groups eases administration efforts by letting you assign the group, rather than each individual policy, to devices and users. You can create a policy group with a single policy and then add policies to the group as and when required.

You can add any number of policies to the group. You cannot add other policy groups to the group.

(Conditional) If you are creating a new group to contain the selected items, the Basic Information page is displayed in the wizard. Fill in the following fields:

- **Group Name.** Provide a unique name for your policy group. The name you provide displays in the ZENworks Control Center interface.
- **Folder.** Type the name or browse to and select the folder that contains this policy group
- **Description.** Provide a short description of the policy group's content. This description displays in ZENworks Control Center.

Add System Requirements to a Policy

- Like Bundles, Policies can have system requirements
 - If a managed device does not meet the requirements, the policy is not enforced
- Filter Conditions
 - System requirements are defined with filters
 - Same process as with Bundles
- Filter Logic
 - One or more filters can be used to determine system requirements
 - Filters can be individual filters or filter sets
 - Filters are combine with AND/OR operators

The System Requirements panel lets you define specific requirements that a device must meet for the specified version of the policy to be assigned to it. You can choose to edit the requirement.

You define requirements through the use of filters. A filter is a condition that must be met by a device in order for the policy to be applied. For example, you can add a filter to specify that the device must have exactly 512 MB of RAM in order for the policy to be applied, and you can add another filter to specify that the hard drive be at least 20 GB in size.

- **Filter Conditions**

The following are a few of the conditions you can choose when creating a filter:

Architecture

Bundle Installed

Configuration Location

Configuration Network Environment

Connected

Connection Speed

Disk Space Free

Disk Space Total

Disk Space Used

Environment Variable Exists

Environment Variable Value

Filter Date

File Exists

File Size

File Version

IP Segment

Logged on to Primary Workstation

- **Filter Logic**

You can use one or more filters to determine whether the policy should be applied to a device. A device must match the entire filter list (as determined by the logical operators that are explained below) for the policy to be applied to the device.

There is no technical limit to the number of filters you can use, but there are practical limits, such as:

- Designing a filter structure that is easy to understand
- Organizing the filters so that you do not create conflicting filters

You can add filters individually or in sets. Logical operators, either AND or OR, are used to combine each filter and filter set. By default, filters are combined using OR (as determined by the Combine Filters Using field) and filter sets are combined using AND. You can change the default and use AND to combined filters, in which case filter sets are automatically combined using OR. In other words, the logical operator that is to combine individual filters (within in a set) must be the opposite of the operator that is used between filter sets.

NOTE: Filters and filter sets cannot be nested. You can only enter them in series, and the first filter or filter set to match the device is used. Therefore, the order in which they are listed does not matter. You are simply looking for a match to cause the policy to be applied to the device.

Copy a Policy to a Content Server

- By default, a policy is copied to each content server
- You can copy to specified content servers

By default, a policy is copied to each content server. If you specify certain content servers as hosts, the policy is hosted on only those content servers; it is not copied to all content servers. You can also specify whether the selected policy is replicated to new content servers (ZENworks Servers and satellite servers) that are added to the Management Zone.

Specify the default replication behavior for new servers added to the system:


- **New Primary Servers Will.** Specify the default replication behavior for new ZENworks Primary Servers added to the system:
 - **Include This Content.** Replicates the content to any servers created in the future.
 - **Exclude This Content.** Excludes the content from being replicated to any servers created in the future.
- **New Satellite Servers Will.** Specify the default replication behavior for new ZENworks satellite servers added to the system:
 - **Include This Content.** Replicates the content to any servers created in the future.
 - **Exclude This Content.** Excludes the content from being replicated to any servers created in the future.

Be aware that any content replication relationships previously set between the content and servers are lost upon completion of this wizard.

1. Select **Next** to display the Finish page, then review the information and, if necessary, use the Back button to make changes to the information.
2. Select **Finish** to create the relationships between the content and the content servers. Depending on the relationships created, the content is replicated to or removed from

content servers during the next scheduled replication.

Review the Status of Policies on a Managed Device

1. Right-click the  icon in the device system tray
2. Select **Show Properties** to display the ZENworks Adaptive Agent dialog
3. Select **Policies**

The ZENworks Adaptive Agent applies policies that your administrator defines. Policies are rules that control a range of hardware and software configuration settings. For example, your administrator can create policies that control the Adaptive Agent features you can use, the bookmarks available in your browser, the printers you can access, and the security and system configuration settings for your.

You cannot change the policies applied by your administrator. Policies might be assigned to you or they might be assigned to your device. Policies assigned to you are referred to as user-assigned policies, and policies assigned to your device are referred to as device-assigned policies

The ZENworks Adaptive Agent enforces your user-assigned policies only when you are logged in to your user directory (Microsoft Active Directory or Novell eDirectory). If you are not logged in, you can log in through the ZENworks Configuration Management login screen. To do so, right-click the ZENworks icon in the notification area, then select **Login**.

The Adaptive Agent always enforces the device-assigned policies regardless of whether or not you are logged in. Therefore, device-assigned policies are enforced for all users of the device.

Exercise 7-1

Configure Policy Management

In this exercise, you configure Policy Management functionality, configure policy groups, and make policy assignments by doing the following:

- Configure a Browser Bookmark Policy
- Configure a Local File Rights Policy
- Configure a Windows Group Policy for Windows XP
- Configure a Windows User Group Policy for Windows 7
- Assign and Test the Policies

Exercise 7-2

Set Up Clientless Dynamic Local User

In this exercise, you set up a clientless Dynamic Local user by completing the following tasks:

- Verify User Accounts
- Create a Bundle to Set Registry Keys
- Modify the Windows 7 Workstation Group Policy
- Configure a Dynamic Local User Policy
- Test the Effects of the Dynamic Local User Policy

Configure Remote Management

Novell.

Objectives

- Describe ZENworks Remote Management
- Set Up Remote Management
- Manage Remote Sessions
- Secure a Remote Session

ZENworks 11.2 Configuration Management provides services for remotely diagnosing and correcting problems on your Windows workstations and servers.

In this section, you learn how to configure and use the Remote Management features of ZENworks 11.2 Configuration Management.

NOTE: In reality, remote management is an extension of policies (although there's a lot more to it).

Describe ZENworks Remote Management

Describe ZENworks Remote Management

- What Is Remote Management?
- What You Can Do With Remote Management in Windows
- Remote Management Terminology
- Remote Operations on a Windows Device
- Remote Operations on a Linux Device
- Remote Management Features on Windows Devices
- Remote Management Proxy

What is Remote Management?

- Novell ZENworks Configuration Management lets you remotely manage devices from the management console

Remote Management gives administrators control of a device without the requirement for an on-site visit. It can save you and your organization time and money. For example, you or your organization's help desk can analyze and remotely fix the managed device's problems without visiting the user's workstation, thereby reducing problem resolution times and increasing productivity.

What You Can Do With Remote Management in Windows

- Diagnose Problems
- Remote Control
- Remotely run executables
- Remotely wake up a powered off managed device
- Transfer Files

Novell ZENworks Configuration Management lets you remotely manage devices from the management console. Remote Management allows you to do the following on a Windows device:

- Remotely control the managed device
- Remotely run executables on the managed device
- Transfer files between the management console and the managed device
- Diagnose problems on the managed device
- Remotely wake up a powered-off managed device

Remote Management Terminology

- Managed device
- Management server
- Management console
- Administrator
- Remote Management service
- Remote Management viewer
- Remote Management listener
- Remote Management proxy

- **Managed device**

A device that you want to remotely manage. To remotely manage a device, ensure that the Remote Management component is installed and the Remote Management service is running on the device.

- **Management server**

A device where the ZENworks Configuration Management server is installed.

- **Management console**

The interface for managing and administering the devices. For performing the remote operations, you must install the Remote Management viewer on the console.

- **Administrator**

A person who can configure Remote Management policies and settings, and grant Remote Management rights to remote operators.

- **Remote Management service**

A managed device component that enables remote operators to perform remote operations on the device.

- **Remote Management viewer**

A management console application that enables a remote operator to perform remote operations on the managed device. It allows the remote operator to view the managed device desktop, transfer files, and execute applications on the managed device.

- **Remote Management listener**

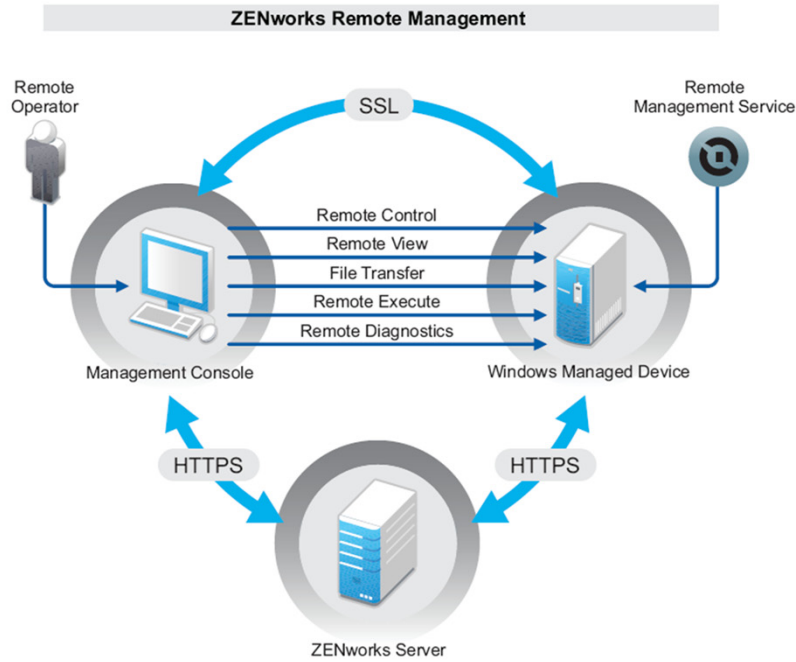
A management console application that enables a remote operator accept remote

assistance requests from managed device users.

- **Remote Management proxy**

A proxy server that forwards Remote Management operation requests from the Remote Management Viewer to a managed device. The proxy is useful when the viewer cannot directly access a managed device that is in a private network or on the other side of a firewall or router that is using NAT (Network Address Translation). As a prerequisite, the proxy must be installed on a Windows managed device or Linux device.

Remote Operations on a Windows Device



Remote Operations on a Windows Device

(continued)

- Remote Control
 - Remotely control the managed device from the console
- Remote View
 - Remotely connect and view the managed device
- Remote Execute
 - Run any executable with system privileges
- Remote Diagnostics
- File Transfer
- Remote Wake-up
 - Wake up single devices or groups with Wake-on-lan

9

© Novell, Inc. All rights reserved.

- **Remote Control**

Remote Control lets you remotely control the managed device from the management console so that you can provide user assistance and help resolve the device's problems.

Remote Control establishes a connection between the management console and the managed device. With remote control connections, you can perform all the operations that a user can perform on the device.

- **Remote View**

Remote View lets you remotely connect with a managed device so that you can view the managed device instead of controlling it. This helps you troubleshoot problems that the user encountered. For example, you can observe how the user at a managed device performs certain tasks to ensure that the user performs the task correctly.

- **Remote Execute**

Remote Execute lets you run any executable with system privileges on the managed device from the management console. To remotely execute an application, specify the executable name in the Remote Execute window. For example, you can execute the `regedit` command to open the Registry Editor on the managed device.

- **Remote Diagnostics**

Remote Diagnostics lets you remotely diagnose and analyze the problems on the managed device. This increases user productivity by keeping desktops up and running.

Diagnostics provide real-time information that you can use to diagnose and fix the problems on the managed device. The default diagnostics applications on the

managed device include

- System Information
- Computer Management
- Services
- Registry Editor

- **File Transfer**

File Transfer lets you perform various file operations on the management console and the managed device, such as

- Copy files between the management console and the managed device.
- Rename files or folders
- Delete files or folders
- Create folders
- View the properties of files and folders
- Open files with the associated applications on the management console

IMPORTANT: The File Transfer program allows you to access the network drives on the managed device.

- **Remote Wake-up**

Remote Wake Up lets you remotely wake up a single node or a group of powered-down nodes in your network provided the network card on the node is enabled for Wake-on-LAN.

Remote Management Features on Windows Devices

- | | |
|--|--|
| <ul style="list-style-type: none"> • Abnormal Termination • Agent Initiated Connection • Audible Beep • Automatic Session Termination • Intruder Detection • Keyboard and Mouse Locking • Override Screen Saver • Remote Management Auditing | <ul style="list-style-type: none"> • Screen Blanking • Session Collaboration • Session Encryption • Visible Signal |
|--|--|

- **Abnormal Termination**

Lets you lock the managed device or log out the user on the managed device if a remote session is abruptly disconnected. This feature is available on a Windows device only.

- **Agent Initiated Connection**

Lets you enable the user on the managed device to request assistance from a remote operator. You can preconfigure the list of remote operators to be available to the user.

NOTE: This feature is currently supported only on Windows.

- **Audible Beep**

When a remote session is active on the managed device you can generate an audible beep at regular time intervals on the managed device as configured in the Remote Management policy. This feature is available on a Windows device only.

- **Automatic Session Termination**

Automatically terminates a remote session if it has been inactive for a specified duration. This feature is available on a Windows device only.

- **Intruder Detection**

The Intruder Detection feature significantly lowers the risk of the managed device being hacked. If the remote operator fails to log in to the managed device within the specified number of attempts (the default is 5), the Remote Management service is blocked and does not accept any remote session request until it is unblocked.

- **Keyboard and Mouse Locking**

Lets you lock the keyboard and mouse controls of the managed device during a

remote session to prevent the managed device user from interrupting the session.

NOTE: On Windows Vista managed devices, mouse and keyboard locks do not function if the Aero theme is enabled.

- **Overriding Screen Saver**

Lets you override any password-protected screen saver on the managed device during a remote session. This feature is available on a Windows device only.

NOTE: This feature is not available on a Windows Vista, Windows Server 2008, and Windows 7 managed devices.

- **Remote Management Auditing**

Lets you generate audit records for every remote session performed on the managed device. The audit log is maintained on the managed device and is viewable by the user. This feature is available on a Windows device only.

- **Screen Blanking**

Lets you blank the screen on the managed device during a remote session to prevent the user from viewing the actions performed by the remote operator during the session. The keyboard and mouse controls of the managed device are also locked.

NOTE: Blanking the screen of a tablet PC managed device during a remote session degrades the session performance.

- **Session Collaboration**

Lets a group of remote operators collaborate to jointly perform a remote session. The master remote operator can invite other remote operators to the session, delegate the remote control rights to another remote operator to solve a problem, regain control from the remote operator, and terminate a remote session. This feature is available on a Windows device only.

- **Session Encryption**

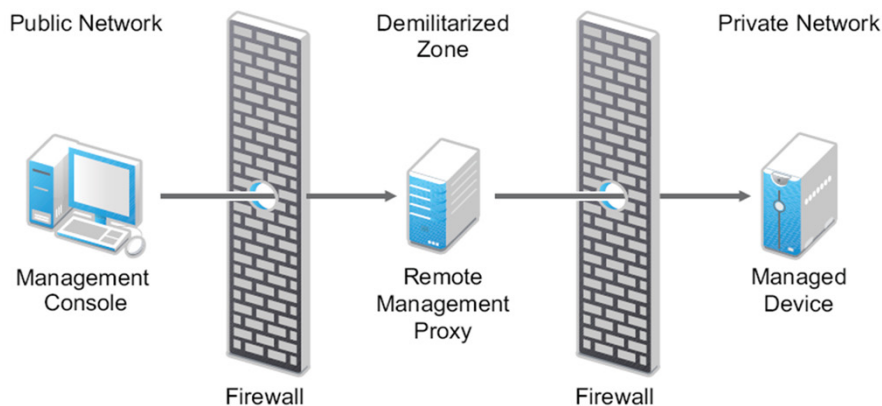
The remote sessions are secured using Secured Socket Layer (TLSv1 protocol). This feature is available on a Windows device only.

- **Visible Signal**

Lets you provide a visible indication on the managed device desktop to inform the user that the device is being remotely managed. The visible signal displays the identification of the remote operator and the session details such as type of the remote session and start time of the session. The user can terminate a particular remote session or close the signal dialog box to terminate all the remote sessions.

Remote Management Proxy

- Remote Management Proxy Configuration
 - Necessary to perform Remote Management on a device on a private network or on the other side of a firewall or router that is using NAT



You cannot perform any remote management operation on a managed device that is on a private network or is on the other side of a firewall or router that is using NAT (Network Address Translation). This is because the NAT firewall hides the device IP address from the external network and thereby blocks any connection request made to the device. To remotely manage such a device, the remote operation must be routed through a Remote Management Proxy.

You must install the proxy on a device that is placed in a demilitarized zone (DMZ). The device where you install the proxy should be accessible from the public network that has the management console and must be able to access devices that are in a private network.

The remote management proxy listens on port 5750 by default for the incoming remote management requests from the Remote Management Viewer, and forwards the requests to the device.

Set Up Remote Management

Set Up Remote Management

- Configure Remote Management Settings
- Configure Remote Management Policy
- Assign Users the Ability to Initiate Remote Management Tasks
- Configure Remote Management Agent Password
- Start an Operator-Initiated Remote Management Session
- Start a User-Initiated Remote Management Session
- Set Up the Remote Management Viewer

Configure Remote Management Settings

- Configuration settings for Remote Management can be set at the zone, folder or device level
- Configuration settings allow you to control
 - Remote Management port on the managed device
 - Performance settings for the managed device
 - Tools that should be available during remote diagnostics
- Read by the Primary agent and used to configure the Remote Management agent

The Remote Management settings are rules that determine the behavior or the execution of the Remote Management service on the managed device. The settings include configuration for the ports, session settings, and performance settings during the remote session. These settings can be applied at zone, folder, and device levels.

- **Configure the Remote Management Settings at the Zone Level of a Windows Device**

By default, the Remote Management settings configured at the zone level apply to all the managed devices.

If the managed device is on a private network or is on the other side of a firewall or router that is using NAT (Network Address Translation), the remote management operation of the device can be routed through a remote management proxy. You must install the proxy separately.

- **Configure the Remote Management Settings at the Folder Level of a Windows Device**

By default, the Remote Management settings configured at the zone level are applied to all the managed devices. However, you can modify these settings for the devices within a folder:

These changes are effective on the device, when the device is refreshed.

- **Configure the Remote Management Settings at the Windows Device Level**

By default, the Remote Management settings configured at the zone level are applied to all the managed devices. However, you can modify these settings for the managed device:

These changes are effective on the device, when the device is refreshed.

TIP: What you're doing is setting up a policy to enable remote management.

Configure Remote Management Policy

- Controls the behavior of the Remote Management agent in the following ways:
 - What Remote Management features are allowed
 - Who can remote manage the machine
 - How each of the Remote Management features operate
 - Enable / Disable Password based Authentication
 - Configure the password and password behavior
 - Configure encryption
 - Configure intruder detection and abnormal termination behavior
- Can be assigned to devices or users

The Remote Management policy lets you configure the behavior or execution of a Remote Management session on the managed device. The policy includes settings for Remote Management operations such as Remote Control, Remote View, Remote Execute, Remote Diagnostics, and File Transfer, and also allows you to control settings for security.

By default, a secure Remote Management policy is created on the managed device when the ZENworks Adaptive Agent is deployed with the Remote Management component on the device. You can use the default policy to remotely manage a device. To override the default policy, you can explicitly create a Remote Management policy for the device.

The Define Details page in the wizard displays the following fields:

- **Policy Name.** Provide a unique name for the policy. The policy name must be different than the name of any other item (group, folder, and so forth) that resides in the same folder.
- **Folder.** Type the name or browse to the ZENworks Control Center folder where you want the policy to reside. The default is /policies, but you can create additional folders to organize your policies.
- **Description.** Provide a short description of the policy's content. This description displays in the summary page of the policy in ZENworks Control Center.

Assign Users the Ability to Initiate Remote Management Tasks

- ZENworks Administrators within the system can be given the rights in ZCC to
 - Only manage specific devices
 - Only manage specific users
 - Only perform specific remote management tasks

You can assign rights to a Remote Operator to perform remote sessions on the managed device. The Remote Operator can have device-specific rights as well as user-specific rights.

Configure Remote Management Agent Password

- Remote Management Passwords can be set from the following:
 - ZENworks Control Center
 - Can be set in the Remote Management Policy
 - ZENworks Adaptive Agent
 - Users on the managed device can set a password if “Allow user to override default password” is set in the policy for the managed device
 - User passwords take precedence over the password set in the policy

- **Setting Up the Remote Management Password Using ZENworks Control Center**

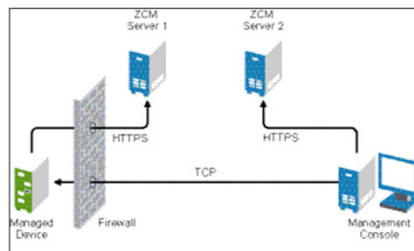
The Administrator can set a Remote Management password in the Security Settings page while creating a Remote Management policy or after creating the policy.

- **Setting Up the Remote Management Password Using ZENworks Adaptive Agent**

The user at the managed device can set a password for the Remote Management service if the Allow user to override default password on the managed device option is enabled in the Remote Management policy effective on the managed device. This password has precedence over the password set in the Remote Management policy.

Start an Operator-Initiated Remote Management Session

- Remote Operator
 - Selects the user or device to remotely manage
 - Initiates the chosen Remote Management session
- ZENworks Configuration Management
 - Validates that the operator has the necessary permissions
 - Initiates the session with the managed device



In this scenario, the remote session is initiated by the administrator on the management console. The management console is typically placed within an enterprise network and the managed device can be either within or outside the enterprise network. The following illustration depicts a remote session initiated on the managed device from the management console.

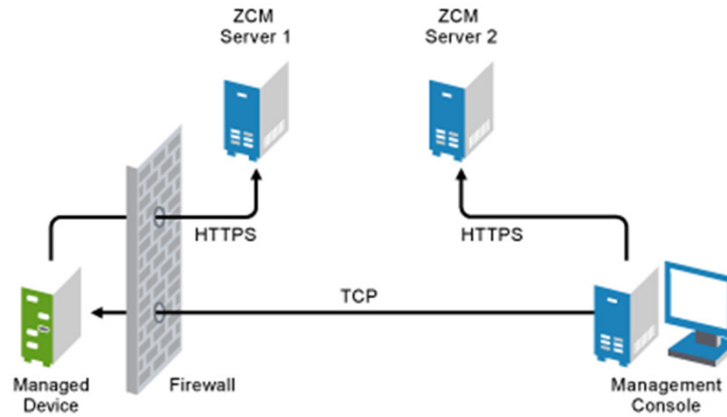
As an administrator, you can initiate a session by starting a Remote Management Operation in ZENworks Control Center. You can initiate the various Remote Management operations from the device context or the user context:

The Remote Management Agent starts automatically when the managed device boots up. A default Remote Management policy is created on the managed device when the device is deployed. You can remotely manage the device using this default policy in rights-based authentication mode only. If you create a new Remote Management policy, the new policy overrides the default policy.


If the ZENworks Management Zone setup is spread across two or more NAT-enabled private networks that are interconnected by a public network, you must deploy DNS_ALG on the gateways of these private networks. DNS_ALG ensures that the DNS lookup queries initiated by the ZENworks components return the correct private address mapped hostname and enables the communication between the management console and the managed devices. For more information on DNS_ALG, refer to DNS ALG RFC - 2694 (<http://www.ietf.org/rfc/rfc2694>).

If you want to remotely manage a device by using its DNS name, ensure that Dynamic DNS service is deployed in the network.

Start an Operator-Initiated Remote Management Session (continued)



Start a User-Initiated Remote Management Session

- Help-desk User
 - Starts the Remote Management Listener
 - Listens for incoming requests from users that need help
- User
 - Initiates request for Remote Management from the  icon in the system tray
- Remote Operator
 - Accepts the request and then the authentication occurs

In this scenario, the remote session is initiated by the user on the managed device. This is useful if the management console cannot connect to the managed device. The following illustration depicts a remote session initiated by the user at the managed device.

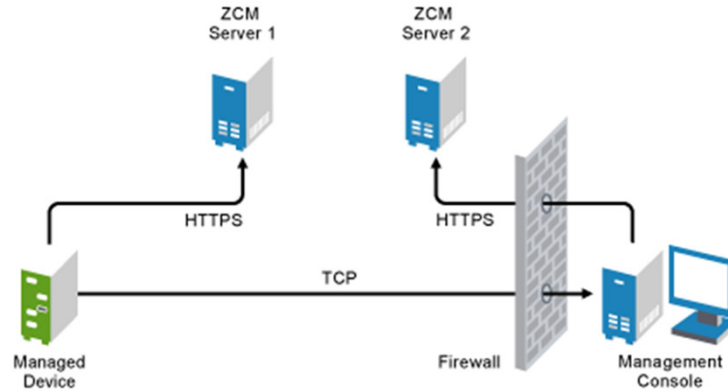
- The user at the managed device can request a remote operator to perform a remote session on the device if:
- The remote operator has launched the Remote Management listener to listen to the remote session requests from the user.
- The Allow user to request a remote session option is enabled in the Remote Management policy.

The port at which the Remote Management listener listens for the remote connections must be opened in the management console firewall. The default port is 5550.

The ability to request a Remote Management session is controlled by your administrator, which means the option might be disabled, particularly if your company or department does not have dedicated help desk personnel to serve as on-call remote operators. If the Request Remote Management Session option is not displayed as linked text, the option is disabled.

If you want to allow connections to be made from a public network into a private network, deploy the DNS Application Level Gateway (DNS_ALG). For more information on DNS_ALG, refer to RFC 2694 (<http://www.ietf.org/rfc/rfc2694>).

Start a User-Initiated Remote Management Session



Set Up the Remote Management Viewer

- Install the Remote Management Viewer
 - Select **Install Remote Management Viewer** link
 - Link is available when performing remote management on a managed device in the ZCC
- Upgrade the Remote Management Viewer
 - Link is available if an older version of the remote management view is already installed

- **Install the Remote Management Viewer**

The Remote Management Viewer is a management console application that enables a remote operator to perform remote operations on the managed device. It allows the remote operator to view the managed device desktop, transfer files, and execute applications on the managed device.

To install the Remote Management Viewer, select the Install Remote Management Viewer link that is displayed in ZENworks Control Center when you are performing a remote management operation on the managed device. This link is displayed only if you are performing a remote management operation on the device for the first time and if the viewer is not already installed on the device.

If an earlier version of the Remote Management Viewer is already installed on the device, then the Upgrade Remote Management Viewer link is displayed. Select this link to upgrade the version of the viewer installed on the device.

NOTE: Installing Remote Management Viewer on a SUSE Linux Enterprise Server 11 (SLES 11) or SUSE Linux Enterprise Desktop 11 (SLED 11) requires dependent glitz package. You must install the appropriate glitz package from the openSUSE® Web site (<http://software.opensuse.org/112/en>).

- **Upgrade the Remote Management Viewer**

If you are performing a remote management operation on a Windows managed device on which an earlier version of the Remote Management Viewer is already installed, the Upgrade Remote Management Viewer link is displayed in ZENworks Control Center. Select this link to upgrade the version of the viewer installed on the device.

To upgrade the Remote Management viewer on a Linux device from Novell

ZENworks 10 Configuration Management SP3 (10.3) to Novell ZENworks 11 Configuration Management, run the following command as a superuser or root user:

```
rpm -Uvh --nopostun novell-zenworks-rm-viewer-<version>.noarch.rpm
```

Alternatively, uninstall the old version novell-zenworks-rm-viewer-10.x.x.rpm, and install the new version.

Manage Remote Sessions

Perform Management Tasks

Task	Description
Manage a Remote Control Session	Lets you remotely control a managed device
Manage a Remote View Session	Lets you remotely connect with a managed device to view the managed device desktop
Manage a Remote Execution Session	Lets you remotely run executables with system privileges on the managed device
Manage a Remote Diagnostics Session	Lets you remotely diagnose and analyze the problems of the managed device
Manage a Files Transfer Session	Lets you transfer files between the management console and the managed device
Wake up a Remote Device	Lets you remotely wake up a single managed device or a group of powered down managed devices in your network

- **Manage a Remote Control Session**

Remote Management lets you remotely control a managed device. With remote control connections, the remote operator can go beyond viewing the managed device to taking control of it, which helps to provide user assistance and resolve problems on the managed device.

- **Using the Toolbar Options in the Remote Management Viewer**

The following table describes the various toolbar options available in the Remote Management viewer during a Remote Control session. It also lists the shortcut keys if they are available.

- **Session Collaboration**

The Session Collaboration feature lets you invite multiple remote operators to join the Remote Management session if the remote operators have launched the Remote Management listener to listen to the remote session requests. You can also delegate the Remote Control rights to a remote operator to help you solve a problem and then regain control back from the remote operator. This option is currently supported only on Windows.

If you launch the Remote Control session on the managed device first, then you gain the privileges of the master remote operator. You can use Session Collaboration to:

- Invite multiple remote operators to join the Remote Control session.
- Delegate the remote control rights to a remote operator to help you solve a problem and then regain control back from him or her.
- Terminate a remote session.

To launch Session Collaboration:

1. Launch the Remote Control session on the managed device in collaborate mode.
2. On the Remote Management viewer toolbar, select the Collaboration icon to display the Session Collaboration window.

- **Manage a Remote View Session**

Remote View lets you remotely connect with a managed device so that you can view the managed device desktop.

- **Manage a Remote Execute Session**

Remote Execute lets you remotely run executables with system privileges on the managed device. To execute an application on the managed device, launch the Remote Execute session.

The remote execution of the specified application might fail if the application is not available on the managed device in the defined path.

WARNING: By default, the Remote Management module runs as a service with system privileges on the managed device. Hence, all the applications launched during the Remote Execute session also run with system privileges. For security reasons, we strongly recommend that you close the application after use.

- **Manage a Remote Diagnostics Session**

Remote Management lets you to remotely diagnose and analyze the problems on the managed device. This helps you to shorten problem resolution times and assist users without requiring a technician to physically visit the problem device. This increases user productivity by keeping desktops up and running.

When you launch a Remote Diagnostics session on the managed device, you can access only the diagnostics applications configured for the device in the Remote Management settings for diagnosing and fixing the problems on the device. During the session, the diagnostics applications are displayed as icons in a toolbar. By default, the following diagnostics applications are configured in the Remote Management Settings.

You can configure the applications to be launched on the managed device during the Remote Diagnostics session.

- **Manage a File Transfer Session**

Remote Management enables you to transfer files between the management console and the managed device.

In the File Transfer window, the Local Computer pane displays all the files and the folders on the management console, and the Remote Computer pane displays all the files and the folders in the directory specified in the File Transfer Root Directory option in the Remote Management policy. If the File Transfer Root Directory is not specified in the policy or if the managed device does not have any policy associated with it, you can perform file transfer operations on the complete file system of the remote device.

- **Wake Up a Remote Device**

Remote Wake Up lets you remotely wake up a single node or a group of powered-down nodes in your network if the network card on the node is enabled for Wake-on-LAN.

Waking up a device that has multiple NICs (Network Interface Cards) is successful only if one or more of the NICs is configured for a subnet that contains the device that is broadcasting the Wake-on-LAN packet.

Before waking up the managed devices, the following requirements must be fulfilled:

- Ensure that the network card on the managed device supports Wake-on-LAN. Additionally, ensure that you have enabled the Wake-on-LAN option in the BIOS setup of the managed device.
- Ensure that the managed device is registered with the ZENworks Management Zone.
- Ensure that the remote node is in a soft-power off state. In the soft-power off state, the CPU is powered off and a minimal amount of power is utilized by its network interface card. Unlike the hard-off state, in the soft-off state the power connection to the machine remains switched on when the machine is shut down.

The default values for the Number of Retries and the Time Interval between Retries options are configured at the zone level. You can override these values at the device level.

Improve Remote Management Performance

- Management Console
 - Select Options from the Remote Management Connection Window, then
 - Select **Use 8 Bit color**
 - Set Custom Compression level to **6**
 - Select **Block Mouse Move Events**
 - Enable **Suppress wallpaper**
- Managed Device
 - Hardware counts, faster machine = better performance
 - Do not set wallpaper pattern

The Remote Management performance during a remote session over a slow link or a fast link varies depending on the network traffic. For a better response time, try one or more of the following:

- **On the Management Console**

In the ZENworks Remote Management Connection window at the console, select Options and set the following values:

 - To maximize the Remote Management performance over slow link:
 - Select the Use 8-bit color option.
 - Set the Custom compression level to level 6.
 - Select the Block Mouse Move Events option.
 - Enable the Suppress Wallpaper option in the Remote Management Settings.
- **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, 700 MHz (or later) with 256 MB RAM or higher.
 - Do not set a wallpaper pattern.

Secure a Remote Session

Secure a Remote Session

- Authentication
- Password Strength
- Ports
- Auditing
- Asking Permission from the User on the Managed Device
- Abnormal Termination
- Intruder Detection
- Remote Operator Identification
- Browser Configuration
- Session Security

27

© Novell, Inc. All rights reserved.

- **Authentication**

The Remote Management service must be installed on a device for the remote operator to remotely manage the device. The service automatically starts when the managed device boots up. When a remote operator initiates a remote session on the managed device, the service starts the remote session only if the remote operator is authorized to perform remote operations on the managed device.

To prevent unauthorized access to the managed device, the Remote Management service on the managed device uses the following modes of authentication:

- **Rights-Based Remote Management Authentication**

In rights-based authentication, rights are assigned to the remote operator to launch a remote session on the managed device. By default, the ZENworks administrator and the super administrator have rights to perform remote operations on all the managed devices regardless of whether the local user or the ZENworks user is logged in to the device.

- **Password-Based Remote Management Authentication**

In password-based authentication, the remote operator is prompted to enter a password to launch the remote session on the managed device.

The two types of password authentication schemes used are ZENworks Password and VNC Password.

- **Password Strength**

Use secure passwords. Keep the following guidelines in mind:

- **Length.** The minimum recommended length is 6 characters. A secure password is

at least 8 characters; longer passwords are better. The maximum length is 255 characters for a ZENworks password and 8 characters for a VNC password.

- **Complexity.** A secure password contains a mix of letters and numbers. It should contain both uppercase and lowercase letters and at least one numeric character. Adding numbers to passwords, especially when they are added to the middle and not just at the beginning or the end, can enhance password strength.

- **Ports**

By default, the Remote Management service runs on port 5950 and the Remote Management Listener runs on port 5550. The firewall is configured to allow any port used by the Remote Management service, but you need to configure the firewall to allow the port used by the Remote Management Listener.

By default, the remote management proxy listens on port 5750.

- **Audit**

ZENworks Configuration Management maintains a log of all the remote sessions performed on the managed device. This log is maintained on the managed device and can be viewed by the user and an administrator who is a member of the administrators group of the managed device. The administrator can view the logs of all the remote sessions performed on the device. The user can view the logs of all the remote sessions performed on the device when he or she was logged in.

- **Ask Permission from the User on the Managed Device**

The administrator can configure the Remote Management policy to enable the remote operators to request permission from the user on the managed device before starting a remote operation on the device.

When the remote operator initiates a remote session on the managed device, the Remote Management service checks if the Ask permission from user on managed device option for that remote operation is enabled in the policy effective on the device. If the option is enabled and no user has logged in the device, the remote session proceeds. But, if the option is enabled and a user has logged in the managed device, then a message configured in the Remote Management policy is displayed to the user requesting permission to launch a remote session on the device. The session starts only if the user grants permission.

- **Abnormal Termination**

When a remote session is abruptly disconnected, the abnormal termination feature lets you lock the managed device or log out the user on the managed device, depending on the configuration in the security settings of the Remote Management policy. The remote session terminates abnormally under the following circumstances:

- The network fails and the Remote Management viewer and the Remote Management service are unable to communicate
- The Remote Management viewer is closed abruptly through the task manager.
- The network is disabled either on the managed device or on the management console.

Under some circumstances, the Remote Management service might take up to one minute to determine the abnormal termination of the session.

- **Intruder Detection**

The Intruder Detection feature significantly lowers the risk of the managed device being hacked. If the remote operator fails to log in to the managed device within the specified number of attempts (the default is 5), the Remote Management service is blocked and does not accept any remote session request until it is unblocked. The administrator can unblock the Remote Management service either manually or

automatically.

- **Automatically Unblocking the Remote Management Service**

The Remote Management service is automatically unblocked after the duration of the time specified in the Automatically start accepting connections after [] minutes option in the Remote Management policy. The default time is 10 minutes. You can change the default time in the security settings of the Remote Management policy.

- **Manually Unblocking the Remote Management Service**

You can manually unblock the Remote Management service from the managed device or from ZENworks Control Center.

To unblock the Remote Management service from ZENworks Control Center, the remote operator must have Unblock Remote Management Service rights over the managed device.

- **Remote Operator Identification**

When a remote operator launches a remote session from ZENworks Control Center, a certificate that helps the managed device to identify the remote operator is automatically generated. However, if the remote operator launches the session in a standalone mode, the certificate is not generated and the remote operator is recorded as An Unknown User in the audit logs, the Visible Signal and the Ask User Permission dialog box. The Remote Management service retrieves the identity of the remote operator by using the certificate provided by the management console during the Secure Socket Layer (SSL) handshake. The SSL handshake happens for all the types of authentication except for the VNC password authentication.

The Remote Management service on the device displays the details of the remote operator in the visible signal dialog box, if the Give Visible Signal to the User on the Managed Device option is enabled in the policy effective on the device. It also logs the information about the remote operator in the Remote Management Audit logs.

- **Browser Configuration**

If you use Internet Explorer to launch ZENworks Control Center on Windows Vista devices, then turn off the protected mode in the security settings of the browser (**Tools > Internet Options > Security**) and restart the browser.

- **Session Security**

ZENworks Configuration Management uses Secure Socket Layer (SSL) to secure remote sessions. However, the remote sessions launched using the VNC password-based authentication are not secured. The authentication process happens over a secure channel as the SSL handshake takes place regardless of whether session encryption is configured in the Remote Management policy or not.

After the authentication is complete, the remote session switches to an insecure mode if the Enable Session Encryption option is disabled in the Remote Management policy and if the Session Encryption option is disabled by the remote operator while initiating a remote session on the managed device. However, we recommend that you continue the session in a secure mode because there is no major impact on the performance of the session.

Exercise 8-1

Configure and Use Remote Management

In this exercise, you perform the following tasks:

- Assign Remote Management Responsibilities
- Create and Assign a Remote Management Policy
- Initiate a Remote Control Session from the Administrator Side

Image Computers with ZENworks Configuration Management

Novell.

Objectives

- Describe Preboot Services and Imaging
- Set Up Preboot Services and Imaging
- Configure and Use Imaging

In Novell ZENworks 11.2 Configuration Management, Preboot Services provides functionality that allows you to perform automatic imaging tasks on managed devices (Windows/ Linux Primary Servers and workstations) before their operating systems boot. You can also perform manual imaging operations on these devices, as well as any other device with the supported file system, such as legacy Windows workstations.

In this section, you learn how to leverage preboot services and imaging to deploy these operating systems, back up users' workstations, and restore the operating system to a user's workstation in the event of a failure.

Describe Preboot Services and Imaging

Describe Preboot Services and Imaging

- Preboot Services
- Preboot Bundles
- Preboot Services and PXE
- ZENworks NBPs
- Preboot Services Example

Preboot Services

Features

- Preboot Services lets you do any of the following to a Windows or Linux device when it boots:
 - Take an Image
 - Restore an Image
 - Apply existing Image to multiple devices
 - Run Imaging Scripts
 - Run AutoYaST and Kickstart Installations
 - Configure Dell Devices

5

© Novell, Inc. All rights reserved.

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

- Make an image of the device's hard drives and other storage devices
- Restore an image to the device
- Apply an existing image to multiple devices
- Run Imaging scripts on the device
- Run AutoYaST and kickstart installations
- Configure Dell devices

To accomplish these tasks automatically using ZENworks Control Center, you simply need to have PXE (Preboot Execution Environment) enabled on your devices, then have Preboot bundles configured and assigned to the devices. The devices automatically execute these bundles when they boot.

Preboot Services

Functionality

- Preboot Services utilizes the following to make its imaging functions possible:
 - PXE (must be enabled on devices)
 - Bootable CD or DVD
 - Bootable Diskette
 - ZENworks Partition

Preboot Services utilizes the following to make its imaging 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 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. This is applicable only for ZENworks Imaging.
- **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. **This is applicable only for ZENworks Imaging.**
- **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. This is applicable only for ZENworks Imaging.

Preboot Services

Use Cases

- Preboot Services Use Cases
 - Automate Linux installation
 - Configure Dell devices
 - Create and restore images
 - Multicast images
 - Restore Devices to a clean state
 - Set up Devices for future Imaging

The following are some of the uses of Preboot Services:

- **Automate Linux installations.** Automate kickstart or AutoYaST installations.
- **Configure Dell devices.** Configure basic boot settings on Dell devices.
- **Create and Restore Standard Images.** Create base images from existing devices, as well as restore images to any manageable device.
- **Multicast Device Images.** Apply an image of one device to many other devices. This is an excellent feature for initially setting up a lab.
- **Restore Devices to a Clean State.** Quickly and efficiently reset devices to an initial state, such as in a lab.
- **Set Up Devices for Future Reimaging.** Set up devices so that the next time they reboot, they do the imaging work that is contained in their assigned Preboot bundle.

Preboot Bundles

Purpose

- Preboot Service tasks are contained in Preboot bundles (in the ZCC)
- Preboot bundles let you perform operations before the operating system boots
- Imaging bundle types let you
 - Install images on one or more devices
 - Run ZENworks scripts containing any commands that you can issue from the imaging bash prompt

Preboot Bundles

Types

- Empty Bundle
- AutoYaST Bundle
- DellIDTK Configuration
- Imaging Script Bundle
- Kickstart
- Multicast Image Set Bundle
- Third-Party Image Bundle
- ZENworks Image Bundle

In ZENworks Control Center, Preboot Services tasks are contained in Preboot bundles. The following Preboot bundle types are available:

- **Empty Bundle.** A bundle with no initial tasks. You can quickly create this bundle without performing all of tasks in the Create New Bundle wizard. Later, you can edit its details to add assignments, actions, and so forth.
- **AutoYaST Bundle.** A bundle that contains the location and access protocol of an AutoYaST configuration file and network installation directory for SUSE Linux. This bundle allows you to launch an automated installation of SUSE Linux using Preboot Services. This is only available for Linux devices that are PXE-enabled. AutoYaST bundles cannot be run using a boot CD or a ZENworks partition.
- **DellIDTK Configuration.** A bundle that contains the location of files and scripts for configuring Dell servers. This bundle allows you to use Preboot Services to configure the BIOS, BMC, RAID, and DRAC for settings and to create a new Dell Utility partition. You can also identify another Preboot bundle to be run immediately after these configurations have completed. This is only available for Linux devices that are PXE-enabled. Dell Configuration bundles cannot be run using a boot CD or a ZENworks partition.
- **Imaging Script Bundle.** Allows you to write a custom Imaging script. This provides detailed control over ZENworks imaging operations, as well as most Windows-based preboot tasks. This is applicable only for ZENworks Imaging.
- **Kickstart.** A bundle that contains the location and access protocol of an KickStart configuration file for Red Hat Linux. This bundle allows you to launch an automated installation of Red Hat Linux using Preboot Services. This is only available for Linux devices that are PXE-enabled. Kickstart bundles cannot be run using a boot CD or a

ZENworks partition.

- **Multicast Image Set Bundle.** Specifies an image that can be sent through the multicast protocol. This bundle allows you to send an image to a large number of devices in a single operation, which minimizes network traffic. It is ideal for labs, classrooms, and staging areas. This is applicable only for ZENworks Imaging.
- **Third-Party Image Bundle.** Allows you to specify the third-party images that can be restored on a device.
- **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.

To create one of these bundles: in ZENworks Control Center, select Bundles in the left pane, in the Bundles panel select **New > Bundle > Preboot Bundle > Next**, then select a bundle type.

Preboot Services and PXE

How Preboot Services uses PXE

- PXE uses DHCP and TFTP to locate and load bootstrap programs for the network
 - PXE is loaded from the BIOS on the NIC
- Preboot Services uses PXE to
 - Discover if there is Preboot Services work specified for the device
 - Provide the device with the files necessary to execute the assigned work
- Use Preboot Services to automatically place an image on a device (even if the hard drive is blank)
 - You do not need to use a CD/DVD or ZENworks Partition

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.

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.

ZENworks NBPs

How NBPs Work

- PXE specification allows PXE device NICs to find bootstrap programs located on Network Servers
- Bootstrap programs are called **Network Bootstrap Programs** (NBPs)
 - NBPs are similar to the bootstrap programs found in the Master Boot Records (MBR) of other boot media
 - Purpose of a Bootstrap program is to find and load a bootable OS
- ZENworks uses two separate NBPs working together
 - nvlnbps.sys
 - pxelinux.0

The Intel PXE specification defines mechanisms and protocols that allow PXE devices to use their network interface cards (NICs) to find bootstrap programs located on network servers. In the PXE specification, these programs are called Network Bootstrap Programs (NBPs).

NBPs are analogous to the bootstrap programs found in the Master Boot Records (MBRs) of other boot media, such as hard drives, floppy disks, CDs, and DVDs. The purpose of a bootstrap program is to find and load a bootable operating system. MBRs on traditional boot media accomplish this by locating the necessary data on their respective media. NBPs accomplish this by using files found on network servers, usually TFTP servers.

ZENworks Preboot Services uses two separate NBPs working together—nvlnbps.sys and pxelinux.0.

ZENworks NBPs

nvlnbps.sys and pxelinux.0

- **nvlnbps.sys**

- Detects various SMBIOS parameters and local hardware
- Reads the ZENworks identity information from the hard drives
- Communicates with novell-zmgprebootpolicy to determine if there is any preboot work applicable to the device
- Presents and manages the Novell Preboot Services Menu
- If necessary, launches pxelinux.0 to execute assigned preboot work

- **pxelinux.0**

- Modified version of syslinux
- Loads the operating system that is required for preboot work

12

© Novell, Inc. All rights reserved.

The nvlnbp and pxelinux are both really mini-operating systems (the pxelinux is a little larger and takes longer to load).

- **nvlnbp.sys**

This NBP has the following responsibilities:

- Detect various SMBIOS parameters and local hardware
- Read the ZENworks identity information from the hard drives
- Communicate with novell-zmgprebootpolicy to determine if there is any preboot work applicable to the device
- Present and manage the Novell Preboot Services Menu
- If necessary, launch pxelinux.0 to execute the assigned preboot work

- **pxelinux.0**

The primary purpose of this NBP is to load the operating system that is required to execute the assigned preboot work.

The pxelinux.0 file is a modified version of part of an open source project called syslinux. Although pxelinux.0 is primarily a Linux loader, it is capable of loading other operating systems. It operates by using configuration files located on a TFTP server to provide boot instructions. The various pxelinux.0 configuration files used by ZENworks 11 can be found on your Imaging Server in the /srv/tftp directory on Linux or the %ZENWORKS_HOME%\share\tftp directory on Windows, where %ZENWORKS_HOME% is the complete path of the ZENworks installation directory.

In ZENworks 11.2, 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 Novell Preboot Services Menu, each menu option corresponds to a pxelinux.0 configuration file.

For a copy of the Novell modifications to the syslinux open source project, see Novell Forge (http://developer.novell.com/wiki/index.php/Novell_Forge).

Preboot Services Example

1. Preboot bundle is created in ZCC and assigned to a PXE-enabled device
2. PXE-enabled device starts to boot
3. Device sends a DHCP discovery request to determine IP address of the Preboot Services Imaging Server
4. DHCP server responds with an IP address for the device to use
5. Novell-proxydhcp responds with
 - IP addresses of the TFTP server
 - nvlnpb.sys filename (Preboot Services bootstrap program)

Preboot Services Example

(continued)

6. PXE device downloads **nvlnbp.sys** using novell-tftp
 - nvlnbp.sys is executed
 - Device checks novell-zmgprebootpolicy to see if there is any imaging work to do
7. If there is imaging work to do (as contained in a Preboot bundle that is assigned to the device), the device performs one of the following task
 - **ZENworks Imaging:** Downloads the Configuration Management imaging environment from the server so that the it can be booted to Linux.
 - **Third-Party Imaging:** Downloads the WinPE environment from the server.

In addition to using PXE for automation, you can also execute Preboot work manually using one of the following:

- Novell Preboot Services Menu (if enabled for the device)
- Preboot Services bootable CD or DVD
- ZENworks partition

Preboot Services Example

(continued)

8. Imaging tasks contained in the Preboot bundle are performed
 - If there are no imaging tasks to perform, files are not downloaded and the device proceeds to boot to its operating system

Set Up Preboot Services and Imaging

Set Up Preboot Services and Imaging

- Prepare a Preboot Services Imaging Server
- Prepare a Satellite Server With the Imaging Role
- Deploy and Manage Preboot Services
- Administer Preboot Services
- Configure Preboot Services Default
- Override Preboot Services Default
- Enable PXE on Devices
- Set Up Devices for Imaging

Prepare a Preboot Services Imaging Server

- Assign a fixed IP address
 - When connecting to the Imaging Server during an Imaging session, a fixed IP address or DNS name is required
- Make sure there is enough space to store device images
 - Images will be nearly the same size as the data stored on the device hard drive
 - Could grow to be many gigabytes or terabytes

When you install Novell ZENworks 11 on a server, the Preboot Service service or daemon (novell-pbserv) makes all Primary Servers an Imaging Server. To avoid confusion, the Proxy DHCP service or daemon (novell-proxydhcp) is installed, but not enabled. For PXE devices to be able to communicate with Preboot Services, this service or 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 service or 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.

In addition to the specific hardware requirements for a ZENworks Server, the server used to store image files must meet the following requirements:

- **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.

Prepare a Satellite Server With the Imaging Role

- Understand the Imaging Role
 - Perform all the Imaging operations on the device by using it as an imaging server
 - Achieve load balance for the Primary Server
 - Replicate add-on images to the satellite
- Configure the Imaging role to the Satellite
 - Use the ZCC to promote device to Satellite and assign the Imaging Role
 - **zman** commands can also be used

A Satellite is a managed device that can perform certain roles that a ZENworks Primary Server normally performs. A Satellite can be any managed device (server or workstation). When you configure a Satellite, you specify which roles it performs (Imaging, Collection, or Content). A Satellite can also perform roles that might be added by third-party products that are snap-ins to the ZENworks 11 framework.

The following provides detailed information:

- **Understand the Imaging Role**

The Imaging role installs the Imaging services and adds the Imaging role to the device. The Satellite with the Imaging role is called Imaging Satellite. The Imaging Satellite requires both Proxy DHCP and DNS server to be running in the Imaging environment.

The Imaging roles allows you to

- Perform all the Imaging operations on the device by using it as an Imaging server. The operations includes taking an image and applying an image within as well as across subnets by using unicast or multicast imaging.
- Achieve load balance for the Primary Server.
- Replicate add-on images to the Satellite.

The Satellite communicates with the Primary Server for the Imaging operations in the Auto mode through ZENworks Control Center.

On the managed device, the Imaging module is inactive until you promote the managed device to be a Satellite with the Imaging role or the Imaging role is added to an existing Satellite. This activates the Imaging services on the device, and enables you to perform the Imaging operations in auto and maintenance mode.

The Imaging components installed on the device include Novell ZENworks PXE Client Files, Novell ZENworks PXE Update Files, and Novell ZENworks Multicast Application (zmgmcast). The Imaging services installed on the device include Novell TFTP, ZENworks Preboot Policy (zmgpbpolicy), ZENworks Preboot (pbserv), and Novell Proxy DHCP. All services, except for proxy DHCP, are automatically started. You can manually start or stop the proxy DHCP service from ZENworks Control Center.

- **Configure the Imaging Role to the Satellite**

You can configure the Imaging role to the Satellite by using ZENworks Control Center or the zman command line utility.

Deploy and Manage Preboot Services

- Check Preboot Services Imaging Server Setup
 - Novell ZENworks Preboot Service
 - Provides imaging services to devices
 - Novell Proxy DHCP Service
 - Runs alongside DHCP to inform PXE devices of the IP address of the TFTP server
 - Novell TFTP
 - Used by PXE devices to request files that needed to perform imaging tasks
 - Novell ZENworks Preboot Policy Service
 - Used by PXE devices to determine if there are imaging bundles assigned to the device

The following components are installed as part of Preboot Services:

- **Novell ZENworks Preboot Service** (novell-pbserv.exe)
Provides imaging services to devices.
- **Provides imaging services to devices** (novell-proxydhcp.exe)
Runs alongside a standard DHCP server to inform PXE devices of the IP address of the TFTP server. The Proxy DHCP server also responds to PXE devices to indicate which bootstrap program (nvlnbp.sys) to use.
NOTE: DHCP is not turned on by default.
- **Novell TFTP Service**
Used by PXE devices to request files that are needed to perform imaging tasks. The TFTP server also provides a central repository for these imaging files, such as the Linux kernel, initrd, and nvlnbp.sys.
A PXE device uses this server to download the bootstrap program (nvlnbp.sys).
- **Novell ZENworks Preboot Policy Service** (novell-zmgprebootpolicy.exe)
The PXE devices use this to check if there are any Preboot bundles that are assigned to the device.

Novell-proxydhcp must be started manually and does not need to be run on all Imaging Servers.

TIP: To automatically start novell-proxydhcp on server start-up, run the following command as root: **chkconfig novell-proxydhcp on.**

While taking an image, the novell-pbserv service must be running on the server where

the ZENworks image is to be stored. During restoring the image, the novell-pbserv service must be running on the server where the ZENworks image is located.

The other three services are started automatically when installing ZENworks 11, or any time the server is rebooted, and must run on all Imaging Servers.

Deploy and Manage Preboot Services

(continued)

- Deploy Preboot Services in a Network Environment
 - Server Configuration
 - You need to understand the Preboot services
 - Network Configuration
 - Design your network so PXE devices can effectively connect to the server where the Preboot Services services or daemons are running
 - Configure Filters on Switches and Routers
 - Only PXE devices on the LAN connect to the Preboot Services Imaging Server
 - Spanning Tree Protocol in Switched Environments
 - Available on certain switches and designed to detect loops in the network

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 services or 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.

- **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 or Daemons.** The four Preboot Services services or daemons (novell-pbserv, novell-tftp, novell-proxydhcp, and novell-zmgprebootpolicy) are all installed on the Imaging Server when you install ZENworks 11. These services or daemons must run together on the same server.
- **Imaging Server.** The Preboot Services services or daemons can be installed and

run on the same or different server than DHCP.

It is seldom necessary to make changes to the default configuration of these services.

- **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 services or 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.

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.

- **Configure 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:

- DHCP and Proxy DHCP servers (UDP Ports 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 novell-tftp and novell-zmgprebootpolicy are not firewall or network filter friendly. You should not attempt to run these services or 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.

Administer Preboot Services

- Preboot Services Imaging Servers Configuration
 - To make changes to the default configuration, you must edit the configuration files, then restart the service
- IP Port Usage Configuration

IP Port	Usage
67	Proxy DHCP server listens for PXE requests
68	DHCP/Proxy DHCP server responds to client requests
69	TFTP server listens for file requests from PXE devices
4011	Proxy DHCP server listens for PXE information requests
998	Novell-pbserv receives all Preboot Services device connection requests
13331	Novell zmgprebootpolicy receives all PXO device connection requests

- **Preboot Services Imaging Servers Configuration**

In Preboot Services, the services or daemons do not use switches. Instead, to configure a service or daemon to do something that is not a default, you need to edit the configuration files.

You can edit configuration files while the service or daemon is running, because they are only read when the service or daemon starts. After editing the file you must restart the service or daemon for the changes to take effect.

- **IP Port Usage Configuration**

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.

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 service or 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. It receives all connection requests from the Preboot Services devices on this port.
- **13331 Decimal.** Novell-zmgprebootpolicy client connection port. It receives all connection requests from the PXE devices on this port.

Although PXE devices make their initial requests to novell-tftp and novell-zmgprebootpolicy 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: Novell-tftp and novell-zmgprebootpolicy are not firewall or network filter friendly. You should not attempt to run these services or 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.

NOTE: The only ports we have control over are 998 and 1331.

Administer Preboot Services

(continued)

- Edit the Novell Preboot Services Menu
 - Menu options
 - Start ZENworks Imaging
 - Start ZENworks Imaging Maintenance
 - Disable ZENworks Partition
 - Enable ZENworks Partition
 - Exit
 - Can be modified by editing the pxemenu.txt file
 - Can change colors

Depending on the configuration settings for Preboot Services in ZENworks Control Center, PXE devices might be able to display the Novell Preboot Services Menu during the boot process. The menu has the following options:

- Start ZENworks Imaging
- Start ZENworks Imaging Maintenance
- Disable ZENworks Partition
- Enable ZENworks Partition
- Exit

There might be circumstances when you want to modify the options on the Novell 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
- Add submenu items
- Change the color scheme
- Change the menu title and screen name

Configure Preboot Services Default

- Configure Menu Options
- Configure Non-Registered Device Settings
- Configure Device Imaging Work Assignments
 - Lets you specify a particular bundle for each set of hardware rules
- Configure the Server Referral List
 - Used to make sure managed devices belonging to other Management Zones can access their home zone

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 Server, and some can be overridden by configurations done for devices or folders containing devices.

The following default settings can be configured in ZENworks Control Center:

- **Configure Menu Options**

The Novell 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:

- **Start ZENworks Imaging.** Executes the assigned Preboot Services bundles.
- **Start ZENworks Imaging Maintenance.** Displays the imaging maintenance mode prompt, where you can execute imaging commands.
- **Disable ZENworks Partition.** Prevents an existing ZENworks partition from being used when booting to execute the assigned Preboot bundles.
- **Enable ZENworks Partition.** Allows an existing ZENworks partition to be used when booting to execute the assigned Preboot bundles.
- **Exit.** Resumes booting of the device without doing any Preboot bundle work.

Generally, if your Preboot Services work is completely automated, you should select to never display the Novell Preboot Services Menu on the device when it boots. Conversely, if you need to do manual Preboot Services functions for some or all devices, then select to always display the menu. A compromise is where you select to

display the menu if Ctrl+Alt is pressed, allowing unattended Preboot Services work while allowing you the opportunity to display the menu when needed.

IMPORTANT: PXE must be enabled on the device for the menu to be displayed.

- **Configure Non-Registered Device Settings**

The following configurations can be set after a device is imaged. The settings are applied to devices that are not registered in the Management Zone and are placed in the devices' image-safe data.

This sets the default device ID method for the Management Zone.

- **Configure Device Imaging Work Assignments**

You can determine what imaging work is to be performed on a device when it boots, based on a set of hardware rules. This configuration section lets you specify a particular bundle for each set of hardware rules. The Custom Hardware Types section allows you to provide specific data for a Hardware Type hardware rule option.

All rules and custom types configured here are applied globally to all managed devices in the Management Zone. However, only those devices that exactly match the rule and its custom types have the assigned bundle applied to them when they boot.

- **Configure the Server Referral List**

Referral lists are used to make sure managed devices belonging to other Management Zones can access their home zone.

To configure the List of Server IP Addresses and DNS Names list box, perform the following tasks:

- **Add a server to the server referral list**

You can add a range of IP addresses by typing the beginning IP address, type a space, a dash, another space, then type the ending IP address of the range. However, these are displayed as you typed them when you select Add; the addresses within the range do not separate into individual IP addresses in the list.

Do the following:

1. In the List of Server IP Addresses and DNS Names field, specify the DNS name or IP address of a server that can host preboot operations, then select **Add** to place it into the list.
2. Repeat as necessary to complete the list of servers in your environment capable of preboot operations.

- **Edit a listed server**

Do the following:

1. Select a server in the list, then select **Edit**.
2. In the Edit String dialog box, edit the IP address or DNS name that is displayed there, then select **OK** to save the changes.

- **Rearrange the order of the servers in the server referral list**

You cannot move multiple servers at one time.

Do the following:

1. Select one server, then select either **Move Up** or **Move Down**.
2. Repeat as necessary to arrange the order of the servers.

- **Remove servers from the server referral list**

You can use the Ctrl or Shift keys to select multiple servers to remove them from the list.

Do the following:

1. Select one or more servers, then select **Remove**.

After you have specified all of the necessary servers in the server referral list, you must place certain files into the tftp directories of each ZENworks 7.x Imaging Server in the list in order for the referrals to work with those traditional ZENworks Imaging Servers.

Do not replicate any directory structure from the ZENworks 11 server. Just copy the files to the tftp directory.

NOTE: 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.

Override Preboot Services Default

- Select one of the following options:
 - Always Show Imaging Menu
 - Never Show Imaging Menu
 - Show Imaging Menu if CTRL+ALT is Pressed

You can determine which Novell Preboot Services Menu displays a configuration to use and whether the menu should be displayed on a device when it boots. By default, the Management Zone configuration applies to all folders and devices. You can override this at the folder or device level.

The menu can be customized by editing the `pxemenu.txt` file.

Enable PXE on Devices

- Enable PXE on a PXE-Capable Device
 - Can lengthen the boot process time slightly
 - Most NICs have PXE turned off by default
 - Access the computer system BIOS to enable
- Verify that PXE is enabled on a Device
 - PXE is correctly enabled on a device when the device attempts to establish a PXE session during the boot process

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.

- **Enable 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 BIOS 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 BIOS 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 Ctrl+S during the boot process to allow you to configure the PXE functionality. Other network adapters might prompt you to press Ctrl+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.

- **Verify 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.

Set Up Devices for Imaging

- **Device Requirements**

- A supported Ethernet card
- Free disk space for a ZENworks partition (optional)
- Standard hardware architecture
- PXE-enabled
- Supported imaging partition type

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 a network-connected device:

- **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.

- **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.

- **Supported imaging partition type**

The supported partition types for imaging are the NTFS, FAT32, ReiserFS, Ext2, and Ext3 file systems.

NOTE: ZENworks 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.

Configure and Use Imaging

Configure and Use Imaging

- Image Devices
- Multicast Images
- Configure Imaging Script Bundles
- Assign Imaging Bundles
- Edit Imaging Work

This section covers a “high-level” look at some of common imaging tasks.

For details on how to complete these tasks, see the *ZENworks 11 SP2 Preboot Services and Imaging Reference*.

Image Devices

- Image Device from ZENworks Control Center
 - Take a Base Image of a Device
 - Create an Add-On Image of an Installed Bundle
 - Configure ZENworks Image Bundle for Automatic Imaging
 - Use a Script to Image a Device
- Image Device from Command Line
 - Manually Take an Image of Device
 - Use Image Explorer to customize an image
 - Create an Add-on Image from files in a file system
 - Manually restore an image on a device
 - Make an Image available for Automatic Imaging

Preboot Services provides tools for creating and compressing images of device hard disks, as well as images of specific add-on applications or sets of files. ZENworks also provides tools for customizing such images and for making images available to auto-imaging operations.

You can take images of devices, then reimage them and other devices with those images. The available devices are Windows and Linux servers and workstations.

ZENworks imaging supports devices that physically connect to the network that meet the minimum requirements for devices.

ZENworks imaging does not support:

- Imaging operations (creating or restoring images) using wireless connectivity.
- Imaging operations for the encrypted LVM partitions.
- PXE booting on Citrix XEN and SUSE Linux Enterprise Server XEN.
- Software RAID configurations (however, hardware RAID is supported).
- 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.

Image Device from ZENworks Control Center

The following imaging tasks are available in ZENworks Control Center:

- **Take a Base Image of a Device**

A base image is an image of partitions and data on a source device's hard disks. Normally, such an image is prepared with the intent to completely replace the contents of a target device's hard disks.

You can take an image of an existing device and use it to image a similar device, or use it as a backup image for reimaging the original device.

- **Create an Add-On Image of an Installed**

For the current bundle, you can create the installed version as a ZENworks add-on image. This is not supported for Third-Party Image bundle formats.

Add-on images of bundles are useful for incorporating predelivery of bundles when you are imaging new devices, or when you are reimaging existing devices.

A newer version of the add-on image is automatically created when the bundle's version number is incremented.

The filename for the add-on bundle is automatically created and uses the following format:

bundle_name-bundle_UID-counter.zmg

where **bundle_name** is the name of the current bundle for which the add-on image is being created, **bundle_UID** is a UID number generated for the image, and **counter** is a four-digit counter (beginning with 0000) that is incremented each time the image is updated (that is, when the bundle's version number is changed). All ZENworks image files end in .zmg.

- **Configure ZENworks Image Bundle for Automatic Imaging**

You can use ZENworks to install software bundles. Software included in a bundle that is assigned directly is considered mandatory (the bundle is directly assigned to the devices, their groups, or their folders).

This bundle is not assigned to any device or group after it is created until you make that assignment on a Relationships tab.

IMPORTANT: If this Preboot bundle has been created on a management device inside the firewall and you are assigning it to a device outside the firewall, port 8089 must be open both ways (PUBLIC -> PRIVATE, and PUBLIC <- PRIVATE).

If PXE is enabled on the device, the bundle's work is performed on the device before its operating system starts when a device assigned to the ZENworks Image bundle boots.

- **Use a Script to Image a Device**

You can perform scripted imaging using the Imaging Script bundle. Any imaging commands can be entered for the script. This is applicable only for ZENworks Imaging.

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 an Imaging Script bundle:

```
echo "Please insert the DVD containing the image into the drive and press a key."  
read  
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 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.

Image Device from Command Line

The following manual imaging tasks are available for ZENworks Imaging:

- **Manually Take an Image of Device**

You can 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.

Ensure that your Imaging Server has enough disk space for the image. Otherwise, you encounter a “Failed to write to proxy” error.

- **Use 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:
- Split the image
- Resize a partition in an image
- Purge deleted files
- Exclude individual files and folders from the image
- Add files and folders to the image

- **Create an Add-on Image from files in a file system**

An add-on image is an archived collection of files to be applied to an existing installation on a target device. 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.

- **Manually restore an image on a device**

The section explains how to restore an image to 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.

- **Make an Image available for Automatic Imaging**

When you boot a device from an imaging method and allow the boot process to proceed in autoimaging mode, the imaging operation that is performed on the device is determined by default Preboot Services settings that you define in ZENworks Control Center.

Creating a Preboot bundle also allows you to combine a base image and one or more add-on images into a single entity that can be applied on target devices. You can specify a standard image file to apply, 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.

Image Devices

(continued)

- Set Up Disconnected Imaging Operations
 - Use CD or DVD for disconnected imaging
 - Use Hard Disk for disconnected imaging

Set 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 restored, 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. This is applicable only for ZENworks Imaging.

- **Use CD or DVD for disconnected imaging**

You can use CDs and DVDs only as the storage medium for an image to be applied, not for an image to be created.

You can apply an image from a bootable or non-bootable imaging CD or DVD using either the imaging maintenance mode prompt or using the ZENworks Imaging Engine menu.

- **Use Hard Disk for disconnected imaging**

When you boot a device from a ZENworks imaging boot media, you can place an image on, or take 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 apply an image, the source partition is not altered.

You can create or apply an image on a hard disk by using either the imaging maintenance mode prompt or by using the ZENworks Imaging Engine menu.

Multicast Images

- Use the ZENworks Control Center to Multicast an Image
 - Configure Multicast Image Set Bundles
 - Add Participants to a Multicast Session
 - Enable or Disable a Multicast Image Set Bundle
- Use a Command Line to Multicast an Image

Multicast Image Set bundles use an image that is previously taken from a device and stored on an Imaging Server. The image is sent to multiple devices at one time to reimage them, rather than being 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. Multicast packets should not be blocked in a switch.

A multicast session consists of all clients (devices) that are assigned to the Multicast Session Set bundle that are booting (joining), but must wait for a start trigger in order to complete booting. In other words, the boot processes for the devices can be held up until one of the triggers is encountered, 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.

There are two triggers that you can use to determine when to start the multicast session. The first trigger to be encountered starts the session. These triggers are useful if you want economy of scale in multiple clients joining, but don't want to stall the session too long.

Use the ZENworks Control Center to Multicast an Image

Multicast Image Set 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 being 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. Multicast packets should not be blocked in a switch.

- **Configure Multicast Image Set Bundles**

With Preboot Services, multicasting is an automated procedure. You simply define a Multicast Image Set bundle and assign it to the devices. The multicast session starts when the trigger event that you configured occurs.

Using Configuration Management, you can install software by 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).

- **Add Participants to a Multicast Session**

There are two sources for Multicast session participants: registered devices and unregistered devices. Either or both can be assigned to a given Multicast Image Set bundle. The participant devices must be PXE booted from the server where the ZENworks image file is located.

- **Enable or Disable a Multicast Image Set Bundle**

By default, a Multicast Image Set bundle is enabled when you create it. However, you can disable the bundle as a means of controlling whether to have the session run, rather than visit each device to unconfigure that work.

If you have disabled the session for this bundle, the multicast session cannot occur, even when devices assigned to the bundle reboot to trigger the session.

Use a Command Line to Multicast an Image

If you want to perform a multicast session from a command line, you need to start the multicast session from the ZENworks Imaging Server and physically visit each participating device. Performing a manual multicast session is particularly useful in a lab environment in which a small number of devices participate.

The following sections contain step-by-step information about performing a manual multicast session. You must perform the steps in both of the following sections; however, the order in which you perform these tasks does not matter.

Configure Imaging Script Bundles

- An Imaging Script bundle contains any ZENworks script that you can run from the imaging maintenance mode prompt

An Imaging Script bundle can contain any ZENworks script (containing the general shell and ZENworks Imaging Engine commands) that you can run from the imaging maintenance mode prompt.

Using Configuration Management, you can install software by 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).

An Imaging Script bundle is not assigned to any device or group after it is created until you make that assignment on a Relationships tab.

IMPORTANT: If this Preboot bundle has been created on a management device inside the firewall and you are assigning it to a device outside the firewall, port 8089 must be open both ways (PUBLIC -> PRIVATE, and PUBLIC <- PRIVATE).

When a device assigned to the Imaging Script bundle boots, the bundle's work is performed on the device before its operating system starts. In the imaging maintenance mode, the script is downloaded as the ZenAdvancedScript file in the /bin directory. Subsequently, you must execute the script in order to apply the bundle. You can execute the script by using the `sh /bin/ZenAdvancedScript` command.

Assign Imaging Bundles

- Use the Device Tab to Assign Bundles
- Use the User Tab to Assign Bundles
- Assign Devices or Users to Bundle Groups
- Use the Bundles Tab to Assign Bundles
- Assign Bundles to Non-Registered Devices

You can assign a bundle from the Devices or Bundles tabs, assign devices to bundle groups, and assign bundles to non-registered devices:

If you are assigning a Preboot bundle that has been created on a management device inside the firewall to a device outside the firewall, port 8089 must be open both ways (PUBLIC -> PRIVATE, and PUBLIC <- PRIVATE).

ZENworks 11 allows you to assign imaging tasks to a dummy device object that is created in the zone prior to actually registering the device with the zone. This allows you to assign the imaging tasks for a given device prior to booting the device based on MAC address, serial number or hostname.

Edit Imaging Work

- Edit Imaging Work page lets you view
 - All images that recently applied to selected device
 - Image that is currently assigned

The Edit Imaging Work page allows you to view all images that have been recently applied to the selected device, and the image that is currently assigned (known as its “effective” image).

NOTE: You use the ZENworks Image Explorer tool to do this.

Exercise 9-1

Create and Deploy Images with ZENworks Configuration Management

In this exercise, you perform the following tasks:

- Configure Preboot Services (PXE)
- Take an Image of the XP-WS Workstation
- Restore an Image Bundle

Manage Inventory and Data Collection

Novell.

Objectives

- Scan Managed Devices
- Scan Inventory-Only Devices
- Scan Demographic Data
- Use Administrator-Defined Fields
- Use Inventory Reports

Novell ZENworks 11.2 Asset Inventory allows you to take an inventory of all the devices in your Management Zone, including data on hardware, software, and demographics.

NOTE: Reporting is now a utility installed separately outside of ZCM 11.2.

Scan Managed Devices

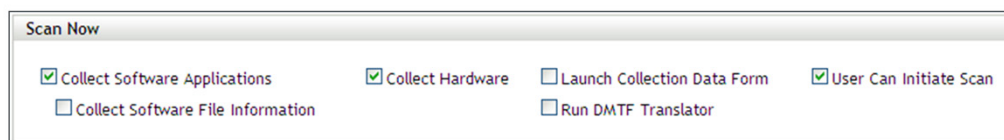
Scan Managed Devices

- Configure an Inventory Scan
- Schedule an Inventory Scan
- View an Inventory Report for a Managed Device

An inventory scan of your managed devices provides you with a detailed report of each device's hardware, software, and demographic data.

Configure an Inventory Scan

- Can be configured at the following levels
 - Management Zone
 - Device Folder
 - Device
- Available Options



Scan Now

☒ Collect Software Applications
 ☐ Collect Software File Information
 ☒ Collect Hardware
 ☐ Launch Collection Data Form
 ☐ Run DMTF Translator
 ☒ User Can Initiate Scan

An inventory scan allows you to collect data from managed devices in your Management Zone. By default, the inventory settings are preconfigured.

Configuration Levels

You can define the scan settings at three levels:

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

Configuration Options

In the Scan Now panel, you can configure how to run an on-demand inventory scan by using a Quick Task, device task, or by using the ZENworks Icon menu with the following options:

- **Collect Software Applications.** Select this option if you want to scan for software applications. This setting is selected by default.
- **Collect Software File Information.** Select this option if you want to scan for software file information that can be used to identify software products that aren't recognized by the ZENworks Knowledgebase. If you plan to create Local Software Products and add them to the knowledgebase, this option must be selected.
- **Collect Hardware.** Select this option if you want to scan for hardware data. This setting is selected by default.
- **Launch Collection Data Form.** Select this option if you want to send out the

Collection Data Form, which is used to collect demographic data.

- **Run DMTF Translator.** Select this option if you want to run the DMTF (Desktop Management Task Force) Translator. The DMTF translator converts the inventory data to formats that can be used by other tools and puts it on the local machine.
- **User Can Initiate Scan.** Select this option if you want to allow the workstation user to initiate a scan by using the ZENworks Icon.

Schedule an Inventory Scan

- Can be set at the following levels

- Management Zone
- Device Folder
- Device

- Available options

- No Schedule
- Data Specific
- Recurring
- Event

Scan Schedule
Specify the schedule the device inventory scanner should run on:

Schedule Type:
 Recurring
 No Schedule
 Data Specific
 Recurring
 Event

Refresh: 0 Days 0 Hours 0 Minutes

Days of the week

Sun	Mon	Tue	Wed	Thu	Fri	Sat
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Start Time: 6 :00

[More Options](#)

Configuration Levels

By default, the inventory schedule is already configured. You can define the scan schedule settings at three levels:


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

Configuration Options

The following are the configuration options available:

- **No Schedule.** No scan is scheduled.
- **Data Specific.** Scans run on specified dates.
- **Recurring.** Scans run on a recurring schedule.
- **Event.** Scans are triggered by an event.

View an Inventory Report for a Managed Device

- ZENworks Control Center
 - Select **Detailed Hardware/Software** from the Inventory tab
- ZENworks Icon Menu ()
 - Select **View Inventory Details** from the Inventory item

Workstation Detail Report				KB Version:3.06.A.0001.016	
Machine Name	Login	IP Address	LAN Address		
XP-ADMIN	Administrator	172.17.6.99	00F297819B		
Serial Number	Asset Tag	Total Memory (MB)	Disk Space (MB)	Free Disk Space (MB)	
564252803078d0ee120f868af2097	No Asset Tag	512	42944	8323	
Hardware					
Manufacturer	Product	Model	Asset Tag	Serial Number	
	Power Capability				
	AC Power Policy				
	ROM BIOS				Release Date:06/02/11
BuLogic	MultiMaster PCI SCSI Controller				
Intel Corporation	IDE Controller	82371AB/EB PIIX4			
HEC/MWAr	VMware IDE CDROM				Drive Letter:D
Intel	Core2 Quad				Speed:2.400000e+003MHz.GenuineIntel
VMware	Virtual IDE Hard Drive			000000000000000000000001	Drive Letters:C, Space:42944186880
	Disquette Drive				
	101/102 keyboard				
AMD	PCI/ET Family Ethernet Adapter				Lan Address:00F297819B
Logitech	PS/2 Mouse				
	USB Mouse				
	USB Mouse				
	Memory Module				Size:512, Speed:0
	Color Monitor				
Microsoft	Windows XP Professional	5.1		55274-640-0931384-23221	
	Available Ports				

A device's inventory includes information on hardware, software, and demographic data, which is gathered in an inventory scan. You can view this report through ZENworks Control Center or by using the ZENworks Icon menu.

This report shows detailed information about the device, including demographic data, hardware information, and software. From this page, you can select the various links to get more detailed information. You can export the report to Excel, CSV, or PDF formats. You can also edit selected data.

Scan Inventory-Only Devices

Scan Inventory-Only Devices

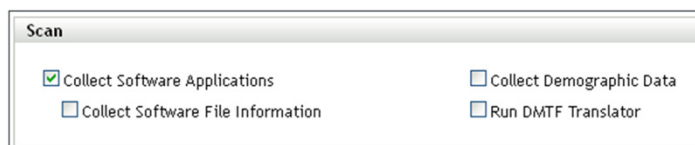
- Configure an Inventory-Only Device
- View an Inventory Report for an Inventory-Only Device
- Use the Portable Collector

An inventory only scan allows you to scan devices in the zone that don't have the ZENworks Adaptive Agent installed but do have the Inventory Only Module installed. For information on installing the Inventory Only Module, see the *ZENworks 11 SP2 Discovery, Deployment, and Retirement Reference*.

Configure an Inventory-Only Scan

• Available Options

- Collect Software Application
- Collect Software File Information
- Collect Hardware
- RUN DMTF translator



An inventory only scan allows you to collect data from devices in the Management Zone that only have the Inventory Only Module installed. By default, the inventory settings are preconfigured.

The server handles requests from devices that have the Inventory Only Module installed, providing files for the settings, scan schedule, and so on. The interval setting determines how often the server evaluates the next scan schedule and when to obtain other settings. The server needs to poll the database at frequent intervals to pass on any changes that affect the devices.

The refresh interval should be set so that refreshes occur more frequently than scans. The default is 15 minutes.

NOTE: Ensure that the time interval of the Collection Server sending over data to the Primary server is lesser than the time interval of the managed devices sending over data to the Collection Server. For example, if Managed device M1 sends data to Collection Server every 12 minutes, configure the Collection Server to send data to the Primary server every 8 minutes.

In the Device Refresh Interval panel, you set the interval time in days, hours, and minutes.

The Device Refresh Interval determines when the device checks the server for a change in settings, the schedule for the next scan, the ZENworks Knowledgebase for inventory, and new agent executables.

The refresh interval should be set so that refreshes occur more frequently than scans and less frequently than server refreshes. The default is 12 hours.

In the Scan panel, you configure how you want to run the scan.

- **Collect Software Applications.** Select this option if you want to scan for software applications installed on the device. This setting is selected by default.
- **Collect Software File Information.** Select this option if you want to scan for software file information that can be used to identify software products that are not recognized by the ZENworks Knowledgebase. If you plan to create Local Software Products and add them to the knowledgebase, this option must be selected.
- **Collect Demographic Data.** Select this option to gather demographic data from an inventoried-only device. This data is gathered from a file on the local machine.
- **Run DMTF Translator.** Select this option if you want to run the DMTF (Desktop Management Task Force) Translator. The DMTF translator converts the inventory data to formats that can be used by other tools and puts it on the local machine.

In the Software Applications panel, you configure which directories to skip.

Skipping directories is useful in limiting the scope of the scan. The directories in the list are skipped.

In the Software Files panel, configure which types of files to scan for.

Software applications discovered in an inventory scan are identified by specific files associated with the product. These identifications are kept in the ZENworks Knowledgebase. To identify products that aren't in the knowledgebase, you can search for files that are associated with an unrecognized product and use the file information to create a new product identification called a Local Software Product. This Local Software Product information can then be merged with the knowledgebase so that these new products are recognized in subsequent scans.

View an Inventory Report for an Inventory-Only Device

- ZENworks Control Center
 - Select **Detailed Hardware/Software** from the Inventory tab

A device's inventory includes information on hardware, software, and demographic data, which is gathered in an inventory scan.

This report shows detailed information about the device, including demographic data, hardware information, and software. From this page, you can select the various links to get more detailed information. You can export the report to Excel, CSV, or PDF formats. You can also edit demographic data.

Use the Portable Collector

- Create the Portable Collector for a Windows Device
- Run the Portable Collector on a Windows Device
- Run the Portable Collector on a OSX Device
- Import Data gathered with the Portable Collector

The Portable Collector is a standalone application that is used to inventory devices that rarely connect to the server or devices that do not have the ZENworks Adaptive Agent installed. This data can then be imported into the Inventoried device list. When the data is imported, you can view and edit it just as you would an inventoried device.

The Portable Collector can be run on Windows and OSX devices. The procedure is as follows:

1. Create the Portable Collector.
2. Run the Portable Collector on a device.
3. Copy the inventory data to a portable media.
4. Upload the inventory data into ZENworks Control Center.

Creating the Portable Collector for a Windows Device

The Inventory Only scan settings are used when you create the Portable Collector. If you want the Portable Collector to scan for software files, for example, that option must be selected on the Inventory Only configuration page.



Scan Demographic Data

Scan Demographic Data

- Configure the Collection Data Form
- Deploy the Data Collection Form
- Schedule the Deployment of the Collection Data Form

Inventory scans include demographic data that is gathered from workstation users through the use of the Collection Data Form. The Collection Data Form can be sent to a workstation user's computer with a prompt to fill out the data fields on the form. This data is then added to the inventory report for that workstation.

Configure the Collection Data Form

- Can be defined at the following levels:

– Management Zone

– Device

– Device

• Configure

– Select

– Configure

Label	Type	Display	Editable	Required	Autofill	Default	Choice List	Edit Mask	Instructions
First Name	Character	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No			<input type="checkbox"/>	
Middle Name	Character	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No			<input type="checkbox"/>	
Last Name	Character	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No			<input type="checkbox"/>	
Email	Character	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No			<input type="checkbox"/>	

When you configure the Collection Data Form, you are selecting what information you want to gather from the workstation user. The Collection Data Form is not configured by default. It must be configured before it can be deployed.

You can define the Collection Data Form at three levels:

- **Management Zone.** The settings are inherited by all device folders and devices.
- **Device Folder.** The settings are inherited by all devices in the folder. Overrides the settings at the Management Zone level.
- **Device.** The settings apply only to the device for which they are configured. Overrides the settings at the folder and Management Zone levels.

NOTE: If you are configuring the Collection Data Form settings on a device, you need to select Override Settings before you can change the system settings.

After it is configured and deployed, the Collection Data Form appears on the desktop of a managed device and prompts the workstation user to respond to a list of predefined questions.

Configure the Collection Data Form

(continued)

Collection Data Form

Introduction Text

☐ Show In ZENworks Icon Menu

☐ Show Cancel button on form

☐ Invisible mode for autofill only

Label	Type	Display	Editable	Required	Autofill	Default	Choice List	Edit Mask	Instructions
First Name	Character	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No				
Middle Name	Character	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No				
Last Name	Character	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No				
E-Mail	Character	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No				
Phone	Character	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No				
Second Phone	Character	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No				

Deploy the Data Collection Form

- You can use the following methods:
 - Collection Data Form Schedule
 - Device Quick Task
 - Device Task
 - Scheduled as part of an inventory scan

There are four ways you can deploy the Collection Data Form to a workstation:

- **Collection Data Form Schedule.** Using the Collection Data Form schedule deploys the form to all the workstations in the Management Zone.
- **Device Quick Task.** Using a device Quick Task deploys the Data Collection Form to one or more workstation in a folder.
- **Device Task.** Using a device task deploys the Data Collection Form to a specified workstation.
- **Scheduled as part of an inventory scan.** Using the inventory scan schedule deploys the Collection Data Form to all the workstations in the Management Zone.

Schedule the Deployment of the Collection Data Form

- Collection schedule can be set at the following levels:
 - Management Zone
 - Device Folder
 - Device
- Schedule Types
 - No Schedule
 - Date Specific
 - Recurring
 - Event

You can define the schedule at three levels:

- **Management Zone.** The settings are inherited by all device folders and devices.
- **Device Folder.** The settings are inherited by all devices in the folder. Overrides the settings at the Management Zone level.
- **Device.** The settings apply only to the device for which they are configured. Overrides the settings at the Management Zone level.

The following are the configuration options available:

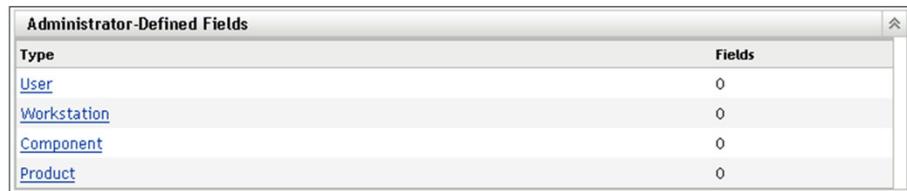
- **No Schedule.** No scan is scheduled.
- **Data Specific.** Scans run on specified dates.
- **Recurring.** Scans run on a recurring schedule.
- **Event.** Scans are triggered by an event.



Use Administrator-Defined Fields

Use Administrator-Defined Fields

- Administrator Fields allow you to add custom fields to inventory data
- Types of Administrator Defined Fields
 - User
 - Workstation
 - Component
 - Product



Type	Fields
User	0
Workstation	0
Component	0
Product	0

Administrator-defined fields allow you to add custom fields to inventory data. There are four types of fields:

- **User.** Used for gathering demographic data about the workstation user through the Collection Data Form.
- **Workstation.** Used for gathering demographic data about the workstation through the Collection Data Form.
- **Component.** Used for defining inventory data about a component.
- **Product.** Used for defining inventory data about a product.

Creating an Administrator-Defined Field

Regardless of the type of administrator-defined field you want to create, the steps are the same, whether it is a User, Workstation, Component, or Product field.

The User Fields panel shows existing defined fields, along with the following information:

- **Name.** The name of the field.
- **Data Type.** The data type: character, integer, decimal, or date.
- **Size.** The number of alphanumeric characters. This applies only to character-type fields.
- **Edit Type.** Specifies how the user enters a response. The values are Edit, List, and Combo.
- **Default Value.** The value that is specified when the field is created.
- **Internal Name.** The field's internal ID.

Use Inventory Reports

Reports allow you to view and analyze inventory data from your Management Zone. ZENworks Control Center includes predefined reports you can run along with reports you can customize.

Inventory Standard Reports

- Standard Reports are predefined reports that can not be modified
- Available in the following categories:
 - Device Lists
 - Software Applications
 - Software Files
 - Hardware Components
 - Upgrade Readiness
- Run reports from the ZCC

ZENworks Control Center includes several predefined reports you can use to analyze the inventory in your Management Zone. From the ZENworks Control Center, select **Reports**, then select a *folder* and then a *report* from the Inventory Standard Reports panel.

The reports are grouped into folders according to their function. The available folders and reports are as follows:

- **Device Lists (folder).** Reports focusing on device details.
 - **Devices by Machine / Login Name.** Lists all devices by machine and login name.
 - **Devices by Mfg / Model.** Shows a count of systems by manufacturer and model.
 - **Lease Details.** Shows leased devices by contract along with the expiration date.
 - **Devices with Virtual Machines.** Shows devices with host virtual machines that have been scanned.
 - **Duplicate Asset Tags.** Shows devices with duplicate asset tags.
 - **Duplicate Machine Names.** Shows devices with duplicate machine names.
 - **Duplicate Serial Numbers.** Shows devices with duplicate serial numbers.
- **Software Applications (folder).** Reports focusing on software applications.
 - **Antivirus Details.** Shows antivirus definition files with links to the devices where they are installed.
 - **Software Applications by Category.** Shows a count of installed software products grouped by category and subcategory.
 - **Software Applications by Manufacturer.** Shows a count of installed products

- grouped by manufacturer.
- **Software Applications by OS and Product.** Shows a count of installed products grouped by operating system and product name.
 - **Duplicate Serial Numbers.** Shows software products that have multiple instances of the same serial number.
 - **High Bandwidth Applications.** Shows a count of high-bandwidth products, such as multimedia and file-sharing software.
 - **Hot Fix Details.** Shows hot fixes and security patches with links to descriptions of the fixes and patches and the machine that they were installed on.
 - **Microsoft Products.** Shows a count of installed Microsoft products grouped by classifications specific to Microsoft.
 - **Operating Systems.** Shows a count of devices grouped by the installed operating system.
 - **OS Service Packs.** Shows a count of devices grouped by operating system and service pack.
 - **Software Files (folder).** Reports focusing on software files, grouping them by category, manufacturer, and device.
 - **Software Files by Category.** Shows a count of software files grouped by category (All, Other, Ancillary, and System) with links to lists of the files.
 - **Software Files by Manufacturer.** Shows a count of software files grouped by manufacturer with links to lists of the files.
 - **Software Files by Device.** Shows a count of software files grouped by device with links to lists of the files.
 - **Hardware Components (folder).** Reports focusing on hardware data.
 - **BIOS.** Shows installed versions and release dates grouped by manufacturer.
 - **Hardware Components by Category.** Shows a count of installed hardware products by category and subcategory.
 - **Hardware Components by Manufacturer.** Shows a count of installed hardware products grouped by manufacturer.
 - **Disk Space.** Shows a count of devices with total disk space within a specific range.
 - **Duplicate Serial Numbers.** Shows hardware products with the same serial number.
 - **Free Disk Space.** Shows a count of devices with free disk space within specific ranges.
 - **Memory Size.** Shows a count of devices grouped by RAM size.
 - **Processors.** Shows a count of devices grouped by CPU speed.
 - **Upgrade Readiness (folder).** Reports that help you determine which devices are ready for an upgrade.
 - **Memory Upgrade.** Lists devices along with data on memory and available slots.
 - **SLED 10 Ready / Not Vista Capable.** Shows devices ready for SUSE Linux Enterprise Desktop 10 that are not ready for Windows Vista.
 - **SLED 10 Ready / Not Vista Premium Ready.** Shows devices ready for SUSE Linux Enterprise Desktop 10 that are not ready for Windows Vista Premium.
 - **SUSE Enterprise Desktop.** Lists devices along with data showing whether the device is ready or not ready for SUSE Linux Enterprise Desktop.
 - **Windows 2003 Server.** Lists devices along with data showing whether the device is ready or not ready for Windows Server 2003.

- **Windows Vista Capable.** Shows devices capable of running Windows Vista.
- **Windows Vista Premium Ready.** Shows devices capable of running Windows Vista Premium.
- **Windows XP Professional.** Shows devices along with data showing whether the device is ready or not ready for Windows XP Professional.

Inventory Custom Reports

- Custom Reports can be created and modified by the administrator
- Several pre-defined custom reports are available
 - Can be modified
- Custom reports can be scheduled and the results emailed
- Custom report definitions can be exported as xml files and imported into another Zone

ZENworks Control Center allows you to create and run custom reports that you can use to analyze the inventory in your Management Zone.

Available Custom Reports

ZENworks Control Center includes several predefined reports you can use to analyze the inventory in your Management Zone. These reports are grouped into folders according to their function. The available folders and reports are as follows:

- **Hardware Components (folder).** Reports focusing on hardware components, such as BIOS and system details.
 - **BIOS and System Details.** Shows the BIOS details for all current systems.
 - **Hardware added or deleted in last 6 months.** Lists the hardware components in the Management Zone and shows the number of additions and deletions over the previous 6 months.
 - **USB devices added in last 30 days.** Shows the workstations that have had a USB device added in the previous 30 days.
 - **Workstations with memory deletions in last 30 days.** Shows the workstations that have had memory module deletions during the previous 30 days.
- **Local Product Creation (folder).** Reports focusing on software files that can be used to create Local Software Products.

WARNING: If you rename, move or delete the Local Product Creation folder or its contents, you will not be able to create the Local Software Products.

- **Software Files by Machine.** Shows the software files on each machine. You can use this report to create Local Software Products.

- **Unique Software Files.** Shows the software files along with Version Resource Block (VRB) data. You can use this report to create Local Software Products.
- **Software Applications (folder).** Reports focusing on software applications, such as how many applications were added during a specified time.
 - **SW apps added in last 30 days (by product).** Shows the software applications that were added during the previous 30 days, grouped by product.
 - **SW apps added in last 30 days (by workstation).** Shows the software applications that were added during the previous 30 days, grouped by workstation.
 - **SW apps deleted in last 30 days (by product).** Shows the software applications that were deleted during the previous 30 days, grouped by product.
 - **SW apps deleted in last 30 days (by workstation).** Shows the software applications that were deleted during the previous 30 days, grouped by workstation.
 - **Workstations with antivirus software.** Shows the Windows workstations (not marked as deleted) with antivirus software installed.
 - **Workstations with suspicious software installed.** Shows the workstations with suspicious software installed.
 - **Workstations without antivirus software.** Shows the Windows workstations (not marked as deleted) without antivirus software installed.
- **Systems (folder).** Reports focusing on system details, such as how many systems were added during a specified time.
 - **Hosts of Virtual Machines.** Shows the systems that are hosting virtual machines.
 - **Systems added in last 90 days.** Shows the systems (Windows, UNIX/Linux) that were added to the inventory database during the last 90 days.
 - **Systems deleted in last 90 days.** Shows the systems (Windows, UNIX/Linux) that were deleted during the previous 90 days.
 - **Systems that have not loaded results in 90 days.** Shows the systems (Windows, UNIX/Linux) that have not been marked as deleted and have not loaded scan results during the previous 90 days.
 - **Systems with less than 100 MB free space.** Shows the systems (Windows, UNIX/Linux) that have not been deleted and have less than 100MB free disk space.
 - **Systems with less than 128 MB memory.** Shows the systems (Windows, UNIX/Linux) that have not been deleted and have less than 128MB total memory.
 - **Virtual Machines.** Shows the virtual machines in your Management Zone.

Configuring E-mail Addresses

You can send notifications to selected people when a custom report is run. To do this, you need to import the e-mail addresses of those you want to notify into ZENworks Control Center.

The E-mail Addresses panel on the Configuration page allows you to import e-mail addresses that can be used to send notifications when a custom report is ready, as configured in the report definition. Previously imported e-mail addresses are listed in the panel, along with the user's first, last, and middle name.

Viewing Scheduled Reports by Date and Title

Reports that are run on a schedule are stored in a database. You can view these reports either by title or date.

The Scheduled Reports by Grouping page opens and shows the saved scheduled custom reports grouped by date or title and a report count. Select the date or title to open the **Scheduled Reports** page, where you can select a report and view it. To delete a group of reports, select the group and select **Delete**.

Importing New Report Definitions

If you have defined reports in ZENworks Asset Management 7.5, you can import them into ZENworks Control Center. You can also re-import reports that have been exported by ZENworks Control Center. A predefined XML format is needed for import.

Exercise 10-1

Configure Inventory Data Collection

In this exercise, you learn how to configure data collection features, and then perform scans of managed and unmanaged devices in your virtual network by doing the following:

- Configure Inventory Collection and Schedule
- Create Administrator-Defined Fields
- Configure Data Forms and Schedule
- View the Inventory of a Managed Device

Manage Linux Devices

Novell.

Objectives

- Deploy the ZENworks Adaptive (XPlat) Agent to Linux Devices
- Describe Linux Management Functionality
- Describe Linux Package Management
- Describe Linux Policy Management
- Describe Linux Remote Management

Deploy the ZENworks Adaptive (XPlat) Agent to Linux Devices

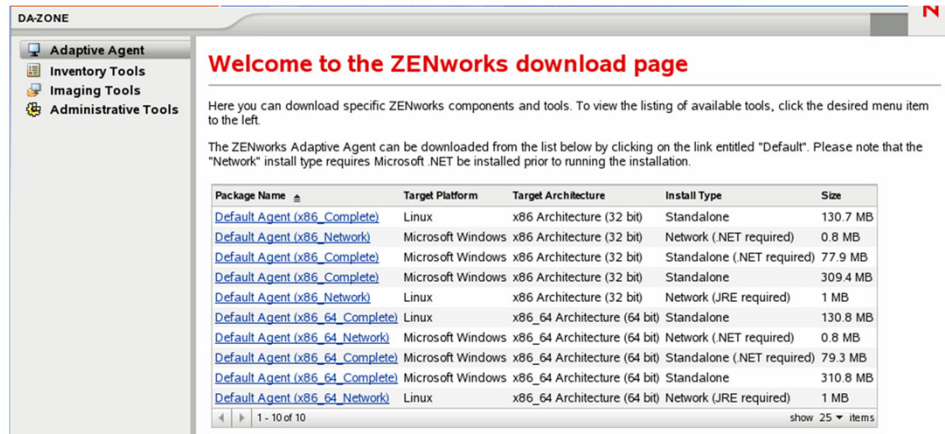
Deploy the ZENworks Adaptive (XPlat) Agent to Linux Devices

- ZENworks Adaptive Agent Packages
- XPlat Agent Packages
- XPlat Agent Installation
- XPlat Agent Deployment

Any devices you want to manage through ZENworks must have the ZENworks Adaptive Agent deployed to them. The Adaptive Agent distributes software, enforces policies, collects software and hardware inventory, monitors software usage and license compliance, and performs all other ZENworks management tasks on the managed device.

ZENworks Adaptive Agent Packages

- Six for Windows Platforms
- Four for Linux Platforms



Welcome to the ZENworks download page

Here you can download specific ZENworks components and tools. To view the listing of available tools, click the desired menu item to the left.

The ZENworks Adaptive Agent can be downloaded from the list below by clicking on the link entitled "Default". Please note that the "Network" install type requires Microsoft .NET be installed prior to running the installation.

Package Name	Target Platform	Target Architecture	Install Type	Size
Default Agent (x86_Complete)	Linux	x86 Architecture (32 bit)	Standalone	130.7 MB
Default Agent (x86_Network)	Microsoft Windows	x86 Architecture (32 bit)	Network (.NET required)	0.8 MB
Default Agent (x86_Complete)	Microsoft Windows	x86 Architecture (32 bit)	Standalone (.NET required)	77.9 MB
Default Agent (x86_Complete)	Microsoft Windows	x86 Architecture (32 bit)	Standalone	309.4 MB
Default Agent (x86_Network)	Linux	x86 Architecture (32 bit)	Network (JRE required)	1 MB
Default Agent (x86_64_Complete)	Linux	x86_64 Architecture (64 bit)	Standalone	130.8 MB
Default Agent (x86_64_Network)	Microsoft Windows	x86_64 Architecture (64 bit)	Network (.NET required)	0.8 MB
Default Agent (x86_64_Complete)	Microsoft Windows	x86_64 Architecture (64 bit)	Standalone (.NET required)	79.3 MB
Default Agent (x86_64_Complete)	Microsoft Windows	x86_64 Architecture (64 bit)	Standalone	310.8 MB
Default Agent (x86_64_Network)	Linux	x86_64 Architecture (64 bit)	Network (JRE required)	1 MB

1 - 10 of 10 show 25 items

XPlat Agent Packages

- *Default_Agent (x86_Complete Standalone)* and *Default_Agent (x86_64_Complete Standalone)* packages contain
 - All RPMs
 - JRE version 1.6
- *Default_Agent (x86_Network)* and *Default_Agent (x86_64_Network)*
 - Just the PreAgent
 - Device must have JRE 1.5 already installed

The following packages are available for installing the ZENworks Adaptive Agent on Linux:

- **Network (JRE required).** Contains only the pre-agent, which downloads the ZENworks Adaptive Agent files from the ZENworks Server. The network (JRE required) package requires that JRE 1.6 is installed on the device prior to the deployment of the agent to the device.
- **Standalone:** Contains the pre-agent, all the ZENworks Adaptive Agent module files, and the JRE 1.6 installables.

To support the various Linux architectures, there are three versions of each package:

- **x86 version.** You use the x86 version for manual deployment to 32-bit Linux devices. The x86 packages (PreAgentPkg_AgentLinux.bin and PreAgentPkg_AgentLinuxComplete.bin) are located in the following directory on the ZENworks Server:
 %ZENWORKS_HOME%\novell\zenworks\install\downloads\setup\x86 on Windows and /opt/novell/zenworks/install/downloads/setup/x86 on Linux.
- **x86_64 version.** You use the x86_64 version for manual deployment to 64-bit Linux devices. The x86_64 packages (PreAgentPkg_AgentLinux.bin and PreAgentPkg_AgentLinuxComplete.bin) are located in the following directory on the ZENworks Server:
 %ZENWORKS_HOME%\novell\zenworks\install\downloads\setup\x86_64 on Windows and /opt/novell/zenworks/install/downloads/setup/x86_64 on Linux.

- **All Architectures version.** This package is used by the ZENworks Server when completing a deployment task. It contains files for both 32-bit and 64-bit Linux devices.
The All Architectures packages (PreAgentPkg_AgentLinux.bin and PreAgentPkg_AgentLinuxComplete.bin) are located in the following directory on the ZENworks Server:
%ZENWORKS_HOME%\novell\zenworks\install\downloads\setup_all on Windows and
/opt/novell/zenworks/install/downloads/setup/_all on Linux.

XPlat Agent Installation

- Packages are installed over SSH
- Either a **Linux Primary Server** or a **Windows Primary Server** can push out the XPlat Agent
 - Possible on Windows because Open Source SSH is installed when ZCM 11.2 is installed

7

© Novell, Inc. All rights reserved.

Before the ZENworks Server can deploy the ZENworks Adaptive Agent to a Linux device, make sure that SSH Port 22 is open. To open SSH port 22 use the following procedures to add SSH as an allowed service on the target device.

To add SSH as an allowed service on Red Hat Enterprise Linux (RHEL):

1. Edit `/etc/sysconfig/iptables` to append the following rule:
`-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT`
2. Save the `iptables` file.
3. Restart the `ip` tables service by running either the `service iptables restart` command or the `/etc/init.d/iptables restart` command.

To add SSH as an allowed service on SUSE Linux Enterprise Server (SLES) and SUSE Linux Enterprise Desktop (SLED):

1. Edit the following file:
`/etc/sysconfig/SuSEfirewall2`
2. Add SSH to the list of ports under `FW_SERVICES_<Firewall Zone>_TCP`.
 For example, for an external zone, add SSH under
`FW_SERVICES_EXT_TCP="ssh"`.
3. Run the following command:
`/sbin/SuSEfirewall2.`

XPlat Agent Deployment

Push Deployment

- You can use a Deployment Task like that of previous versions of ZCM (for Windows devices), but
 - If deploying to a machine not running X Windows, select **Do not install the GUI Packages**
 - Otherwise install will fail with dependency errors
 - If deploying to a RHEL 4 or 5 box running SELinux, select **Disable SELinux for Red Hat**
 - Will shut down this service, do the install, and then restart SELinux

The Linux Options page lets you configure the installation options to make the ZENworks Adaptive Agent functional after the installation of the agent on the Linux devices.

- **Deployment Package.** Depending upon the processor architecture of the managed device, select the deployment package to be used for installing ZENworks Adaptive Agent on the device. If you are not sure about the device's processor architecture, choose the package with target architecture as All, which applies to 32-bit and 64-bit platforms. If the selected package has been deleted from the Primary Server, then the default deployment package is deployed.
- **Installation Options.** Configure the following options for deploying the ZENworks Adaptive Agent:
 - **Do Not Install the GUI Packages.** Select this option if you do not want to install the RPMs that provide a GUI interface for the ZENworks Adaptive Agent such as the icon.
 - **Disable SELinux for Red Hat Devices.** Select this option to disable SELinux (Security-Enhanced Linux).

SELinux provides limited access control on Linux. Select this option to disable SELinux if the agent is unable to open the ports required by ZENworks. SELinux is temporarily disabled only if the agent is unable to open the ports, and is automatically enabled again after the agent installation.

NOTE: The Linux Options page is displayed only if you have provided Linux credentials on the Enter Credentials page.

XPlat Agent Deployment

Push Deployment

• Configure a Deployment Task

Deploy Device Wizard **Deploy-to-Linux**
Step 7: Linux Options

Deployment Package

Depending upon the processor architecture of the managed linux device, choose the deployment package to be used for installing ZENworks Adaptive Agent on the device. If you are not sure about the device's processor architecture, choose the package with target architecture as All, which applies to 32-bit and 64-bit platforms. If the selected package has been deleted from the Primary Server, then the default deployment package is deployed.

Default Agent (Target Architecture : All, Install Type: Standalone)

Installation Options

Select this option if you do not want to install the GUI packages of ZENworks Adaptive Agent.

☐ Do Not Install the GUI Packages

Select this option to disable SELinux. SELinux is disabled if any rpm included in the deployment package fails to install.

☐ Disable SELinux for Red Hat Devices

Check this box if pushing XPlat Agent to a box that is not running X Windows.

Check this box if pushing XPlat Agent to Red Hat box running their SELinux Services.

XPlat Agent Deployment

Pull Deployment

- Launch the browser and enter the zenworks-setup page URL to run the .bin file manually
- Leverage the `/opt/novell/zenworks/share/tomcat/webapps/zenworks-agent-addon` directory on the Primary Server
- Directory contains
 - An Initial Web Service File used for Registration
 - ZYPP Repositories for SLE10 and SLE11
 - Used to create a YaST Add-on to install the XPlat Agent
 - YUM Repositories for Red Hat 4 and 5
- Directory maintained by System Update

10

© Novell, Inc. All rights reserved.

Instead of having a ZENworks Server deliver the Adaptive Agent to a device, you can manually download the Adaptive Agent deployment package from the server and install the agent.

1. Make sure the device meets the necessary requirements (see “Managed Device Requirements” in the *ZENworks 11 SP2 Server Installation Guide*).
2. On the target device, open a Web browser and access the following address:

<http://server:port/zenworks-setup>

Replace **server** with the DNS name or IP address of a ZENworks Server and replace the **port** only if the ZENworks Server is not using the default port (80 or 443).

The Web browser displays a list of deployment packages. For each architecture (32-bit and 64-bit), there are two types of packages:

- **Network (JRE required).** The network (JRE required) package installs only the pre-agent on the target device; the pre-agent then downloads and installs the ZENworks Adaptive Agent from the ZENworks Server. The network (JRE required) package requires that JRE 1.6 or later is installed on the device prior to the deployment of the agent on the device.

NOTE: It is required to install only Sun’s Java Runtime Environment (JRE) on the Linux managed devices for the ZENworks Adaptive Agent to work.

- **Standalone.** The standalone package installs the pre-agent and extracts all executable files required for Adaptive Agent installation, including the JRE installer on the target device. The pre-agent then installs the Adaptive Agent from the local device. The standalone package is useful when you need to install the ZENworks Adaptive Agent on a device that is currently disconnected from the

network. You can save the package to removable media (CD, USB flash drive, and so on) and have the standalone device run the package from the media. The Adaptive Agent is installed on the device, but no registration or management occurs until the device connects to the network.

- **Custom.** The package name, Default Agent, refers to predefined deployment packages. The custom deployment packages created through Deployment > Edit Deployment Package are shown with the name assigned during the creation of the package.
3. Click the name of the deployment package you want to use, save the package to the local drive of the device, then assign executable permissions to the file by running the command `chmod 755 filename`.
 4. (Optional) On a RHEL device, run the following command:
chcon -u system_u -t rpm_exec_t filename
 5. In the terminal window, go to the directory where you have downloaded the package, then launch the package on the device by running the command `./filename`, where **filename** is the name of the package you downloaded in Step 3.
 6. (Conditional) If you want to view the ZENworks notify icon in the notification area after agent installation for the Linux device, log out of and log in to the device.

In ZENworks Control Center, the device appears in the \Servers folder or \Workstation folder on the Devices page.

NOTE: After deploying the ZENworks Adaptive Agent on Linux device, `/opt/novell/zenworks/bin` is not added to the PATH variable and hence the commands in that directory cannot be used directly. Do any of the following on the Linux device to run the commands from `/opt/novell/zenworks/bin`:

- Relogin to the device.
- Specify the complete path to access the command.

For example: `/opt/novell/zenworks/bin/zac`.

Describe Linux Management Functionality

Describe Linux Management Functionality

- Discovery and Deployment
- NAL Windows for Linux
- Linux Imaging
- Linux Devices Inventory
- Linux Policy Management
- Linux Bundle Types

Discovery and Deployment

- SSH and SNMP are the supported protocols
 - SSH allows more information to be gathered about the device
 - Such as being able to use `uname` to get kernel version information
- Support for Linux Proxy Devices
 - Linux Proxy lets you discover Linux devices that are on the far side of a firewall from the Primary Server
 - Linux Proxy supports SSH and SNMP as well as ICMP and ARP
 - All discovery and deployment messages are logged by the Linux Proxy in the **zmd-messages.log** file

SNMP and Linux

SNMP issues a request to the SNMP service on the devices identified by the IP-based discovery task. SNMP versions 2 and 1 are supported, with SNMP version 2 tried first. Retrieves the OS type and version, MAC address, Network Adapters, and CPU details

Because the discovery process uses Windows-based SNMP technology, requests generated from a ZENworks Server running on Linux must be routed to a Windows Proxy for processing.

Linux Proxy Devices


You can select a Linux managed device (server or workstation) to be used as a Linux Proxy for performing the discovery and deployment tasks instead of a ZENworks Server. The Linux Proxy must reside in the same network as the target devices.

A Linux Proxy is primarily used for Primary Servers if you want to deploy to Linux devices in a different subnet than the Primary Server. When a Primary Server receives a deployment task that includes devices in a different subnet, it offloads the deployment tasks to the Linux Proxy. A Linux Proxy is also used for performing deployment tasks on Linux devices in a network enabled for NAT.

The SSH discovery requires port 22 to be reachable in order to enable the Primary Server to connect to the target device. If the SSH port is blocked in the Network Firewall, you use a Linux managed device in the same subnet as the target device.

The connection between the ZENworks Server and Linux Proxy is secured through SSL.

NAL Windows for Linux

- NALWIN binary located in **/opt/novell/zenworks/bin**
- Launch NALWIN
 - Right-click  and select **ZENworks Window**
 - Click the **Computer** button, then select **More Applications > System > NAL**
- Capabilities of NAL for Linux
 - Doesn't integrate with Nautilus the way NALWIN integrates with Windows Explorer
 - Can't make NAL for Linux the sole desktop shell like in Windows

NALWIN (NALWIN.exe) is the shortcut command for launching the ZENworks Application Window on a Windows Managed Device in ZENworks Configuration Management.

There are various options that can be used with the NALWIN Command that help the user launch the ZENworks Application Window in various modes.

- **NALWIN /?**
Displays a list of options available with NALWIN in a small Help Console.
- **NALWIN /S**
Launches the ZENworks Application in a Shell (or Silent Mode). The user will not be allowed to close the window. The “X” button of the window will be grayed out. The user has to either logout from the machine or kill the NALWIN.exe process from the Task Manager.

This option can be used when the Administrator wants the logged-in users to be disallowed from closing the ZENworks Application Window.
- **NALWIN /C=”Custom Title Message”**
This option allows the user to launch the ZENworks Application Window with a Title Message of his / her choice. For example, NALWIN /C=”This is your Application Window” will launch a console.
- **NALWIN /MIN**
Launches the ZENworks Application Window in Minimized mode.
- **NALWIN /MAX**
Launches the ZENworks Application Window in Maximized mode.

- **NALWIN /NORM**

Launches the ZENworks Application Window in Normal mode.

- **NALWIN :**

Launches the ZENworks Application Window without displaying the Splash Screen that's popped by default (before launching).

Linux Imaging

- Support for imaging LVM Partitions
 - Can image up to four physical drives in one LVM volume
 - Images Reiser, EXT2, or EXT3 file systems within the LVM volume
 - Supports the imaging of LVM Groups


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

- Make an image of the device's hard drives and other storage devices
- Restore an image to the device
- Apply an existing image to multiple devices
- Run Imaging scripts on the device
- Run AutoYaST and kickstart installations
- Configure Dell devices

Support for imaging LVM Partitions includes the following:

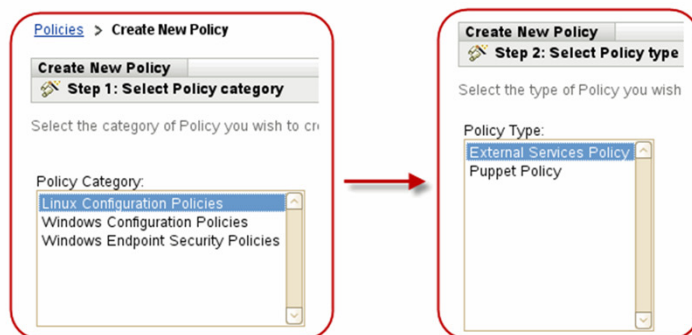
- You can image up to four physical drives in one LVM volume
- Images Reiser, EXT2, or EXT3 file systems within the LVM volume
- Supports the imaging of LVM Groups

Linux Devices Inventory

- New *Collection Data Form* (CDF) like that in ZAM and ZCM for Windows Devices
- CDF access
 - Manually from 
 - Command: **zac inv cdf**
 - As part of the scheduled scan process
- Inventory information captured for Linux
 - Installed RPMs
 - Hardware information via **hwinfo**

Linux Policy Management

- Reflects emphasis of managing Linux Servers rather than Linux Desktops
- Linux Management Policies implemented in ZCM 11.2
 - External Services Policy
 - Puppet Policy



Linux Configuration Policies let you configure policies supplied by ZENworks Configuration Management that are used to manage configuration settings for Linux devices.

The following policies are located in this category:

- **External Services policy**

The External Services policy lets you configure the external services on a Linux managed device for YUM, ZYPP or MOUNT repositories. It enables you to download and install the software packages or updates from these repositories on the managed devices.

- **Puppet policy**

The Puppet policy lets you apply the Linux configuration on the Linux devices.

Linux Bundle Types

- **Linux Bundle**
 - Exists in a default ZCM Installation
 - Categories of Linux Bundles -
 - “Empty Bundle, “Create/Delete Directory”, “Install Directory”, “Install File(s)”, “RPM Application
 - “Empty Bundle” has all the Action Sets: Distribute, Install, Launch, Verify, Uninstall, and Terminate
- **Linux Dependency Bundle**
 - Exists in a default ZCM Installation
 - Only used for dependency resolution
- **Linux Patch Bundles**
 - Will only exist if the zone is licensed for Patch Management

The Linux Package Management features lets you create the Linux bundles and the Linux Dependency bundles by using Subscriptions, by using the bundle wizard in ZENworks Control Center, or by using the zman command line utility.

You can create two types of bundles on Linux devices - Linux bundles and Linux Dependency bundles. Linux bundles allow you to configure, manage applications, and store the package updates on Linux devices. Linux Dependency bundles allow you to distribute software to Linux devices and provide the dependent packages.

For more information on how to create these bundles, see “Using Bundles for Linux Devices” in the *ZENworks 11 SP2 Linux Package Management Reference*.

Linux Dependency Bundles

You can create Linux Dependency bundles to store the dependency packages in order to resolve package dependencies on the managed device.

Linux Dependency bundles cannot be installed on a device by using the zac bundle-install command. However, on the agent, you can install packages from a Linux Dependency bundle by using the zac install command if the Publish Package flag is set to true for those packages. The agent command to list the packages of a bundle does not list any package for the Linux Dependency bundles unless the Publish Package flag is set to true for the package.

Linux Patch Bundles

You can replicate patches from remote update repositories to create Patch bundles. If you want to replicate only the patches of a selected category, you can use category-based filters.

Describe Linux Package Management

Describe Linux Package Management

- Linux Bundles
- Subscriptions
- Patch Management and Subscription

Linux Bundles

Overview

- Can be “pushed” to force the install of one or more RPM packages
- Has the same Action Sets and Actions as a Windows Bundle
- Includes **Install RPM(s) Action** with the following options:
 - **Set Freshen only**
 - Installs RPM if its newer than what's already on managed device
 - **Install File (or Directory)**
 - Lets you set file system permissions

ZENworks 11 SP2 Configuration Management lets you efficiently deliver RPM-based software. Additionally, because Linux uses the bundle management framework in ZENworks Configuration Management, you can now perform additional configuration tasks, deploy additional files and directories, and execute scripts.

Action Sets and Actions

The Actions panel displays the action sets available for the bundle. The action sets available for Linux Bundles are Distribute, Install, Launch, Verify, and Uninstall. The action set available for Linux Dependency Bundles is Distribute.

You can add an action to any of the available action sets. When you do so, that action is performed whenever the action set is applicable. For example, when you add an action to the Install action set, that action is performed whenever the bundle is installed.

Install RPMs Action

The Action - Install RPMs dialog box lets you enable the install options and add packages. You can also specify parameters such as Freshen and Install Type for the files.

Set Freshen checks if the previous version of the package is installed to upgrade the package to the newer version. Selecting this action displays Yes in the Freshen column of the selected package.

Linux Bundles

Linux Dependency Bundles (LDBs)

- Equivalent to a Catalog in ZLM
 - Used only for resolving dependencies when installing software
- Has one Action Set with only a **Distribute RPM** Action
- Repository Types supported with LDBs
 - ZCM
 - YUM (used for Red Hat)
 - ZYPP (used for all SUSE-based distros)
- Linux Bundles generally created for
 - Supported distros
 - Major packages like mono or samba

You can create Linux Dependency bundles to store the dependency packages in order to resolve package dependencies on the managed device.

Linux Dependency bundles cannot be installed on a device by using the `zac bundle-install` command. However, on the agent, you can install packages from a Linux Dependency bundle by using the `zac install` command if the Publish Package flag is set to true for those packages. The agent command to list the packages of a bundle does not list any package for the Linux Dependency bundles unless the Publish Package flag is set to true for the package.

NOTE: You cannot assign any schedules while assigning Linux Dependency bundles to devices.

Linux Bundles

YUM Repository

- Any Linux Bundle or LDB can create
 - A **YUM Repository** on the Primary based on all the packages in the bundle
- YUM Repo created in
 - **/var/opt/novell/zenworks/yum-repo**
- Allows devices without XPlat Agent to access the content with a
 - YUM Client
 - ZYPP Client
 - RUG Client

The RPM packages in the ZENworks package repository are published in a format that can be used only by the ZENworks Agent. In other Linux distributions, some package management tools like YaST, ZYpper, and YUM cannot understand this package repository format of the ZENworks Server, so they cannot access the necessary packages. In order to make the ZENworks published packages available to these package management tools, you can export the packages in a bundle to a YUM repository and publish the YUM repository on any ZENworks Server. You can then add the YUM repository to YaST, ZYpper, or YUM, or to any tool that understands the format of the YUM repository, and make use of the packages on the ZENworks Server.

You can also create a YUM service for bundle groups. Each bundle in the group is created as a patch in the exported YUM service.

NOTE: If you create a YUM repository from a bundle, this new YUM repository will contain only packages. If you create a YUM repository from a bundle group, this new YUM repository will contain both packages and patches, with each patch corresponding to a member bundle of the bundle group. YUM repositories created by ZENworks do not support patterns.

You can create a YUM service for a published version (not a sandbox version) of a Linux bundle or a Linux Dependency bundle.

Subscriptions

Overview

- Equivalent to ZLM Mirror capability in ZLM but with a GUI front-end
 - A location from which content can be downloaded
 - Subscriptions always end up creating bundles in the zone
- A Subscription creates
 - One or more LDBs or Linux Bundles
 - Bundle Groups or Folders

The Subscriptions feature in ZENworks 11 SP2 Configuration Management makes it easy to set up a subscription to repositories such as Novell Update, Red Carpet Enterprise, or other external repositories, and replicate content to the ZENworks Primary Servers. The managed devices can obtain the updates directly from the ZENworks Server instead of obtaining them from the remote repositories. ZENworks 11 SP2 Configuration Management provides an easy-to-use graphical user interface to create these subscriptions. You can also specify a schedule to run the subscription replication.

Overview

ZENworks 11 SP2 Configuration Management lets you use subscriptions to replicate content from NU, RCE, RHN, YUM or RPM-MD (authenticated and unauthenticated), ZENworks Linux Management, and Static repositories.

Subscriptions help you to obtain most of the software you want to distribute to managed devices. You can create subscriptions to:

- Select the targets for which to replicate the content and create bundles.
- Replicate content and create Linux bundles to deploy the software to managed devices.
- Replicate content and create Linux Dependency bundles to make the software packages available to the managed devices to resolve package dependencies.
- Download the source RPMs from remote repositories and create monolithic Linux bundles.
- Replicate patches from remote update repositories to create Patch bundles. If you want to replicate only the patches of a selected category, you can use category-based filters.

Subscriptions

Subscription Types

Subscription Type	Description
Novell Subscription	For YUM Repos or accessing the NCC
RCE Subscription	For Red Carpet ZLM 6.x servers
RHN Subscription	For Red Hat's patch Network Service
RPM-MD Subscription	Use for any YUM repository
STATIC Subscription	For "Air gap" patching environments
ZLM Subscription	For ZLM 7.x patch services

Subscription Types

The following types of subscriptions are available in Linux Package Management:

Novell Subscription. Allows you to select subscriptions that you are entitled to download from Novell Customer Center based on your credentials. By using this subscription, you can replicate updates for SUSE Linux Enterprise 10 Service Pack 1 or later distributions, all SUSE Linux Enterprise 11 distributions, and OES 2 distributions. You can create bundles in your Management Zone with the replicated content.

- **RCE Subscription.** Allows you to select subscriptions that you are entitled to download from Novell Customer Center based on your credentials. By using this subscription, you can replicate updates for SUSE Linux Enterprise 10. You can also create bundles in your Management Zone with the replicated content.
- **RHN Subscription.** Allows you to replicate content from the Red Hat network for Red Hat Enterprise Linux distributions.
- **RPM-MD Subscription.** Allows you to replicate subscriptions and packages from both authenticated and unauthenticated RPM-MD (YUM) repositories.
- **Static Subscription.** Allows you to replicate content from the file system located on your local server and create bundles. You must have a static replication source available in the file system. You can create the static replication source by using the static replication option from any other subscription type.
- **ZLM Subscription.** Allows you to select subscriptions that you are entitled to download from the ZENworks Linux Management server based on your credentials. You can use these subscriptions to create bundles in your Management Zone.

Patch Management and Subscriptions

- Patching Options
 - Via Subscription capability and the LDBs generated by the Subscription process
 - ZENworks Patch Management
- Considerations
 - ZPM only creates Linux Patch Bundles
 - Can't be used for dependency resolution
- ZPM wrapper program doesn't understand Delta RPMs
 - Used by our SUSE distros

RPM Dependency

The RPM package manager (RPM) is a new feature which will only be enabled when you select the operating system platform for Linux. Now you can select the Linux check box, then you can select the Resolve all RPM Dependencies to download all the patches.

The option should only be selected if you want to resolve all the root level dependency as it is very time consuming and performance intensive. It will download all the RPM that are required to patch the particular vulnerabilities.

This is an improvement compared to the previous version. By default it will only download the RPM files required at the top level unless you select the check box to resolve the RPM dependencies.

Patch Subscription Credentials.

The Patch Subscription Credentials page allows you to specify the network credentials associated with Linux subscription providers such as Red Hat and SUSE. Credentials are stored in the Credential Vault and are used by actions and tasks that require authentication to access a particular resource. If you do not specify the patch subscription credentials, you cannot successfully download and install patches for your Red Hat and SUSE servers and agents.

Patch Management and Subscriptions

(continued)

- Recommendations

- Use Patch Management if
 - Customer needs full Linux Management capabilities
 - You only want to patch a device and report on what patches are installed
- Use ZCM 11.2 Subscription model if you
 - Need to leverage dependency resolution provided by LDBs
 - Need to leverage SUSE Delta RPMs
 - Want full Linux Management (Policies, Imaging, Remote Management...)
 - Need to access patch repos for things other than SLES, SLED, & Red Hat
 - Such as some kind of Open Source YUM repository

Describe Linux Policy Management

Describe Linux Policy Management

- External Services Policy
- Linux Puppet Policy

External Services Policy

Overview

- XPlat Agent lets you define “external sources”
 - Populates Agent's SQL Lite database with a pointer to a source of content outside ZCM Content Repository
- Use cases
 - Using AutoYaST to install OS and XPlat Agent is installed as part of this process
 - When Agent refreshes after installation the External Services Policy is effective making that content that is outside the ZCM Content-repo available to the device
 - May already have ZYPP Repository set up in your environment.
 - External Services Policy can be used to point XPlat Agent to that repository
 - RPMs don't have to be uploaded in the ZCM Content Repository

External Services Policy

Configuration

- External Services Policy configuration requires
 - External Source name
 - External Source URL
 - External Source type
 - ZYPP
 - YUM
 - MOUNT
 - AUTO
 - External Source access credentials

Linux Configuration Policies let you configure policies supplied by ZENworks Configuration Management that are used to manage configuration settings for Linux devices.

The following policies are located in this category:

- **External Services policy**

The External Services policy lets you configure the external services on a Linux managed device for YUM, ZYPP or MOUNT repositories. It enables you to download and install the software packages or updates from these repositories on the managed devices.

Linux Puppet Policy

Definition

- Open Source Change Management Framework designed for the Data Center
- Can establish and enforce approved system configurations by automatically correcting systems that drift from their baseline
- Can provide an audit trail of the changes to your servers
- Uses a declarative language (Ruby) to define a system's configuration so that configuration can be reproduced on other systems

Puppet policy

The Puppet policy lets you apply the Linux configuration on the Linux devices.

Linux Puppet Policy

Use Cases and Recommendations

- Use Cases

- Changing configuration files of a server-based service like FTP or SAMBA
- Seeing if services are installed, or starting and stopping services

- Recommendations

- We implement it much like a bundle
 - The XPlat Agent has a component that enforces the Puppet Template (manifest)

Linux Puppet Policy Configuration

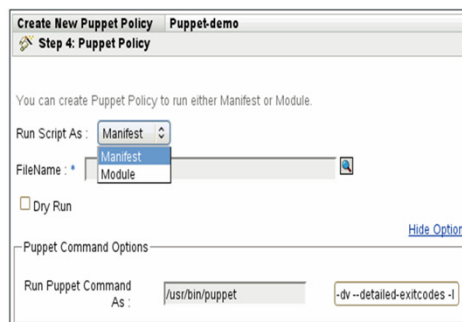
- Run script as **Manifest** or **Module**

- Manifest

- Manifest file name (.pp file)
 - Whether or not to do a “dry run”

- Module

- Module Name
 - Name of file containing module.
 - .zip, .tar, .tar.gz, .bz2, or .tgz format
 - File contains the manifest
 - Whether or not to do a “dry run”



Describe Linux Remote Management

Describe Linux Remote Management

- What You Can Do With Remote Management in Linux
- Remote Operations on a Linux Device

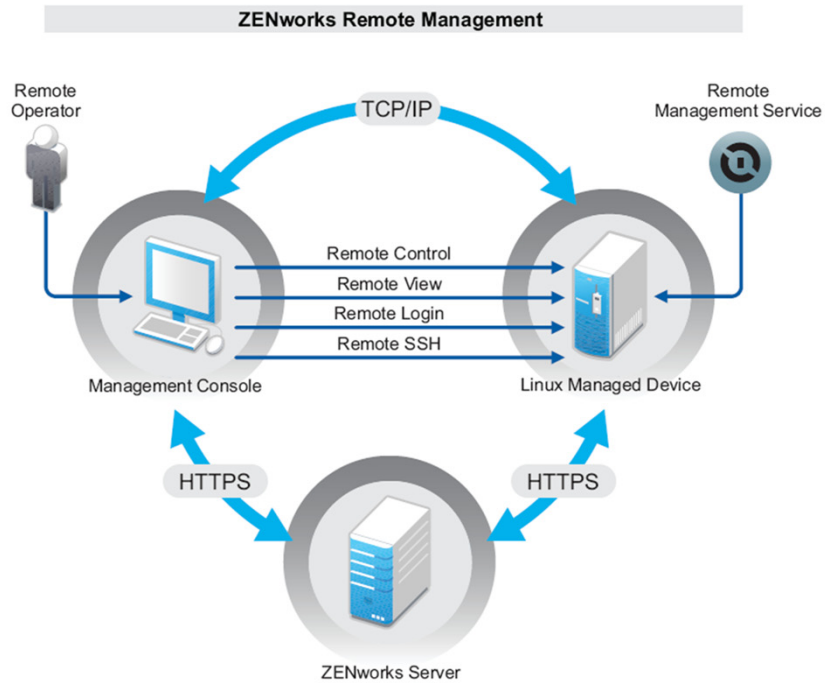
What You Can Do With Remote Management in Linux

- Remote Control
- Remote execute commands
- Remote Log in
- Remote Wake-up

With Remote Management, you can do the following on a Windows device:

- Remotely control the managed device
- Remotely wake up a powered-off managed device
- Remotely Log in to the managed device and start a new graphical session without disturbing the user on the managed device
- Remotely execute commands on a managed device through SSH

Remote Operations on a Linux Device



Remote Operations on a Linux Device

(continued)

- Remote Control
 - Remote control the managed device from the console
- Remote View
 - Remotely connect and view the managed device
- Remote Login
 - Login to managed device and start a new graphical session
- Remote Execute (SSH)
- Remote Wake Up
 - Remote wake up a single device or a group

39

© Novell, Inc. All rights reserved.

- **Remote Control**

Remote Control lets you remotely control the managed device from the management console so that you can provide user assistance and help resolve the device's problems.

Remote Control establishes a connection between the management console and the managed device. With remote control connections, you can perform all the operations that a user can perform on the device.

- **Remote View**

Remote View lets you remotely connect with a managed device so that you can view the managed device instead of controlling it. This helps you troubleshoot problems that the user encountered. For example, you can observe how the user at a managed device performs certain tasks to ensure that the user performs the task correctly.

- **Remote Login**

Remote Login lets you log in to a managed device from the management console and start a new graphical session without disturbing the user on the managed device; however, the user on the managed device cannot view the Remote Login session. You must log into the device with a non-root user credentials. This operation is supported only on a Linux managed device.

- **Remote SSH**

Remote SSH lets you securely connect to a remote Linux device and safely execute commands on the device. To launch a Remote SSH session from a Management Console device, JRE version 1.5 or higher must be installed on the device.

- **Remote Wake Up**

Remote Wake Up lets you remotely wake up a single node or a group of powered-down nodes in your network provided the network card on the node is enabled for Wake-on-LAN.

Exercise 11-1

Manage Linux Devices with ZENworks 11.2 Configuration Management

In this exercise, you complete the following tasks:

- Manually Deploy the ZENworks Adaptive Agent on a Linux Server
- Deploy the ZENworks Adaptive Agent Using a Pull Method
- Deploy the ZENworks Adaptive Agent Using a Deployment Task
- Create and Deploy RPM-based Applications