

System Planning, Deployment, and Best Practices Guide

ZENworks® 11 Support Pack 2

May 17, 2012

Novell.

Legal Notices

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

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

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. 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 © 2007-2012 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.

About This Guide

The purpose of this *System Planning, Deployment, and Best Practices Guide* is to describe the items that need to be considered when designing a Novell ZENworks 11 SP2 solution and deploying it across small and large scale enterprises.

The information in this guide is organized as follows:

- ♦ Chapter 1, “ZENworks Configuration Management: A Single Solution for Systems Management,” on page 9
- ♦ Chapter 2, “Performing Pre-Design Activities,” on page 15
- ♦ Chapter 3, “Gathering Critical Information for Design Activities,” on page 21
- ♦ Chapter 4, “Performing Design Activities,” on page 69
- ♦ Chapter 5, “Deploying ZENworks Configuration Management,” on page 127
- ♦ Chapter 6, “Best Practices for Deploying ZENworks on a Citrix Server,” on page 149
- ♦ Chapter A, “ZENworks Services,” on page 155
- ♦ Chapter B, “The ZENworks Configuration Management Architecture,” on page 165
- ♦ Appendix C, “Reference Materials,” on page 173

Audience

This guide is intended for ZENworks administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation.

Additional Documentation

ZENworks Configuration Management is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the [ZENworks 11 SP2 documentation \(http://www.novell.com/documentation/zenworks11/\)](http://www.novell.com/documentation/zenworks11/).

Contents

About This Guide	3
1 ZENworks Configuration Management: A Single Solution for Systems Management	9
1.1 The Goal: Total Management, Zero Effort	9
1.2 The Management Paradigm	10
1.2.1 Management by Exception	10
1.2.2 User-Based Management	11
1.2.3 Device-Based Management	11
1.2.4 Location-Based Management	12
1.3 The Solution: ZENworks Configuration Management	12
1.4 Additional ZENworks Products	13
1.4.1 ZENworks Application Virtualization	13
1.4.2 ZENworks Endpoint Security Management	13
1.4.3 ZENworks Patch Management	13
1.4.4 ZENworks Asset Management	14
1.4.5 Novell Service Desk	14
1.4.6 ZENworks Full Disk Encryption	14
2 Performing Pre-Design Activities	15
2.1 Perform a Business Assessment	15
2.2 Perform a Technical Assessment	16
2.3 Gather Other Critical Information	17
2.4 Develop High-Level Design	18
2.5 Develop Documentation	18
2.6 Outputs from Pre-Design Activities	19
3 Gathering Critical Information for Design Activities	21
3.1 Design Criteria/Decisions	21
3.1.1 Decisions to Make Before Installing the Primary Server	21
3.1.2 Infrastructure Placement	25
3.1.3 Infrastructure Scale Assumptions	26
3.2 Scalability of the Primary Server	26
3.2.1 Factors Influencing Scalability	27
3.2.2 Load Testing in the Novell SuperLab	27
3.2.3 Achieving Scalability in the Real World	30
3.2.4 Tuning the JVM and Tomcat	31
3.3 Scalability of Satellite Devices	34
3.3.1 Factors Influencing Scalability	34
3.3.2 Load Testing in the Novell SuperLab	34
3.3.3 Achieving Scalability in the Real World	36
3.4 ZENworks Database	37
3.4.1 Virtualizing the ZENworks Database Server	37
3.4.2 ZENworks Database Scalability	37
3.4.3 Saving the ZENworks Database Password	38
3.4.4 Sybase	38
3.4.5 Using Sybase Mirroring to Enable High Availability of the Sybase Database	51
3.4.6 Microsoft SQL Server	53

3.4.7	Oracle	59
3.4.8	Database Sizing and Performance Considerations	61
3.5	Virtualization Considerations	62
3.6	Ports Used by ZENworks Components	63
3.7	Network Considerations	65
3.7.1	Infrastructure vs. Bandwidth: Satellite Devices	65
3.7.2	DNS and DHCP Services	67
3.7.3	Time Synchronization	68
3.7.4	Support for the NetWare Operating System	68

4 Performing Design Activities **69**

4.1	Design Workshops	69
4.2	Developing a Detailed Design	71
4.2.1	Locations and Network Environments	71
4.2.2	Tuning Adaptive Agent Parameters for Slow Links	75
4.2.3	Linux Subscription Options	77
4.2.4	Device Folder and Group Structures	80
4.2.5	User Sources	81
4.2.6	Role-Based Administrative Accounts	83
4.2.7	Licensing ZENworks Components	84
4.2.8	Configuration Settings for the Management Zone	85
4.2.9	Device Discovery	93
4.2.10	Adaptive Agent Deployment	95
4.2.11	Registration Rules and Keys	98
4.2.12	Remote Management	100
4.2.13	Inventory	102
4.2.14	Application Management	103
4.2.15	Policy Management	108
4.2.16	Linux Patch Management	111
4.2.17	Imaging	112
4.2.18	Configuring a Layer 4 Switch	112
4.2.19	ZENworks System Update	114
4.2.20	Content Management	115
4.2.21	Offline Content Replication and Management	121
4.2.22	Satellite Authentication Role	122
4.3	Lab Testing and Validation	124
4.4	Documentation	125

5 Deploying ZENworks Configuration Management **127**

5.1	New ZENworks Customer	127
5.1.1	Building a Model Office Environment	128
5.1.2	Planning a Deployment	130
5.1.3	Deploying the Product	131
5.2	Migrating from a Previous Version of ZENworks	133
5.2.1	Application Deployment Strategy	133
5.2.2	Application and Policy Migration	134
5.2.3	Active Directory	134
5.2.4	Repurposing Hardware Used by Previous ZENworks Products	134
5.2.5	Introducing ZENworks Patch Management to an Existing ZENworks Zone	134
5.3	Pre-Deployment Planning	139
5.4	Pre-Deployment Documentation	139
5.5	Deployment Rules of Thumb	140
5.5.1	Scenario 1: One Major Location with 1, 500 Devices	140
5.5.2	Scenario 2: One Major Location with Several Remote Locations and More Than 1,500 Devices	140
5.5.3	Scenario 3: ZENworks 7 Migration to ZENworks 11	142

5.6	Pre-Deployment Testing	144
5.7	Pilots	144
5.8	Migration	145
5.9	Wider Deployment	147
5.10	Post-Deployment Documentation and Validation	147
6	Best Practices for Deploying ZENworks on a Citrix Server	149
6.1	Understanding the Need for Integrating ZENworks and the Citrix Server	149
6.2	Gathering Critical Information for Design Activities	150
6.2.1	Performing a Technical Assessment	150
6.2.2	Factors Influencing Scalability	151
6.2.3	Scale Numbers	151
6.2.4	Ports Used by the ZENworks Agent	151
6.3	Performing Lab Tests and Validation	152
6.4	Deploying the ZENworks Configuration Management Agent on Citrix Server	152
6.5	ZENworks Configuration Management Tuning Parameters	152
6.5.1	User Sessions on a Citrix Server Fail to Terminate	153
6.5.2	High Utilization of Resources on a Citrix Server	153
6.5.3	High Consumption of Memory on a Citrix Server	153
6.5.4	Disabling Random Refresh Might Cause the ZENworks Adaptive Agent to Crash on a Citrix Server	153
6.5.5	Logging in to the User Source on a ZENworks Server is Slow	154
A	ZENworks Services	155
A.1	ZENworks Services	155
A.1.1	Checking the Status of a ZENworks Service	155
A.1.2	Starting a ZENworks Service	155
A.1.3	Stopping a ZENworks Service	156
A.1.4	Restarting a ZENworks Service	156
A.1.5	ZENworks Services	156
A.1.6	Web Services Test Pages	157
A.1.7	Agent Log Files	157
A.1.8	Server Log Files	158
A.2	Useful URLs	158
A.2.1	Discovery	158
A.2.2	Deployment	158
A.3	Critical File Locations	158
A.3.1	Installation Directories	159
A.3.2	The ZENworks Content Repository	159
A.4	Logging Information	161
A.4.1	Local Log File	161
A.4.2	Installation Log File	162
A.4.3	Registration Log File	162
A.5	Backing Up and Restoring the ZENworks Certificate Authority	162
B	The ZENworks Configuration Management Architecture	165
B.1	ZENworks Architecture Reference	165
B.1.1	Standard Protocols	166
B.1.2	ZENworks Primary Server Architectural Components	167
B.1.3	Agent Architecture	169
B.1.4	Agent Communication	169
B.2	Detailed ZENworks Components Diagram	170

C	Reference Materials	173
C.1	Online Documentation	173
C.2	Sample Business Requirements Survey Questions	173
C.3	Sample Technical Requirements Survey Questions	175
C.4	Extended Port Chart Including Port Usage	176
D	Understanding the Performance and the ZENworks Login Process	181
D.1	Supported Authentication Mechanisms	181
D.2	Supported Directories for Authentication	181
D.3	The Login Process	182
D.3.1	Windows Login Process	182
D.3.2	ZENworks Configuration Management Login Process	183
D.4	Best Practices to Optimize ZENworks User Login Times	184
D.5	Registry Keys and Configuration Files	186
D.5.1	Using Registry Keys to Reduce Login Time	186
D.5.2	Using Configuration Files to Reduce Application Startup Times	187
D.6	ZENworks Configuration Management Policies	187
D.6.1	Group Policy	188
D.6.2	DLU or Roaming Profile Policy	188
D.6.3	Printer Policy	188
D.6.4	LFR Policy	188
D.7	ZENworks Configuration Management Bundles	188
D.8	Logging in to a Terminal Server or Citrix Environment	188
D.9	Troubleshooting Login Issues	189
D.9.1	Enabling the CASA Server and Client Logs	189
D.9.2	Time Synchronization	190
D.9.3	Checking Certificates	190
D.9.4	Checking ATS Status	191
E	Documentation Updates	193
E.1	May 17, 2012: ZENworks 11 SP2	193

1 ZENworks Configuration Management: A Single Solution for Systems Management

The purpose of this *System Planning, Deployment, and Best Practices Guide* is to describe the issues you need to consider when designing a Novell ZENworks 11 SP2 solution and deploying it across small and large scale enterprises. This guide is not meant to replace the other online resources that Novell provides, but to supplement that material so that you have a better understanding of certain topics related to design and requirements.

ZENworks Configuration Management is also supported by other documentation (in PDF and HTML) formats that you can use to learn about and implement the product. For additional documentation, see the [ZENworks 11 SP2 documentation \(http://www.novell.com/documentation/zenworks11/\)](http://www.novell.com/documentation/zenworks11/).

The following sections contain more information:

- ♦ [Section 1.1, “The Goal: Total Management, Zero Effort,” on page 9](#)
- ♦ [Section 1.2, “The Management Paradigm,” on page 10](#)
- ♦ [Section 1.3, “The Solution: ZENworks Configuration Management,” on page 12](#)
- ♦ [Section 1.4, “Additional ZENworks Products,” on page 13](#)

1.1 The Goal: Total Management, Zero Effort

Over the last decade, Novell ZENworks has provided the gold standard for centralized configuration and management of network endpoints in today’s complex and heterogeneous corporate networks. ZENworks Configuration Management is a key implementation of ZENworks technology, enabling policy-based automation of software and patch deployment, asset tracking, endpoint security, OS migration, and many other routine tasks.

With ZENworks Configuration Management, the IT staff can synchronize the Windows desktop environment with their company’s business policies, while saving IT time, budget, and resources for strategic projects. All of this focuses on the goal to provide total network management while bringing the associated management effort as close to zero as possible.

Introduced in the last quarter of 2007, ZENworks 10 Configuration Management moved towards that goal by using a completely redesigned architecture to greatly simplify, consolidate, and integrate policy-based management of Windows network endpoints, including systems running Windows 7.

The latest version of ZENworks, released in March 2012, moved the bar even higher, offering the following:

- ♦ Provides a single modular architecture, platform, and agent for all ZENworks products.
- ♦ Provides a unified, Web-based administration console.

- ◆ Uses only standards-based protocols.
- ◆ Reduces overall wire traffic.
- ◆ Allows full manageability over the Internet.
- ◆ Simplifies and speeds installation, deployment, and updates.
- ◆ Scales to support a maximum limit of 40,000 devices to a single Management Zone.
- ◆ Offers support for the Macintosh platform.

1.2 The Management Paradigm

All design features of the ZENworks Configuration Management architecture flow from the basic Novell philosophy of the Open Enterprise: a simple, secure, productive, and integrated IT environment across mixed systems. ZENworks Configuration Management empowers IT staff to manage systems to support real users, with all their various security, location, device, and other needs, while keeping simple, centralized control over the entire end-user environment. It also supports the idea that IT staff should be empowered to manage systems according to the paradigm that best reflects the organization's business policies and the IT staff's preferred working style.

ZENworks Configuration Management provides the flexibility to manage systems tactically (on a device-by-device basis) or strategically, using any combination of the following four distinct management paradigms:

- ◆ [Section 1.2.1, "Management by Exception," on page 10](#)
- ◆ [Section 1.2.2, "User-Based Management," on page 11](#)
- ◆ [Section 1.2.3, "Device-Based Management," on page 11](#)
- ◆ [Section 1.2.4, "Location-Based Management," on page 12](#)

1.2.1 Management by Exception

Two of the most important considerations when evaluating any configuration management solution are: how well the administration design scales and what burden it places on the IT staff as they update the solution to accommodate changing business policies. Novell is a pioneer of "management by exception," and ZENworks Configuration Management continues to offer this powerful method of continuously adapting, with minimal IT effort.

Management by exception is a complement to policy-driven management. It allows the general rules of configuration management to be at a high level across user or device groups, while permitting exceptions at a more granular level to accommodate more specialized needs.

For example, normal business policies might allow employees to remotely access the corporate network. However, applying this policy across the board to all desktops, including devices in the finance and legal departments, could expose the company to regulatory penalties and corporate spies. Exception-based management allows IT staff to create and automatically enforce general access policies, as well as more restrictive policies that are enforced on top of the general policies to protect devices and users that require a higher degree of security. In this case, the exception policy restricts access to normal business hours, on-site, and by authorized users. Exception-based management allows complete management flexibility in accordance with business policies, without requiring IT staff to manage separate policy silos for each type of user and machine.

1.2.2 User-Based Management

User-based management, which leverages user identities, group roles, and business policies, is the gold standard for automation, security, and IT control. User-based management has always been a Novell specialty. Although the underlying architecture has been dramatically enhanced in ZENworks Configuration Management, the full power of user-based management has been retained.

True user-based configuration management separates users from the specific devices they use, and treats the users as the company's most valuable asset to be managed. Devices serve their proper role as tools. Allowing users, rather than devices, to be managed as a first-class configured entity means that policies, applications, and other configuration details can follow users from device to device. User-based management also ties IT policies directly to business policies, which increases responsiveness to the changing business conditions. User-based management also leverages identity stores and business systems across the enterprise to eliminate errors, increase security, standardize workflows, document regulatory compliance, and support effective decision making.

User-based management can be defined as strategic, while device-based management is tactical. In ZENworks Configuration Management, both can be mixed and matched according to business and IT requirements by using management by exception. For example, a general policy can be applied to a specific device and then overridden, depending on the identity information for the user who is currently logged on. Or, a general policy based on user identities and roles can be overridden, depending on the device being used and its context, such as a mobile device attempting to access the network from beyond the firewall.

1.2.3 Device-Based Management

Many organizations base their configuration management practices on the devices being managed. In fact, this is the default method used by most of the configuration management products on the market today. Without user-based and exception-based policy management, products that target specific device configurations treat actual business policies and user needs as an afterthought - essentially equating a specific user with a specific device. Applications, policies, and other configuration information are associated to a managed device or set of managed devices. This approach tends to force users into rigid roles instead of supporting users as dynamic participants in evolving business processes. For that reason, Novell has not focused on device-based management in the past.

However, the new ZENworks Configuration Management architecture adds device-based management as a tool that can be used, in addition to the other management styles, to fill specialized needs. For example, manufacturing-floor devices, public kiosks, and call centers where multiple users work different shifts and share a single device are all instances where device-based management might be more appropriate than user-based management. Additionally, companies that normally rely on user-based management might need the ability to quickly set up a device for one-time use. For example, a customer might need to configure a device to auto-run a presentation in a conference center without having to bother about creating a new "user" for this one instance. With the new ZENworks Configuration Management architecture, customers now have the option of using device-based management whenever it suits their specific needs.

Because device-based management is the most familiar method to most IT professionals, and because it is the fastest way to configure a device in the short term, before setting up long-term user-based policies, device-based management is the default management model after installing ZENworks Configuration Management.

1.2.4 Location-Based Management

ZENworks 11 introduces the concept of locations to Endpoint Management to further enhance the flexibility and power of managing endpoints. Locations can use the concept of Closest Server Rules (first introduced in ZENworks 10 Configuration Management) to allow the administrator to define in detail all locations that contain managed devices.

Locations can be defined using very specific criteria such as DNS server, gateway and, subnet. After a location and its network environments have been defined, ZENworks policies and bundles can be applied to allow ZENworks to automatically adjust the configuration and security posture of the device.

Location awareness originates from Novell's Endpoint Security Management product which is now integrated into the common ZENworks architecture. The ability to utilize locations is another example of the benefits of an integrated architecture for all Endpoint Management products.

1.3 The Solution: ZENworks Configuration Management

ZENworks Configuration Management is based on a web-services architecture designed to provide a secure, highly usable, open environment for managing all your Windows devices. ZENworks Configuration Management provides you with a single, modular architecture that maximizes flexibility and scalability, simplifies and speeds management throughout the device life cycle, minimizes processing demands on managed clients, reduces bandwidth consumption for management processes, and uses standards-based protocols to seamlessly integrate with your choice of user directories and object databases.

ZENworks Configuration Management lets you manage systems based on user identities, roles, groups, and locations, so IT can work seamlessly with the company's business organization and policies. ZENworks Configuration Management gives you a secure, Web-based console for unified control over all management tasks, from virtually anywhere.

ZENworks 11 is the only Endpoint Management tool in the market that provides management based on three key criteria:

- ♦ **What you are:** The device chosen by the user to access resources.
- ♦ **Who you are:** Your identity in the corporate directory.
- ♦ **Where you are:** The end user's physical location.

Combining these three criteria, ZENworks can automatically invoke different security and configuration postures as the user changes devices, locations, and roles within the enterprise. For example, when a user travels to a remote office, ZENworks can automatically and transparently enforce different printer policies, provide group policies to configure the device, offer an alternative method to access an application (such as thin version) and define security details such as the applications that can run, the firewall settings, and what removable storage can be used by the device. No other Endpoint Management tool can come close to offering this level of flexibility. Refer to "Locations" on page 71 for more information on Locations.

If your organization is undertaking an Information Technology Infrastructure Library (ITIL) initiative, ZENworks Configuration Management is the right choice for you. It has been built as a modular set of components that uses industry standards to build a product and set of solutions that completely align with ITIL best practices and disciplines.

To find out more about our vision, visit the [Novell ZENworks Configuration Management product page \(http://www.novell.com/zenworks\)](http://www.novell.com/zenworks) and download the white paper entitled *A Blueprint for Better Management from the Desktop to the Data Center*.

1.4 Additional ZENworks Products

The core functionality included within ZENworks Configuration Management includes remote control, inventory, imaging, software deployment, and application and policy management. In addition, ZENworks provides easy access to even more solutions that help you to meet the needs of your workforce.

- ◆ [Section 1.4.1, “ZENworks Application Virtualization,” on page 13](#)
- ◆ [Section 1.4.2, “ZENworks Endpoint Security Management,” on page 13](#)
- ◆ [Section 1.4.3, “ZENworks Patch Management,” on page 13](#)
- ◆ [Section 1.4.4, “ZENworks Asset Management,” on page 14](#)
- ◆ [Section 1.4.5, “Novell Service Desk,” on page 14](#)
- ◆ [Section 1.4.6, “ZENworks Full Disk Encryption,” on page 14](#)

1.4.1 ZENworks Application Virtualization

ZENworks Application Virtualization reduces the costs, complexity, and delays associated with application compatibility testing and management, while maintaining endpoint security. You can turn Windows, .NET and Java-based applications into self-contained applications in minutes for pain-free deployment via the Web, USB keys, or a desktop management infrastructure.

1.4.2 ZENworks Endpoint Security Management

Novell ZENworks Endpoint Security Management provides a comprehensive set of policy-enforced solutions that address every aspect of endpoint security, all managed through a single console. Solutions can be deployed individually to meet specific needs, or as a fully integrated suite to provide complete endpoint protection, from perimeter to core.

ZENworks Endpoint Security Management delivers wireless security, a personal Firewall, port control, data encryption, USB security and application control, and it also allows you to set alerts based on policy violations. This granular level of control enables your business to define policies that reflect working practices. For example, you can whitelist certain approved USB devices, while denying access to any other USB removable storage that is connected, or only you can allow laptop devices to attach only to approved wireless networks.

1.4.3 ZENworks Patch Management

ZENworks Patch Management is a powerful solution to automate patch management, including the processes of discovering security alerts, retrieving patches, and deploying the right patches to the right machines.

You use ZENworks Patch Management to maintain and monitor patch compliance throughout the entire enterprise, so you can accurately detect security vulnerabilities. This powerful tool provides dynamic graphical reports so you can easily see which devices are in security compliance and quickly assess vulnerabilities. The highly accurate inventory process, lets you run reports to identify any patch deployments that haven't been successful, or to identify when devices aren't properly patched.

ZENworks Patch Management provides patches across all Windows operating systems, SUSE Linux, Red Hat Linux, and Macintosh for more than 40 popular applications such as Adobe Acrobat, Macromedia Flash, Citrix ICA, Internet Explorer, MSN Messenger, and SharePoint.

1.4.4 ZENworks Asset Management

With this component, ZENworks Configuration Management provides an integrated asset inventory, that tracks software usage and license compliance. ZENworks Asset Management ensures compliance with all purchased license agreements and contracts. It also includes an auto-reconciliation feature that matches the products discovered on the network with the licenses purchased. ZENworks Asset Management discovers and tracks more than 65,000 products. ZENworks Asset Management also gives a deep visibility into both desktop application and server-side application usage trends. Reports can be quickly generated to show which products and types of software are being used most, and which products are not being used at all.

1.4.5 Novell Service Desk

Novell Service Desk enables delivery of services that are closely aligned to business needs and objectives. By supporting ITIL best practices out of the box, Novell Service Desk helps move from a reactive to a proactive stance by providing high-quality managed services. Novell Service Desk makes it possible to fulfil any type of business request by combining strong self-service capabilities and easy-to-use built-in reporting. It also offers advanced incident, problem, change, configuration and knowledge management capabilities and supports integration with numerous external systems to make the most of existing infrastructure investments, including ZENworks Configuration Management.

1.4.6 ZENworks Full Disk Encryption

Recently announced along with ZENworks 11 SP2, Novell ZENworks Full Disk Encryption provides the security of full disk encryption, without all the management headaches of traditional solutions. It goes beyond simply securing mobile devices, and makes it easy to automatically secure your laptops and desktops with centralized key management.

2 Performing Pre-Design Activities

A firm understanding of the organization's business and technical requirements and the existing infrastructure components that will take part in the Novell ZENworks Configuration Management system is the first step in developing a solid design that meets the organization's immediate and future needs.

IMPORTANT: Throughout this document, we refer to the need for proper documentation. Documentation is of the utmost importance. Documentation is a complete and accurate reference to the system you have designed and built, but most importantly, it is a reference for the future. As individuals transition in and out of the IT organization, the design documents become a reference as new employees learn the infrastructure they support, including techniques, policies, and design decisions. Documentation is also a good reference for others inside the organization who might not be involved in the day-to-day management of the ZENworks Configuration Management environment, but are involved in the management of other projects that might have an impact on the ZENworks Configuration Management environment, including dependencies.

The following activities should be performed during the pre-design phase of implementing ZENworks Configuration Management:

- ♦ [Section 2.1, "Perform a Business Assessment," on page 15](#)
- ♦ [Section 2.2, "Perform a Technical Assessment," on page 16](#)
- ♦ [Section 2.3, "Gather Other Critical Information," on page 17](#)
- ♦ [Section 2.4, "Develop High-Level Design," on page 18](#)
- ♦ [Section 2.5, "Develop Documentation," on page 18](#)
- ♦ [Section 2.6, "Outputs from Pre-Design Activities," on page 19](#)

2.1 Perform a Business Assessment

Your first need is a detailed business assessment. If you do not have a solid understanding of what the overall business (or individual business units) needs or desires, you cannot design a solution to meet business needs.

Systems management software affects the entire business, so the various departments should provide input and influence on what the system should look like. This does not mean that departments outside of IT need to understand the technical complexities of the infrastructure and how it is designed; they simply need to provide business requirements to the IT organization so that their needs are met.

The best way to handle this is through a set of informal workshops, which include high-level introduction to the technology, what it does, how the departments and end users benefit, and possibly a short demonstration of the product. The three main reasons you hold these workshops are to inform departments of what you are doing, get their buy-in, and get their feedback in the form of technical requirements. The meetings should sufficiently inform department members so they begin to give you feedback as to how they will leverage the system.

The following list presents some ideas on how to perform the business assessment. You might think of more ideas; use your imagination and tailor your business assessment according to each organization's unique landscape.

- ◆ Hold informal workshops and invite leaders from each department.
- ◆ Survey departmental leaders and find out what they need to become more effective in their roles. Find out how their staff can become more effective, given the software you are deploying. Getting departmental leaders to answer a written survey can be very effective and can give you detail that can be used when building both the high-level and the detailed designs. A sample survey is provided in [Section C.2, "Sample Business Requirements Survey Questions,"](#) on [page 173](#).
- ◆ Make sure you completely understand how the organization is dispersed and which departments of the organization are represented at each of its physical locations.
- ◆ Make sure you understand the monthly cycles for each of the departments in the organization. This will assist you with determining peak times when the organization cannot afford to be impacted by downtime.
- ◆ Determine whether the organization is going through an ITIL (IT Infrastructure Library) initiative. This has a direct impact on the solution you design and the services you provide. If there is an initiative underway, you need to be involved in it and be completely informed. You want to avoid making design changes mid-project because of the output from another project.

2.2 Perform a Technical Assessment

Your next need is for a technical assessment to review what you already have, identify what you need, and document your requirements.

It is important to note that the technical assessment should be performed at the same time as the business assessment. The two assessments should take no longer than a week to perform, depending on the size and complexity of the organization and its infrastructure.

You need to have a good understanding of the existing infrastructure well before you introduce ZENworks Configuration Management into the environment. In order to do this, you should hold a set of workshops or meetings to obtain the information you need.

The two main outputs from a technical assessment are documentation on your findings, along with a set of tasks that you need to perform. Information that you should gather includes the following:

- ◆ Which operating systems must be supported?
- ◆ How many users must be supported by the proposed solution?
- ◆ Will there be support for roaming users?
- ◆ How many offices and sites must the solution support, and how many users are at each location?
- ◆ Where are data centers located?
- ◆ What is the network architecture, with details on link speeds, and so forth?
- ◆ Will existing servers will be leveraged to support the ZENworks Configuration Management infrastructure?

If so, you should gather the following software and hardware information:

- ◆ Service pack levels (and whether they meet the minimum requirements for ZENworks Configuration Management as listed in ["Primary Server Requirements"](#) in the [ZENworks 11 SP2 Server Installation Guide](#)).
- ◆ Other software, for example, .NET.

- ◆ CPU and memory requirements (and whether they meet the minimum requirements for ZENworks Configuration Management)
- ◆ IP addressing for all servers and other devices that will be part of the ZENworks Configuration Management infrastructure
- ◆ Previous versions of ZENworks that might already be hosted
- ◆ What is the DNS infrastructure?
- ◆ What is the DHCP infrastructure?
- ◆ How should the IP subnet design be handled?
- ◆ Which network access methods (VPN, Access Manager, and so forth) must be supported?
- ◆ Which network infrastructure components and design (DMZ, NAT, and so forth) must be supported?
- ◆ What is the directory services design, including which directory services are being utilized (Novell eDirectory, Microsoft Active Directory, and so forth), and for what purpose (Application support, LDAP, and so forth)?

2.3 Gather Other Critical Information

You should also be familiar with other services that are running on the network and that rely on the infrastructure. You should prioritize these services to better understand bandwidth utilization and service levels that have been assigned to specific functions. If the customer is implementing ITIL best practices, you should know about all disciplines that are currently being leveraged.

You should collect information about the following:

- ◆ Which Service Desk software is currently used by the customer, and how does the deployment of ZENworks Configuration Management fit within this framework?
- ◆ Does the customer have a formal Service Level Agreement (SLA) process in place? If so, what is it and can you access the documentation that explains it?
- ◆ What is the customer's Disaster Recovery and Service Continuity plans? How does this impact the ZENworks Configuration Management design?
- ◆ How does the customer plan for availability of services and resources? Is the customer fully aware of availability requirements?
- ◆ Does the customer leverage a Configuration Management Database (CMDB)? If so, which CMDB? Does the customer have plans to include information that is stored in the ZENworks database in their CMDB?
- ◆ Does the customer have a formal method for keeping track of changes to applications that are published to the end-user communities?
- ◆ Does the customer have a Definitive Software Library (DSL) and Definitive Hardware Library (DHL)?
- ◆ Is the customer using another framework product in its infrastructure, such as IBM Tivoli, CA Unicenter, or HP OpenView?
- ◆ Does the customer leverage other products, such as SAP?
- ◆ What other major projects are currently taking place at the customers' sites?

2.4 Develop High-Level Design

After you have completed gathering data to use when building the design of the infrastructure, you can then develop a high-level design. It is important at this point to understand what the infrastructure is going to look like, so documenting your high-level thoughts and plans is critical to the success of the project.

Developing a high-level design consists of building two main outputs:

- ◆ **Assessment document:** A high-level design document outlines the general placement of services across the company's infrastructure. This document does not need to identify servers to be utilized or deployed to host the specific ZENworks services. The document should simply outline the services themselves, and where they will reside across the network. Your high-level design should include the following information:
 - ◆ Number of ZENworks Management Zones needed
 - ◆ Placement of Primary Servers
 - ◆ Placement of Satellite devices
 - ◆ Placement of the Database Servers
 - ◆ Services that run at each location, based on the requirements gathered during the business assessment.
 - ◆ Configuration of network services, such as DNS (forward/reverse lookup), DHCP, and so forth
 - ◆ Utilization of network infrastructure, such as L4 switches to front the Primary Servers, Satellite devices, or both
 - ◆ Remote access capabilities
- ◆ **High-level graphical design diagram:** As a supplement to the assessment document, you should also develop a graphical representation of the infrastructure. This diagram should reflect exactly what you have described in the document, and it should be at a high enough level so that everyone can see what the infrastructure is going to look like after the ZENworks Configuration Management deployment is complete.

2.5 Develop Documentation

It is important to develop your documentation and then discuss it with all parties that have an interest in the success of the project. Discussing the findings and recommendations in detail is important to the success of this phase of the project and the success of the more detailed design phase.

After you have conducted meetings to discuss the findings and recommendations, there will be items in the high-level design that must be modified or changed. This is normal. Ensure that you capture the changes and include them in documents you created during this phase. This is important so that you have accurate information throughout the life cycle of the project. The information in these documents will be leveraged during the design phase, so it needs to be complete and accurate.

2.6 Outputs from Pre-Design Activities

As mentioned in [Section 2.4, “Develop High-Level Design,”](#) on page 18, there are two main outputs (or deliverables) from your pre-design activities:

- ♦ **Assessment document:** This document highlights all of your findings from the business and technical assessments that you perform. The document is the foundation for performing your design activities, and needs to be kept up to date. The document includes information such as:
 - ♦ Requirements gathered during meetings and workshops with department leaders and others inside the organization that will have an influence on the services ZENworks Configuration Management will deliver.
 - ♦ A detailed summary of your technical findings, and what needs to change in order to support ZENworks Configuration Management in the infrastructure. Suggestions should include best practices and detailed recommendations to resolve any known issues.
 - ♦ High-level design information, including general placement of services and other infrastructure components.
- ♦ **High-level graphical design diagram:** This diagram is used to visually understand what the infrastructure will look like after the deployment is complete. This is a foundational document, and it should be further refined during the design phase of your project.

3 Gathering Critical Information for Design Activities

After you have created your high-level design, you need to gather additional information to help you design your specific implementation. Introducing Novell ZENworks Configuration Management into an environment involves efforts, considerations, and input from multiple sources.

The following sections highlight the major areas of concern:

- ♦ [Section 3.1, “Design Criteria/Decisions,” on page 21](#)
- ♦ [Section 3.2, “Scalability of the Primary Server,” on page 26](#)
- ♦ [Section 3.3, “Scalability of Satellite Devices,” on page 34](#)
- ♦ [Section 3.4, “ZENworks Database,” on page 37](#)
- ♦ [Section 3.5, “Virtualization Considerations,” on page 62](#)
- ♦ [Section 3.6, “Ports Used by ZENworks Components,” on page 63](#)
- ♦ [Section 3.7, “Network Considerations,” on page 65](#)

3.1 Design Criteria/Decisions

A fundamental objective of a design is to balance the need for hardware while easing the load on the customer's network during deployments:

- ♦ [Section 3.1.1, “Decisions to Make Before Installing the Primary Server,” on page 21](#)
- ♦ [Section 3.1.2, “Infrastructure Placement,” on page 25](#)
- ♦ [Section 3.1.3, “Infrastructure Scale Assumptions,” on page 26](#)

3.1.1 Decisions to Make Before Installing the Primary Server

A number of decisions should be made before installing the first ZENworks Primary Server:

- ♦ [“Required Functionality” on page 22](#)
- ♦ [“Certificate Authority” on page 22](#)
- ♦ [“Management Structure” on page 23](#)
- ♦ [“Application Store” on page 23](#)
- ♦ [“Staging and Grouping” on page 24](#)

Required Functionality

Only the functionality that is needed by the customer should be enabled. Start with a simple approach, harden the implementation, and then expand it in the future. For example, if Patch Management, User Sources, and ZENworks Reporting Server are not required by the customer, do not enable or install them.

Certificate Authority

ZENworks Configuration Management provides the choice of using an external Certificate Authority (CA) or an internal ZENworks CA. If you choose an internal ZENworks CA, it is created during the installation of the first ZENworks Primary Server and is used throughout the life of that ZENworks Management Zone. The current lifespan of the internal certificate is 10 years.

When an internal CA is used, its certificate is signed by the CA, as each subsequent Primary Server is installed.

When external CA is used, each Primary Server installation requires a signed certificate to be provided by the Administrator. The first Primary Server also requires the CA's public certificate.

The CA's certificate is distributed to all managed devices as part of the ZENworks Adaptive Agent installation. This lets each Adaptive Agent connect to any Primary Server because each server's certificate is signed by the now trusted CA. Each Primary Server's certificate is automatically distributed to every managed device as part of the configuration refresh.

As the expiry period for the Primary Server certificates signed by the internal CA is 10 years, the issue of expiration is something that you do not need to deal in the immediate future. However, the Primary Server certificates from an external CA within 1 or 2 years of the Primary Server certificates. If a Primary Server certificate expires, the agent communication with that Primary Server stops. In order to address this issue, ZENworks can allow the new Primary Server certificates that have been signed by an external CA to be imported into the Zone, and then automatically distributed to all managed devices as part of the standard configuration refresh. To add a new Primary Server certificate, use the following command:

```
zman server-add-certificate
```

This command should be used before the existing certificate expires. When the administrator is satisfied that every managed device has received the updated certificates via the configuration refresh, the following command needs to be run at the back end to instruct the Primary Servers to use the new certificate when establishing an SSL connection with a managed device:

```
novell-zenworks-configure -c SSL -Z
```

The ZENworks Control Center automatically informs the administrator 90 days before the certificate is going to expire.

If the Certificate Authority itself is going to expire, or if new certificates are signed by a new CA, the new CA's certificate needs to be installed into the trusted root store of each managed device. To achieve this, the following steps need to be automated with a ZENworks bundle and be executed on each agent before the CA certificate expires:

1. Copy the new CA certificate to the device.
2. Import the new CA certificate by using the following command:

```
zac cert-info <path to the CA cert file>
```

Management Structure

With the previous generation of ZENworks, the technology was tied closely to Novell eDirectory. In traditional NetWare or eDirectory file and print environments, ZENworks is structured according to the design of eDirectory and was therefore based on geography. However, geography is no longer a requirement for the structure of folders in the Management Zone. Because devices can connect to any Primary Server, and all Primary Servers should be linked over fast links, the structure of management can be based on other criteria.

Customers might want to base the folder structures for devices on business functions, such as Human Resources, Finance, Sales, and so forth.

Basing the device folder structure on geography is still possible and might be required by many customers. Some customers might want to implement policies and applications site by site, room by room, and so forth.

The choice of a folder structure should also take into account the potential use of dynamic groups. Dynamic groups are groups whose members are automatically decided based on rules. In some environments, departments have a pool of devices for their users, so the standard tools remain static over its life. However, the location of the device can change frequently based on mobility of the user. In this scenario, the departmental structure of the business can be created by using folders, because the folders are fairly static and the geographical locations can be modelled using dynamic groups. This allows for easy definition of standard tool sets and configurations for common-interest groups but still allow for updates to be rolled out on a location-by-location basis.

Application Store

Traditional ZENworks implementations require file repositories to store application content. Users and devices access this content via mapped network drives or directly via UNC paths defined in the application object. Although this fits well with a traditional file and print model, it has the following drawbacks:

- ♦ **Synchronization:** If an application is to be made available to all users, the source content must be copied to all servers. This requires additional products and processes to be introduced to manage the location of content, such as the Tiered Electronic Distribution component of ZENworks Server Management.

Rights: When files are stored in a traditional file and print model, the rights to these locations must be managed carefully. If you roam between sites, you might need access to all application repositories to ensure that applications can be installed and verified at any location. In a traditional model, if you have the read access to an application store, you have the ability to manually install any application that resides there, provided you know where to look.

With ZENworks Configuration Management, bundles can be created to install applications from mapped network drives and UNC paths as before. If you used mapped drives and UNC paths, file synchronization and the rights to those files must be managed outside of ZENworks Configuration Management.

ZENworks Configuration Management also allows for application content to be injected in to the ZENworks Content Repository. By default, the Content Repository is synchronized between all Primary Servers and is downloaded by devices using HTTP. You can, however, specify which of the Primary Servers host content (at least one Primary Server must host the content).

Using the ZENworks Content Repository has the following advantages:

- ♦ **Synchronization:** Content is automatically synchronized to other Primary Servers and the defined Satellite devices. This allows devices to download content from the most appropriate location. The synchronization schedule and bandwidth consumption can be tightly controlled to avoid negative impacts on the customer's network
- ♦ **Rights:** Rights to files do not need to be managed. Only devices and users who are assigned to the content via relationships to Bundles and Policies in ZENworks Configuration Management have access to that content. If a user accesses a ZENworks Content Repository, the content files are encrypted and cannot be used.
- ♦ **Content is firewall and location friendly:** Files are securely delivered in an encrypted fashion via HTTP protocol. This means that there is no need for the user to have the correct drive mapping with the necessary rights. If the user has been assigned the content, it is downloaded via HTTP from the most suitable location.

Downsides to using the Content Repository include the following:

- ♦ **Disk Space:** Additional disk space is required. Many customers have extremely large application repositories distributed over many servers. These repositories must be re-created in ZENworks Configuration Management. If a customer has a 100 GB application repository, ZENworks Configuration Management requires at least 100 GB on each Primary Server with a content role to store applications, in addition to the space needed for other content, such as patches and system updates.
- ♦ **MSI applications cannot be easily changed:** After an MSI application is uploaded to the Content Repository, it cannot be changed. To make changes, the original MSI must be updated and then re-injected back into the Content Repository. In this scenario, a master store of all applications must reside outside of ZENworks Configuration Management to allow for edits.

Staging and Grouping

Grouping devices is very important in ZENworks Configuration Management because it allows applications, policies, and system updates to be deployed in a staged manner.

In ZENworks, if a change is made to an application or a policy, everyone receives the change. Controlling the introduction of change is vitally important in maintaining a secure and stable environment.

We recommend that you identify the following groups in your customer environment:

- ♦ **Test devices:** Identify test devices that are first to receive updates. Ensure that build versions are represented for each operating system in the field.
- ♦ **IT departments:** Identify IT staff that are typically the first users to receive live updates and applications.
- ♦ **Early adopters:** Identify early adopters who will test deployment in each business unit and geographical location.
- ♦ **Home workers/VPN users:** Identify home workers or users who use a VPN so they can help test deployment via DMZ and VPN connections.
- ♦ **VIP users:** Identify important users whose devices require special focus and attention. You might want to transition executive laptops and workstations at the end of deployment.
- ♦ **General population:** Create logical groups for the rest of managed devices, based on business function or geography.

Creating these groups or folders is an important factor in releasing new configurations, applications, and updates in a controlled manner to the managed environment.

In situations where an application or policy is already live in an environment, grouping does not help in executing change on this object in a controlled manner. After the bundle or policy has been changed, all users and devices with an association or inheritance receive the change automatically on the next refresh. To provide control in this scenario, ZENworks 11 has introduced change and release management capabilities through the concept of sandboxing for all policies and bundle types in ZENworks.

Sandboxing allows for devices and users to be marked as test devices or users, and when a change is made to a bundle or policy, only the test devices or users will receive the change. This allows selected devices and users in different locations and departments to test and ensure the quality of the change before it is released to the rest of the environment.

3.1.2 Infrastructure Placement

In order to calculate what infrastructure is required and where it should be located, you need to plan for the scalability of ZENworks Configuration Management.

NOTE: At the time of writing this document, the SuperLab facility in Provo, Utah has provided metrics and results, as seen in various places in this section, that give you a better understanding about how the individual components scale. These figures will be kept up-to-date as this document continues to grow over time.

Based on the connection information, the number of ZENworks Primary Servers and Satellite devices needed to support thousands of devices can be calculated with the following rules in mind:

- ♦ [“Primary Servers” on page 25](#)
- ♦ [“Satellite Devices” on page 25](#)

Primary Servers

Each Primary Server must be connected to every other Primary Server, the database, and the user source by LAN speed or close links. Placing Primary Servers behind strong links allows for content synchronization, credential verification from the user source, and access to the ZENworks Configuration Management Database Server to occur quickly and efficiently. Performance suffers, including response times when you use ZENworks Control Center to perform administrative tasks, if there are any barriers between Primary Servers and the Database Server.

Satellite Devices

When you configure satellite devices, consider the following:

- ♦ Currently, Satellite devices are primarily designed to reduce load on the network, not to reduce load on the Primary Servers.

Consider a scenario in which a Primary Server is located at Site1, and 10 managed devices are located at Site2. Site1 is connected to Site2 over a WAN or a slow link. The managed devices are on a LAN or a high-speed link. If you do not choose to configure a Satellite at Site2, then each managed device must traverse the network to get content from the Primary Server. If you choose to configure a Satellite at Site2, then only the Satellite would traverse the network to get content from the Primary Server, and all the managed devices would get the content that is locally available at the Satellite.

- ◆ Bandwidth calculations are based on ZENworks Configuration Management having access to a known percentage of the total bandwidth for a given link.
- ◆ Satellite devices should be located at remote sites to provide content local to devices on the local network.

3.1.3 Infrastructure Scale Assumptions

The following scale assumptions can be made when building the design of the infrastructure. These actual scale assumptions might be different, based on the services you are providing and how you break up the services across multiple servers.

- ◆ **ZENworks Primary Server:** A single ZENworks Primary Server can provide all ZENworks services (content, collection, and configuration) for as many as 3,000 devices in a ZENworks Management Zone.

This is based on a Primary Server handling approximately 1,000 concurrent connections for all service types (content, configuration, and content).

This is not real-world; see [Section 3.2, “Scalability of the Primary Server,” on page 26](#) for additional details on how these figures can change, and what you need to consider to ensure that you are scaling to meet the needs of the organization.

- ◆ **Server-grade Satellite device:** A single ZENworks Satellite (dedicated server) can provide content services for as many as 1,000 concurrent devices.

This is not real-world; see [Section 3.3, “Scalability of Satellite Devices,” on page 34](#) for additional details on how these figures can change, and what you need to consider to ensure that you are scaling to meet the needs of the organization.

- ◆ **Workstation-grade Satellite device:** A single ZENworks Satellite (dedicated workstation) can provide content services for as many as 250 concurrent devices.

This is not real-world; see [Section 3.3, “Scalability of Satellite Devices,” on page 34](#) for additional details on how these figures can change, and what you need to consider to ensure that you are scaling to meet the needs of the organization.

3.2 Scalability of the Primary Server

Understanding the scalability of the individual components that make up the ZENworks infrastructure is of the greatest importance. You need to understand the limitations and where you can expect to see performance degradation to ensure that you build an infrastructure that can perform well, regardless of the load that your end-user community places on it.

The first area that you need to consider is the scalability of the Primary Server. It is important to design your Primary Server placement based on the information you collected during your assessment phase and what you anticipate your overall design will require. You should design your infrastructure so that there are always Primary Servers available to service devices and the administrators that are managing the system:

- ◆ [Section 3.2.1, “Factors Influencing Scalability,” on page 27](#)
- ◆ [Section 3.2.2, “Load Testing in the Novell SuperLab,” on page 27](#)
- ◆ [Section 3.2.3, “Achieving Scalability in the Real World,” on page 30](#)
- ◆ [Section 3.2.4, “Tuning the JVM and Tomcat,” on page 31](#)

3.2.1 Factors Influencing Scalability

The main physical factors that govern the scalability of the Primary Servers are:

- ♦ **RAM:** The majority of operations are performed by zenserver and zenloader. Each of these services can consume approximately 1.2 GB of RAM on a 32-bit operating system. ZENworks 11 provides a 64-bit JVM for 64-bit operating systems and therefore these memory limitations are no longer applicable. For further details on how to tune the JVM and Tomcat for better performance, see [Section 3.2.3, “Achieving Scalability in the Real World,” on page 30](#).
- ♦ **Disk I/O:** Disk I/O is used when serving content for applications and updates.

The minimum hardware recommendations are listed in “[Primary Server Requirements](#)” in the [ZENworks 11 SP2 Server Installation Guide](#). If you can provide hardware that exceeds these recommendations, your system will perform better. Additional processing power and faster drives can make the systems more responsive, for example:

- ♦ Using a quad core processor
- ♦ Using 4 GB RAM or even more
- ♦ Allocating as much disk space as you can (such as RAID 5 with separate physical drives to separate content and ZENworks Configuration Management from the OS)

There are other factors that you need to consider, including:

- ♦ Device refresh frequency
- ♦ Number of Primary Servers being used to deliver content to the managed devices (software, policies, images, patches, inventory collection, and so forth)
- ♦ Number of administrators who have access to ZENworks Control Center
- ♦ Frequency of uploading content in the ZENworks Content Repository
- ♦ Number and frequency of reports run by administrators

3.2.2 Load Testing in the Novell SuperLab

ZENworks Configuration Management is tested in the Novell SuperLab in Provo, Utah to see how much load can be placed on the individual components, and more importantly, where the individual components start to break down and when performance is dramatically affected.

These tests provide insight on how far you can stretch the infrastructure design (for example, how many Primary Servers you need, based on the components and services you plan to deliver).

The following three tests show how Primary Servers react under different loads, and how quickly they can service individual requests when load is increased.

The tests included the following hardware and software:

- ♦ A Dell 2950 Dual Quad Core 2.0Ghz, 4 GB RAM, RAID 5 (4 X 300 GB) server was used for the Primary Server.
- ♦ The operating system was Windows Server 2003 Enterprise on a 64-bit device.
- ♦ ZENworks Configuration Management shipping code was used.
 - ♦ The test deployed 100 MB of bundles (11 bundles) to an increasing number of devices.
- ♦ All ZENworks Control Center settings used the default; after the 500-device test, retries were boosted to 800/10/20.
 - ♦ Three test passes for each test were run (for example, three test runs with 250 devices).

- ◆ All devices were refreshed “simultaneously” (within 30 seconds).
- ◆ The bundles were chained, with the first bundle being associated to a device group set to launch on refresh.
- ◆ All tests were run on a full gigabit network.
- ◆ [“Test 1: Average Time to Refresh” on page 28](#)
- ◆ [“Test 2: Average Time to Download” on page 28](#)
- ◆ [“Test 3: Administrative Tasks Performed Under Load” on page 29](#)

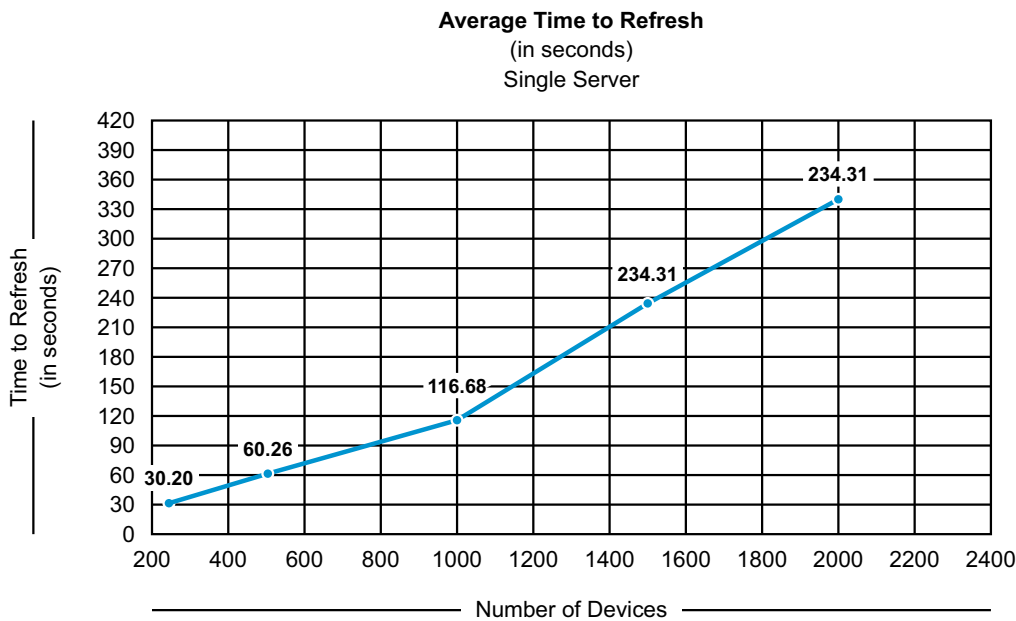
Test 1: Average Time to Refresh

In this test, we used a single ZENworks Primary Server and refreshed all machines inside the lab at the same time. The devices then contacted the Primary Server at approximately the same time. We calculated the amount of time it took for the refresh of the ZENworks Adaptive Agent to complete. As the load increased, the average time also increased. In fact, the time to complete the refresh increased considerably at the 1,000 device mark. Between 1,000 and 2,000 devices, the amount of time it takes to complete the refresh more than doubled.

The Primary Server scaled well to this point; however, this does not mean that you should implement a single Primary Server to manage 3,000 managed devices. You must always consider the services that are being implemented, and most importantly, fault tolerance and load balancing.

The following graphic shows the average time to refresh managed devices:

Figure 3-1 Average Time to Refresh

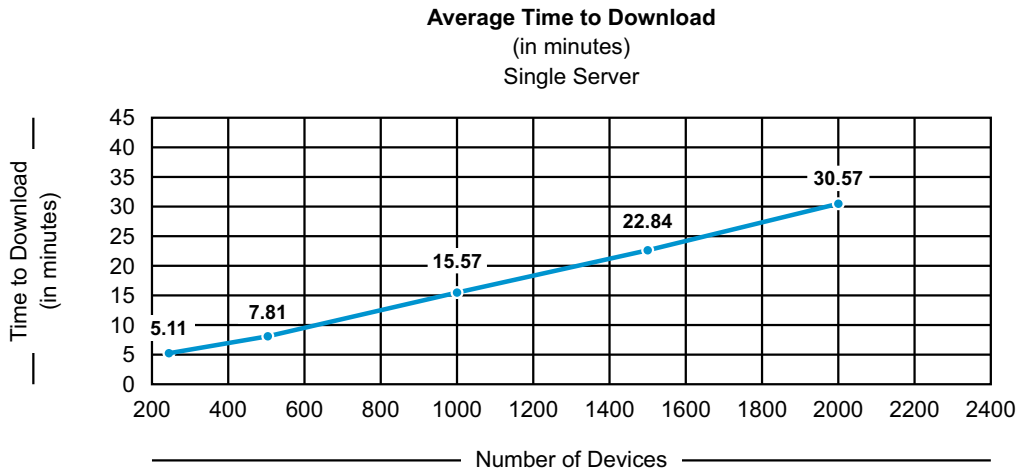


Test 2: Average Time to Download

This test demonstrates the results of a download of 100 MB of bundle content, spread across 11 bundles that are chained together. The server load increased as the load (in terms of devices) increased.

The following graphic shows the number of minutes it took to download the content:

Figure 3-2 Average Time to Download



Test 3: Administrative Tasks Performed Under Load

This test used a series of administrative tasks performed on a server with no load and then with a load. These results demonstrate what to expect in a given environment when a certain load is placed on a Primary Server that is multi-tasking. This test provides insight into what you can expect if you do not properly distribute services across multiple Primary Servers. These are conditions that should not exist in a real-world environment; Novell runs these tests to see when the processes begin to break. A well-designed infrastructure should perform well for you regardless of the load you are placing on the servers.

The load consisted of 480 devices running the Daily Use Test.

The Daily Use Test environment in the SuperLab consisted of the following:

- ◆ Single Server: Windows Server 2003 x86_64
- ◆ Server hardware: Dell 2950, Quad Core 2.0 MHz, 8 GB RAM
- ◆ External Microsoft SQL Server 2008 R2 database

Definition of the “Daily Use” included the following:

- ◆ 24-hour period simulated in four hours
- ◆ Three bundle pushes of 105 chained bundles (30 MB to 1 KB) per device
- ◆ One full and three delta inventory scans per device
- ◆ One patch distribution per device
- ◆ Four device refreshes per device
- ◆ Ten devices continually restoring images

This test environment stretched the limits of what the ZENworks Configuration Management system is able to achieve, giving us a good idea of where the system starts to reach its limitations. It comes close to a real-world simulation.

Table 3-1 Tests and Results.

Test Name	Test Description	Primary Server Under No Load	Primary Server Under Load
BOE Report	Run Predefined BOE report - Bundle Deployment Status (313 pages)	15 seconds	18 seconds
Inventory Report	Run canned report "Devices By Machine / Login Name"	7 seconds	8 seconds
Policy	Create policy, assign it to 60 devices, and perform a quicktask on all 60 devices to get the policy	7 minutes 43 seconds	7 minutes 45 seconds
Multicast	Create Multicast bundle and multicast to 60 devices	4 minutes 20 seconds	4 minutes 27 seconds
Bundle	Create an MSI Bundle of OpenOffice, assign it to 60 devices, and refresh all 60 by using a quicktask	25 minutes 30 seconds	1 hour 10 minutes 17 seconds

When the server is under load, and we created an MSI bundle and assigned it to 60 devices, there was a large increase in the amount of time it took to complete the task. In this situation, you should have a dedicated server for ZENworks Control Center so that there would be virtually no impact on performance.

The ZENworks Control Center is used by administrators to perform administrative tasks, including the management of content within the system. For environments that are managed by a small number of administrators (one or two), accessing ZENworks Control Center from a Primary Server that is also performing work might not cause performance issues. For larger implementations (several thousand devices, large amounts of daily content activity, and several administrators), having a dedicated Primary Server in place for ZENworks Control Center resolves potential performance issues.

3.2.3 Achieving Scalability in the Real World

Section 3.2.2, "Load Testing in the Novell SuperLab," on page 27 discussed testing in the Novell SuperLab to determine the limits of the ZENworks system. Scalability, on the other hand, is achieved through the proper placement of services, a well thought-out design, and the proper configuration of services within the ZENworks Configuration Management system itself.

For example, even though we know that a Primary Server can manage 3,000 devices, you should never deploy only one Primary Server in a 3,000-device environment. For this situation, we recommend the following as a starting point:

- ♦ Three Primary Servers to manage load and build a system that is fault tolerant.
- ♦ A dedicated Database Server using Sybase, Oracle, or Microsoft SQL Server.

This system should be further enhanced by considering the following:

- ♦ Using an L4 switch to manage fault tolerance and load balancing.

- ◆ Using DNS and aliases for managing the load placed on Primary Servers during deployment and registration.
- ◆ Using Closest Server Rules in ZENworks Locations to designate certain servers for specific functions (content, collection, etc.) and to exclude servers from specific functions, or all functions. If a Primary Server is not listed in the Closest Server Rule of a location for a particular role, then devices do not attempt to connect to it for that feature.
- ◆ Using a dedicated Primary Server for reporting.
- ◆ Using a dedicated Primary Server for imaging.
- ◆ Using a dedicated Primary Server for ZENworks Control Center. This is done mainly to control where the administrators upload content to ensure that the load is dedicated to a single Primary Server.
- ◆ Using Satellite devices for distribution of content.

The Primary Servers are the heart of your ZENworks Configuration Management environment. You want to protect these systems from major disruption. Primary Servers can be used for distribution of content, but this needs to be factored in to your design.

Some of the major factors that you need to consider with ZENworks Configuration Management and Primary Servers are the following:

- ◆ Each Primary Server can handle 1,000 concurrent connections.
- ◆ Each Primary Server can manage 3,000 devices that are registered with the ZENworks Management Zone.
- ◆ A ZENworks Management Zone can scale to 40,000 devices. This has been validated in the SuperLab and is what Novell recommends as the upper limit to the Management Zone size.

We also recommend that Primary Servers and the Database Server be on the same network, in the same data center. We do not recommend spanning WAN links with Primary Servers because replication of the Content Repository can cause utilization issues. Placement of services in a multi-site environment is done by utilizing the Satellite role, which is discussed in more detail in [Section 3.3, “Scalability of Satellite Devices,” on page 34](#).

3.2.4 Tuning the JVM and Tomcat

To utilize the 64-bit JVM (Java Virtual Machine) of ZENworks 11 SP2 to the best possible extent, you can increase the following values beyond the defaults:

- ◆ [“Maximum HTTP/HTTPS Tomcat Threads” on page 31](#)
- ◆ [“Increasing Heap Memory Size for the ZENworks Services” on page 32](#)

Maximum HTTP/HTTPS Tomcat Threads

ZENworks uses HTTPS threads to service incoming configuration, and authentication Web requests, and uses HTTP threads for content, and collection requests. By default, these threads are set to 200 for HTTP and 200 for HTTPS. This was originally a limitation of the 32-bit JVM, but it is no longer necessary, because ZENworks now uses the 64-bit JVM.

These values are found in the `server.xml` file in the following locations:

- ◆ Windows: `%ZENWORKS_HOME%\Share\tomcat\conf`
- ◆ Linux: `/opt/novell/zenworks/share/tomcat/conf`

To achieve further performance increases from your Primary Servers, you can change the thread values:

- 1 Stop the ZENworks services (ZENmonitor, ZENserver, and ZENloader)
- 2 Open the `server.xml` file for the operating system on which the Primary Server is running.
- 3 Locate the line with the text `<Connector port="80"`, and change the value for `maxThreads` as desired.
- 4 Locate the line with the text `<Connector port="443"`, and change the value for `maxThreads` as desired. Ensure that the values for the two ports are the same.
- 5 Save the file.
- 6 Start the ZENworks services again.

For the testing completed in our engineering labs, we used a server with 16 GB of RAM and found that increasing the thread counts to 600 each was the optimal point in terms of performance.

We suggest that you increment the threads in stages of 100 for both HTTP and HTTPS in order to monitor your performance.

Increasing Heap Memory Size for the ZENworks Services

ZENworks 11 SP2 uses the 64-bit JVM, so you can tune the Java memory allocations to allow ZENworks services to utilize more than the default 1 GB of memory. The sample settings in the following procedures were tested in the engineering lab on a server with 16 GB of RAM.

- ♦ [“Configuring the Maximum Heap Memory Size on a Linux Primary Server” on page 32](#)
- ♦ [“Configuring the Maximum Heap Memory Size on a Windows Primary Server” on page 33](#)

Configuring the Maximum Heap Memory Size on a Linux Primary Server

- 1 Stop the ZENworks services (ZENmonitor, ZENserver, and ZENloader).
- 2 Using a Linux text editor such as `vi` or `gedit`, create or modify the `/opt/novell/zenworks/bin/zenserversettings.sh` file with the following content:

```
JAVA_MIN_HEAP="-Xms1024m"
JAVA_MAX_HEAP="-Xmx1024m"
JAVA_MIN_PERM_SIZE="-XX:PermSize=128m"
JAVA_MAX_PERM_SIZE="-XX:MaxPermSize=256m"
JAVA_THREAD_STACK_SIZE="-Xss1m"
```

IMPORTANT: Change the `JAVA_MAX_HEAP` value from `"-Xmx1024m"` to `"-Xmx<desired memory in MB>m"`. For example, `"-Xmx4096m"` to configure 4GB.

When you increment the `JAVA_MAX_HEAP` value, ensure that you make the same changes for the ZENserver and the ZENloader services, so that they always have the same value. For example, if you configure the ZENserver heap memory as 4096 (4GB), you must configure the same for ZENloader.

You need to reserve RAM for the operating system, so change the values in increments that make sense.

- 3 Save the file.
- 4 Using a Linux text editor such as `vi` or `gedit`, create or modify the `/opt/novell/zenworks/bin/zenloadersettings.sh` file with the following content:


```
JAVA_MIN_HEAP="-Xms256m"  
JAVA_MAX_HEAP="-Xmx1024m"  
JAVA_MIN_PERM_SIZE="-XX:PermSize=128m"  
JAVA_MAX_PERM_SIZE="-XX:MaxPermSize=128m"
```

IMPORTANT: Change the `DEFAULT_MAX_HEAP` value from `"-Xmx1024m"` to `"-Xmx<desired memory in MB>m"`. For example, `"-Xmx4096m"` to configure 4GB.

When you increment the `JAVA_MAX_HEAP` value, ensure that you make the same changes for the ZENserver and the ZENloader services, so that they always have the same value. For example, if you configure the ZENserver heap memory as 4096 (4GB), you must configure the same for ZENloader.

You need to reserve RAM for the operating system, so change the values in increments that make sense.

5 Save the file.

6 Run the following commands:

```
chown zenworks.zenworks /opt/novell/zenworks/bin/zenserversettings.sh  
chown zenworks.zenworks /opt/novell/zenworks/bin/zenloadersettings.sh
```

7 Run the following commands:

```
chmod 755 /opt/novell/zenworks/bin/zenserversettings.sh  
chmod 755 /opt/novell/zenworks/bin/zenloadersettings.sh
```

8 Start the ZENworks services.

Configuring the Maximum Heap Memory Size on a Windows Primary Server

To configure the maximum heap memory size on a Windows Primary Server:

1 Stop the ZENworks services (ZENmonitor, ZENserver, and ZENloader).

2 Run `zenserverw`.

3 On the *Java* tab, change the *Maximum memory pool* from 1024 to a higher value. For example, 4096.

You need to reserve RAM for the operating system, so change the values in increments that make sense.

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

5 Run `zenloaderw`.

The *Novell ZENworks Server Properties* dialog box is displayed.

6 On the *Java* tab, change the *Maximum memory pool* from 1024 to a desired value. For example 4096.

When you increment the values, ensure that you make the same changes for both services, so they always have the same value. For example, if you increment the ZENserver settings to 4096, you must use the same settings for ZENloader.

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

8 Start the ZENworks services.

3.3 Scalability of Satellite Devices

The second area that you should carefully consider is the scalability of the Satellite devices. Satellite devices are primarily designed to reduce load on the network, not to reduce load on the Primary Servers. Satellite devices help reduce redundant traffic, load, and utilization from the WAN. Even if devices are located at a remote site, they connect to the central site for configuration and to check in with the Primary Servers to see if there is work to do. The actual work should be performed with remote Satellite devices strategically placed to service work requests from managed devices, including authentication, content distribution, collection, and imaging.

The following sections contain more information:

- ♦ [Section 3.3.1, “Factors Influencing Scalability,” on page 34](#)
- ♦ [Section 3.3.2, “Load Testing in the Novell SuperLab,” on page 34](#)
- ♦ [Section 3.3.3, “Achieving Scalability in the Real World,” on page 36](#)

3.3.1 Factors Influencing Scalability

The major factors influencing scalability of Satellite devices include:

- ♦ Disk I/O and the requests that the Satellite device is concurrently managing
- ♦ Size of the subnets and their respective network speed
- ♦ Services the Satellite device is performing (imaging, inventory collection, and distribution)
- ♦ Disk capacity (the Satellite device must have enough capacity to cope with the required content)
- ♦ Physical memory (RAM) installed on the Satellite device
- ♦ The number of managed devices the Satellite device is managing
- ♦ The frequency of distributions and the number of concurrent connections
- ♦ Whether inventory collection or software distributions are randomized
- ♦ Whether an L4 switch fronts the Satellite devices at a particular location
- ♦ Whether Satellite device groups are used
- ♦ Class of hardware (server-class hardware performs better than workstation-class hardware)
- ♦ Class of operating system (a Satellite device running on Windows Server can handle more requests and workload than a Satellite device running on Windows XP or Windows 7)

Keeping these factors in mind, you should build your design to manage the known devices and estimated ongoing workload.

3.3.2 Load Testing in the Novell SuperLab

Novell performed Satellite device scale tests using both server-class and workstation-class operating systems. As with testing that was performed on the Primary Server, the purpose of the tests was to find the point where the systems began to reach their limits. This gives us an understanding of scale under severe load.

The tests included the following:

- ♦ **Server-class Satellite devices:** Dell PowerEdge 2950, Dual Quad Core 2.0Ghz, 8 GB RAM, 2 X 300 GB SAS hard drives running Windows 2003 Enterprise.
- ♦ **Workstation-class Satellite devices:** White box, AMD 3400+, 2 GB RAM, 80 GB SATA hard drive running Windows XP SP3.

The Novell Corporate Configurations Test (CCT) team, using the baseline test of 250 bundles (1 KB file bundles), had the following results:

- ♦ A server operating system (Windows 2003 Enterprise) machine can scale to 1,000 managed devices.
- ♦ A workstation operating system (Windows XP SP3) machine can scale to 250 managed devices.

The following sections contain information about three tests performed in the SuperLab with Satellite devices:

- ♦ [“Test 1: Bundle Size” on page 35](#)
- ♦ [“Test 2: Server OS Delivering Multiple Chained Bundles” on page 36](#)
- ♦ [“Test 3: Workstation OS Delivering Multiple Chained Bundles” on page 36](#)

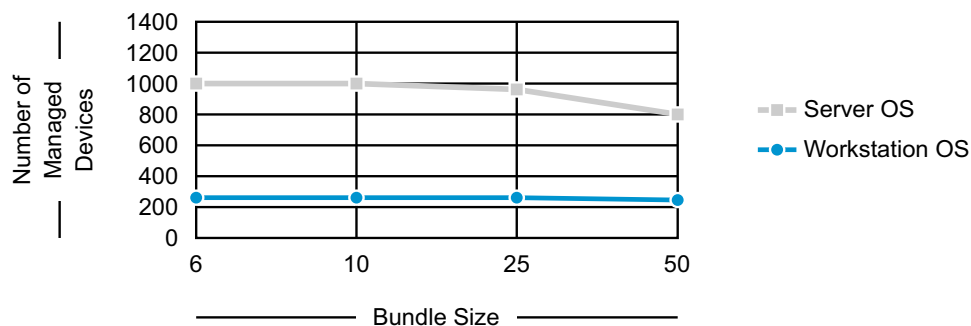
Test 1: Bundle Size

Test results show how large a single bundle can be to be distributed by a Satellite device to managed devices. These results are useful when you begin to estimate how many Satellite devices are required based on the ongoing estimated load. You need to calculate estimated load during the design phase as you work with the different groups that manage processes around software distribution, patch distribution, inventory collection, and image distribution. You need to know how frequently these processes are required, and the estimated size of the typical distribution or collection.

Bundle Size (MB)	Server OS	Server OS	Workstation OS	Workstation OS
	Number of Managed Devices in Test	Number of Managed Devices Successful	Number of Managed Devices in Test	Number of Managed Devices Successful
6	1004	1004	259	259
10	1004	1004	259	259
25	1004	968	259	259
50	1004	801	259	248

The following graph shows what you can expect in terms of Satellite device scalability given the conditions of the test:

Figure 3-3 Bundle Size.



The graph illustrates the probable scalability limitations of the Satellite device. Under normal load, and through the use of proper configuration parameters (for example, randomizing distributions and collections) we can comfortably conclude that a Satellite device running on server-class hardware

and Windows Server can scale to approximately 1,000 managed devices, and a Satellite device running on workstation-class hardware and Windows XP or Windows 7 can scale to approximately 250 managed devices.

Test 2: Server OS Delivering Multiple Chained Bundles

This test shows the results of a Satellite device running on a server OS delivering multiple chained bundles to connected managed devices. This information is useful when calculating how much load you can place on the Satellite device running on a Server OS when deploying applications that are chained. This obviously can differ greatly from deploying single bundles.

Number of Bundles	Bundle Sizes in MB	Total Number of Managed Devices	Number of Devices Successful Managed
5	10, 15, 20, 25, 30	999	996
4	5, 10, 15, 20	999	996

Test 3: Workstation OS Delivering Multiple Chained Bundles

This test shows the results of a Satellite device running on a workstation OS delivering multiple chained bundles to connected managed devices. This information is useful when calculating how much load you can place on the Satellite device on a workstation OS when deploying applications that are chained together. This obviously can differ greatly from deploying single bundles.

Number of Bundles	Bundle Sizes in MB	Total number of Managed Devices	Number of Devices Successfully Managed
5	10, 15, 20, 25, 30	259	259
4	5, 10, 15, 20	259	259

3.3.3 Achieving Scalability in the Real World

The testing in the SuperLab tests the upper limits of a Satellite device. It is important to note that if you are deploying a bundle that is less than 25 MB in size, we see successful distributions to both 250 and 1,000 managed devices from workstation-class and server-class Satellite devices. If this is known, we can safely assume that by doing the following, you can achieve these levels of scalability, and quite possibly much more:

- ◆ For larger sites (more than 250 managed device):
 - ◆ Have a dedicated Satellite device for imaging purposes.
 - ◆ Have a dedicated Satellite device for inventory collection if the collection frequency is high. In other words, if you are collecting daily, you want the server to be dedicated, but if you are collecting monthly, you can collapse this service into another Satellite device onsite.
 - ◆ Have a dedicated set of Satellite devices for software and patch distributions if the frequency of distributions is high. You want to randomize the distribution of software and avoid massive numbers of devices hitting the Satellite device at the same time.
 - ◆ Randomize the refreshes of managed devices at the site with Satellite devices.
- ◆ For smaller sites (fewer than 250 devices):
 - ◆ Have multiple Satellite device that share load and responsibility.

- ◆ Do not be significantly concerned about designating specific servers for specific functions.
- ◆ Randomize the refreshes of managed devices at the site with Satellite devices.

3.4 ZENworks Database

The ZENworks database is the most important aspect of the ZENworks infrastructure. The database contains all information about bundles, policies, configuration, and how these apply to the devices and users under management.

The main considerations that influence the choice of ZENworks database platform are as follows:

- ◆ **Number of devices you manage:** For environments with more than 3,000 devices, consider using Oracle or Microsoft SQL Server as the database platform.
- ◆ **Using clustering technologies for fault tolerance of database:** Using clustering ensures that the database is always available.
- ◆ **Virtualization**

For more information on ZENworks database see the following:

- ◆ [Section 3.4.1, “Virtualizing the ZENworks Database Server,” on page 37](#)
- ◆ [Section 3.4.2, “ZENworks Database Scalability,” on page 37](#)
- ◆ [Section 3.4.3, “Saving the ZENworks Database Password,” on page 38](#)
- ◆ [Section 3.4.4, “Sybase,” on page 38](#)
- ◆ [Section 3.4.5, “Using Sybase Mirroring to Enable High Availability of the Sybase Database,” on page 51](#)
- ◆ [Section 3.4.6, “Microsoft SQL Server,” on page 53](#)
- ◆ [Section 3.4.7, “Oracle,” on page 59](#)
- ◆ [Section 3.4.8, “Database Sizing and Performance Considerations,” on page 61](#)

3.4.1 Virtualizing the ZENworks Database Server

Novell does not recommend virtualization of the ZENworks database server. You should use a dedicated server for the ZENworks database to ensure that the available resources for the database are known and are under control. Placing the database on a server with other virtual machines can lead to performance degradation, which in turn can affect other aspects of ZENworks, from the performance of the ZENworks Control Center to the responsiveness of ZENworks on managed devices.

If you want to virtualize your database on a VMware ESXi server, and you are planning to utilize Microsoft SQL Server, please refer to VMware’s documentation regarding [Virtualizing Microsoft SQL Server on VMware ESXi \(http://communities.vmware.com/docs/DOC-8964\)](http://communities.vmware.com/docs/DOC-8964). This document needs to be reviewed prior to installing the database and other ZENworks services.

3.4.2 ZENworks Database Scalability

The following table lists the number of devices that different databases can handle in a production environment:

Table 3-2 Database Platform and Supported Number of Devices

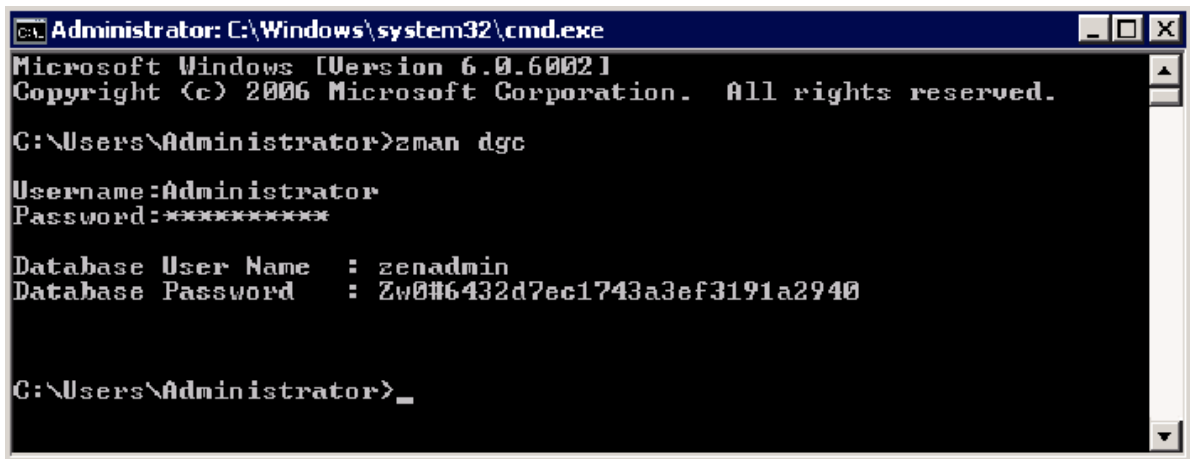
Database Platform	Number of devices
Sybase (embedded)	As many as 1,000 (lab environments)
Sybase (remote)	As many as 3,000
Microsoft SQL Server 2008 R2	1,500 to 40,000
Oracle 11g	1,500 to 40,000

Use the vendor database backup tools to regularly back up the database to ensure that if the database is lost, you can restore from a backup.

The following sections highlight the best practices when managing and maintaining your Database Server.

3.4.3 Saving the ZENworks Database Password

When you create a new ZENworks Zone, a database password is generated and subsequently used by each Primary Server. To back up the ZENworks database password, run the `zman dgc` command and save the retrieved password.



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>zman dgc

Username:Administrator
Password:*****

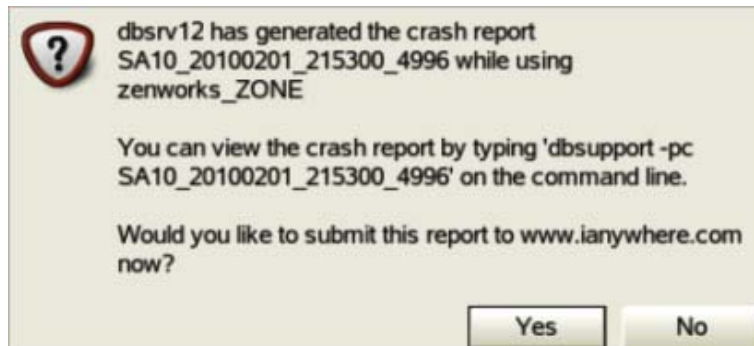
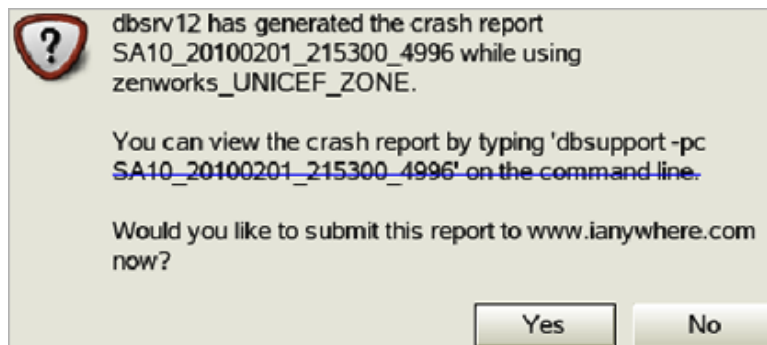
Database User Name : zenadmin
Database Password  : Zw0#6432d7ec1743a3ef3191a2940

C:\Users\Administrator>_
```

3.4.4 Sybase

Regular backups must be created on the ZENworks database. You cannot create backups of the database if:

- ♦ The `dbsrv12` process is crashing periodically.



- ◆ The database service does not start.
- ◆ Database server crashes irrecoverably.

For more information on different tasks performed on the Sybase, see:

- ◆ “Full Backups” on page 40
- ◆ “Incremental Backups” on page 40
- ◆ “Online Backups” on page 40
- ◆ “Offline Backups” on page 40
- ◆ “Sybase Backup Strategy” on page 40
- ◆ “Sybase Database Backups” on page 40
- ◆ “Database Validation” on page 41
- ◆ “Database Recovery” on page 41
- ◆ “Sybase Tuning and Maintenance” on page 42
- ◆ “Enabling Sybase Debug mode” on page 42
- ◆ “Enabling Sybase Debug mode (Verbose)” on page 43
- ◆ “Moving Database Files” on page 44
- ◆ “Sybase Performance Monitoring” on page 44
- ◆ “Index Fragmentation” on page 45
- ◆ “Table Fragmentation” on page 46
- ◆ “Rebuilding the Sybase Database” on page 48
- ◆ “Tips for rebuilding a Sybase Database” on page 51
- ◆ “Engaging with Novell Support” on page 51

Full Backups

Creating a full backup is the best option as it includes a copy of both the database and the transaction log file. In this situation, the restoration and recovery of the database is much easier but can be expensive in terms of the required storage. You must perform full backups regularly, but less frequently than other backups. In order to reduce the required disk space, the transaction log can be truncated. In conjunction with this, administrators have a choice of performing the following:

- ♦ **Archive backup:** ZENworks database and transaction log is stored in one file.
- ♦ **Image backup:** ZENworks database and transaction logs are stored in separate files.

Incremental Backups

An incremental backup makes a copy of the transaction log file only and can be restored using the `dbtran` command. They are used frequently. The data is lost if this file gets corrupt.

Online Backups

An online backup is performed without stopping the ZENworks Database server using the `zman database-backup <path to backup directory>` command. They are used for incremental backups. Though this provides higher availability for the database server, it results in a slower backup process. Use `"SET TEMPORARY OPTION BACKGROUND_PRIORITY = 'ON';"`

Online backups can use incremental backup (transaction logs only) or full backup.

Offline Backups

An offline database backup requires the database server to be stopped. This method can be used in conjunction with a scheduling mechanism to automate the process, such as Windows Task Scheduler or `crontab`. Offline backups can use incremental backup (transaction logs only) or full backup and lend itself better to do a full backup quickly. They are used with full backups at less frequent intervals.

Sybase Backup Strategy

Some general tips to consider when defining the database backup strategy are as follows:

- ♦ Back up your database after every server update.
- ♦ Make sure your database backup has the same name as your current database.
- ♦ Check disk space as this can impact the best strategy for your backup.
- ♦ Events and notifications can be scheduled through the database server itself.

Sybase Database Backups

The simplest method for backing up the Sybase database is to use the `zman` command: The `zman` command does a full online backup, and truncates the transaction log. For more information, see [Database Commands \(http://www.novell.com/documentation/zcm10/pdfdoc/zcm10_utils/zcm10_utils.pdf\)](http://www.novell.com/documentation/zcm10/pdfdoc/zcm10_utils/zcm10_utils.pdf) in the *ZENworks 10 Configuration Management Asset Management Command Line Utilities Reference guide*. Also, you can see information on Sybase backup techniques at the following location: (<http://tldp.org/HOWTO/Sybase-ASA-HOWTO/backup.html>)

```
BACKUP DATABASE DIRECTORY '<backupDirectory>' TRANSACTION LOG TRUNCATE
```


Starting in the Sybase that ships with 10.3 (also available as an FTF), you can use Sybase Central.

- ♦ %ZENWORKS_HOME%\share\ASA\Sybase Central 5.0.0\win32\scjview.exe
- ♦ /opt/novell/zenworks/share/sybase/bin32s/sybcentral500/scjview

Back up not only your database, but also the data in the content repository, certification information, and other recommended files.

Database Validation

Novell recommends that you validate the data before and after backups. The validation process does not check the ZENworks schema, but focuses on maintaining the database integrity. The validation process can be run using Sybase Central or from the command line as follows:

```
dbvalid -c "UID=zenadmin;PWD=<password>; ENG=<database service name>"
```

If the ZENworks database validation fails, try unloading the database and restoring the last known good backup.



Database Recovery

To recover the ZENworks database in Sybase, you first need to understand the problem. The best recovery strategy depends on the type of problem that has occurred. When recovering, Novell recommends that you perform recovery in offline mode. Make sure that the database is stopped and all services on all Primary Servers have also been stopped to ensure that the Primary Servers do not attempt to connect to the database. To recover, use one of two methods:

- ♦ Apply the good transaction logs to the last full backup copy of your database. (Sybase has a utility called dbtran for this purpose.)
- ♦ Restore the last good backup of your database by copying it in place.

Sybase Tuning and Maintenance

Tuning the database is an important step in improving the performance of ZENworks. If possible, place the transaction log on a separate physical drive from the database and the operating system to improve disk I/O completion. For more information, see “[Improving Performance in SQL Anywhere](http://www.sybase.de/detail?id=1023801)” (<http://www.sybase.de/detail?id=1023801>).

Also consider changing the startup options of Sybase by editing the `zenworks_database.conf` file. The `zenworks_database.conf` file contains all of the database server startup options and as is located in the following locations:

- ♦ Linux: `/etc/opt/novell/zenworks`
- ♦ Windows: `%ZENWORKS_HOME%\conf`

Some of the parameters to be changed are as follows:

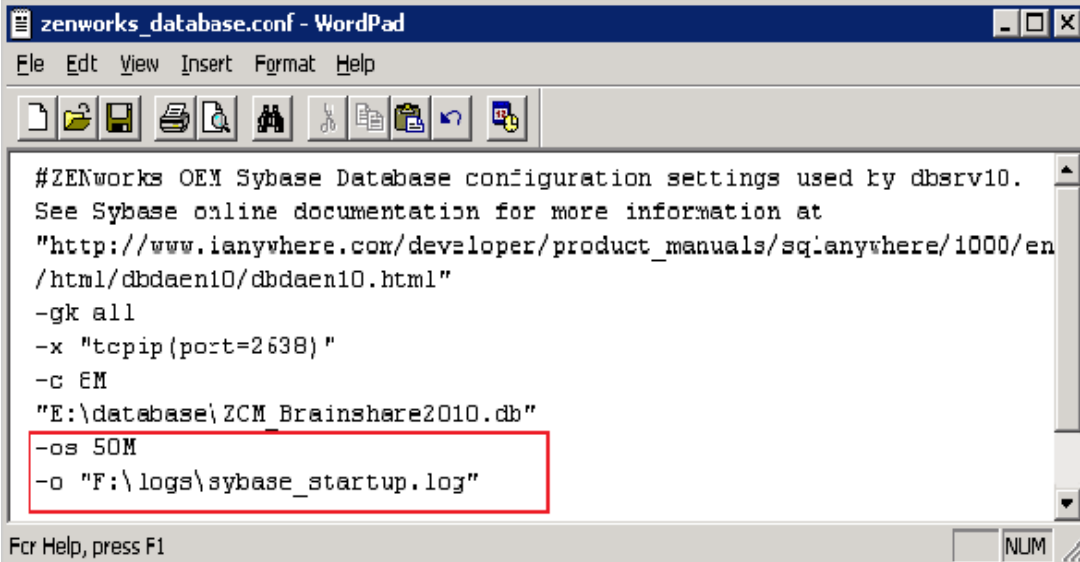
- ♦ Increase the cache size (`-c`).
- ♦ Set the minimum cache size to a value larger than the default (`-cl`).
- ♦ Change the checkpoint interval (`-gc`).
- ♦ The number of physical processors to use (`-gt`). This can be useful way of limiting the processors used when using an embedded database to allow for processing power to be assigned to the ZENworks Primary Server.

By default the cache size is set to 8 MB. Change this to a value more aligned with your environment.

Enabling Sybase Debug mode

If necessary, the database can be placed in debug mode by updating the `zenworks_database.conf` file as follows:

- ♦ `-os 50M` (size of log file for messages)
- ♦ `-o <location>`
- ♦ For custom logging include the `-zr` option and set options specific to the types of statements you are debugging



```
zenworks_database.conf - WordPad
File Edit View Insert Format Help
#ZENworks OEM Sybase Database configuration settings used by dbsrv10.
See Sybase online documentation for more information at
"http://www.ianywhere.com/developer/product_manuals/sqlanywhere/1000/en
/html/dbdaen10/dbdaen10.html"
-gk all
-x "tcpip(port=2638)"
-c 8M
"E:\database\ZCM_Brainshare2010.db"
-os 50M
-o "F:\logs\sybase_startup.log"
```

Enabling Sybase Debug mode (Verbose)

To place the Sybase database in verbose debug mode, set the following parameters:

- ◆ -zs 50M (size of request logging)
- ◆ -os 50M (size of log file for messages)
- ◆ -zr all (log sql operations)
- ◆ -z (connection diagnostics)
- ◆ -zt (timing information)
- ◆ -o <location>

When logging is enabled, verify the log sizes as well as the disk space that is being consumed.

More information on Sybase startup parameters can be at the Sybase Web site:

http://www.iAnywhere.com/developer/product_manuals/sqlanywhere/1001/en/html/dbdaen10/dabengines.html

A sample Sybase is seen below:

- ◆ (Blue) Database fragmentation warnings
- ◆ (Green) Loading transaction log
- ◆ (Red) Database server starts

```
I. 02/23 15:14:30. SQL Anywhere Network Server Version 10.0.1.3960
I. 02/23 15:14:30.
I. 02/23 15:14:30. Copyright © 2001-2007, iAnywhere Solutions, Inc.
I. 02/23 15:14:30. Portions copyright © 1988-2007, Sybase, Inc.
I. 02/23 15:14:30. All rights reserved. All unpublished rights reserved.
I. 02/23 15:14:30.
I. 02/23 15:14:30. This software contains confidential and trade secret information of
I. 02/23 15:14:30. iAnywhere Solutions, Inc.
I. 02/23 15:14:30. Use, duplication or disclosure of the software and documentation
I. 02/23 15:14:30. by the U.S. Government is subject to restrictions set forth in a license
I. 02/23 15:14:30. agreement between the Government and iAnywhere Solutions, Inc. or
I. 02/23 15:14:30. other written agreement specifying the Government's rights to use the
I. 02/23 15:14:30. software and any applicable FAR provisions, for example, FAR 52.227-19.
I. 02/23 15:14:30.
I. 02/23 15:14:30. iAnywhere Solutions, Inc., One Sybase Drive, Dublin, CA 94568, USA
I. 02/23 15:14:30.
I. 02/23 15:14:30. 1 physical processor(s) detected.
I. 02/23 15:14:30. Networked Seat (per-seat) model. Access to the server is limited to 10000 seat(s).
I. 02/23 15:14:30. This server is licensed to:
I. 02/23 15:14:30. ZENworks
I. 02/23 15:14:30. Novell, Inc.
I. 02/23 15:14:30. Running windows Vista Build 6001 Service Pack 1 on x86 (X86_64)
I. 02/23 15:14:30. Server built for x86 processor architecture
I. 02/23 15:14:30. Authenticated Server licensed for use with Authenticated Applications only
I. 02/23 15:14:30. 8192K of memory used for caching
I. 02/23 15:14:30. Minimum cache size: 8192K, maximum cache size: 1506816K
I. 02/23 15:14:30. Using a maximum page size of 16384 bytes
I. 02/23 15:14:30. TCP using winsock version 2.2
I. 02/23 15:14:30. IPv6 support enabled
I. 02/23 15:14:30. Starting database "ZCM_Brainshare2010" (E:\database\ZCM_Brainshare2010.db) at Tue Feb 23 2010 15:14
I. 02/23 15:14:30. Database recovery in progress
I. 02/23 15:14:30. Last checkpoint at Tue Feb 23 2010 15:12
I. 02/23 15:14:30. Checkpoint log...
I. 02/23 15:14:30. Performance warning: Database file "E:\database\ZCM_Brainshare2010.db" consists of 6 disk fragments
I. 02/23 15:14:31. Transaction log: ZCM_Brainshare2010.log...
I. 02/23 15:14:31. Rollback log...
I. 02/23 15:14:31. Checkpointing...
I. 02/23 15:14:31. Starting checkpoint of "ZCM_Brainshare2010" (ZCM_Brainshare2010.db) at Tue Feb 23 2010 15:14
I. 02/23 15:14:31. Finished checkpoint of "ZCM_Brainshare2010" (ZCM_Brainshare2010.db) at Tue Feb 23 2010 15:14
I. 02/23 15:14:31. Recovery complete
I. 02/23 15:14:31. Database "ZCM_Brainshare2010" (ZCM_Brainshare2010.db) started at Tue Feb 23 2010 15:14
I. 02/23 15:14:31. This database is licensed for use with:
I. 02/23 15:14:31. Application: ZENworks
I. 02/23 15:14:31. Company: Novell, Inc.
I. 02/23 15:14:31. Database server started at Tue Feb 23 2010 15:14
```

```

I. 02/23 15:14:36. Starting UDP listener on IP address (::1):2638
I. 02/23 15:14:36. Starting UDP listener on IP address 127.0.0.1:2638
I. 02/23 15:14:36. This is a class A network address
I. 02/23 15:14:36. TCP/IP link started successfully
I. 02/23 15:14:36. Now accepting requests
I. 02/23 15:14:36. TCP/IP link, function WSAREcv, error code 10053
I. 02/23 15:14:36. TCP/IP link, function WSAREcv, error code 10053
I. 02/23 15:14:36. TCP/IP: Received connection request from 127.0.0.1:49660.
I. 02/23 15:14:36. Connection from 127.0.0.1:49660 assigned connection ID 3
I. 02/23 15:14:36. <,3,CONNECT
I. 02/23 15:14:36. C,3,UID=zenadmin
I. 02/23 15:14:36. Connection ID 3: "zenadmin" connected to database "ZCM_Brainshare2010" from SQL Anywhere 10.0.1 (3960) client over TCPI
I. 02/23 15:14:36. Connection ID 3: AppInfo is IP=151.155.170.157;HOST=VM12-W2K8-32;OS='windows Vista Build 6001 Service Pack 1';PID=0xf2E
I. 02/23 15:14:36. Connection ID 3: Server character set conversion is enabled, but not required
I. 02/23 15:14:36. using character set "windows-1252"
I. 02/23 15:14:36. >,3,CONNECT,3
I. 02/23 15:14:36. <,3,PREPARE,SELECT @@version, if 'A'<>'a' then 1 else 0 endif, isnull(property('ISIQ'),'NO'), isnull(connection_propert
I. 02/23 15:14:36. >,3,PREPARE,65536
I. 02/23 15:14:36. <,3,EXEC,65536
I. 02/23 15:14:36. P,3,[S]DUMMY<seq>
I. 02/23 15:14:36. >,3,EXEC
I. 02/23 15:14:36. <,3,DROP_STMT,65536
I. 02/23 15:14:36. >,3,DROP_STMT
I. 02/23 15:14:36. <,3,PREPARE,SET TEMPORARY OPTION time_format = 'hh:nn:ss';SET TEMPORARY OPTION timestamp_format = 'yyyy-mm-dd hh:nn:ss.
I. 02/23 15:14:36. >,3,PREPARE,65537
I. 02/23 15:14:36. <,3,EXEC,65537

```

Moving Database Files

If you need to move the database files, such as to a new separate physical disk, this operation is as simple as a file copy. When the file has been moved, adjust the `zenworks_database.conf` file to point to the new location.

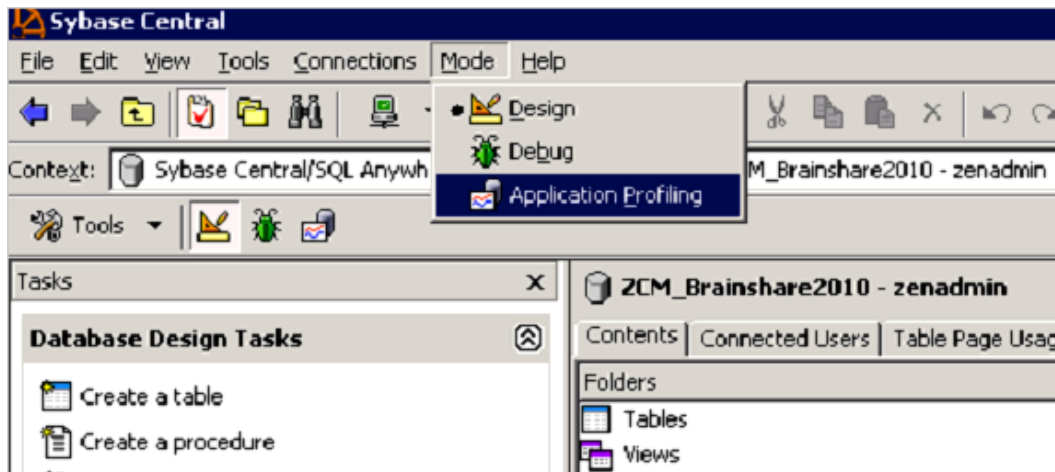
If the transaction log needs to be separated from the database, this can be achieved by using the `dblog` command.

```
dblog -t <location of new transaction log> <path to database>
```

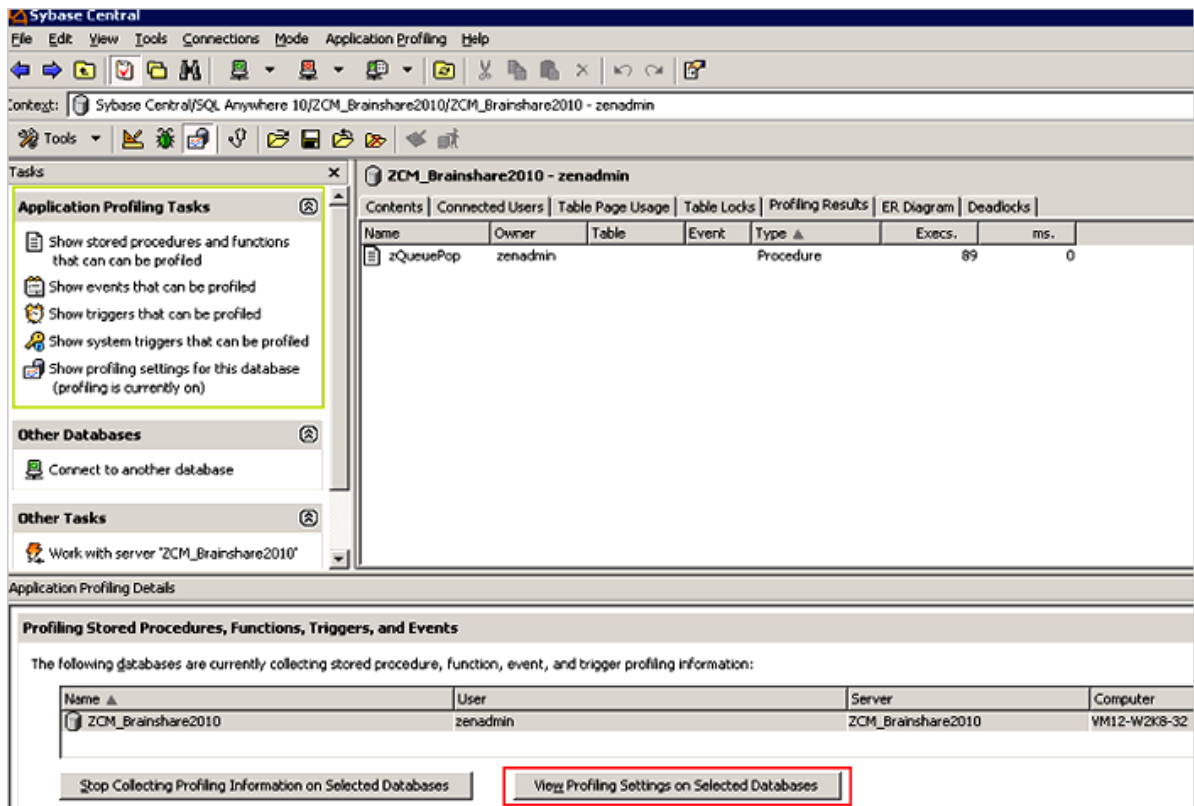
When this is done, the transaction log can be moved and once again placed on a separate physical disk. Make sure that logs are still included in the future backups.

Sybase Performance Monitoring

Sybase SQL Anywhere comes with built-in performance monitoring capabilities in the Sybase Central tool.



After starting the Application Profile Wizard, the tool tracks the transactions, such as stored procedures being run and queries that are performed on the database during that period of time. Do not leave this process running because it can have detrimental effects on database performance.



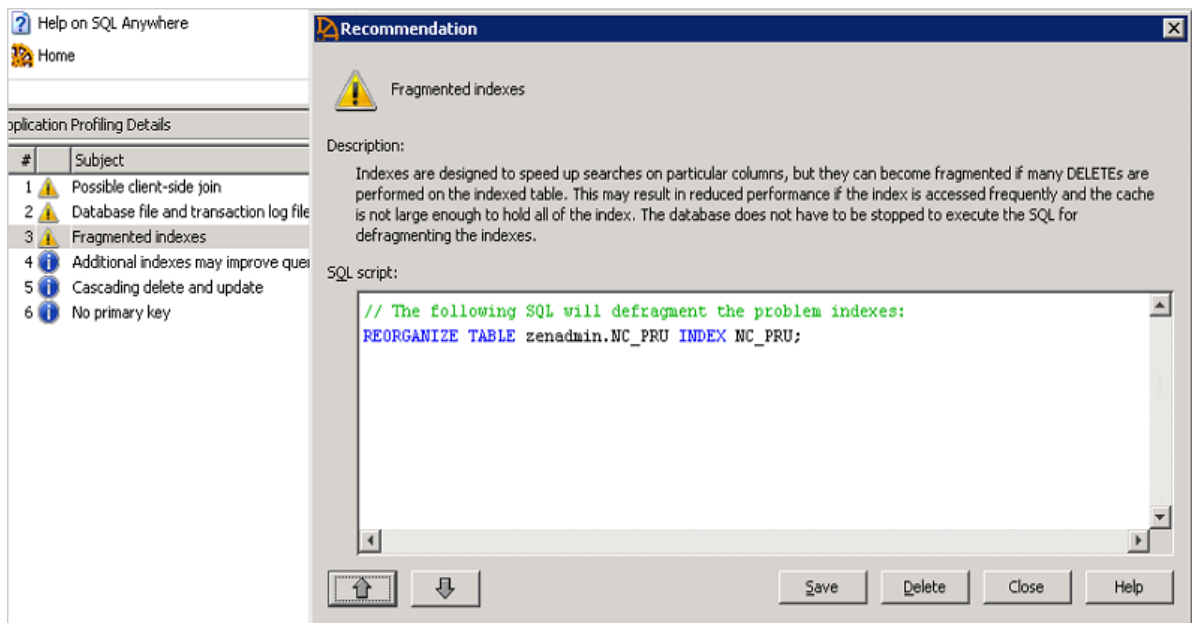
Performance monitoring can report on items such as:

- ◆ Deadlock information
- ◆ CPU usage
- ◆ Trigger and stored procedure efficiency
- ◆ Queries being executed
- ◆ Query run times

Longer profiling times provide greater accuracy but can cause the database to become less responsive so it is important to only use this tool for short periods of time.

Index Fragmentation

Fragmented indexes are a top reason for performance degradation of the ZENworks database.



Novell recommends that indexes that you check and rebuild in the following scenarios:

- ◆ System Update
- ◆ After enabling ZENworks Patch Management in the Zone
- ◆ After adding a large number of devices
- ◆ After adding a large number of bundles, or bundles with lots of content defined

Table Fragmentation

In addition to this, you might need to use the `REORGANIZE TABLE <table name>` command if the database has become severely fragmented. The following tables should be watched closely for fragmentation:

- ◆ zMessage
- ◆ zObjectInfo
- ◆ zStatusEvent

The following example shows an SQL report detailing the table fragmentation that exists within the database.

The screenshot shows a SQL client window with a menu bar (File, Edit, SQL, Data, Tools, Window, Help) and a toolbar with navigation icons. The 'SQL Statements' pane contains the query: `select * from sa_table_fragmentation() where segs_per_row > 1;`. The 'Results' pane displays a table with the following data:

	TableName	rows	row_segments	segs_per_row
1	ISYSPHYSIDX	899	943	1.048943270300334
2	ISYSTAB	568	608	1.070422535211268
3	NC_Component	37,657	37678	1.000557665241522
4	NC_Product	72,240	72244	1.000055370985604
5	NC_Workstation	105	106	1.00952380952381
6	PATCHFLAGS	16,167	19626	1.213954351456671
7	PATCHLICENSE	356	365	1.025280898876404
8	PATCHPACKAGE	2,943	3087	1.048929663608563
9	PATCHSIGNATURE	2,007	2037	1.014947683109118
10	zAction	4,460	4483	1.005156950672646
11	zActionSet	2,221	2230	1.004052228725799
12	zContent	3,135	4006	1.277830940988836
13	zInstallationPackage	155	170	1.096774193548387

The following example shows how to reorganize the PATCHFLAGS and zContent by using an SQL query.

SQL Statements

```

SET TEMPORARY OPTION BACKGROUND_PRIORITY = 'ON';
REORGANIZE TABLE PATCHFLAGS;
REORGANIZE TABLE zContent;
CHECKPOINT
SET TEMPORARY OPTION BACKGROUND_PRIORITY = 'OFF';
select * from sa_table_fragmentation() where segs_per_row > 1;

```

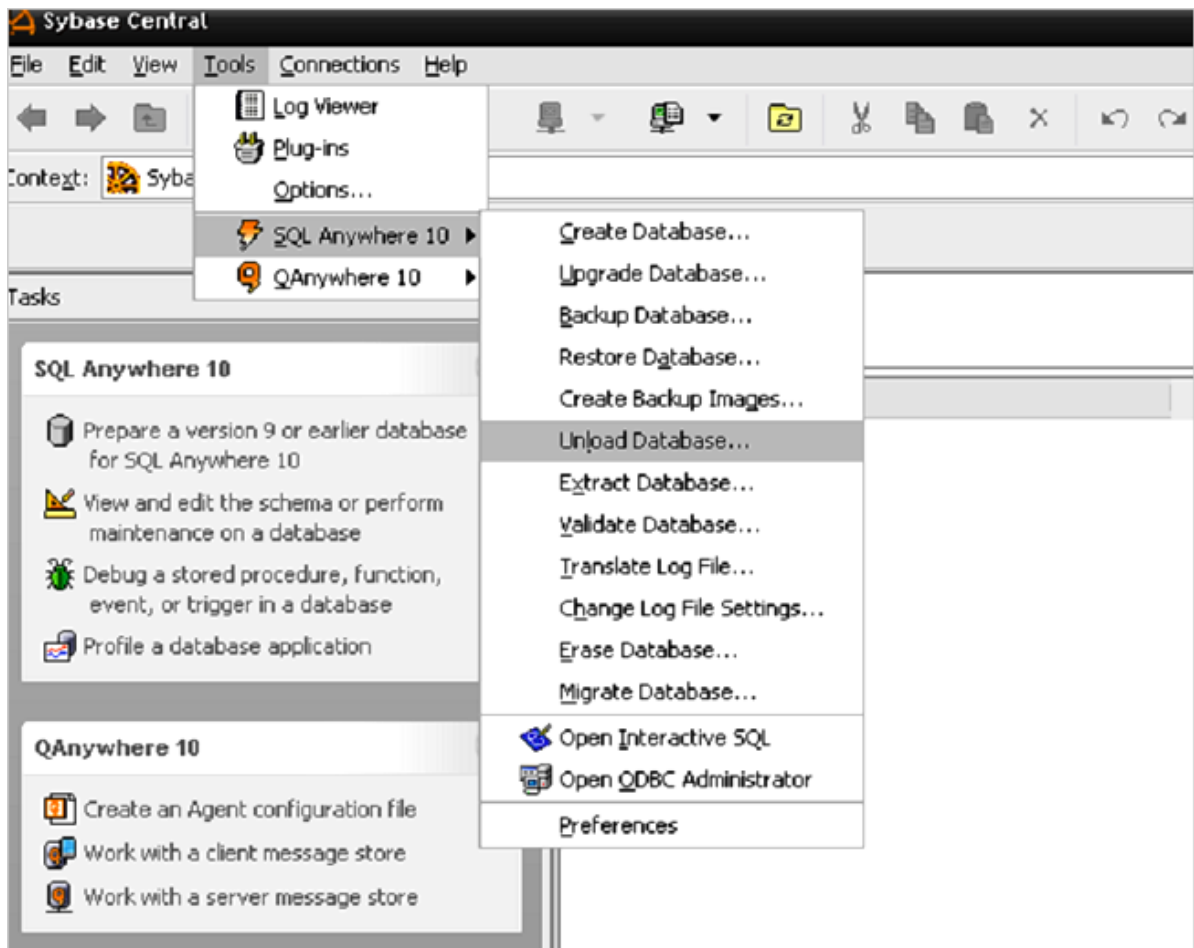
Results

	TableName	rows	row_segments	segs_per_row
1	ISYSPHYSIDX	899	943	1.048943270300334
2	ISYSTAB	568	608	1.070422535211268
3	NC_Component	37,657	37678	1.000557665241522
4	NC_Product	72,240	72244	1.000055370985604
5	NC_Workstation	105	106	1.00952380952381
6	PATCHLICENSE	356	365	1.025280898876404
7	PATCHPACKAGE	2,943	3087	1.048929663608563
8	PATCHSIGNATURE	2,007	2037	1.014947683109118
9	zAction	4,460	4483	1.005156950672646
10	zActionSet	2,221	2230	1.004052228725799
11	zInstallationPackage	155	170	1.096774193548387

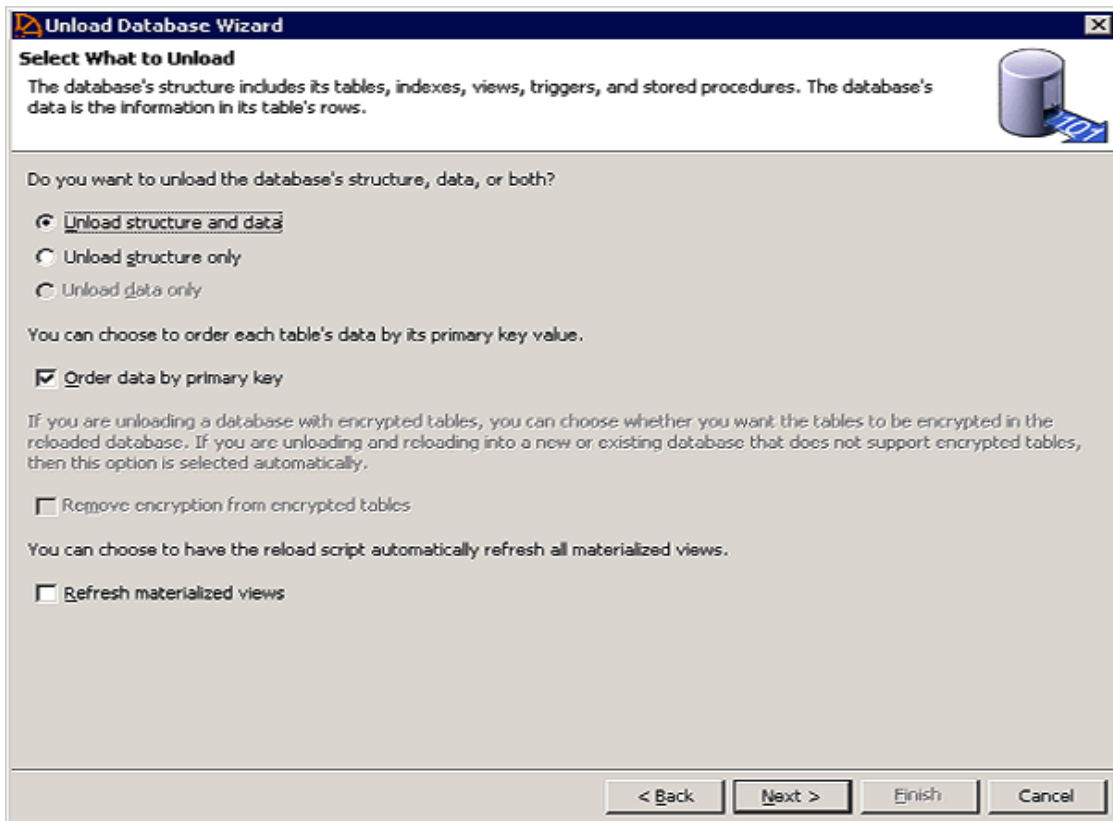
	TableName	rows	row_segments	segs_per_row
1	PATCHFLAGS	16,167	16167	1
2	zContent	3,135	3135	1

Rebuilding the Sybase Database

If fragmentation exists on numerous tables and the database is large, a quicker method for fixing fragmentation is to rebuild the entire database by using the Sybase Central tool.



When you unload the database, select all objects to re-build the entire database.



When you unload and reload the database, you are given an option to encrypt the database. Novell recommends that you do not use this option.

The database can also be rebuilt on the command line by using the `dbunload` command:

- ♦ Unload into a new database:
 - ♦ `dbunload -c "UID=zenadmin;PWD=<database password>;ENG=<database service name>" -an "<path to new db>"`
- ♦ Unload database definitions into .dat files and reload
 - ♦ `dbunload -c "UID=zenadmin;PWD=<database password>;ENG=<database service name>" "<path to unload directory>"`
 - ♦ `dbinit -p 4096 <path to new db>`
 - ♦ `dbisql -c "UID=DBA;PWD=sql;DBF='<path to new db>'" read reload.sql`

When you rebuild the database, if the database is large, performance increases can be made by increasing the page size. The options for Sybase Page Sizing are the following:

- ♦ 2048
- ♦ 4096
- ♦ 8192
- ♦ 16384

Since ZENworks 10 SP3, new Sybase databases are created with a page size of 16384. However, each time the database is unloaded, the page size can be adjusted. Novell recommends page size of either the 16384 or 8192 for customers using Sybase. Setting the page option can be performed using Sybase Central or using the `dbinit -p` option as show above.

Tips for rebuilding a Sybase Database

Until you copy the newly built database in place of your existing database (remember to stop the service), your servers will use the old database. If you have a problem connecting to the database service, use the `dblocate` command to verify the following:

- ♦ The service name that you are trying to connect to.
- ♦ If the service is running.

Engaging with Novell Support

If you encounter problems with your database, collect the following information before engaging with Novell Support:

- ♦ The output from the log file enabled and specified in the `zenworks_database.conf` file.
- ♦ The version of the database you are running (The Sybase tool 'dblocate' will provide that information when run from a command prompt).
- ♦ The transaction log and approximate time of the issue
- ♦ The date of your last backup
- ♦ Optional: Deadlock information, connection, information, and profiling statistics from the Sybase Central tool

3.4.5 Using Sybase Mirroring to Enable High Availability of the Sybase Database

Sybase SQL Anywhere supports database mirroring as a method to implement high availability and fault tolerance. This technique requires multiple database servers and is therefore not set up by default with ZENworks 11 SP2.

NOTE: Mirroring should not be implemented as a means to distribute the database work to remote locations. Mirrored database servers should be connected over a high-speed link.

For more information on, see Database Mirroring on the Sybase Web site:

(http://www.ianywhere.com/developer/product_manuals/sqlanywhere/1000/en/html/dbdaen10/da-da-highavailability-s-4980336.html)

Useful Reference Sites for Sybase

- ♦ Getting the latest Sybase packages.
 - ♦ (<http://download.novell.com/protected/Summary.jsp?buildid=JhOYPc1Q5Tc~>)
- ♦ Sybase Reference Documentation
 - ♦ (http://www.ianywhere.com/developer/product_manuals/sqlanywhere/1001/en/pdf/dbdaen10.pdf)

- ♦ (http://www.ianywhere.com/developer/product_manuals/sqlanywhere/1001/en/html/)
- ♦ (http://www.ianywhere.com/developer/product_manuals/sqlanywhere/1001/en/html/dbdaen10/da-dbengines.html)
- ♦ Sybase Physical Limitations
 - ♦ (http://www.ianywhere.com/developer/product_manuals/sqlanywhere/1001/en/html/dbdaen10/da-lt-size.html)
- ♦ Rebuilding the database
 - ♦ (<http://realworlddba.wordpress.com/2008/02/04/index-rebuild-versus-reorganize-whats-the-difference/>)
 - ♦ (<http://breckcarter.sys-con.com/node/107002/mobile>)
- ♦ Automated Database Backup
 - ♦ (<http://iablog.sybase.com/hinsperg/2009/02/automated-database-backups/>)
 - ♦ (http://www.novell.com/documentation/zcm10/zcm10_system_admin/data/bjm5wmx.html)
- ♦ Increase your Database Performance
 - ♦ (<http://www.sybase.com/detail?id=1023801>)
- ♦ Backup Syntax and Help
 - ♦ (http://www.ianywhere.com/developer/product_manuals/sqlanywhere/1001/en/html/dbrfen10/rf-backup-statement.html)
- ♦ Setting up Mirroring (High Availability)
 - ♦ (http://www.ianywhere.com/developer/product_manuals/sqlanywhere/1000/en/html/dbdaen10/da-da-highavailability-s-4980336.html)
- ♦ Changing the location of the transaction log
 - ♦ (http://dcx.sybase.com/1100en/dbadmin_en11/changing-log-location-backup.html)
- ♦ Moving to dbspaces
 - ♦ (<http://m.sybase.com/detail?id=1011479>)
- ♦ Database Startup Options
 - ♦ (http://www.ianywhere.com/developer/product_manuals/sqlanywhere/1001/en/html/dbdaen10/da-dbengines.html)
- ♦ Location of Sybase Bug Fixes
 - ♦ (http://origin1.sybase.com/swx/12952/rdme_1001_ebf_3974.html)
- ♦ Other Sites
 - ♦ (http://www.dba-oracle.com/concepts/starting_database.htm)
 - ♦ (<http://tldp.org/HOWTO/Sybase-ASA-HOWTO/backup.html>)
- ♦ Backing up the database using ZMAN
 - ♦ *ZENworks 11 SP2 System Administration Reference*
- ♦ Sybase Central
 - ♦ (http://m.sybase.com/files/Product_Overviews/iAS_techdoc_sa10_command_line_utilities_1054563.pdf)
- ♦ Performance Monitoring
 - ♦ (<http://www.sybase.com/detail?id=1023801>)

3.4.6 Microsoft SQL Server

The most important aspects of managing and maintaining a Database Server that is hosted on a Microsoft SQL Server are the following:

- ♦ The customer must have the skills in-house, or readily available (contractor, consultant, or partner) to manage and maintain the Microsoft SQL Server based on the best practices that Microsoft outlines for regular database management.
- ♦ There must be regular database backup routines in place. This should also be documented in the design document.
- ♦ There must be regular database maintenance routines in place. This should also be documented in the design document.
- ♦ Considerations for clustering (high availability) of the Database Server should be made and documented.
- ♦ In general Novell does not recommend virtualizing the ZENworks database server. However, it is possible to run Microsoft SQL Server on a virtual host. Please see the following documentation for more information on [VMware communities \(http://communities.vmware.com/docs/DOC-8964\)](http://communities.vmware.com/docs/DOC-8964).

Microsoft SQL Server 2008 R2 has a Maintenance Plan Wizard in the SQL Server Management Studio. This tool should be readily available to any customer that is utilizing Microsoft SQL Server in their data centers.

Maintenance tasks that can be scheduled include the following:

- ♦ Check database integrity
- ♦ Shrink database
- ♦ Reorganize index
- ♦ Rebuild index
- ♦ Update statistics
- ♦ Back up database

These tasks should be thoroughly understood before performing them on a live system that is hosting the ZENworks Configuration Management database.

Microsoft recommends the following best practices for managing Microsoft SQL Server 2008 R2:

- ♦ Backups should be performed daily.
- ♦ A Database Integrity Check should be performed every 14 days.
- ♦ Reorganizing or rebuilding indexes should be done when fragmentation is excessive. If fragmentation is greater than 30 percent, an index should be rebuilt. To determine the fragmentation of the indexes in your database, use the dynamic memory view `sys.dm_db_index_physical_stats`. Novell recommends that rebuilding indexes should be done at least once per week because the clustered indexes will be fragmented over 75 percent within a few days of insert/update activity. This is a contributing factor to lag, escalating locks, and eventual deadlocks.

A good overview of the Maintenance Plan Wizard is found on the [MSSQLTips Web site \(http://www.mssqltips.com/tip.asp?tip=1127\)](http://www.mssqltips.com/tip.asp?tip=1127).

Microsoft also offers the SQL Server 2008 R2 Best Practices Analyzer Tool. This tool addresses a wide variety of best practices as outlined by Microsoft. This tool can be found on the [Microsoft TechNet Web site \(http://www.microsoft.com/downloads/details.aspx?FamilyId=DA0531E4-E94C-4991-82FA-F0E3FBD05E63&displaylang=en\)](http://www.microsoft.com/downloads/details.aspx?FamilyId=DA0531E4-E94C-4991-82FA-F0E3FBD05E63&displaylang=en).

For example, the following recommendations were listed for a ZENworks Configuration Management installation on SQL Server 2008 R2:

- ◆ Place data and log files on separate drives for database [zenworks_database] on server [server_name]
- ◆ Check database integrity at least every 14 days for database [zenworks_database] on server [server_name]

The Best Practices Analyzer tool also indicates that log files and data files should be placed on separate hard drives to improve I/O, thus improving overall performance of the Database Server. However, this can be a problem if the database files are hosted on a SAN or inside virtual machines, which are both trends in the industry. Any exceptions to recommend best practices should also be well documented in the design document created during the design phase.

The Microsoft SQL Server Tuning Wizard makes suggestions about indexes you might want to add to the database. However, it uses the term “missing indexes,” which is misleading to anyone who might interpret this as a mandate. Each of these suggestions must be analyzed, balancing the performance trade-offs between inserting or updating data in a given table versus the variety of queries that might be made against a table. Indexes slow inserts and updates, while benefiting specific queries. There are a number of ways this analysis can be performed; the tuning wizard is just a first step. You should use SQL tracing tools and analyze the SQL demands that ZENworks Configuration Management is making on the database while it performs various functions, such as registration, bundle creation and deployment, policy enforcement, inventory, and so forth. After you have accurate information on what kind of load ZENworks Configuration Management is placing on the database, you can then add your indexes.

Tips for using Microsoft SQL as the ZENworks Database platform

- ◆ “Don't use Dynamic Ports” on page 54
- ◆ “Managing Large Transaction Logs” on page 55
- ◆ “Read Committed Snapshot” on page 55
- ◆ “Index Fragmentation” on page 56

Don't use Dynamic Ports

Dynamic Ports can automatically reassign connections to different ports. This can potentially cause problems with ZENworks install or post-installation tasks which in some cases rely on static ports such as 1433 to be active. To disable the dynamic ports, go into the MS SQL Configuration Manager and edit the ports used on the database for TCP/IP. The *Dynamic Ports* field should be left blank and a static port should be specified.

See the following links for more information:

- ◆ (<http://blogs.msdn.com/b/sqlserverfaq/archive/2008/06/02/how-to-change-the-dynamic-port-of-the-sql-server-named-instance-to-an-static-port-in-a-sql-server-2005-cluster.aspx>)
- ◆ (<http://www.mssqltips.com/tip.asp?tip=1412>)

Managing Large Transaction Logs

Large and growing transactions are an indication that a backup plan could be optimized. For example, it is not desirable to have transactions logs larger than the database. Large transaction logs are typically caused by three factors:

1. Old transactions not being disregarded as part of the backup. When configuring the backup, it is important that old transactions from the backup point are not included as they have already been committed into the database.
2. Infrequent backups
3. Initial transaction log size initially set too low and the auto grow size percentage is not set large enough

Please see the following links and excerpts on this topic:

- ♦ (http://sqlblog.com/blogs/aaron_bertrand/archive/2009/07/27/oh-the-horror-please-stop-telling-people-they-should-shrink-their-log-files.aspx)
- ♦ (<http://support.microsoft.com/kb/873235>)

In rare cases, you might need to shrink the transaction log, b/c of a performance issue or otherwise, run:

```
--Shrink the transaction log a lot!!  
USE <database_name>;  
GO  
DBCC SHRINKFILE(<database_name>_log, 1)  
BACKUP LOG <database_name> WITH TRUNCATE_ONLY  
DBCC SHRINKFILE(<database_name>_log, 1)  
GO
```

Where <database_name> is the name of the database on which you wish to shrink the transaction log.

For more information on this topic see:

(http://www.karaszi.com/SQLServer/info_dont_shrink.asp)

Read Committed Snapshot

Read Committed Snapshot allows transactions to share locks to databases so you can allow two distinct processes to update the same table at the same time. If this setting is not enabled, large amounts of blocking can occur that decreases ZENworks performance.

To enable Read Committed Snapshot (no quotes on db name), run the following command from an SQL editor run:

```
USE '<database name>';  
GO  
ALTER DATABASE <database name> SET SINGLE_USER WITH ROLLBACK IMMEDIATE;  
GO  
ALTER DATABASE <database name> SET READ_COMMITTED_SNAPSHOT ON;  
GO
```

```
ALTER DATABASE <database name> SET MULTI_USER;
```

```
GO
```

To verify that `read_committed_snapshot` has been successfully enabled, run:

```
SELECT is_read_committed_snapshot_on
```

```
FROM sys.databases
```

```
WHERE name= '<database name>'
```

Index Fragmentation

Novell recommends that you defragment indexes every two weeks. You can do this by creating scripts or by using third-party utilities to easily defragment the entire database. You can use the following scripts to rebuild indexes and detect fragmentation in MS SQL server:

```
DBCC SHOWCONTIG
```

```
DBCC DBREINDEX
```

If a table or index is more than 50% fragmented, you should re-index it to increase performance.

For more information, see:

- ♦ (http://www.mssqlcity.com/Articles/Adm/index_fragmentation.htm)
- ♦ (http://www.sql-server-performance.com/tips/rebuilding_indexes_p1.aspx)

Troubleshooting Microsoft SQL

- ♦ “Enabling Deadlock Tracing” on page 56
- ♦ “ERRORLOG Location” on page 56
- ♦ “Backing up Microsoft SQL Databases” on page 57
- ♦ “Taking a Backup” on page 57
- ♦ “Performance Tuning and Profiling a Microsoft Database” on page 58

Enabling Deadlock Tracing

If the database is experiencing high utilization caused by blocking or deadlocks, enable deadlock logging from an SQL editor, such as Microsoft SQL Management Studio, as follows:

```
dbcc traceon(1204,1222,-1)
```

See (<http://msdn.microsoft.com/en-us/library/ms188396.aspx>, for more information.)

NOTE: Do not perform maintenance during production or when servers are running. If this is not possible, you should use single user mode for long, resource-intensive operations.

ERRORLOG Location

The Microsoft SQL error log is found by default at: Program Files\Microsoft SQL Server\MSSQL.n\MSSQL\LOG\ERRORLOG

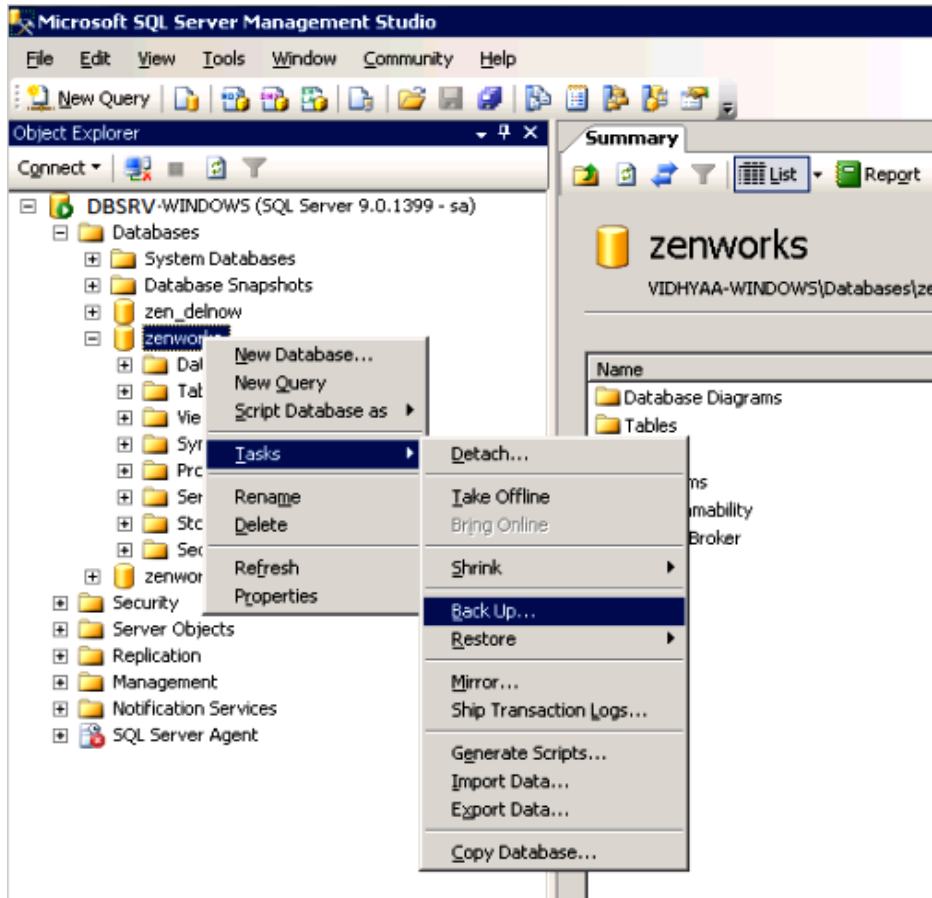
For more information see, (<http://msdn.microsoft.com/en-us/library/ms187885.aspx>)

Backing up Microsoft SQL Databases

Novell recommends that the Microsoft SQL Server Management Studio is used to manage backups, alternatively customers can create automatic scripts to do regular backups.

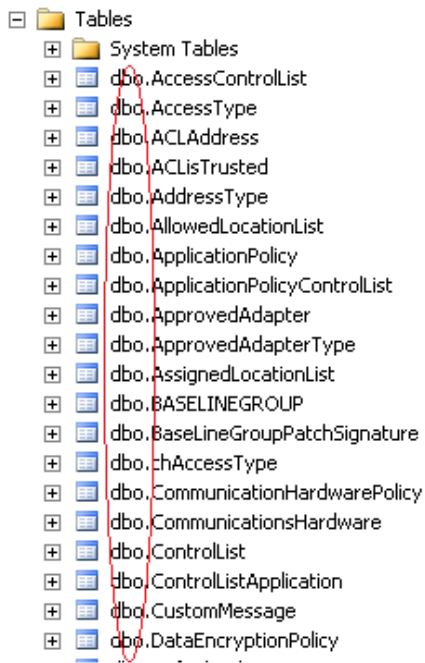
Taking a Backup

The following screen shots show the process of starting the backup process of a Microsoft SQL database using Microsoft SQL Server Management Studio.



For more information on backup best practices for Microsoft SQL server, see (<http://msdn.microsoft.com/en-us/library/ms175477.aspx>)

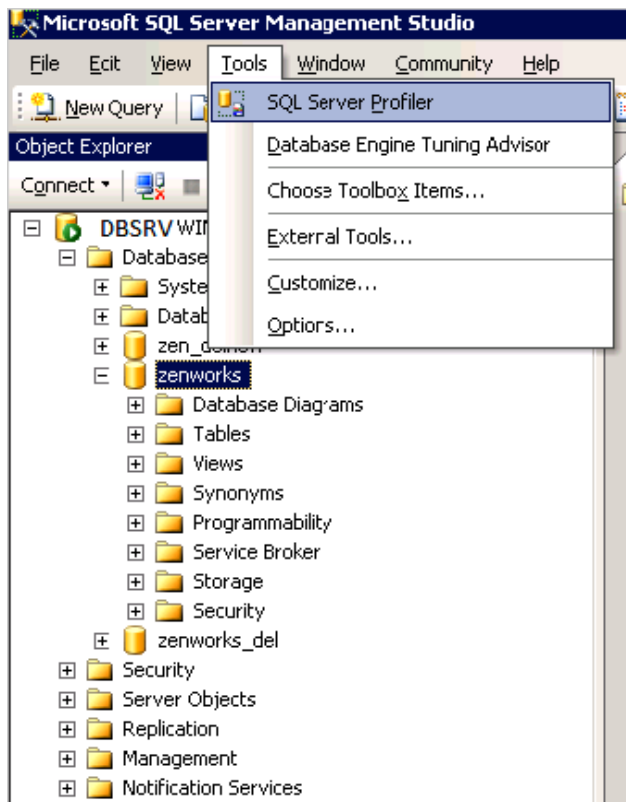
During the backup configuration, check the Ownership of tables and procedures to ensure that ZENworks tables are owned by dbo and not DB Owner. Ownership can change if you authenticate as a user other than the ZENworks user, then make changes.



Performance Tuning and Profiling a Microsoft Database

Microsoft SQL Server Management Studio provides the SQL Server Profiler application as shown below. This program will allow the administrator to see what SQL statements are being made in real-time and can be a useful tool in debugging database issues.

NOTE: Novell recommends that you consult with Novell Support before using the Database Engine Tuning Advisor for additional indexing of the ZENworks database.



3.4.7 Oracle

For performance and maintenance suggestions in an environment where Oracle is the Database Server hosting the ZENworks Configuration Management database, you must rely on the knowledge and expertise of the Oracle database administrator at the customer site. The individuals responsible for the day-to-day management of the Oracle infrastructure must be involved in the ZENworks Configuration Management deployment project from the beginning.

However, you should familiarize yourself with some of the administrative concepts about Oracle database management. The [Oracle Database Documentation Web site \(http://www.oracle.com/technology/documentation/database11g.html\)](http://www.oracle.com/technology/documentation/database11g.html) contains information about Oracle 11g and should be used as a reference.

In addition, you should also familiarize yourself with some of the performance tuning concepts for an Oracle Database Server, especially the reference documentation on the SQL Performance Analyzer. This information is available in the [Oracle Database Performance Tuning Guide \(http://download.oracle.com/docs/cd/B19306_01/server.102/b14211/toc.htm\)](http://download.oracle.com/docs/cd/B19306_01/server.102/b14211/toc.htm).

Best practice information suggested by Oracle regarding backup and recovery can be found on the [Oracle Web site \(http://download.oracle.com/docs/cd/B19306_01/server.102/b14220/backrec.htm#CNCPT031\)](http://download.oracle.com/docs/cd/B19306_01/server.102/b14220/backrec.htm#CNCPT031). The onsite Oracle database administrators should be familiar with these concepts and procedures. They administrators simply need to know what additional information they need to back up as a result of the implementation of ZENworks Configuration Management.

The following section describes some key points to consider when configuring an Oracle database for use with ZENworks:

- ◆ “Shared vs Dedicated Server Modes” on page 60
- ◆ “Important Log Locations” on page 60

- ♦ “Character Encoding” on page 60
- ♦ “SQL Developer vs. SQL Plus” on page 60

Shared vs Dedicated Server Modes

Most customers use Dedicated Server Mode as the default, and in some cases Shared connection mode can be used. At any given time a ZENworks Primary Server can have up to approximately 150 connections to the ZENworks database. Each connection with Oracle utilizes a certain amount of RAM, if the number of Primary Servers multiplied by the number of connections causes the required RAM to exceed what can be addressed by the operating system, such as with a 32bit OS which is limited 4GB, Shared Server Mode can be used to combat this. Shared Server Mode allows connections to be pooled and shared across a single memory allocation.

If the customer notices a large number of dedicated connections being rejected, use the following command to determine the status of connection rejection for a particular listener:

```
lsnrctl status
```

For more information, see (http://www.dba-oracle.com/t_mts_multithreaded_servers_shared.htm)

Important Log Locations

The `alert.log` is located at the path specified by the `sql` command:

```
show parameter BACKGROUND_DUMP_DEST
```

The `listener.log` is be found by checking the `Listener Log File` path after running `lsnrctl status` from a command prompt.

See the following locations for more information:

- ♦ (http://download.oracle.com/docs/cd/B14117_01/network.101/b10775/listenercfg.htm)
- ♦ (http://www.orafaq.com/wiki/Alert_log)

Character Encoding

Oracle supports some hybrid versions of UTF-8, but ZENworks requires true UTF-8 or UTF-16. The following commands report on the character encoding supported by the database:

- ♦ `select value from nls_database_parameters where parameter = 'NLS_CHARACTERSET';`
- ♦ `select value from nls_database_parameters where parameter = 'NLS_NCHAR_CHARACTERSET';`

SQL Developer vs. SQL Plus

SQL Developer and SQL Plus are two tools traditionally used by the administrators to execute SQL commands to manage the Oracle server. SQL Developer allows you to maintain history and is easier to run queries from. You can find more information on SQL Developer at:

SQL Developer (<http://www.oracle.com/technetwork/developer-tools/sql-developer/downloads/index.html>)

Sqlplus can output to a file. For example, to output the information contained in the `zZENServer` table into a file at `/tm/sqldata.dat`, simply run the following command:

```
SQL>SPOOL /tmp/sqldata.dat
```

```
SQL>select * from zZENServer;
```

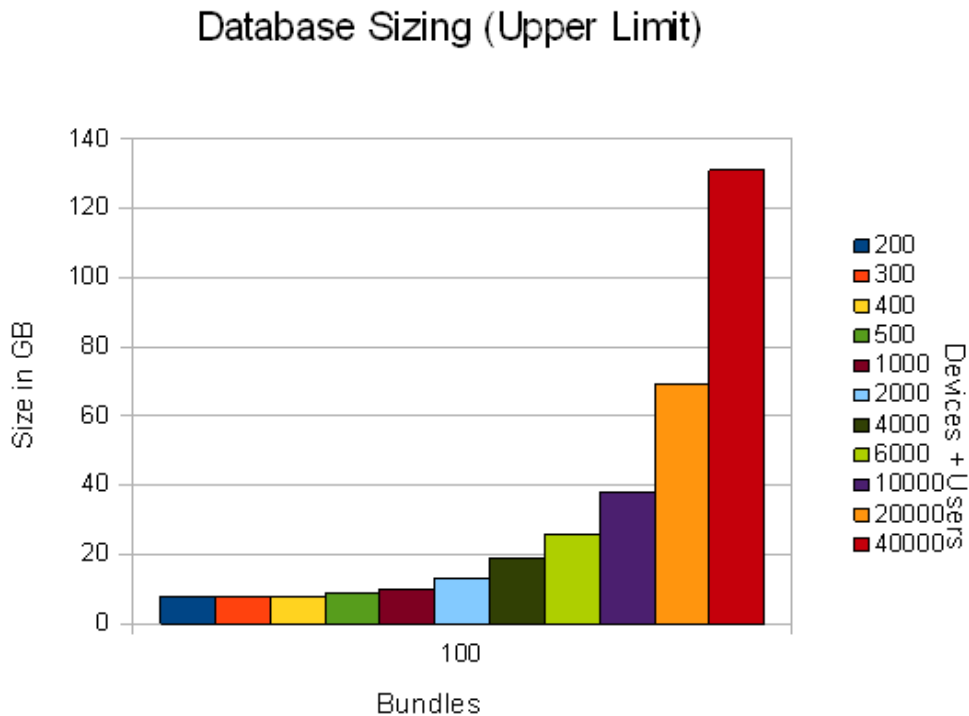
```
SQL>SPOOL OFF
```

3.4.8 Database Sizing and Performance Considerations

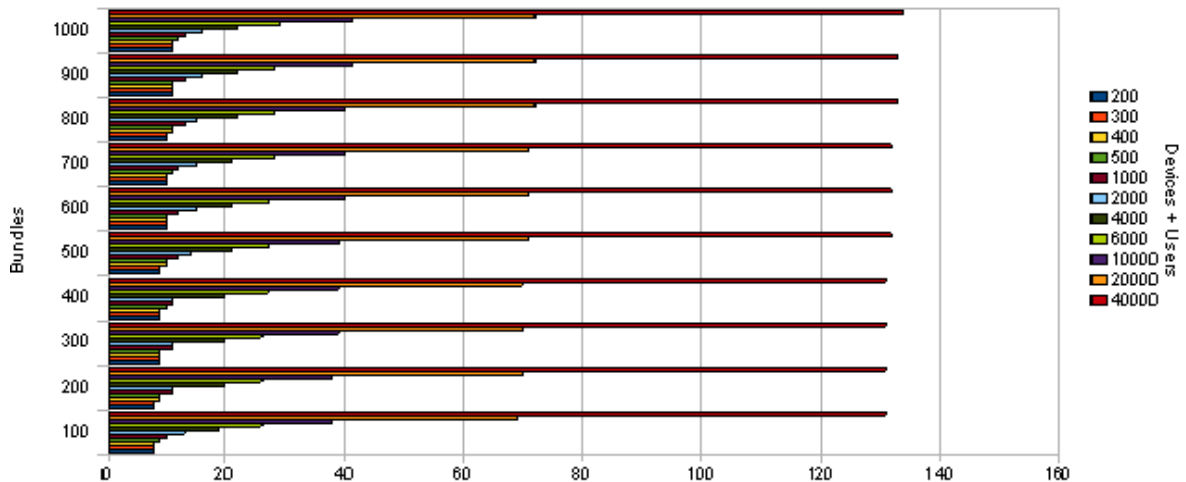
Although it is not possible to accurately predict the size of ZENworks database, it is possible to identify the factors that influence database size and provide some basic guidelines. The factors that affect the size of the ZENworks database are as follows:

- ◆ Number of users under management
- ◆ Number of devices under management
- ◆ Number of bundles
- ◆ Number of ZENworks policies
- ◆ Products that are enabled in the ZENworks Zone, such as Asset Management, Configuration Management, Patch Management, Endpoint Security Management, and ZENworks Reporting Server.

The following chart gives an indication of the types of database size to expect based on the numbers of users and devices in a ZONE with 100 bundles.



The following chart gives an indication of the types of database sizes to expect based on the number of bundles, devices, and users in a ZENworks Zone.



Disk space requirements are not the only consideration to make when designing the Database Server. Best practices for fault tolerance, maintenance, and performance need to be considered along with the general calculations for overall database size.

Most larger customers have Service Level Agreements that commit to minimal downtime and require robust storage capabilities. For sites with more than 10,000 devices, RAID (mirror with stripe) is recommended for the database, the transaction log, the TempDB, and the TempDB log. In fact, these four items need to be located on four separate LUNs (four separate disks or four separate logical arrays of disks). This addresses potential reliability issues.

Database Servers are very sensitive to disk performance. More small disks are always faster than a few large disks. This must be discussed while planning the database because a single 10 GB drive for a site with 10,000 devices might not perform adequately, although it might meet the database sizing formula. Ten smaller drives should perform much better.

Testing and monitoring are an essential part of database configuration. You must measure the throughput (MB/sec) that the application is demanding of the database, and size the disk array accordingly. In addition, the operating system and executables do not have high I/O requirements and can reside on a mirrored array (a single mirrored pair) to provide reliability with no added performance.

ZENworks Configuration Management requires a dedicated Database Server that is not shared with other database applications. This needs to be discussed during the design phase so that everyone involved in the project (especially the database administrator) is fully aware of the requirements. This might not be the case in very small implementations of ZENworks Configuration Management.

3.5 Virtualization Considerations

A major consideration for the design of the customer’s infrastructure is whether or not the customer is willing to virtualize some of the ZENworks Configuration Management infrastructure components. With version 10.2, the components are supported on both VMware and Xen. This could be an excellent low-cost alternative to hosting more ZENworks Configuration Management servers on fewer physical servers.

For example, if the customer needs to deploy three physical servers in the data center, it might be possible to increase this number to two or three hosted virtual servers on two physical servers. This would create additional fault tolerance and redundancy, as well as better performance across the board.

NOTE: For optimal performance of the Primary Servers running on VMware ESX, set the reserved memory size to the size of the guest operating system memory. For more information, see TID 7005382 in [Novell Support Knowledgebase \(http://support.novell.com/search/kb_index.jsp\)](http://support.novell.com/search/kb_index.jsp).

3.6 Ports Used by ZENworks Components

ZENworks Configuration Management uses a number of ports to communicate, based on specific functions and features. These ports must be considered when building the design of the infrastructure because they need to be open on firewalls if services reside behind them.

The following table outlines the ports that are used by ZENworks Configuration Management, and gives a description of what services use them, and why. This information should be shared early in the design phase, and should be reviewed by the network services teams.

Table 3-3 ZENworks Configuration Management Ports

Port	Description
HTTP (TCP 80) Stateful Primary Server and Satellite devices	Used to transmit content between the Primary Server or Satellite devices and managed devices. The Primary Server downloads patch license information and checksum data over HTTPS (port 443), and the actual patch content files over HTTP (port 80). ZENworks Patch Management license information is obtained from the Lumension licensing server (http://novell.patchlink.com) , and the patch content and checksum data is retrieved from an AKAMAI hosted content distribution network (novell.cdn.lumension.com). You must ensure that the firewall rules allow outbound connections to these addresses because the patch content distribution network is a large fault tolerant network of cache servers.
HTTPS (TCP 443) Stateful Open on the Primary Server	Used to transmit configuration metadata, authentication credentials, and tokens between the Primary Server and managed devices. Used for the Tomcat secure port. It is also used by default to download system updates from the Novell Customer Center and to download Product Recognition Update (PRU). Primary Server downloads patch license related information and checksum data over HTTPS (port 443), and the actual patch content files over HTTP (port 80). ZENworks Patch Management license information is obtained from the Lumension licensing server (http://novell.patchlink.com) , the patch content and checksum data is retrieved from an AKAMAI hosted content distribution network (novell.cdn.lumension.com). You must ensure that the firewall rules allow outbound connections to these addresses because the patch content distribution network is a large fault tolerant network of cache servers.
CASA (TCP 2645) Stateful Open on the Primary Server	Used to transmit authentication credentials and tokens between the Primary Server and managed devices when the Tomcat server listening on Port 443 is busy.

Port	Description
LDAP / LDAPS (TCP 389 / TCP 636) Stateful Open on the Directory Server	Used to transmit directory information between the Primary Server and Directory Server (Novell eDirectory or Microsoft Active Directory).
Sybase (TCP 2638) Stateful Open on the Database Server	Used for JDBC communication between Primary Servers and an internal or external Sybase database.
SQL (TCP 1433) Stateful Open on the Database Server	Used for JDBC communication between Primary Servers and an internal or external Microsoft SQL Server database.
Oracle (TCP 1521) Stateful Open on the Database Server	Used for JDBC communication between Primary Servers and an internal or external Oracle database.
Imaging (TCP 998) Stateful Open on the Primary Server and imaging Satellite devices	Used to transmit images and requests for work to do between the Primary Server and machines being imaged.
Proxy DHCP (UDP 67 / UDP 4011) Open on the Primary Server and imaging Satellite devices	Used to answer DHCP requests for PXE information. The standard DHCP port (67) is used if the server is not also a DHCP server; otherwise, the BINL port (4011) should be used.
TFTP (UDP 69) Open on the Primary Server and imaging Satellite devices	Used to send and receive TFTP data for PXE devices.
ZMGPreboot (UDP 13331) Open on Primary Server and imaging Satellite devices	Allows PXE devices to communicate with the PBServ service to determine work to do. Required because the TCP stack now exists in the PXE environment.
ZENworks VNC (5950) Open on the managed device	Allows remote control and other remote operations to be performed. Communication is between the managed device and the Administration Console.
ZENworks VNC Request (5550) Open on the Administration Console	Allows remote management requests to be sent by managed devices. Communication is between the Administration Console and the managed device.
Windows File and Print Sharing / CIFS (137-139) Open on devices you want to discover via WinAPI and on CIFS servers where you want to store 3rd party images.	Communication is between the Primary Server and the managed device or the WinProxy and the managed device.
ICMP Open on devices you want to discover	Used to determine if a device exists on the network so that it can be further interrogated. Communication is between the Primary Server or WinProxy and the device you want to discover.

Port	Description
Agent Management Port (TCP 7628)	Communication is between the Primary Server and the Agent.
Open on managed devices used to send quick tasks to the managed device	
Wake-On-LAN Port (UDP 1761)	Used to forward subnet-oriented broadcast magic packets for Wake-On-LAN.
Remote Management Proxy Port (5750)	Used by the remote management proxy to listen for the incoming remote management requests from the remote management viewer.

A more comprehensive version of this table is found in [Section C.4, “Extended Port Chart Including Port Usage,”](#) on page 176.

3.7 Network Considerations

How network services are used plays a big role in the success of the overall deployment. Ensure that you understand this area very well and involve the right people in the project from the start.

Individuals and departments that you want to notify and involve include:

- ♦ **Network services:** The teams that manage the physical network infrastructure and hardware.
- ♦ **Security services:** The teams that manage the security aspects of the network infrastructure and services.
- ♦ **Operations:** The teams that manage the provisioning of services and resources to the devices that ZENworks Configuration Management will manage.

The following sections contain more information:

- ♦ [Section 3.7.1, “Infrastructure vs. Bandwidth: Satellite Devices,”](#) on page 65
- ♦ [Section 3.7.2, “DNS and DHCP Services,”](#) on page 67
- ♦ [Section 3.7.3, “Time Synchronization,”](#) on page 68
- ♦ [Section 3.7.4, “Support for the NetWare Operating System,”](#) on page 68

3.7.1 Infrastructure vs. Bandwidth: Satellite Devices

When you consider the requirements for infrastructure, it is important to look at the available bandwidth for a workstation, in addition to the requirements of the management product. It might be necessary to update all devices as soon as possible.

By reducing the amount of infrastructure in place, ZENworks Configuration Management becomes more reliant on the available bandwidth to each device when deploying software.

To calculate the available bandwidth for a given site, a number of formulas can be used. The examples in this section indicate the amount of data that can be transmitted to a device within a given one-hour period. The formula assumes that a local Satellite device is not present. Therefore, all software downloads must be served by the WAN link to a Primary Server. Although these formulas are not completely accurate, and are based on a number of assumptions, they can be used to indicate which sites are good candidates for a Satellite device. As a rule of thumb, most remote sites are good candidates for a Satellite device because your goal is to always deliver content and collect

information from managed devices quickly and efficiently. Generally speaking, delivering content across a WAN infrastructure to multiple managed devices is not an efficient use of network resources.

The following formula defines how to calculate the maximum amount of data that can be transmitted to a device within a given one-hour period:

$$\frac{\left(\left(\frac{\text{Available Bandwidth (Mbps)}}{8} \right) \times 3600 \right)}{\text{(Connected Devices)}} = \text{MB per device per hour}$$

The result of this formula provides information on the amount of data that can be transmitted to each device within a one-hour period.

Available bandwidth in this formula is not the total link speed. Other data is transmitted over the link within a given hour and must be taken into account, for example:

- ♦ Internet traffic
- ♦ File and print
- ♦ Directory authentication
- ♦ Line of Business applications
- ♦ VOIP

In the following examples, sites with different numbers of devices and link speeds are used to demonstrate the levels of bandwidth available to a device within a one-hour period.

Two sites have been chosen: SITE 1 (650 devices with a 100 MB link) and SITE 2 (20 devices with a 10 MB link). For the purposes of the calculation, the formula assumes that approximately 95 percent of the available bandwidth is being used by other applications.

Based on link speeds, number of devices, and assumed available bandwidth, the formula gives the following results for SITE 1:

$$\frac{\left(\left(\frac{5 \text{ Mbps}}{8} \right) \times 3600 \right)}{650} = 3.46 \text{ MB per device per hour}$$

In a one-hour period, it is possible to transmit 3.46 MB to every device at SITE 1 if you use all of the bandwidth available to ZENworks Configuration Management. This site, because of its size and lack of bandwidth per device, should be considered as a candidate to host a Satellite device.

Based on link speeds, number of devices, and assumed available bandwidth, the formula gives the following results for SITE 2:

$$\frac{\left(\left(\frac{0.5 \text{ Mbps}}{8} \right) \times 3600 \right)}{20} = 11.25 \text{ MB per device per hour}$$

In a one-hour period, it is possible to transmit 11.25 MB to every device at SITE 2 if you use all of the bandwidth available to ZENworks Configuration Management. In this situation, you might not choose to place a Satellite device at this site because the level of bandwidth per device is relatively high.

When you take this all into account, the main requirements for choosing which sites should host a Satellite device vary from one installation to the next. For example, some customers, even though the available bandwidth with SITE 2 is high, might still want to have a device locally designated as a Satellite device. In this case, a workstation-class machine should be more than sufficient to manage the devices at that site.

The suggested placement of Satellite devices should be based on simple rules. Some examples of sites that are good candidates for Satellite devices are as follows:

- ♦ Sites with more than 200 devices.
- ♦ Sites that have high cost or limited access links between the MD and Primary Servers.
- ♦ Sites where the bandwidth per device per hour is less than x . In the examples above, 5 MB was chosen because this is the average size of a patch.
- ♦ Sites that have secure locations to store devices. Customers might not want to place dedicated Satellite devices in locations where they cannot be secured. In other words, you want to avoid a situation where a user turns off the Satellite device or physically removes it from the network.
- ♦ Sites with limited or costly access to WAN infrastructure.

3.7.2 DNS and DHCP Services

You should ensure that your network environment is well designed for ZENworks Configuration Management. You need to ensure the following:

- ♦ DNS forward and reverse lookup are properly configured so that you can resolve servers by using their DNS names and IP addresses. VNC, for example, relies on the DNS infrastructure. For this reason, it is important that the DNS service is well designed and implemented. If it is not, the problem needs to be addressed during the design phase, properly documented, and resolved before deployment begins.
- ♦ We recommend that you register all of your managed devices in DNS, which makes it easy to resolve by name. This is possible only if Dynamic DNS is in place and properly configured.
- ♦ DHCP must be properly configured for imaging purposes, and your network team should work closely with you to ensure that you can image across multiple subnets if necessary.
- ♦ PXE must be enabled on your workstations if you choose to leverage the automated imaging functionalities.

3.7.3 Time Synchronization

Time synchronization is an important factor for a stable ZENworks Configuration Management design. Configuration items and deployment tasks, such as bundles, inventory uploads, and access to user sources, rely on time stamps to ensure secure access to the relevant data. If servers and devices have different times, this can cause a number of communication issues with the Management Zone.

We recommend that all devices have their time synchronized. This includes Primary Servers, the ZENworks database, and managed devices.

For eDirectory customers, we recommend pointing the ZENworks Configuration Management Servers to eDirectory Time Sources via NTP. All clients usually use the same time source via the Novell Client, so the system is synchronized. For all customers, we recommend that a single source be used for synchronization.

3.7.4 Support for the NetWare Operating System

The introduction of the new ZENworks Configuration Management architecture means discontinued support for the NetWare operating system for both the Primary Server and the Satellite devices.

Customers are encouraged to consider migrating to Open Enterprise Server (OES) Linux or to SUSE Linux Enterprise Server (SLES) 10, which are supported as hosted platforms for the ZENworks Configuration Management Server services. As part of the migration, consider the following options:

- ◆ Migrating existing NetWare servers to OES Linux.
 - ◆ Complete migration away from the NetWare kernel
 - ◆ Virtualized on Xen on top of OES Linux
- ◆ Running the ZENworks Configuration Management core Server services (Primary Server) on OES Linux
- ◆ Running the ZENworks Configuration Management core Server services (Primary Server) on SUSE Linux Enterprise Server (SLES).
- ◆ Running the ZENworks Configuration Management core Server services in a virtualized instance of either OES Linux, SLES, or Windows Server on top of OES Linux or SLES.

Refer to the [Section 3.1, “Design Criteria/Decisions,” on page 21](#), for details on how to leverage an existing NetWare infrastructure for application deployment. Remember that by doing this you also require additional technologies and products, such as ZENworks Server Management.

4 Performing Design Activities

The design phase of any project is the most intensive part of any Novell ZENworks Configuration Management deployment or migration. This is where you conduct the most meetings, and identify granular details for the design document and the plan to get ZENworks Configuration Management successfully deployed across the infrastructure.

The design phase of the project is where you will spend the most time. Up to 80 percent of the project time is spent in this phase, so do not approach this lightly.

Success is the critical measure of all deployments. If the design is built correctly and is based on Novell best practices, the infrastructure should behave properly and you should see fewer performance issues. A good design should seldom, if ever, need to be changed. You want it to in place for years to come and simply extend upon it.

A combination of the business and technical assessments gives the design team the ability to forecast future needs so the design is based on what you foresee the company infrastructure is like in the future.

The following sections contain more information:

- ◆ [Section 4.1, “Design Workshops,” on page 69](#)
- ◆ [Section 4.2, “Developing a Detailed Design,” on page 71](#)
- ◆ [Section 4.3, “Lab Testing and Validation,” on page 124](#)
- ◆ [Section 4.4, “Documentation,” on page 125](#)

4.1 Design Workshops

Before you start the design phase and workshops, you must complete the assessment phase, in its entirety. This is covered in detail in [Chapter 2, “Performing Pre-Design Activities,” on page 15](#).

The first thing you must do during the design phase is to work with the teams across the organization to identify who is responsible for what, and identify how to structure the design teams and schedule the meetings to get everyone with a stake in the project in a room to flesh out the details of the design elements. Plan to break down the design into manageable chunks, then put it all together as you develop the detailed design document and infrastructure architecture diagrams.

Conducting design workshops is the best way to consider each of these individual elements of the overall design. A workshop is an informal gathering of all individuals that have a stake in the success of that particular element, where you use a detailed agenda to direct the discussion.

For example:

- ◆ How is a function currently performed?
- ◆ How will the function be performed after ZENworks Configuration Management has been fully deployed?
- ◆ How many locations does the organization have?

- ◆ How many users work at each location?
- ◆ How many devices are located at each location?
- ◆ Do users roam from site to site?
- ◆ Do devices roam from site to site?
- ◆ What additional components of ZENworks are required, such as Asset Management, Patch Management, and Security Management?
- ◆ Is the customer limited to the use of a specific database vendor (Microsoft SQL, Oracle, or Sybase)?
- ◆ How do devices connect internally and externally?
 - ◆ VPN?
 - ◆ Internet?
- ◆ Which platforms should be used for the ZENworks Configuration Management servers?
- ◆ Which platforms are used by the organization? This includes both Windows and Linux.

Topics for design activities should include, but are not limited to, the following:

1. Infrastructure topics, including Management Zone configuration, Locations and Network environments, user sources, role-based administrative accounts, folder structure, and placement of services. The overall infrastructure layout should be developed with the most senior members of the customer's IT departments.
2. Device discovery and agent deployment.
3. Migration tactics, if applicable.
4. Software packaging.
5. Software delivery.
6. Device and user policies.
7. Inventory gathering and reporting.
8. OS deployment, including consolidation of existing OS images (for example, Universal Imaging).
9. Remote management capabilities.
10. Database design, including maintenance, performance, scalability, fault tolerance, disaster recovery, backup, and restore procedures.
11. Administrative roles, including individual roles required by the customer, and identifying who is required to have an assigned administrative account with what level of access.

It is important that everyone involved agrees on each of the individual design elements. If you do not have consensus, you will likely face deviation from the design in the future. The objective of this phase is to build a solid design for the overall infrastructure that is based on best practices outlined by Novell. Every intricacy of the design needs to be well documented because this will be a reference during the deployment and long after the deployment is completed.

4.2 Developing a Detailed Design

After you have held all of the necessary workshops, you must create a design document to detail your findings and what you have agreed upon.

The following sections contain information that should be addressed and documented in detail. These sections cover areas that Novell recommends as best practice when deploying ZENworks Configuration Management across the infrastructure.

- ♦ [Section 4.2.1, “Locations and Network Environments,” on page 71](#)
- ♦ [Section 4.2.2, “Tuning Adaptive Agent Parameters for Slow Links,” on page 75](#)
- ♦ [Section 4.2.3, “Linux Subscription Options,” on page 77](#)
- ♦ [Section 4.2.4, “Device Folder and Group Structures,” on page 80](#)
- ♦ [Section 4.2.5, “User Sources,” on page 81](#)
- ♦ [Section 4.2.6, “Role-Based Administrative Accounts,” on page 83](#)
- ♦ [Section 4.2.7, “Licensing ZENworks Components,” on page 84](#)
- ♦ [Section 4.2.8, “Configuration Settings for the Management Zone,” on page 85](#)
- ♦ [Section 4.2.9, “Device Discovery,” on page 93](#)
- ♦ [Section 4.2.10, “Adaptive Agent Deployment,” on page 95](#)
- ♦ [Section 4.2.11, “Registration Rules and Keys,” on page 98](#)
- ♦ [Section 4.2.12, “Remote Management,” on page 100](#)
- ♦ [Section 4.2.13, “Inventory,” on page 102](#)
- ♦ [Section 4.2.14, “Application Management,” on page 103](#)
- ♦ [Section 4.2.15, “Policy Management,” on page 108](#)
- ♦ [Section 4.2.16, “Linux Patch Management,” on page 111](#)
- ♦ [Section 4.2.17, “Imaging,” on page 112](#)
- ♦ [Section 4.2.18, “Configuring a Layer 4 Switch,” on page 112](#)
- ♦ [Section 4.2.19, “ZENworks System Update,” on page 114](#)
- ♦ [Section 4.2.20, “Content Management,” on page 115](#)
- ♦ [Section 4.2.21, “Offline Content Replication and Management,” on page 121](#)
- ♦ [Section 4.2.22, “Satellite Authentication Role,” on page 122](#)

4.2.1 Locations and Network Environments

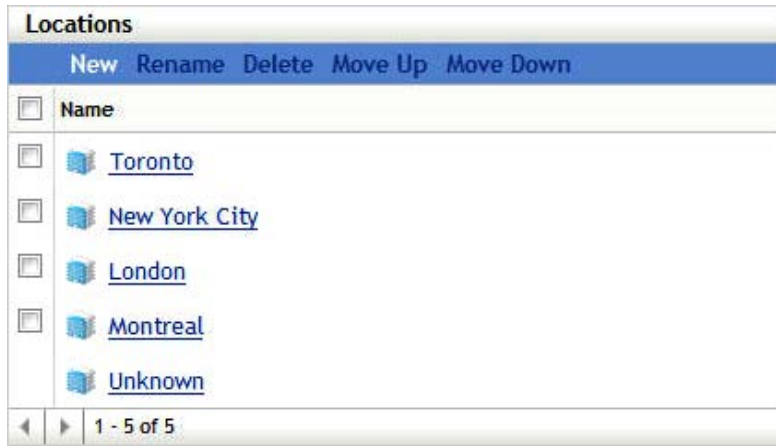
- ♦ [“Locations” on page 71](#)
- ♦ [“Network Environments” on page 72](#)
- ♦ [“Location Closest Server Rules” on page 73](#)

Locations

The concept of location awareness is new to ZENworks Configuration Management, but not new to Novell. This technology originated with ZENworks Endpoint Security Management and is now part of the core architecture of ZENworks. This means that it can be utilized across all ZENworks features. In essence, your organization can now create locations (which can be physical office locations, cities,

floors, or buildings), and define them with physical networking attributes. This allows devices to traverse the network from location to location, and get services, software, and policies from local ZENworks servers.

The following graphic displays a number of locations set up for regional offices, in cities around the world.



These locations do not need to be physical locations or cities. They can be floors, buildings, or whatever else defines your organization's physical structure and distribution. You can create locations that make sense for your particular circumstances.

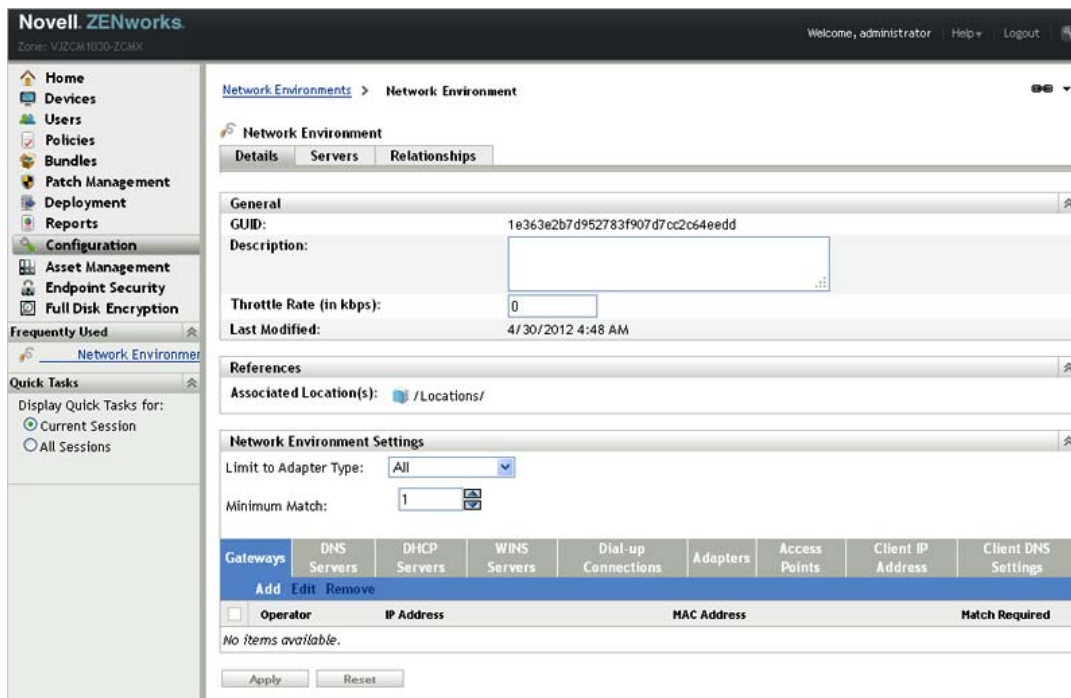
Location awareness affects many aspects of your organization:

- ◆ It provides greater control and management for the mobile user.
- ◆ It connects the user to resources, based on location.
- ◆ It defines endpoint throttling rates based on the location's bandwidth considerations.
- ◆ It enforces policies or access to applications, when the device is in a specific location.

IMPORTANT: Locations need to be considered for all designs. You can use very granular settings, as well as identify and control roaming users much more accurately.

Network Environments

Network environments define locations by using attributes to make the locations unique. When a device powers up at one of the physical locations, it gets services from the servers at that location.



You should configure as many of the attributes as possible, and set the maximum match to more than 1. This ensures that when a machine powers up at a location, the machine and the location are accurately identified.

Location Closest Server Rules

Understanding and configuring location Closest Server Rules is essential to a successful ZENworks Configuration Management infrastructure. Location Closest Server Rules are used to inform devices which Primary Servers and Satellite devices to contact for a particular service (configuration, collection, content, and authentication) and in which order. As you configure the rules you should consider the placement of ZENworks Primary Servers and Satellite devices. These rules might change as the design changes, so ensure that the requirements are tracked.

You configure and manage location Closest Server Rules in two primary places within ZENworks Configuration Management 11.

- ◆ The Default Closest Server Rule that is set up and updated as infrastructure servers are added to the Management Zone.
- ◆ The location Closest Server Rules that you set up and manage for each configured location.

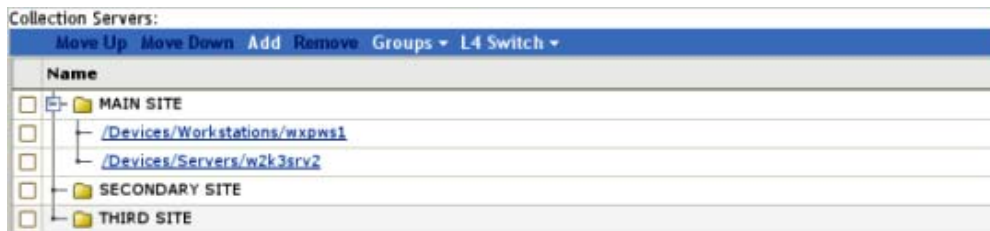
If you have a single site with no remote locations, it is possible to utilize the default Closest Server Rule, but if you have more than one site or have a need to granularly direct where managed devices go for content, collection, configuration, and authentication, you need to set up locations and network environments, and configure Closest Server Rules for each location. This gives you a great deal of flexibility managing the performance of your Management Zone.

In addition to configuring the location Closest Server Rules, you can also override the rules at the location level by configuring rules for each network environment you create and configure. This can be useful if you need an additional layer of granularity when a location is defined by more than 1 network environment, such as a location with both a wired and wireless network.

You need to keep in mind the following points when you upgrade from ZENworks Configuration Management 10.3, and you have a mixed zone of ZENworks Configuration Management 10.3 and ZENworks 11 managed devices:

- ◆ ZENworks 11 agents ignore Closest Server Rules that you have previously set up in your ZENworks Configuration Management 10.3 environment, and only obey location Closest Server Rules.
- ◆ ZENworks 11 agents obey the default Closest Server Rule.
- ◆ ZENworks 10.x agents ignore locations and location Closest Server Rules.

To balance the load, we recommend using Closest Server Groups. A Server Group is a list of Primary Servers and Satellite devices that can be accessed in a random order. By randomizing server access, it is possible to balance the number of requests sent to each ZENworks Configuration Management Server listed in the group.



If load balancing and fault tolerance is a fundamental requirement of the infrastructure, the best way to achieve it is through a Layer 4 (L4) switch. An L4 switch can front either Primary Servers or Satellite devices, or both, in order to guarantee results when directing traffic to the devices behind the switch. Most importantly, it ensures that services are always available to the end user community. If you use an L4 switch, ensure that it is properly configured. If the switch is not properly configured, the traffic is not properly directed, and there might be issues with connections, responses, and so forth.

The L4 switch is configured in the location Closest Server Rules in a similar way to the Closest Server Groups. When you are prompted, specify the L4 definition name, which must be either the DNS name or IP address of the L4 virtual device.

Keep in mind the following considerations:

- ◆ The L4 switch definition is displayed in each of the listings, no matter where it is created, with the selected servers listed under each instance of the L4 switch.
- ◆ Servers can be members of multiple groups and L4 switch definitions.
- ◆ Servers that are members of an L4 switch definition or group are no longer listed at the top level of the server listing.

If there are no matching Location Closest Server Rules for a given device, the managed device falls back to the default Closest Server Rule. This rule is an ordered list of all the ZENworks Configuration Management Primary and Satellite devices installed in the Management Zone. The list must be ordered so that all the ZENworks Configuration Management Primary Servers are at the top and all the ZENworks Configuration Management Satellite devices are at the bottom.

You should consider excluding the default Closest Server Rule to ensure that you are only connecting to the appropriate servers at each location. You do this when you configure the location Closest Server Rules for each location. You might want to exclude the default Closest Server Rule for the following reasons:

- ♦ **Agent refresh speed:** When a device is refreshed, the applicable ZENworks Configuration Management Primary Server and Satellite device list for a device is calculated, serialized, and sent via the SOAP service. Excluding the default Closest Server Rule optimizes the response from the server, which also shortens the time required to complete a refresh.
- ♦ **Satellite devices:** Devices at one site should not attempt to access a Satellite device or Primary Server at another location. Excluding the default Closest Server Rule ensures that a device only connects to Satellite server if it is in the Closest Server rule for that subnet. If a Satellite device is temporarily unavailable, this ensures that content is not pulled across a WAN connection by local devices.
- ♦ **Server roles:** If a Primary Server is dedicated to a particular task, such as reporting, excluding the default Closest Server Rule ensures that devices do not attempt to use this server for other services.



For more information, see the [ZENworks 11 SP2 System Administration Reference](#).

4.2.2 Tuning Adaptive Agent Parameters for Slow Links

ZENworks Configuration Management has different parameters that can be tuned to improve agent performance. There are certain instances when the agent's response time is delayed because of slow links or because the agent is managing other device requests in the Zone. The following sections provide you with information about the registry settings that can be used to improve the agent performance.

- ♦ ["Upload-timeout" on page 76](#)
- ♦ ["Read-timeout" on page 76](#)
- ♦ ["Cache-read-retry-interval" on page 76](#)
- ♦ ["Cache-read-retries" on page 77](#)

Upload-timeout

The agent periodically uploads the status and collection data to the Primary or Satellite Servers in the Zone. On slow links or when the server is too busy managing other device requests in the Zone, this attempt to upload the data might time out. To address this, the upload-timeout setting must be increased to more than the default value of 100 seconds.

To change the default upload timeout value of the ZENworks Adaptive Agent on a Windows managed device:

- 1 On a Windows managed device, open the Registry Editor.
- 2 Go to `HKLM\Software\Novell\ZCM\`.
- 3 Add the upload-timeout parameter as `upload-timeout=200 seconds`.

To change the default upload timeout value of the ZENworks Adaptive Agent on a Linux managed device:

- 1 On a Linux managed device, open the `/etc/opt/novell/zenworks/conf/xplatzmd.properties` file in a text editor.
- 2 Add the upload-timeout parameter as `upload-timeout=200 seconds`.

Read-timeout

On slow links, the file downloads could fail because of read-timeouts. When the agent log files are in the debug mode, the administrator observes a read-timeout error in the agent log file. To address this, the read-timeout setting must be increased to more than the default value of 30 seconds.

To change the default read timeout value of the ZENworks Adaptive Agent on a Windows managed device:

- 1 On a Windows managed device, open the Registry Editor.
- 2 Go to `HKLM\Software\Novell\ZCM\`.
- 3 Add the read-timeout parameter as `read-timeout=100 seconds`.

To change the default read timeout value of the ZENworks Adaptive Agent on a Linux managed device:

- 1 On a Linux managed device, open `/etc/opt/novell/zenworks/conf/xplatzmd.properties` in a text editor.
- 2 Add the read-timeout parameter as `read-timeout=100 seconds`.

Cache-read-retry-interval

When you download a file on the ZENworks Adaptive Agent, the download might not finish or might time out because of slow connectivity or because the file size is too large. To ensure that the process finishes, you need to set the retry interval to one second.

To change the default read-timeout value of the ZENworks Adaptive Agent on a Linux managed device:

- 1 On a Linux managed device, open the `/etc/opt/novell/zenworks/conf/xplatzmd.properties` file in a text editor.
- 2 Add the cache-read-retry-interval parameter as `cache-read-retry-interval=1 second`.

Cache-read-retries

When you download a file on the ZENworks Adaptive Agent, the download might not finish or might time out because of slow connectivity or because the file size is too large. To ensure that the process finishes, you need to set the number of retries to 1000.

To change the default read-timeout value of the ZENworks Adaptive Agent on a Linux managed device:

- 1 On a Linux managed device, open the `/etc/opt/novell/zenworks/conf/xplatzmd.properties` file in a text editor.
- 2 Add the `cache-read-retries` parameter as `cache-read-retries=1000`.

4.2.3 Linux Subscription Options

You can use Subscription options to control what type of software is downloaded from the remote server, and how to store that software on your local server.

- ♦ [“Sub-Options for Subscriptions” on page 77](#)
- ♦ [“Scenarios” on page 78](#)
- ♦ [“Other Considerations” on page 79](#)

Sub-Options for Subscriptions

- ♦ **Dry Run:** Displays the packages and software that will be downloaded as part of the Subscription Replication process, without actually downloading them.
- ♦ **Force-Replication:** Downloads the packages again from the remote server if the packages are corrupted or do not exist on the local server.
- ♦ **Create Sandbox:** Creates sandbox versions of bundles created by the Subscription. This option is not applicable when the *Static Replication* option is enabled.
- ♦ **Rollback on Failure:** Enables or disables the *Rollback on Failure* feature for each *Install RPM* action in the bundle created by this subscription. If this option is enabled and bundle installation fails during an *Install RPM* action execution, it reverts all the transactions that happened during this action execution.
- ♦ **Patches:** Downloads both patches and monolithic bundles and creates a Linux bundle for each patch. If the *Patches* option and the *Create Dependency Bundle* option are disabled, it downloads only the monolithic bundle and creates a Linux bundle.
- ♦ **Monolithic Bundle:** If the *Patches* option is disabled, it replicates only the monolithic bundle packages and automatically creates Linux bundles with the latest package RPMs. Either the *Patches* option or the *Monolithic bundle* option is enabled, but not both.
- ♦ **Source RPMs:** Downloads source RPMs (`*.src.rpm`) from the monolithic bundle and creates a Linux bundle with an *Install File(s)* action. This option is effective only if the *Patches* option and the *Create Dependency Bundle* option are disabled.
- ♦ **Create Dependency Bundle:** Replicates monolithic bundle packages and automatically creates Linux Dependency bundles with the package RPMs.
- ♦ **Publish Packages:** Applicable only if the *Create Dependency Bundle* option is enabled. The value is set for all the packages that are downloaded as part of the Linux Dependency bundle. This option allows users to use the `zac install` command to install packages that are a part of Linux Dependency bundle from a managed device.

- ♦ **Static Replication:** Supports the Air Gap solution. This option replicates the package updates from the remote server to the file system on your local server and creates a Static Source). The location of the downloaded content is `/var/opt/novell/zenworks/cache/package-repo/Static_Subscriptions` on a Linux server and `%ZENWORKS_HOME%\work\cache\pkg-repo\Static_Subscriptions` on a Windows server. The created static source is used as input for the Static Subscription.
- ♦ **Create Category based Bundle Groups:** If this option is enabled, it creates one bundle group for each patch category, such as *Security*, *Recommended*, *Optional* and adds patch bundles (Linux bundles) to the corresponding bundle group, based on category. This option is effective only if the *Patches* option is enabled and the *Static Replication option* is disabled.
- ♦ **Retain Bundle GUID:** Applicable only for a ZENworks Linux Management subscription. If this option is enabled, a bundle is created with the same GUID as that of the ZENworks Linux Management Linux bundle.

Scenarios

- ♦ **Download patches and create Linux bundles:** Enable the *Create Linux Bundle* option and the *Patches* sub-option. This creates a bundle group and adds all the bundles to this group. If you want to create bundle groups based on patch categories, select the *Create Category based Bundle Groups* option.

NOTE: If there is no patch filtering configured, this option also downloads the monolithic bundle. Patch filtering implies, that you download only a few patches, which are specified using a regular expression or that you download patches based on the selected category.

- ♦ **Download patches and create a Static Source:** Enable the *Static Replication* option and the *Patches* sub-option to download patch bundles into the file system of the replicating server and create a static source. The created static source can be copied to a CD or USB device. Mount the CD or USB on a device on which the bundles need to be replicated to the other Management Zone, then create a Static subscription to replicate ZENworks Configuration Management bundles to the zone from the mounted static source.

NOTE: If there is no patch filtering configured, this option also downloads the monolithic bundle. Patch filtering implies that you download only a few patches, which are specified using a regular expression, or that you download patches based on the selected category.

- ♦ **Download only Monolithic bundles and create Linux bundles:** Enable the *Create Linux Bundle* option and the *Monolithic Bundle* sub-option. This creates one Linux bundle per catalog (service pack or updates release). If you want to download source RPMs, enable the *Source RPMs* option. This option creates a Linux bundle with the Install Files action.
- ♦ **Download only Monolithic bundles and create a Static Source:** Enable the *Static Replication* option and the *Monolithic Bundle* sub-option. This downloads monolithic bundle RPMs and creates a Static Source. This can be used for Air gap solution. If you want to download source RPMs, enable the *Source RPMs* option.
- ♦ **Create a Linux Dependency bundle:** Enable the *Create Linux Dependency Bundle* option. This downloads packages and creates a Linux Dependency bundle that is a monolithic bundle. By default, Linux Dependency bundle packages can not be installed on a managed device. If you want to enable the installation of the packages part of the Linux Dependency bundle on the managed device, enable the *Publish Packages* option.
- ♦ **Re-download the corrupted or missed packages in the content system:** Enable the *Force Replication* option. This is not effective when *Static Replication* is enabled.

- ♦ **Download Pool catalogs:** Because Pool catalogs do not contain any patches, they can be downloaded by using one or more of the following options:
 - ♦ If you are replicating the Pool catalogs for distribution, first upgrade, then replicate them by using the *Create Linux Bundles* option and the *Monolithic Bundle* sub-option.
 - ♦ If you are replicating the Pool catalogs for dependency resolution then it is recommended that you replicate them using the *Create Linux Dependency Bundle* option.
 - ♦ If you want to create a Static Source for the Air Gap solution, enable the *Static Replication* option and the *Monolithic Bundle* sub-option.

Other Considerations

- ♦ [“Air Gap Solution” on page 79](#)
- ♦ [“Static Subscription Option” on page 79](#)
- ♦ [“Static Replication Option” on page 79](#)

Air Gap Solution

An Air Gap is a security measure often taken for computers and computer networks that must be extraordinarily secure. It is implemented by ensuring that a secure network is completely isolated from insecure networks. The only connection between two devices or networks is via a human being providing media-switching such as floppies, CDs, or USB drives. The [Static Replication](#) and [Static Subscription](#) options are used to support this scenario.

Static Subscription Option

The Static Subscription option helps administrators in replicating updates from a remote repository to a static location and then importing the updates to another ZENworks server. Before creating a Static Subscription, make sure that you have a Static Source available on your server. To create Static Source (see [“Static Replication Option” on page 79](#)). When you create the Static Subscription make sure you specify the Static Source location (file system path on the replication server). When the Static Subscription is replicated, it creates ZENworks bundles from the packages in the Static Source location.

Static Replication Option

This option is used to create a Static Source on the Replication server's file system. The directory where the subscription content is downloaded is `/var/opt/novell/zenworks/pkg-repo/Static_Subscriptions/<subscription guid>/` on a Linux server and `%ZENWORKS_HOME%\work\cache\pkg-repo\Static_Subscriptions/<subscription guid>/` on a Windows server. The Static Source can be created in a Management Zone where the server can go outside of the firewall to connect to the remote repository and download the software updates. This structure is copied to the secure Management Zone from the non-secure Management Zone by using media such as CDs or USB drives. The administrator can create ZENworks Configuration Management bundles by using the Static Subscription in the destination zone.

4.2.4 Device Folder and Group Structures

Using ZENworks Control Center, you can manage devices by performing tasks directly on individual device objects. However, this approach is not very efficient unless you have only a few devices to manage. To optimize management of a large number of devices, ZENworks Configuration Management lets you organize devices into folders and groups. You can then perform tasks on a folder or group to manage its devices.

You can create folders and groups at any time. However, the best practice is to create folders and groups before you register devices in your Management Zone. This allows you to use registration keys and rules to automatically add devices to the appropriate folders and groups when the devices register. Membership for dynamic groups is automatically updated based on the defined schedule and the configuration of the dynamic group. By default, platform-specific dynamic groups are created when ZENworks Configuration Management is installed, but you can create your own as well.

The following information should be considered when designing the folder structure and groups for a Management Zone:

- ♦ Do you need to implement site administrators and sub-administrators who have limited rights to the system or only to part of the Management Zone? For example, you might need a site administrator who is only responsible for a specific location.
- ♦ Do you need Help Desk users who are allowed to assign bundles and perform some remote management tasks, but not allowed to create or modify items such as bundles and policies?
- ♦ Do you need site-specific settings, such as inventory schedules or system variables?
- ♦ Do you need department-specific configuration, such as system variables to set working directories or host IDs?

The following graphic is an example of a company that is organized by country. Further organizational folders can be included under each of these country folders. You can be as granular as you want, and this is encouraged to implement specific levels of management.

Devices		
Status	Name	Type
<input type="checkbox"/>	Bangalore (Details)	Folder
<input type="checkbox"/>	Brazil (Details)	Folder
<input type="checkbox"/>	Canada (Details)	Folder
<input type="checkbox"/>	Chile (Details)	Folder
<input type="checkbox"/>	England (Details)	Folder
<input type="checkbox"/>	France (Details)	Folder
<input type="checkbox"/>	USA (Details)	Folder
<input type="checkbox"/>	Red Hat Enterprise Linux Desktop 4	Dynamic Workstation Group
<input type="checkbox"/>	Red Hat Enterprise Linux Desktop 5	Dynamic Workstation Group
<input type="checkbox"/>	SUSE Linux Enterprise Desktop 10	Dynamic Workstation Group
<input type="checkbox"/>	SUSE Linux Enterprise Desktop 11	Dynamic Workstation Group
<input type="checkbox"/>	Windows 7 Workstations	Dynamic Workstation Group
<input type="checkbox"/>	Windows Vista Workstations	Dynamic Workstation Group
<input type="checkbox"/>	Windows XP Workstations	Dynamic Workstation Group

4.2.5 User Sources

User-based management requires an authoritative source of user information to govern access privileges, permissions, and configurations. The new architecture allows you link to multiple user directories for this information, including your choice of Active Directory, eDirectory, or both.

User Sources		
Status	Name	
<input type="checkbox"/>	 zenworks11.com	

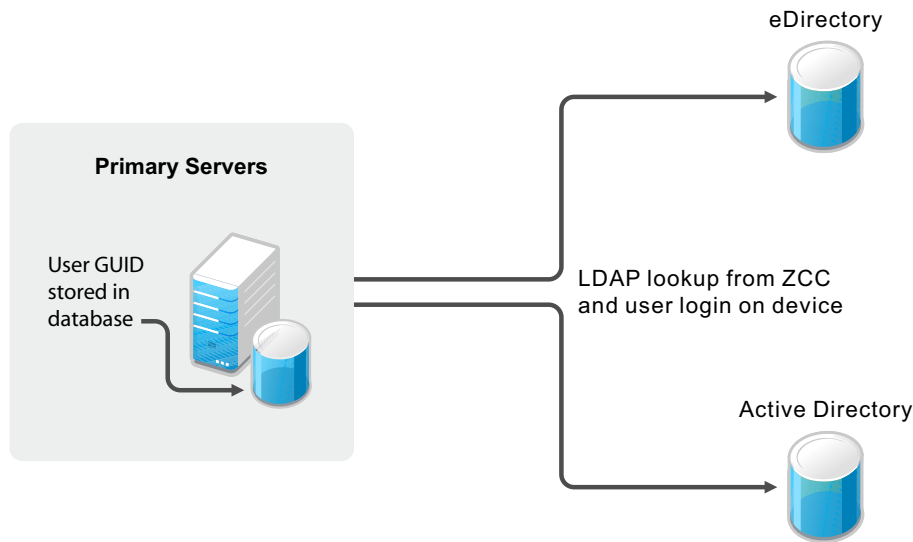
Linking system management with authoritative user directories ensures that new hires, terminations, internal moves, and other business changes immediately result in the appropriate provisioning, deprovisioning, reconfiguration, and other system management changes. Other systems typically require you to synchronize or copy Active Directory or eDirectory information to your management database, which increases the change management burden by requiring installation of additional software on the authoritative servers. If synchronization happens once a week, for example, users can wait for several days for the directory to be synchronized—or perhaps have several days when they can access resources they should not be able to use.

In ZENworks Configuration Management, all communication with authoritative sources is read-only, through LDAP. There is no need to extend schemas, so you avoid a potentially big change management issue. Also, there is no need to install new software or make any other changes to the user directories you currently use. Nor is there a need to install an intermediary identity management system between ZENworks Configuration Management and authoritative sources.

Primary Servers can link directly to any number of authoritative sources of any type, and user groups can span authoritative sources. This architecture allows simple management of resources through user, user group, and container assignments, without the limitation of a single authoritative source or the need to install and manage additional infrastructure to mediate between authoritative sources and ZENworks Configuration Management.

The following graphic illustrates how Primary Servers link to various user sources:

Figure 4-1 Primary Server and User Sources



As a best practice, you should set up your user sources prior to any deployment activities (discovery of devices and deployment of the ZENworks Adaptive Agent). Before beginning, you must understand your directory services infrastructure, and the systems you will be referencing from your ZENworks Primary Servers. In addition, if your deployment is a migration from an existing ZENworks infrastructure (for example, ZENworks 7 Desktop Management), you must have your user sources defined prior to running any of the migration steps. If you do not do this, you cannot migrate user-based associations (including associations to user groups).

You can connect to Novell eDirectory and Microsoft Active Directory for your user sources. After you connect to either of these LDAP directories, you define the containers within the directory that you want exposed. Or, you could reference the top-level containers of the user source as the source or the containers that contain users. This limits access within the directory to only those containers that include users.

Both methods have some advantages and disadvantages that are mostly related to administration. There is no difference in assigning bundles or policies.

Selecting top-level containers ensures that all users in subcontainers and all containers added to the structure are maintained automatically and can be used for assignments without changes within ZENworks Configuration Management.

In addition, it is not possible to add subcontainers if the parent container is already listed. If you want to change the structure, you need to delete the parent container. This means that you lose all assignments, so it is important to do it correctly the first time.

You can avoid the problem by structuring your containers and contexts. First ensure that you use only containers where users reside. This means adding multiple sublevel folders from an eDirectory or Active Directory rather than using only one. Consider the following two options when you set up user sources:

- ♦ **Single Context:** You can set up a single context if your eDirectory container structure, or Active Directory folder structure runs deep and there are users in many folders throughout the tree. This makes it easy to search from a base DN high up in the tree to locate users wherever they are located.
- ♦ **Multiple Contexts:** You can use multiple contexts for your setup if you have users in a set number of containers or folders, your tree is not deep, or you know this configuration will not change too much. For example, you have a massive tree, but all user objects reside in the USERS1, USERS2, and USERS3 containers or folders. This would have a positive impact on search, because you would not need to search the other areas of the tree in order to locate user or group objects, especially when you know nothing relevant is there.

In order to achieve fault tolerance for your user source, multiple connections can be created within the ZENworks Control Center to point to multiple LDAP servers. If an error occurs during the bind request from the Zenworks Configuration Management server, the next LDAP server is used. However the server does not keep a list of failed LDAP servers, so the Zenworks Configuration Management server starts at the top of its connection list for every LDAP request.

Remember, the user source definition defines which users are affected and the Connections list in the user source itself defines where the server checks for LDAP servers to use. In turn, when you set up your user source, you should point that source to multiple eDirectory or Active Directory servers to provide fault tolerance.

To ensure proper load balancing, and to ensure that all authentication does not go to the same LDAP server, the authentication connections can be manually organized on a per -server basis. This ensures that Primary Server 1 goes to LDAP Connection 1 first, and Primary Server 2 goes to LDAP Connection 2 first. You can use Closest Server Groups to balance which Primary Server a device goes to for authentication to ensure that the load is balanced among LDAP servers.

If there is only one Primary Server or dedicated ZENworks Control Center server that handles authentication, and you want to balance the load of every LDAP request through the *User* tab in ZENworks Control Center, modify the following file on the Primary Server:

```
%ZENWORKS_HOME%\conf\datamodel\authsource\authsourceconfig.xml
```

```
<AuthSourceConfig>
  <DoConnectionRoundRobin>false</DoConnectionRoundRobin>
</AuthSourceConfig>
```

You need to modify the value to true.

4.2.6 Role-Based Administrative Accounts

The roles feature allows you to specify rights that can be assigned as roles for ZENworks administrators. You can create a specialized role, then assign administrators to that role to allow or deny them the ZENworks Control Center rights that you specify for that role. For example, you could

create a Help Desk role with the ZENworks Control Center rights that you want help desk operators to have. You can also create individual administrative accounts and assign these to managers of the system.

Common roles in most installations of ZENworks Configuration Management include the following:

- ♦ **Help Desk:** The Help Desk role should include common tasks, such as remote control, remote view, and so forth, and be bound to specific boundaries (device folders), especially where there are multiple sites and administration is not centralized.
- ♦ **Application Management:** The Application Management role should include tasks and functions for creating bundle content in specific folders and restricting it to folder boundaries. Some administrators require more rights than others, so multiple roles could be created.
- ♦ **Backup Administrator:** The Backup Administrator role is used if the default administrator account can no longer be used.
- ♦ **Individual Administrator Accounts:** It is also a best practice to create different levels of administrator accounts and assign these separately to individuals. Do not give the administrator credentials (the default Administrator account set up during the initial installation) to everyone.

The following graphic is an example of the kinds of roles you should consider when implementing ZENworks Configuration Management:

<input type="checkbox"/>	Name	Types	Allow	Deny
<input type="checkbox"/>	Deployment Technicians	Deployment Rights	DP	
<input type="checkbox"/>	Patch Management Administrators	Patch Management Rights	PD PE PDIS PUC AB RB W EV SN RP	
<input type="checkbox"/>	Service Desk Technician	Remote Management Rights	RV RD	RC TF RE URM
<input type="checkbox"/>	Software Delivery Technicians	Bundle Rights	M CD MG CDG MGM MF CDF MS	
<input type="checkbox"/>	Tier 1 User Support	Remote Management Rights	RV RD	RC TF RE URM

4.2.7 Licensing ZENworks Components

Components of ZENworks are licensed individually. To activate a component, go to ZENworks Control Center and enter the license key provided by Novell. After you have entered the license key, you see new pages added to ZENworks Control Center that are specific to that feature set.

The following diagram shows the individual components that can be licensed:

Licenses		
Product Licensing		
Product/Component Name	License State	Expiration Date
ZENworks 11 Patch Management	Active	
ZENworks 11 Configuration Management	Active	
Asset Inventory for Unix/Linux	Active	
ZENworks 11 Endpoint Security Management	Active	
ZENworks 11 Asset Management	Active	
Asset Inventory for Windows/Mac	Deactivated	
ZENworks 11 Full Disk Encryption	Evaluation	

1 - 7 of 7

4.2.8 Configuration Settings for the Management Zone

The Management Zone Settings panel lets you manage the global configuration settings for your Management Zone. These global configuration settings are inherited by other objects (devices, users, and folders) within your Management Zone and remain in effect unless they are overridden at the folder or object level.

You should configure the global settings to accommodate the largest possible number of objects, and then use the override option on any objects you want to configure differently. For example, you should use the *Device Refresh Schedule* setting to define the schedule that you want the majority of devices to use, and then override the schedule on individual devices or device folders if those devices require a different schedule. This is the best practice for almost all Management Zone configuration settings.

This section highlights configuration settings that you should consider setting at the global level, then adjust as needed at the folder or object level. Not all settings are covered in this section because they might not be relevant in your given situation, or they might differ greatly to what we would minimally recommend. For more information, see the [ZENworks 11 SP2 System Administration Reference](#).

The following sections contain more information:

- ♦ [“Content Blackout Schedule” on page 86](#)
- ♦ [“Content Replication” on page 86](#)
- ♦ [“ZENworks Explorer Configuration” on page 86](#)
- ♦ [“System Variables” on page 87](#)
- ♦ [“Local Device Logging” on page 87](#)
- ♦ [“Device Refresh Schedule” on page 88](#)
- ♦ [“Device Removal Schedule” on page 89](#)
- ♦ [“Dynamic Groups Refresh Schedule” on page 90](#)
- ♦ [“ZENworks Agent” on page 90](#)
- ♦ [“Inventory Schedules” on page 92](#)

Content Blackout Schedule

You should define a Management Zone setting only if you are sure that you want to use this setting for all devices. In normal environments, you should not use a common blackout schedule for all devices.

A content blackout schedule is needed only for special devices, such as device in the finance department or production PCs that are used for controlling production processes.

The following graphic shows a corporate (global) blackout schedule of the last Friday of every month, from 12:00 a.m. until 7:00 a.m. In this case, no content is sent to managed devices during this time.

<input type="checkbox"/>	Start Date	Start Time	End Date	End Time
<input type="checkbox"/>	10/31/08	12:00:00 AM	10/31/08	7:00:00 AM
<input type="checkbox"/>	11/28/08	12:00:00 AM	11/28/08	7:00:00 AM
<input type="checkbox"/>	12/26/08	12:00:00 AM	12/26/08	7:00:00 AM

For more information, see the [ZENworks 11 SP2 System Administration Reference](#).

Content Replication

These settings dictate how frequently Primary Servers replicate content in the Content Repository, along with settings for throttling and checksums.

When ZENworks Configuration Management is initially set up, the replication schedule is set to run every 5 minutes. You should change this to something more realistic for your environment, based on how frequently you anticipate making changes to the system and how quickly you need the changes replicated to other Primary Servers in your Management Zone. You might want to start by setting it to run every 20 minutes.

Content Replication
Configure the settings for content replication schedules and throttle rates.

Primary Server Recurring Content Replication Schedule: 0 Days 0 Hours 20 Minutes

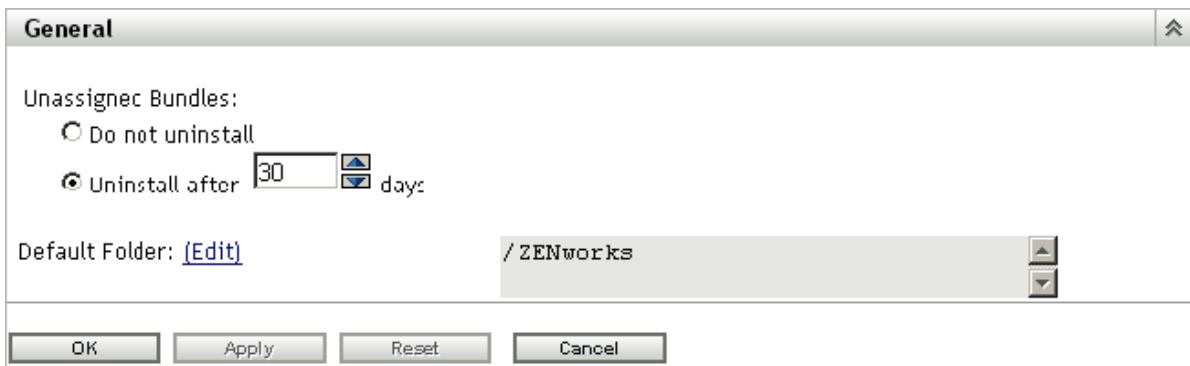
Primary Server output throttling in KB/sec: None

Agent Content Checksum: On Off

Satellite Content Checksum: On Off

ZENworks Explorer Configuration

This setting defines the uninstall feature. If your customer does not need to uninstall applications, disable this feature in your Management Zone.



For more information, see the [ZENworks 11 SP2 System Administration Reference](#).

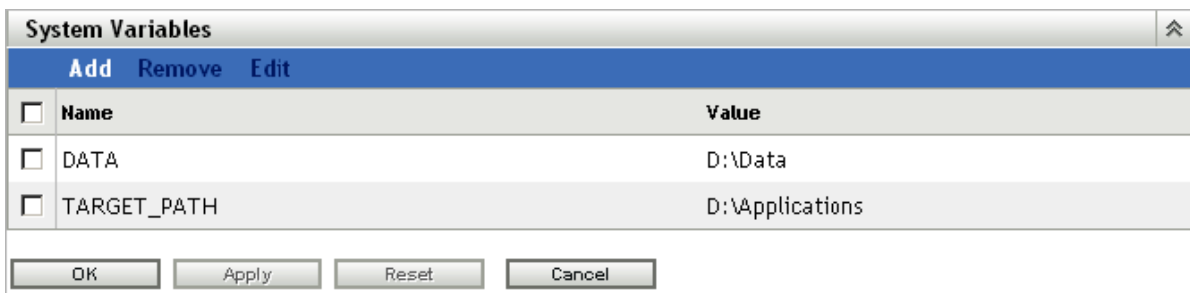
System Variables

System variables are used to define paths, names, and other items in your system. In addition to the predefined variables, Novell recommends using variables in bundles. This makes it much simpler to create, manage, and deliver applications moving forward. You need to standardize on this early and stay with your standard.

Common variables are SOURCE_PATH or TARGET_PATH

- ◆ Define variables for your Management Zone.
- ◆ Define variables for your folders if you need different or additional settings.
- ◆ Define variables in your bundles only if the above settings do not fit your needs.

The following is an example of system variables that are set at the Management Zone level. These can then be used in bundles for distribution. Because these are set at the Management Zone level, it is assumed that these variables are resolvable on any device registered in the Management Zone.



For more information, see the [ZENworks 11 SP2 System Administration Reference](#).

Local Device Logging

Use a severity setting of *Error* for log messages. If you set the severity to *Warnings and Above*, you might end up collecting more data than you really need. If you understand the errors you are encountering, this is more than enough for troubleshooting your infrastructure.

This settings page allows you to set the rollup schedule for a specific time or date. We recommend that you create a new log file every day to ensure accurate information for troubleshooting purposes.

Local File	
<input checked="" type="checkbox"/> Log message to a local file if severity is	Error
<input type="radio"/> Rolling based on size	
Limit file size to	10 MB
Number of backup files	1
<input checked="" type="radio"/> Rolling based on date	
Rolling pattern	Daily Pattern
System Log	
<input checked="" type="checkbox"/> Send message to local system log if severity is	Warning and above
<input type="button" value="OK"/> <input type="button" value="Apply"/> <input type="button" value="Reset"/> <input type="button" value="Cancel"/>	

For more information, see the [ZENworks 11 SP2 System Administration Reference](#).

Device Refresh Schedule

Use the default schedule as a starting point. Discuss the schedules with your customer and adjust according to their needs. This information should have been collected during the assessment phase of your project. Remember, shorter refresh schedules means more frequent ZENworks Configuration Management traffic on the network. This could cause issues with over-utilization of available bandwidth. Make sure you involve the network management team when you decide on this setting.

Short refresh times for a large number of devices can also cause extensive server load, which might cause distribution failures or failures at the server side (uploading inventory and so forth).

Use random refresh rates to future prevent server overload during peak periods. This setting can be instrumental in increasing the scalability of the infrastructure components. Remember, the tests Novell performs in the SuperLab are designed to test the breaking point of the components. In the real world, thousands of devices should not regularly contact a server in the Management Zone.

Device Refresh Schedule ⌵

Manual Refresh
Device won't get refreshed until the user manually does so

Timed Refresh

Full Refresh Schedule
Refresh everything: Policies, Bundles, Settings, Registration, etc.

Days Hours Minutes

Random Time to Wait
Minimum: Seconds Maximum: Seconds

Partial Refresh Schedule
Only perform Policies, Settings, and Registration refresh

Days Hours Minutes

Device Removal Schedule ⌵

If the device has not made contact after days: Flag Remove

OK
Apply
Reset
Cancel

For more information, see the [ZENworks 11 SP2 System Administration Reference](#).

Device Removal Schedule

This setting needs to be discussed in detail with the customer during the assessment and design phases to ensure that you are removing devices that should be removed. You want to avoid removing devices that have been inactive for a certain number of days because the inactivity might result from circumstances such as maternity leave or a leave of absence. The customer should be able to give you the details on how long these situations should last, and what is acceptable. After you have this information, you can configure the schedule appropriately.

Take the following into consideration when setting up the schedule:

- ◆ How do we maintain actual reporting data? Do you need very accurate data?
- ◆ How long are the devices off-line (average time)? Possible cases are vacation, illness, maternity leave, extended leave of absence, and so forth.
- ◆ Do you need statistics on removed devices?

If devices are to be flagged for removal and not actually removed from the Management Zone, these devices can be easily found by specifying the Device State as *Lost* when searching for devices.

If you are required to report on all devices, even if they are not active on the network, managed devices can be “retired” instead of removed. When a managed device is retired, its identity and inventory information is retained but all policy and bundle assignments are removed. A retired device is in a holding state until you un-retire or delete the device from the Management Zone.

For more information on retiring devices, see the [ZENworks 11 SP2 Discovery, Deployment, and Retirement Reference](#).

For more information, see the [ZENworks 11 SP2 System Administration Reference](#).

Dynamic Groups Refresh Schedule

Novell recommends the use of dynamic groups wherever possible. The membership of these groups is recalculated on a regular basis to get the expected (and accurate) results.

For your initial configuration, Novell recommends a daily refresh schedule (*All days of the Week*). This ensures that the membership lists of the dynamic groups accurately represent what you have registered in the system.

Refresh Schedule

Schedule Type:
Recurring

Days of the week

*
Sun Mon Tue Wed Thu Fri Sat

Start Time: 12 : 00 am

[Hide Options](#)

Process immediately if device unable to execute on schedule
 Use Coordinated Universal Time (Current UTC 10:41 PM)
 Start at a random time between Start and End Times
End Time 1 : 00 am
 Restrict schedule execution to the following date range:
Start Date: 10/30/08
End Date: 10/30/08

OK Apply Reset Cancel

For more information, see the [ZENworks 11 SP2 System Administration Reference](#).

ZENworks Agent

At every client refresh, all Primary Servers and Satellite devices are marked as Unknown. When a particular module requires a service, the Connection Manager (based on the Closest Server Rules) makes a call to the first Primary Server or Satellite device hosting this service. If a Primary Server or Satellite device is down or is not contactable, it is immediately marked as Bad. If it is in a Busy state, it returns a busy error and the client waits and retries again.

There are three settings that control how many times and for how long a managed device should wait before marking a Primary Server or Satellite device as Bad and then moving to the next Primary Server or Satellite device in the closest server rule. These three client settings are available in ZENworks Control Center, under *Configuration > Device Management > ZENworks Agent*.

General	
Cache life:	336 hour(s)
Cache orphaning threshold:	90 day(s)
Times to retry requests to a busy server:	20
Initial retry request wait (each subsequent request incremented by 1 second):	10 second(s)
Maximum retry request wait:	20 second(s)

- ♦ **Times to Retry Requests to a Busy Server:** The maximum number of retries a device attempts to contact a Busy Primary Server or Satellite device.
- ♦ **Initial retry request wait:** The initial wait time between each of the above retries. All subsequent waits increment by 1 second. This means that the first wait time is 10 seconds, the second wait time is 11 seconds, then 12 seconds, 13 seconds and so on, up to the amount in the *Number of Retries* setting.
- ♦ **Maximum retry request wait:** The maximum time the device waits between retries. This overrides the incremental time to wait in the *Initial retry request wait* setting.

If a Primary Server or Satellite device is contactable but busy, a client waits for the initial wait period, retries, increments the wait interval by the value specified, then retries again. This process continues until the number maximum retries has been reached or until the connection load on the server goes down. The default settings in ZENworks Configuration Management are 20 retries, an initial wait time of 10, and a maximum wait time of 20. This means that a device waits a maximum of 345 seconds before marking a busy Primary Server or Satellite device as Bad. All the HTTP or HTTPS calls are sequential, so if the closest server rules are correctly configured, the wait should be very short. Connecting to a different Primary Server or Satellite device might not be the best option because it might be overloaded or across a low-bandwidth, high-latency connection.

These settings should be based on the placement of Primary Servers and Satellite devices within the environment. If there are many Primary Servers in a location connected to the clients by high-bandwidth, low-latency links, these settings can be lowered. If there are fewer Primary Servers and clients connecting over low-bandwidth, high-latency links, or to a Satellite device across a WAN, these settings can be increased to "wait out" the busy period. These settings can be overridden on the device or folder level.

During Novell testing, retries were set at 60/30/60. A server was never marked as Bad, and all content was delivered. No degradation of performance at the client was observed when the retries were set high.

Additionally, you should configure the behavior of the ZENworks Adaptive Agent by disabling the features that you will not use. For example, if you do not intend to use ZENworks Imaging, then turn off the feature by disabling it. This keeps the agent streamlined by using only the resources it needs. If you decide to utilize Imaging later, you can simply enable it again without any additional deployment.

Agent Features			
Policy Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Remote Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Asset Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Image Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
User Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Bundle Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Patch Management	<input checked="" type="checkbox"/> Installed	<input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled
Endpoint Security Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled

Inventory Schedules

Inventory scan frequency depends on how often the hardware and software in the environment changes, and how accurate the information needs to be. Under normal circumstances, it should be adequate to collect inventory data on a weekly, biweekly, or monthly basis, but this might not be sufficient for all deployments. Be aware of the workload placed on the ZENworks Primary Servers. Every inventory scan a device does must be processed by the ZENworks Primary Server and stored in the ZENworks database. Ensure that the schedule does not unnecessarily scan thousands of devices on a daily basis, but if this is necessary, closely monitor the load and performance of both the Primary and database servers. Inventory schedules can be set at the Management Zone folder, and device level. We recommend that you configure inventory schedules on a folder basis to ensure that the load is spread through a given time period. If you must immediately update the inventory of a device, a scan-now request can be sent to the device via ZENworks Control Center.

For a weekly scan, select a day that is most likely to capture the largest number of devices connected to the network. To capture all workers, consider doing a scan on every fifth day so that all days are eventually targeted.

For restricted scan times, use the random wait time carefully. If a scan window of 9:00–17:00 is configured with the *Randomize scan time* option, devices that disconnect during this period might not be scanned. This can cause many to consistently miss their scans. The *Process immediately if device unable to execute on schedule* option instructs any device that missed the schedule to scan when it next connects to ZENworks. This is useful for ensuring that devices perform an inventory when they are offline during their assigned inventory schedule.

Use a schedule that best fits the environment and avoiding restricting the scan times severely. A very small “scan potential” window can lead to many devices not performing regular inventory scans.

If some devices are always on, consider starting the scan schedule before or after normal office hours, so these devices can be processed when there is low utilization.

We recommend using a combination of inventory reporting and the advanced device search function to compare last scan dates with last contact dates, so you can ensure that devices are being scanned according to their schedules.

Scan Schedule

Specify the schedule the device inventory scanner should run on:

Schedule Type:
 Recurring

When a device is refreshed

Delay execution after refresh: 0 Days 0 Hours 0 Minutes

Days of the week

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

Start Time: 1 :00 am
[More Options](#)

Monthly

Day of the month: 1

Last day of the month

First Sunday

Start Time: 1 :00 am
[Hide Options](#)

Process immediately if device unable to execute on schedule

Use Coordinated Universal Time (Current UTC 10:53 PM)

Start at a random time between Start and End Times

End Time: 8 :00 pm

Restrict schedule execution to the following date range:

Start Date: 10/30/08

End Date: 10/30/08

Fixed Interval

0 Months 0 Weeks 0 Days 0 Hours 0 Minutes

Start Date: 10/30/08 Start Time: 1 :00 am
[More Options](#)

OK Apply Reset Cancel

For more information, see the [ZENworks 11 SP2 System Administration Reference](#).

4.2.9 Device Discovery

When it comes to device discovery, you need to perform your discoveries and deployments in stages. Use the recommendations in this section for discovery and deployment in order to avoid massive amounts of discovery traffic on the LAN/WAN.

Some ideas to consider when performing device discovery include:

- Discover assets subnet by subnet.
- Discover assets building by building.
- Discover assets site by site.
- Import devices from Active Directory or eDirectory by using LDAP discovery tasks

- ◆ Import devices from a spreadsheet (CSV) if they are well documented and the list is available for you to use.
- ◆ Use the ZENworks Migration Wizard to migrate your devices from eDirectory and target them for deployment to avoid discovery of the initial assets that are already part of an existing ZENworks system.
- ◆ Use pilot groups.

These tips help you discover assets and roll out the ZENworks Adaptive Agent in a very manageable way, which avoids failures for deployment and installation.

Table 4-1 lists the duration and CPU usage for a discovery task performed by using the MAC Address technology. This information helps you configure the discovery settings in an efficient way.

Table 4-1 Duration and CPU Usage for a Discovery Task

IP Address Range	Duration of the Discovery Task	CPU Usage	Additional Details
Single IP address	Less than 1 minute	Less than 5%	The discovery task starts immediately when it is launched.
164.99.94.0–164.99.94.255 (254 devices)	10 minutes	5%	The discovery task starts immediately when it is launched.
164.99.0.0–164.99.255.255 (65,534 devices)	30 hours	36%	The discovery task starts immediately when it is launched.
164.0.0.0–164.255.255.255 (16,277,214 devices)	Always in a <i>Pending</i> state	100%	<ul style="list-style-type: none"> ◆ The discovery task is not started. The status of the task remains as <i>Pending</i>. ◆ CPU usage is normal 10 minutes after the time the discovery task is launched. ◆ If any other discovery or loader task is running simultaneously, it might take a considerable time to complete.

There are several things you can do to increase the speed of IP Discovery tasks.

- ◆ Increase the *Maximum Concurrent Discoveries* from 5 to 20. This allows more addresses to be scanned simultaneously.
- ◆ Select only the discovery technologies that are required. We recommend enabling only the discovery technologies that are configured within the environment. If SSH, NMAP, or SNMP is not available or is not configured in the environment do not enable it. Every discovery technology that is scanned for an IP address adds time to the discovery task. As a rule of thumb, start with only WinAPI and the ZENworks discovery technologies enabled for the Management Zone. You can override discovery technologies in the Discovery task, which means that specific discovery technologies can be directed at certain subnets.
- ◆ Configure only the necessary authentication credentials. The more authentication credentials that are configured, the longer each scan takes.
- ◆ Disable the MAC Address discovery technology. Any device with a MAC Address is discovered via this technology. The devices show up in the discovered list with an Unknown operating system, which causes the deployable device list to be inaccurate.

All discoveries are performed from the *Deployment* tab in ZENworks Control Center.

Agent State

A Discovery task returns Management Zone information on devices with a ZENworks Configuration Management Agent installed. The discovered devices can be viewed from the ZENworks Control Center > Devices > Discovered tab. It is possible to see which devices are registered with another Management Zone and which agents are currently unregistered.

The name of a managed device residing within the same Management Zone as the Primary server is displayed in green and the name of the managed device residing in a different management zone is displayed in the yellow.

Schedule

A discovery only returns device information if the device is turned on and contactable. A discovery task should be run regularly on different days and times to ensure the entire environment is captured.

For more information, see the [ZENworks 11 SP2 Discovery, Deployment, and Retirement Reference](#).

4.2.10 Adaptive Agent Deployment

Novell ZENworks Configuration Management provides a variety of methods you can use to install the ZENworks Adaptive Agent to devices:

- ◆ Use ZENworks Control Center to deploy the agent from the ZENworks Server to the device.
- ◆ At the device, use a Web browser to download and install the Agent from the ZENworks Server.
- ◆ Include the Agent in an image and apply the image to the device.
- ◆ Use a login script, Windows group policy, or ZENworks 7 Application object to install the Agent.
- ◆ Deploy to the OSX environment using a custom Macintosh package.

Because ZENworks Configuration Management is usually implemented in larger environments, we recommend deploying the ZENworks Adaptive Agent automatically and you should not manually install the Agent wherever possible.

The following sections contain more information:

- ◆ [“Default Deployment Packages” on page 95](#)
- ◆ [“Custom Deployment Packages” on page 96](#)
- ◆ [“Macintosh Agent Install Packages” on page 96](#)

Default Deployment Packages

The best option for accessing the default deployment packages is through ZENworks Control Center:

- 1 From the *Home* page in ZENworks Control Center, click *Download ZENworks Tools* in the left frame.
- 2 Download the default package that you require.

We recommend using one of the following deployment methods:

- ♦ Use the *Deployment* task from ZENworks Control Center, after discovering or importing devices.
- ♦ Use your existing software distribution tool to deploy the agent.
- ♦ Include the ZENworks Adaptive Agent in a new image.

For all methods you must have registration keys in place as described in [Section 4.2.11, “Registration Rules and Keys,” on page 98](#).

For more information, see the [ZENworks 11 SP2 Discovery, Deployment, and Retirement Reference](#).

Custom Deployment Packages

During the ZENworks Configuration Management installation, default ZENworks Adaptive Agent deployment packages are created. These packages are tied to the ZENworks Primary Server and contain the URI from this server to register devices. There are no registration keys configured and the registration process use default rules to register devices.

It is best practice to always use custom deployment packages when pushing the ZENworks Adaptive Agent to your discovered or imported devices. You should avoid the use of the default Agent deployment packages that are created because these include only default parameters that likely do not meet the needs of the customer.

You must be familiar with these concepts before testing begins.

Macintosh Agent Install Packages

ZENworks 11 SP2 now includes support for managing Macintosh OS X devices via ZENworks. This section describes how to wrap the installation files for the ZENworks 11 SP2 Adaptive Agent in a Macintosh OS X package file.

Because ZENworks uses a Linux or Windows server to build the adaptive agent packages after an install or system update, it is not possible to automatically build a Mac OS X package (.pkg). The default is to build a self-extracting .bin file that can be used by running standard shell commands. However, many Macintosh users are uncomfortable or unfamiliar with this process. They might resist installing the agent unless it is packaged in a familiar format. You can use the Apple Package Maker utility to create a Macintosh Package File (.pkg) that can be sent to users so they install the ZENworks Adaptive Agent. To do this, you need ZENworks 11 SP2, a Mac OS X device, and the latest version of the Apple Xcode tools.

- 1 Ensure that you have the latest version of Xcode installed so that the Package Maker application is available.

To do this, follow the instructions described [here \(http://developer.apple.com/xcode/\)](http://developer.apple.com/xcode/).

- 2 On the Macintosh device on which you installed Xcode, navigate to the home directory and create a directory named ZenAgent .

For example, if you are logged in as admin, the path to this directory would be /Users/admin/ZenAgent.

- 3 Copy the Macintosh installer package from your Primary Server to the ZenAgent directory on the device on which you installed the Xcode tools.

The agent is located on the Primary Server in the
%ZENWORKS_HOME%\install\downloads\setup_all\PreAgentPkg_AgentMacComplete.bin
directory.

- 4 Use vi to create a script file using vi with the following content: zenagentinstall.log.


```
#!/bin/sh
```

```
/tmp/PreAgentPkg_AgentMacComplete.bin > /tmp/zenagentinstall.log
```

This will be used to launch the installer and log the output to the `zenagentinstall.log` file.

- 5 Save the file as `zenagent.sh` in the `ZenAgent` folder that you created in [Step 2](#).

- 6 At a terminal prompt, enter the following commands to set ownership and make the files executable:

```
chmod -R +rx /Users/<username>/ZenAgent
```

```
chown -R root:admin /Users/<username>/ZenAgent
```

- 7 Launch Package Maker by running the following command:

```
open -a /Developer/Applications/Utilities/PackageMaker.app
```

- 8 Go to `Install Properties` and enter `com.novell` in the *Organization* field.

- 9 In the *Minimum Target* field, select *Mac OS X v 10.5 Leopard*.

- 10 Click *OK*.

- 11 Configure the package properties:

- 11a Select the *Configuration* tab of the *Untitled (Package)* pane.

- 11b In the *Title* field specify `ZENworks Adaptive Agent for Mac OS-X`.

- 11c In the *Install Destination* section, deselect *Volume* selected by user and then select *System volume*.

- 11d Select the *Requirement* tab, then click the plus symbol `+`.

- 11e In the *is* drop-down list, select `>=`.

- 11f In the textbox enter `200`.

- 11g In the message box, if you find the `Insufficient disk space` message, make sure that you have at least `200 MB` available.

- 11h Click *OK*.

- 12 Add the files required for installing the agent to your package:

- 12a In *Finder*, locate your `ZenAgent` folder.

- 12b Drag the `ZenAgent` folder to the *Drop contents here* pane in `Package Maker`.

- 12c In the *Destination* field of the *Configuration* tab, enter `/tmp`.

- 12d Select the *Scripts* tab.

- 12e Click the gear icon next to the *Postinstall* box, then select *Choose*.

- 12f Browse to and select your `zenagent.sh` script; then click *Choose*.

- 13 Save the package definition.

- 14 Specify `ZENagent` in the *Save As* field, then click *Save*.

- 15 Click *Build*.

- 16 When `ZENworks Adaptive Agent` is displayed in the *Save As* field, click *Save*.

- 17 Transfer the `ZENagent.pkg` file to a test Macintosh device on which you want to install the `ZENworks` agent.

- 18 Run the package and follow the prompts. Use the administrative credentials.

The agent automatically registers the device with `ZENworks`. If you want the `z`-icon to appear, you can log out, then log back in.

4.2.11 Registration Rules and Keys

When you deploy the ZENworks Adaptive Agent to a device, the device is registered in the Management Zone and becomes a managed device. As part of the registration, you can specify the device's ZENworks name and the folder and groups to which you want the device added.

By default, when a device's host name is used as its ZENworks name, it is added to the `/Servers` or `/Workstations` folder, and it is not given membership in any groups. You can manually move devices to other folders and add them to groups, but this can be a burdensome task if you have a large number of devices or if you are consistently adding new devices. The best way to manage a large number of devices is to have them automatically added to the correct folders and groups during registration.

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

The following sections contain more information:

- ♦ [“Registration Rules” on page 98](#)
- ♦ [“Registration Keys” on page 98](#)
- ♦ [“Recommendations Regarding Registration” on page 99](#)
- ♦ [“Registration” on page 100](#)

Registration Rules

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

ZENworks Configuration Management includes a default registration rule for servers and another one for workstations. If a device registers without a key, the default registration rules are applied to determine the folder and group assignments. The two default rules cause all servers to be added to the `/Servers` folder and all workstations to the `/Workstations` folder.

The two default rules are designed to ensure that no server or workstation registration fails. Therefore, you cannot delete or modify these two default rules. You can, however, define additional rules that enable you to filter devices as they register and add them to different folders and groups. If you've established folders for devices with similar configuration settings and groups for devices with similar assignments, newly registered devices automatically receive the appropriate configuration settings and assignments.

For more information, see the [ZENworks 11 SP2 Administration Quick Start](#).

Registration Keys

A registration key is an alphanumeric string that you manually define or randomly generate. During deployment of the ZENworks Adaptive Agent on a device, the registration key must be provided. When the device connects to a ZENworks Server for the first time, the device is added to the folder and groups defined within the key.

You can create one or more registration keys to ensure that devices are placed in the desired folders and groups. For example, you might want to ensure that all of the Sales department's workstations are added to the `/Workstations/Sales` folder but are divided into three different groups

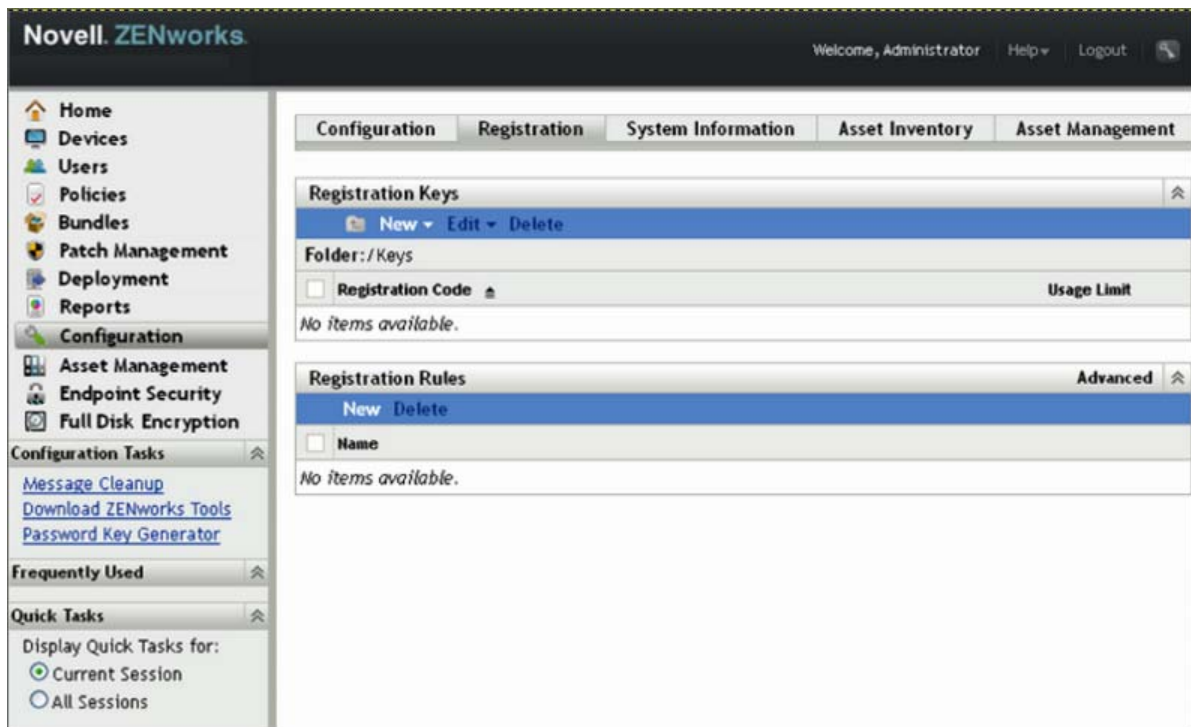
(SalesTeam1, SalesTeam2, or SalesTeam3) depending on their team assignments. You could create three different registration keys and configure each one to add the Sales workstations to the / Workstations/Sales folder and the appropriate team group. As long as each workstation uses the correct registration key, it is added to the appropriate folder and group.

For more information, see the [ZENworks 11 SP2 Administration Quick Start](#).

Recommendations Regarding Registration

Based on your final folder and groups design, we recommend that you create registration keys for each folder you have created or defined.

The following graphic illustrates using registration keys to place devices in folders.



New York City: Registers the New York City folder, below USA.

Montreal: Registers the Montreal folder, below Canada.

London: Registers the London folder, below England

In combination with dynamic groups that are based on departments, it is possible to manage device registration very easily. You use these keys in your deployment packages to auto-register all devices in your Management Zone.

Registration

You should enable dynamic device renaming, which is disabled by default.

This feature provides a very flexible way to handle some desktop management processes such as renaming or re-installation. During the ZENworks Configuration Management framework-based installation process, the device name changes to a randomly generated name, but if this feature is place and you have a working imaging partition, all references are automatically maintained by the ZENworks Adaptive Agent registration process.

This prevents having duplicated device entries and GUIDs in the database.

The screenshot displays the configuration interface for device registration, organized into several sections:

- Device Naming Template:** A text input field contains the template `$(HostName)` with a small icon to its right.
- Registration Rules:** Two checkboxes are checked: "Enable use of registration rules." and "Enable use of default registration rules."
- Device Dynamic Rename:** A checkbox labeled "Enable automatic renaming of devices." is unchecked.
- Reconcile Settings:** A section titled "Indicate which device attributes will be used in reconciliation" contains three checkboxes: "Serial Number" (checked), "Mac Address" (checked), and "Machine Name" (unchecked). Below this, a checkbox for "Enable Differentiation" is checked.

For more information, see the [ZENworks 11 SP2 System Administration Reference](#).

4.2.12 Remote Management

All guidelines for Remote Management are concerned with the configuration settings for performance and security.

- ♦ ["Security" on page 101](#)
- ♦ ["Performance" on page 102](#)

Security

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

- ♦ [“Rights-Based Remote Management Authentication” on page 101](#)
- ♦ [“Password-Based Remote Management Authentication” on page 101](#)

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, ZENworks administrators 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.

The remote operator does not need any exclusive rights to perform a remote session on the managed device if no user has logged in to the managed device or if a user has logged in to the managed device but not in to ZENworks. However, the remote operator needs exclusive Remote Management rights to perform the remote operation on the managed device when a ZENworks user has logged in to the device. We strongly recommend using the rights-based authentication because it is safe and secure.

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. There are two types of password authentication schemes:

- ♦ **ZENworks Password:** This scheme is based on the Secure Remote Password (SRP) protocol (version 6a). The maximum length of a ZENworks password is 255 characters.
- ♦ **VNC Password:** This is the traditional VNC password authentication scheme. The maximum length of a VNC password is 8 characters. This password scheme is inherently weak and is provided only for interoperability with the open source components.

If you use password-based authentication, we strongly recommend using the ZENworks Password scheme because it is safer and more secure than the VNC Password scheme. Ensure that any passwords used are of an adequate length and complexity.

The password schemes operate in the following modes:

- ♦ **Session Mode:** A password set in this mode is valid only for the current session. The user on the managed device must set the password at the start of the remote session and communicate the password to the remote operator through out-of-band means. If you use password-based authentication, we strongly recommend that you use this mode of authentication because the password is valid only for the current session and is not saved on the managed device.
- ♦ **Persistent Mode:** In this mode, the password can be set by the administrator through the Remote Management policy or by the managed device user through the ZENworks icon if the *Allow user to override default passwords on managed device* option is selected in the security settings of the Remote Management policy.

If the password is set by both a remote control policy and the user, the password set by the user takes precedence over the password configured in the policy.

Performance

The performance features are enabled by default in the Remote Management policy or configuration page. They can be disabled, but we do not recommend doing this.

For more information, see the [ZENworks 11 SP2 System Administration Reference](#).

4.2.13 Inventory

ZENworks Configuration Management contains a powerful feature for collection and reporting on software and hardware inventory in the environment. The configuration of the inventory collection should be managed before deployment to ensure that the devices are collecting only relevant information.

Inventory collection settings are split into three main sections. Each section is configured independently of the others.

- ♦ **Scan Now:** If a device is manually forced to perform an inventory scan.
- ♦ **First Scan:** The first time the agent is installed and a scan happens. Controlled by the *Logins before first scan* configuration setting in ZENworks Control Center. This setting should complement the build process of the devices.
- ♦ **Recurring Scan:** Controlled by the Inventory Scan Schedule. See [“Inventory Schedules” on page 92](#) for further information.
- ♦ [“Software File Information” on page 102](#)
- ♦ [“Collection Data Form Schedules” on page 103](#)

Software File Information

Select the *Collect Software File Information* option only if you must identify software products that aren't recognized by the ZENworks Knowledgebase. This option forces a very granular collection of inventory information, which has performance impacts throughout the ZENworks infrastructure. If you must create local software products based on software file information, we recommend that you override inventory settings only on the individual target devices.

Inventory			
Configure device inventory settings.			
Scan Now			
<input checked="" type="checkbox"/> Collect Software Applications	<input checked="" type="checkbox"/> Collect Hardware	<input type="checkbox"/> Launch Collection Data Form	<input checked="" type="checkbox"/> User Can Initiate Scan
<input type="checkbox"/> Collect Software File Information		<input type="checkbox"/> Run DMTF Translator	
First Scan			
<input checked="" type="checkbox"/> Collect Software Applications	<input checked="" type="checkbox"/> Collect Hardware	<input type="checkbox"/> Launch Collection Data Form	
<input type="checkbox"/> Collect Software File Information		<input type="checkbox"/> Run DMTF Translator	
Recurring Scan			
<input checked="" type="checkbox"/> Collect Software Applications	<input checked="" type="checkbox"/> Collect Hardware	<input type="checkbox"/> Launch Collection Data Form	
<input type="checkbox"/> Collect Software File Information		<input type="checkbox"/> Run DMTF Translator	

For more information, see the [ZENworks 11 SP2 Asset Inventory Reference](#).

Collection Data Form Schedules

The collection data form is used to collect demographic information for a device or user. The information can be collected on several schedules or events, or it can be collected manually. You can also use the *Scan Now*, *First Scan*, or *Recurring Scan* options. This information can be very useful when attempting to identify where devices are located and who is using them.

Select a schedule that best fits your requirements. Collecting this information on a monthly basis should be a good choice. Ensure that you run a new collection after a change, such as a move or user change.

Use the auto-fill function to avoid user input. System variables and registry settings can be used to silently collect the demographic data. These variables or settings can be delivered through the install process or through bundles. Administrator-defined fields should be created to collect additional information.

For more information, see the [ZENworks 11 SP2 Asset Inventory Reference](#).

4.2.14 Application Management

You are not required to organize bundles into different folders, but we recommend that you use a minimal folder structure to divide applications and images. If bundles are organized logically and granularly, it becomes very easy to create special administrative accounts that only have limited rights to a given folder or set of folders.

- ◆ [“Recommendations for Organizing Bundles” on page 104](#)
- ◆ [“Bundle Groups” on page 105](#)
- ◆ [“Assigning Bundles” on page 105](#)
- ◆ [“Importing and Exporting Bundles” on page 105](#)
- ◆ [“Application Delivery Mechanism” on page 106](#)

Recommendations for Organizing Bundles

Every organization is different and has different requirements for organizing content. The important thing to keep in mind is that you should always organize your content according to how your organization views it. If you do not organize the content and simply put everything into the default folder, it becomes unmanageable within a very short time.

Keeping this in mind, some best practices for organizing your bundle objects include:

- ◆ Creating a folder for application bundles.
- ◆ Creating a folder for imaging bundles.

The ZPM folder is an auto-generated folder that contains all -service related bundles. Although the bundles in this folder can be changed and additional ones created, we recommend that you do not change the folder and the bundles within it.

We recommend that you create folders under the base Bundles folder to group imaging and application bundles together. The following list provides examples of the types of folders that can be created:

- ◆ Create a folder for software vendors:
 - ◆ Microsoft (Office, Internet Explorer, MediaPlayer)
 - ◆ Adobe (Reader, Photoshop)
 - ◆ SAP (Basis, HR)
 - ◆ Novell
- ◆ Create a folder for special applications:
 - ◆ CAD
 - ◆ Database applications
 - ◆ Software development
- ◆ Create a folder for tools:
 - ◆ Windows tools (WinZip, WinRAR, UltraEdit, and so forth)
- ◆ Create a folder for base images.
- ◆ Create a folder for add-on images.

Categorizing application and imaging bundles into separate folders also allows for administrator roles to be created so you can limit the bundles that an administrator can edit or assign to devices.

Bundles						
New Edit Delete Action Quick Tasks						
<input type="checkbox"/>	Status	Name	Type	Category	Enabled	Version
<input type="checkbox"/>		Adobe (Details)	Folder			
<input type="checkbox"/>		Microsoft (Details)	Folder			
<input type="checkbox"/>		Mozilla (Details)	Folder			
<input type="checkbox"/>		Tools (Details)	Folder			
<input type="checkbox"/>		Standard-Apps	Bundle Group			
<input type="checkbox"/>		LDAP-Browser	Windows Bundle		Yes	2
<input type="checkbox"/>		TEST-APP	Directive Bundle	Directive Bundle	Yes	1

1 - 7 of 7 show 25 items

The important thing is to arrange your content with your company organization in mind. This might be different with each company or site. This information should be gathered during the design phase of the project and detailed in the design document.

For more information, see the [ZENworks 11 SP2 Software Distribution Reference](#).

Bundle Groups

In addition to using folders, it is a good idea to create bundle groups for some applications to make assignments easier. Each group contains a set of bundles that belong together. These groups can be organized for special functions or tasks.

The following are some examples of how you might want to leverage bundle groups to keep things simple:

- ◆ APPS-Base: Contains all applications needed by all users.
- ◆ Finance-Applications: Contains bundles needed to work with finance applications.
- ◆ Help Desk-Tools: Contains bundles that are related to the Help Desk.

The following is a graphical representation of how you might want to leverage bundle groups:

For more information, see the [ZENworks 11 SP2 Software Distribution Reference](#).

Assigning Bundles

A major feature in ZENworks Configuration Management is the ability to inherit assignments from multiple places within the system. With this feature, it is very easy to assign a bundle or bundle group to many devices in seconds. You do not need to assign bundles to each device, which saves time and money.

Based on your folder and group design, we recommend that you use folder or group assignments instead of direct assignments. Use these indirect assignments wherever possible to increase speed and reduce administration effort. If you utilize folders and groups for as many of your assignments as possible, you can deliver updates to hundreds of devices when you need to get them there, even immediately.

Best practices on how to leverage folders and groups include:

- ◆ If you have a set of bundles that are required for all devices in a site, use the site folder to assign these bundles or bundle groups.
- ◆ If you have special bundles that are used in one or more departments, assign these bundles only to the department folders.
- ◆ If you have bundles that are used by several devices in different folders, set up groups for assignments.
- ◆ Only use direct assignments if a single device or a small number of devices need special assignments.

For more information, see the [ZENworks 11 SP2 Software Distribution Reference](#).

Importing and Exporting Bundles

Novell best practice dictates that a new application or change to an existing application in the environment should use a testing phase that does not affect the production network. We recommend that a development zone (DEV-ZONE) be created with its own ZENworks Configuration Management structure that mirrors the production network. After an application has been approved

for production deployment, it should then be moved from the DEV-ZONE to the production zone (PROD-ZONE). Currently there is no way to export MSI files from the Content Repository, so we recommend that all source files are retained; otherwise, there will be no source to be imported into production (see [TID 7002543 \(http://www.novell.com/support/\)](http://www.novell.com/support/) on the Novell Support page).

To export bundles:

- 1 From the DEV-ZONE ZCM server, export the bundle to a specific export directory by using the following command:

```
zman bundle-export-to-file /bundle_path/bundle_name bundle_filename.xml
```

If the application has no dependencies and is not a Windows MSI bundle, a single *bundle_filename.xml* is created. If there are dependencies or MSI content to be imported into the Content Repository, two files will be created: *bundle_filename.xml* and *bundle_filename_ActionContentInfo.xml*.

For example, you can export the officeXP bundle to *officeXP.xml* by using the `zman bundle-export-to-file officeXP officeXP.xml` command. The *officeXP.xml* and *officeXP_ActionContentInfo.xml* files are created.

- 2 Copy all files related to the application MSI (not all MSI files are self-contained) to the same application export directory. It is possible to place the application MSI in a separate folder; however, the following section of the *bundle_filename_ActionContentInfo.xml* file needs to be modified to specify the content location:

```
includeAllFilesinSubFolders="false">E:\files\ApplicationX.msi</ContentFilePath>
```

- 3 Copy the entire directory by whatever method of communication is approved from the DEV-ZONE server to the PROD-ZONE server.
- 4 Create the bundle on the PROD-ZONE ZCM server by using the following command:

```
zman bundle-create new_bundle_name bundle_xml_filename.xml bundlefolder --actioninfo bundle_name_ActionContentInfo.xml (using /bundlefolder/bundle_name results in an error because of invalid characters).
```

For example, use the following command to create a bundle called ApplicationX:

```
zman bundle-create OfficeXP officeXP.xml "/Bundles/Microsoft Applications" --actioninfo officeXP_ActionContentInfo.xml
```

Application Delivery Mechanism

There are a number of different methods to deliver content to your managed devices with ZENworks Configuration Management.

- ♦ [“Tomcat via HTTPS” on page 106](#)
- ♦ [“NetWare” on page 107](#)
- ♦ [“Microsoft” on page 107](#)
- ♦ [“Other Network Shares \(NetStorage\)” on page 108](#)
- ♦ [“Recommendation for the Delivery Mechanism” on page 108](#)

Tomcat via HTTPS

Benefits:

- ♦ ZENworks Configuration Management controls the distribution of content to the various Satellite devices and Primary Servers that exist within the Management Zone.

- ◆ Data is encrypted within Tomcat, so anyone with file access to the server will not be able to access applications.
- ◆ HTTP is used to deliver content, rather than SSL, so there is no overhead to re-encrypt the content for transmission.
- ◆ Access to data is based upon the relationships defined within ZENworks Configuration Management. If you are not a target device or user of ZENworks Configuration Management, you have no access to application, image, or policy data.
- ◆ This is a firewall-friendly solution. It is very easy to allow DMZ access to content for remote, Internet-based devices, without cumbersome configuration changes on routers, switches, and firewalls.

Drawbacks:

- ◆ The ZENworks Configuration Management server becomes less scalable because it is serving more HTTP requests from managed devices.
- ◆ It can take some time before an application has finished encrypting and injecting its data into the Web server.

NetWare

You can use the Novell Client (Client32) and existing mapped network drives or directly via UNC to provision application data to your managed devices.

Benefits:

- ◆ Uses the existing infrastructure.
- ◆ Less overhead is required on the ZENworks Server.

Drawbacks:

- ◆ ZENworks Configuration Management has no control over the distribution of the application content. The distribution must be managed outside of ZENworks Configuration Management with products such as ZENworks Server Management.
- ◆ ZENworks Configuration Management has no control over who has access to the data.
- ◆ Application content is not encrypted and can potentially be installed by anyone with access to the server.
- ◆ This is not a firewall-friendly solution. Access from outside the firewall requires VPN access in order to deliver applications.

Microsoft

You can use Microsoft Active Directory servers, or file and print servers.

Benefits:

- ◆ Uses existing infrastructure servers.
- ◆ Less overhead is required on the ZENworks Server.
- ◆ Uses existing domain credentials of devices and users to control access to the files you are provisioning to managed devices.

Drawbacks:

- ◆ ZENworks Configuration Management has no control over the distribution of the application content. The distribution must be managed outside of ZENworks Configuration Management with products such as ZENworks Server Management.

- ♦ ZENworks Configuration Management has no control over who has access to the data.
- ♦ Application content is not encrypted and can potentially be installed by anyone with access to the server.
- ♦ This is not a firewall-friendly solution. Access from outside the firewall requires VPN access in order to deliver applications.

Other Network Shares (NetStorage)

It is also possible to use NetStorage devices for content hosting and delivery of application content to your managed devices.

Benefits:

- ♦ Uses existing infrastructure.
- ♦ Less overhead is required on the ZENworks Server.

Drawbacks:

- ♦ ZENworks Configuration Management has no control over the distribution of the application content. The distribution must be managed outside of ZENworks Configuration Management.
- ♦ ZENworks Configuration Management has no control over who has access to the data.
- ♦ Application content is not encrypted and can potentially be installed by anyone with access to the server.
- ♦ This is not a firewall friendly solution. Access from outside the firewall requires VPN access in order to deliver applications.

Recommendation for the Delivery Mechanism

Novell recommends using the ZENworks Configuration Management internal delivery mechanism (HTTP) for bundles and policies. Although it might be easier to use other delivery methods you will lose most of the benefits within ZENworks Configuration Management. Some of these benefits include:

- ♦ Content replication capabilities
- ♦ Rights to the content store
- ♦ Data encryption and security wrapped around content

4.2.15 Policy Management

In general, it is not a good idea to have thousands of different policies in place to fulfill all requirements. In desktop management, there are usually sets of policies for certain groups, such as normal users, administrative users, and special user groups, such as software developers.

However, you might also want to organize policies in more than one folder to restrict access and administration to specific groups or users.

Some policies definitely need to be restricted to a set number of people within the organization (such as remote management policies), so you need to consider this best practice recommendation carefully.

However, it is a good idea to organize different sets of policies in different folders. In addition, we recommend that you use policy groups to put different policies together in a single package and then assign these policy groups to devices or users, (policy groups are loosely synonymous to policy packages in previous versions of ZENworks Desktop Management).

To make sure that every device receives the required and effective settings, we recommend that you define the order in which policies are applied. There are four options you can use here, and you need to understand your policy requirements before you make these decisions:

- ◆ Apply device policies first, user policies last (user-assigned policy wins)
- ◆ Apply user policies first, device policies last (device-assigned policy wins)
- ◆ Use only device policies
- ◆ Use only user policies

All policies are applied in the following order: folder, group, then device or user.

The following graphic shows the effective policies on a given device:

Assigned Policies					
Direct			Inherited		
Name	Type	Log in User	Deployment Status	Status	Source
DLU-ADMIN	Dynamic Local User Poli		Unknown		NCS
Policies-ADM	Policy Group				NCS
DLU-ADMIN	Dynamic Local User Poli		Not Effective		
RemMgmt-ADM	Remote Management Pc		Unknown		
Policy-STD	Policy Group				BRA
Bookmarks-STD	Browser Bookmarks Polk		Failure [Details]		
Printer-STD	Printer Policy		Success [Details]		
RemMgmt-STD	Remote Management Pc		Not Effective		
ZEN-EXPLORER-STD	ZENworks Explorer Conf		Success [Details]		
DLU-STD	Dynamic Local User Poli		Not Effective		

In the above example, there is a policy group assigned to a folder BRA. This group contains all policy settings (Policy-STD) that are required for all users in BRA. Additionally there is policy group assigned to the NCS folder (below BRA). Finally, there is a direct policy assignment to the NCS folder that modifies the DLU settings only.

The following sections contain more information:

- ◆ [“Recommendations for Managing Policies” on page 109](#)
- ◆ [“Advantages to Assigning Group Policies through ZENworks Configuration Management” on page 110](#)
- ◆ [“Linux Puppet Policies” on page 110](#)

Recommendations for Managing Policies

Organizing policies into folders and policy groups makes it easier to manage the assignment process to devices and users. When managing policies, you should consider the following items:

When managing policies, you should:

- ◆ Define user and device categories during the assessment phase, such as Standard-user, Administrative-user, Management-user, Help Desk-device, and so forth.
- ◆ Define required policies and sets that can be used for policy groups.
- ◆ Define the order in which policies are applied.
- ◆ Assign policy groups to folders as needed.
- ◆ Use folder or group assignments wherever possible.

Advantages to Assigning Group Policies through ZENworks Configuration Management

With ZENworks Configuration Management, you can use plural group policies, meaning you can layer multiple group policies on top of each other, applying what is referred to as effective policies at the endpoint level. Using ZENworks Configuration Management to do this allows you to handle roaming users effectively, making policies available to end users no matter where they are logging in from. Most organizations use group policies to manage the look and feel of the user's desktop experience. There are two choices when it comes to using Group Policies in your environment:

- ♦ Import your policy files into ZENworks Configuration Management and replicate them across your infrastructure.
- ♦ Deliver your policies through Microsoft Active Directory.

Linux Puppet Policies

The Puppet policy follows a client/server deployment model to automate configuration management of multiple hosts in the ZENworks environment. As a client/server model, the ZENworks Server replaces the role of puppet master, allowing it to centrally store and deploy the puppet configuration resources and catalogs by using the Puppet policy.

The ZENworks managed device acts as the puppet client to invoke the puppet standalone executable as part of its policy enforcement to locally compile and apply the puppet catalogs and scripts to every managed node. The puppet content is distributed as either manifest (puppet programs) or modules (self-contained archives with a collection of manifests, types, templates, libraries and files) in puppet directory structure and format. These configuration changes are applied as root on every refresh of the device node.

ZENworks managed devices running Linux use the custom packaging for puppet (supported version = 0.24.8), Ruby, and Facter packages with ZENworks puppet configurations. It does not use the system puppet if it is already installed. Using the ZENworks puppet client to communicate with a standard puppetmaster is not supported, and standard puppet clients are not authorized to retrieve puppet configuration information from a ZENworks Server.

Unlike the standard puppet master, the Puppet policy stores the imported puppet content in the content repository on the ZENworks Server and does not maintain the directory structure. However, the ZENworks puppet client maintains the directory structure under the configured modules path for the deployed modules.

The ZENworks puppet client polling interval is based on the device refresh interval (the default value is 24 hours). The puppet client is preconfigured to use the default puppet settings (for example, modulepath, confdir and log path) for ZENworks. These settings can be modified or overwritten in the policy settings, based on the requirement.

You must ensure that the same puppet module is not deployed to the identical node as part of different policies, and you must also avoid using dependencies among modules. The puppet catalogs (module) can be imported as an archive to different policy versions and deployed to all managed devices on refresh. This allows you to keep it in sync with the central repository on the server and apply changes to achieve baseline configurations. Puppet policies can serve as the best way to scale up basic Puppet deployment through ZENworks, so you can configure and manage more hosts per server.

Refer to the following resources to learn more about Puppet policies and how to utilize them:

- ♦ [Puppet Official Web site \(http://www.puppetlabs.com/\)](http://www.puppetlabs.com/)

- Find and share Puppet modules (<http://forge.puppetlabs.com/>)
- Modules (http://projects.puppetlabs.com/projects/1/wiki/Puppet_Modules)

4.2.16 Linux Patch Management

Publishing ZENworks RPM Packages in the YUM Repository

Whenever RPM packages from external package repositories like NU or RHN are replicated to ZENworks Server, they are stored in the ZENworks content repositories as content. Sometimes it might be necessary for other package management tools like YaST/zypper or YUM to use this RPM content from the ZENworks Server in the local network instead of going to the remote NU or RHN server. You can do this by publishing the ZENworks bundle as a YUM repository. When you create a YUM service from a Linux bundle or Linux Dependency bundle, the packages of the bundle are published as a YUM repository on the ZENworks Server. The repository can then be added as an installation source for package management tools like YaST/zypper or YUM.

For example, suppose that you have installed SUSE Linux Enterprise Server or Open Enterprise Server 2 from media, but you have been applying updates by using ZENworks replicated bundles. If you try to install or edit any pattern or install a new package in YaST, you might get dependency resolution errors, because YaST has no knowledge of the package updates available on the ZENworks Server. It has knowledge of only the installed packages and packages available on the media. YaST must have access to the package updates in ZENworks server to resolve the dependencies properly. However, YaST does not understand the ZENworks bundles and content format. The only way to provide access to ZENworks server packages is to publish the ZENworks bundles containing the package updates as YUM repositories and add the YUM repositories as installation sources in YaST.

Adding External Services by Using an External Service Policy

RPM package distributors publish packages in repository formats like YUM or ZYPP. There might be scenarios where you need to install some packages from these repositories or use these packages for dependency resolution. For example, your SUSE Linux Enterprise media might be available as a ZYPP installation source in a FTP or HTTP (URL) and the packages in the media might be required for dependency resolution while installing SUSE Linux Enterprise package updates. You can add these repositories as external services to the ZENworks agent on managed devices. To add external services to a large number of devices, you can use the External Service policy. You create the External Service policy with repository details and assign the policy to the managed devices to which you want to add the repositories.

Adding ZENworks-Hosted YUM Services to External Package Management Tools

The External Service policy also has an option to synchronize the services with the external package management tools. If you use this option along with adding the external services to ZENworks agent, it also adds the services to external package management tools like YaST/zypper (SLES 10 and SLES 11), rug/zmd (SLES 10), and YUM (RHEL 4 and RHEL 5). You can use both of these features to easily make the ZENworks hosted RPM packages available to external package management tools. To do this, you export the ZENworks bundles to YUM repositories and then create external service policies for these repositories by selecting the option to synchronize the services with external package management tools. Upon enforcement of these policies on managed devices, the service is added to external package management tools.

Using a ZENUSER System Variable

The `{ZENUSER}` system variable maps to the user logged into the graphical session on the Linux device. For example, if user 'bob' is logged into the `display:0` of a Linux device, then any bundle that references the `{ZENUSER}` variable resolves to 'bob'. There are various applications to do this. For example, the `{ZENUSER}` variable can be used to install Desktop icons in the home directory of the logged-in user by setting the path of the icon file to `/home/{ZENUSER}/Desktop/`. A system variable could also be used to set the permission of a installed file to the logged-in user.

4.2.17 Imaging

We highly recommend that you adopt a methodology for creating and delivering Universal Images to your endpoints. A universal image is a single image of Windows XP, Windows Vista, or Windows 7 that can be deployed to multiple hardware types. After you have established the Universal Images, you can deliver core applications and line-of-business applications as add-on images during the imaging process. This method can be further extended to also provide hardware-specific drivers during the imaging process. Tools such as ENGL's Imaging Toolkit for ZENworks Configuration Management can be used to make the process of creating a Universal Image very easy to manage.

For more information, see the [ZENworks 11 SP2 Preboot Services and Imaging Reference](#).

4.2.18 Configuring a Layer 4 Switch

ZENworks Configuration Management supports achieving load balancing and fault tolerance for your infrastructure services though using a Layer 4 (L4) switch. An L4 Switch can front either Primary Servers, Satellite devices, or both. This allows the organization to achieve guaranteed results when directing traffic to the devices behind the switch. Most importantly, this allows organizations to ensure that services are always available to their end user community.

L4 switches are expensive and not affordable for many smaller organizations. Smaller organizations often turn to other forms of load balancing and fault tolerance solutions that are readily available to them. These include solutions such as DNS Round Robin, Microsoft Load Balancing Services, and other open source solutions on the market.

When you do use an L4 switch, you need to ensure that it is properly configured. If the switch is not configured properly, the traffic is not directed properly and there might be issues with connections, responses, and so forth.

The following sections explain the general requirements for properly configuring an L4 switch to be used in front of ZENworks Primary Servers and Satellite devices:

- ♦ [“Foundry Networks ServerIronXL Configuration” on page 112](#)
- ♦ [“Summary of Configuration Settings” on page 113](#)
- ♦ [“Configuring the Closest Server Default Rule” on page 113](#)
- ♦ [“Configuring an L4 Switch Definition from Selected Servers” on page 114](#)
- ♦ [“Additional Details” on page 114](#)

Foundry Networks ServerIronXL Configuration

The following example shows the configuration requirements for a Foundry Networks ServerIronXL switch that was used for testing purposes in the Novell SuperLab. Other vendor products are similar when it comes to configuration and the parameters used. Refer to vendor documentation for further details.


```

ServerIron#sh run
Current configuration:
!
ver 07.3.03T12
no global-stp
global-protocol-vlan
!
server predictor round-robin
server sticky-age 2
server source-nat
server source-ip 151.155.184.107 255.255.252.0 151.155.187.254
!
server real r-ps-1 151.155.184.109
    source-nat
    port http
    port http keepalive
    port http url "HEAD /"
    port http status_code 100 499
    port ssl
    port ssl keepalive
!
server real r-ps-2 151.155.184.110
    source-nat
    port ssl
    port ssl keepalive
    port http
    port http keepalive
    port http url "HEAD /"
    port http status_code 100 499
!
server virtual ps-v1 151.155.184.108
    port ssl sticky
    port http sticky
    track-group http 443
    bind ssl r-ps-1 ssl r-ps-2 ssl
    bind http r-ps-1 http r-ps-2 http
!
vlan 1 name DEFAULT-VLAN by port
    no spanning-tree
!
boot sys fl sec
ip address 151.155.184.107 255.255.252.0
ip default-gateway 151.155.187.254
snmp-server community ..... rw
!
end

```

Summary of Configuration Settings

server source-ip: The IP address given to the L4 device.

server real r-ps-1: The IP address of server1. This server will be selected in [Step 1 on page 114](#).

server real r-ps-2: The IP address of server2. This server will be selected in [Step 1 on page 114](#).

server virtual ps-v1: The virtual IP address used to configure the L4 device in ZENworks Control Center. See [Step 3 on page 114](#).

Configuring the Closest Server Default Rule

In addition to setting up and configuring the L4 switch, you need to also configure the Closest Server Default Rule. For more information, see [“Setting Up Location Closest Server Rules”](#) in the *ZENworks 11 SP2 System Administration Reference*.

Configuring an L4 Switch Definition from Selected Servers

- 1 In one of the role section listings, select the check boxes for one or more servers.
- 2 Click *L4 Switch > Create L4 Switch Definition from Selection*.
- 3 Specify an L4 switch definition name, then click *OK*.
The L4 switch definition name must be either the DNS name or IP address of the L4 virtual server.
- 4 Click *Apply* to make the change effective.

Additional Details

- ♦ The created L4 switch definition is displayed in each of the listings, no matter where it is created, with the selected servers listed under each instance of the L4 switch definition.
- ♦ Servers can be members of multiple groups and L4 switch definitions.
- ♦ Servers that are members of an L4 switch definition or group are no longer listed at the top level of the server listing.

4.2.19 ZENworks System Update

The System Updates feature allows you to obtain updates to the Novell ZENworks 10 Configuration Management software on a timely basis, and also allows you to schedule automatic downloads of the updates.

Software updates are provided periodically and you can choose whether to deploy each update after viewing its content. After you have updated your zone and baselined it to latest version, it is recommended that you delete all other previous updates from the System Update page in ZENworks Control Center. The System Updates page must contain only updates for your existing version, and those regarding updating to a newer version of the product. Even if the system is baselined at the latest version, the Primary Servers calculate which Managed Devices need the updates listed, including older updates.

Before you receive System updates, you need to configure the System Update settings on the Configuration page in ZENworks Control Center. For customers with maintenance contracts, Novell provides an activation code that allows you to start receiving periodic updates. After you have activated your zone, you are ready to start receiving content from Novell. You simply enter your e-mail address and the activation code as seen in the following diagram.

System Update Entitlement	
Use this setting to configure System Update entitlement.	
Email Address	<input type="text" value="msmsms@novell.com"/>
Activation Code	<input type="text" value="*****"/>
Entitlement State	<input type="text" value="ACTIVE"/> Configure
Check For Updates Schedule	
This setting allows the administrator to configure a schedule to check for available updates from Novell.	
Schedule Type:	<input type="text" value="No Schedule"/>
Download Schedule	
This setting allows the administrator to configure a download schedule for updates.	
Schedule Type:	<input type="text" value="No Schedule"/>

For more information, see the [ZENworks 11 SP2 System Administration Reference](#).

4.2.20 Content Management

The “content” in this guide is data that has been uploaded to the ZENworks zone for distribution to a managed endpoint. After the content is uploaded, it is encrypted and distributed to other Primary Servers and Satellite Content Servers in the zone. The ZENworks content repository is accessed by managed devices by using HTTP, a firewall-friendly protocol, allowing content to be provisioned to devices in any location, even outside of the corporate firewall.

A few examples of content include Windows Bundles, Patch Remediation data in ZENworks Patch Management, and ZENworks System Update content. After the content resides centrally on the Primary Servers of the zone, the next stage is to define which content belongs at which Satellite location and how to send the content to that location.

- ◆ [“Defining the What in Content Management” on page 116](#)
- ◆ [“Organizing Bundles” on page 117](#)
- ◆ [“Defining the How in Content Management” on page 118](#)
- ◆ [“Critical Information Required To Determine Content Synchronization Settings” on page 120](#)

Defining the *What* in Content Management

An important improvement in Content Management is the ability to define content replication at the bundle-folder level. This ability provides several advantages over previous releases of ZENworks Configuration Management because it allows groups of applications or patches to be sent to sites with a few mouse clicks.

To define the Satellite devices to which the content located in the folder should be replicated, click the *Details* hyperlink of any bundle folder and click the *Settings* tab. If bundles are subsequently created in the folder, the content synchronization rules of the bundle folder are automatically applied.

In the following screen shot, all bundles in the *Human Resources* bundle folder are sent to the *Stockholm* remote office. A bundle created in the *Human Resources* bundle folder is automatically marked as *included* for the Stockholm location.

Bundles > Novell > Satellite Server Replication

Novell

Displayed Version: 1 (Published)

Satellite Server Replication

Configure content replication to satellite servers.

Current: (System) [Override settings](#)

Satellite Server Replication Status

Replication to new Satellite Servers:

New Satellite Servers added to the system will include this content by default

New Satellite Servers added to the system will exclude this content by default

Include		Exclude			
<input type="checkbox"/>	Name	Path	Parent	Status	Included
<input type="checkbox"/>	blr-cit-176	/Devices/Servers	blr-srm-rrt235		

1 - 1 of 1

show 25 items

Close

The technique of configuring content synchronization at the bundle-folder level is particularly useful when dealing with patches. As patches are stored in bundle folders organized by vendor, and then by month or year of release, groups of related patches can be sent to a given site in one operation. For

example, automatically synchronizing all Microsoft patches for the previous month is extremely easy because this can be accomplished by configuring the relevant ZENworks Patch Management bundle folder, as displayed in the following screen shot:

Bundles > ZPM > PatchAgents > patch-agent-windows-x64

patch-agent-windows-x64

Displayed Version: 1 (Published)

Summary Relationships Requirements Actions Settings

Settings

Bundle Management

Category	Description	Inherited From
System Variables	Configure system variables.	(System)
Primary Server Replication	Configure content replication to primary servers.	(System)
Satellite Server Replication	Configure content replication to satellite servers.	(System)
Sandbox Settings	Configure sandbox-specific settings.	N/A
Endpoint Throttle	Configure endpoint throttling.	N/A
Image Bundle Flag Settings	Configure image related settings.	N/A

Organizing Bundles

Before considering content management, you should organize bundles into separate folders for ease of administration. Bundles can be grouped into folders by function, such as “Productivity Applications,” “Collaboration Applications,” or by business function, such as “Finance Applications” and “Human Resources Applications.” Introducing content control at the bundle-folder level means that the decision of how to organize bundles can also take into account the locations that the applications will be accessed from. For example, if a particular remote location has specific application needs unique to that site, consider creating a bundle folder for that location, thus allowing the content settings to be configured once for the core applications for that site.

If bundles are to be presented to users in the Windows *Start* menu, the default folder structure is a mirror of your bundle folder structure. For example, if the Novell Pulse Login bundle is associated with a user or device and instructed to be included in the *Start* menu, the Start Menu displays *Core Applications > Collaboration Applications > Novell Pulse Login*.

[Bundles](#) > **Bundles_11.2.0**

Bundles							
New ▾ Edit ▾ Delete Action ▾ Quick Tasks ▾							
<input type="checkbox"/>	Status	Name ▲	Type	Category	Enabled	Version	Has Sandbox
<input type="checkbox"/>		Facebook	Windows Bundle	Web Application	Yes	0	No
<input type="checkbox"/>		Perl 5.10	Windows Bundle	MSI Application	Yes	0	No
<input type="checkbox"/>		Perl 5.12	Windows Bundle	MSI Application	Yes	0	No
<input type="checkbox"/>		Python2.5	Windows Bundle	MSI Application	Yes	0	No
<input type="checkbox"/>		Python2.6	Windows Bundle	MSI Application	Yes	0	No
<input type="checkbox"/>		Python2.7	Windows Bundle	MSI Application	Yes	0	No
<input type="checkbox"/>		SVN	Windows Bundle	MSI Application	Yes	0	No

1 - 7 of 7 show 25 ▾ items

This behavior can be overwritten in each bundle object, allowing the administrator to define for each bundle what the Windows Start menu structure should look like. This process can be cumbersome for each bundle; therefore you must consider the balance needs of content replication, ease of administration, and end-user presentation to decide about the folder structure for your bundle objects.

Defining the *How* in Content Management

ZENworks 11 contains power mechanisms for granular control over content that should be hosted at specific locations. When you distribute content to Satellite locations, the concept of creating a *window of opportunity* for synchronization becomes very important. A *window of opportunity* involves defining the amount of time and the amount of bandwidth available to transfer a particular piece of content. In the versions of ZENworks Configuration Management previous to ZENworks Configuration Management 10 SP3, all content was treated the same way; however, in ZENworks 11, several content types are exposed in ZENworks Control Center. The list of content types has been expanded, since version 10 SP3.

The following figure highlights the specific content types that you can configure in ZENworks 11 SP2.

Configure Content Type Replication

Content Type:

Throttle (in KB/sec):

Duration (in mins):

Schedule Type:

Days of the week

*

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

Start Time: :

[More Options](#)

Monthly

Day of the month:

Last day of the month

Start Time: :

[More Options](#)

Fixed Interval

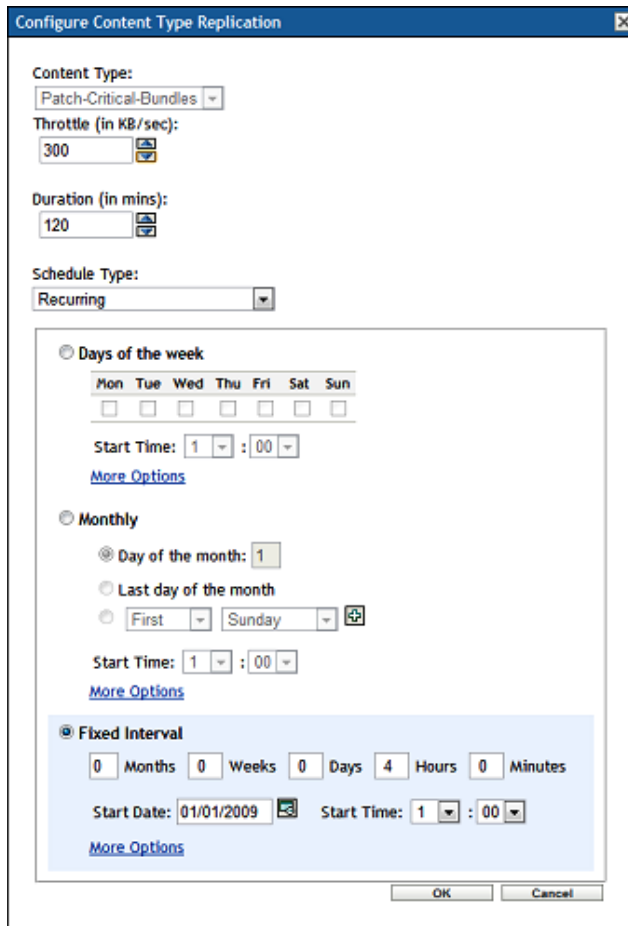
Months Weeks Days Hours Minutes

Start Date: Start Time: :

[More Options](#)

After you have defined *what* content should be available, the next stage is to define *how* and *when* it gets to the defined locations. For each content type, the administrator can specify the *window of opportunity* for synchronization, the recurrence period, and the bandwidth to be consumed during these operations. Administrators can now ensure that other services at remote sites are not affected by content delivery. If the *window of opportunity* and throttled bandwidth rate is not sufficient to completely synchronize all content, the process resumes from where it stopped when the *window of opportunity* opens again.

The following screen shot shows that Critical Security Patches have the opportunity to synchronize every 4 hours for up to 2 hours, consuming only 300 KB/s during the transfer.



In this scenario, the customer wants to ensure that critical security patches are available promptly but still wants to protect bandwidth at the same time. If the content to be synchronized takes only 10 minutes to complete, the *window of opportunity* closes after 10 minutes. If the transfer takes more than 2 hours, the remainder of the content is synchronized 2 hours later when the next *window of opportunity* opens, because of the 4-hour interval.

Critical Information Required To Determine Content Synchronization Settings

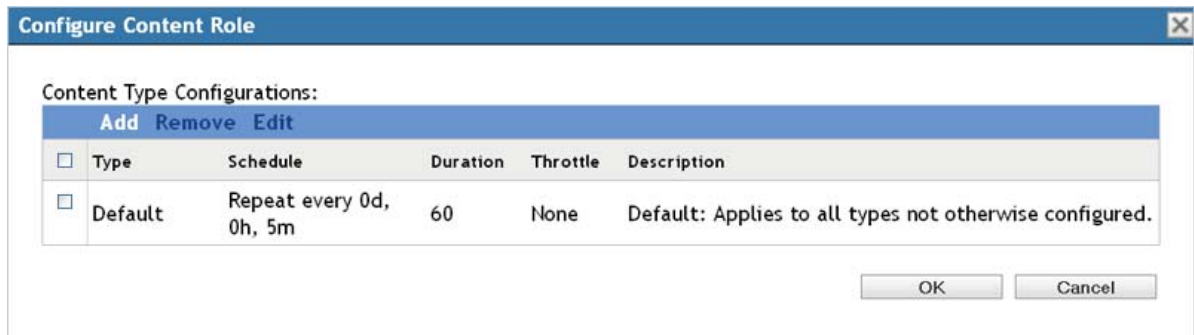
Before defining the content rules for a given location, you must collect the following information:

- ◆ The customer's content priority.

For example, what should be available as soon as possible and what content can wait until after hours or perhaps weekend transfers.

- ◆ The network bandwidth available from the data center to each site and network utilization at each site. In some cases, a site might have a large data pipe but it might be subject to high utilization because of other applications and services that are running.

The following screen shot shows that each content type can be configured with its own *window of opportunity* so that it can accommodate any customer requirement.



ZENworks Configuration Management offers the administrator significant flexibility in managing content synchronization, ensuring that content is always available at only the relevant locations, but more importantly that ZENworks does not consume all the bandwidth during this process.

4.2.21 Offline Content Replication and Management

ZENworks Configuration Management allows you to easily promote any managed device to a Satellite device with the roles of content repository, inventory and status collection point, imaging server, or an authentication point for local Active Directory or eDirectory instances. These roles are defined centrally in ZENworks Control Center and are applied automatically when the device next checks in.

Consider a situation where you need to launch a new site for management that is behind a very slow or saturated link. ZENworks can easily automate the delivery of content and throttle bandwidth to get the data needed to that location without adversely affecting other services hosted at that location. However, if the location needs GBs of application content, this process might take days or even weeks if small windows of opportunity and low-bandwidth throttles have been configured. If network providers charge customers on the basis of network utilization, sending large amount of content across WAN links should be avoided. ZENworks 10 Configuration Management SP3 provides the ability to export the content required by a Satellite device. Subsequently, the content can be transferred to a site through removable media, and imported into the content repository of the local Satellite. The process can save the customer unnecessary bandwidth consumption along with the associated time and financial costs.

The process for offline content synchronization is as follows:

- 1 Promote a managed device to be a Satellite device.
- 2 Assign the content role to the Satellite device.
- 3 Set the content synchronization schedule to *none*.
- 4 Specify the content that is needed at the location.
- 5 Export the content by using the zman command line utility with the Satellite Server Export Content option.

```
C:\>mkdir \content
```

```
C:\>cd content
```

```
C:\content>zman ssec "Devices/Workstations/EMEA/novell-f7d8d036" c:\content
```

The command looks up the content that is marked as *include* for a given Satellite that is currently not available, and exports the content to the defined location. If this is a new site, [Step 3](#) and [Step 4](#) ensure that this is all of the required content to launch the site.

- 6 Copy the content to a removable media and send it to the remote location.
- 7 After the data is available at the remote site, import it by using the zac command line utility with the Content Import option.

```
C:\>zac cic c:\tools\content -l:c:\content.log
```

```
Importing 125 items for content type Default...
```

```
Imported 125 items.
```

```
Successfully imported content (125 items).
```

- 8 After the content has been successfully imported, configure the content schedule and bandwidth throttling as is required for the site.

After this process is complete, setting the content synchronization schedule instructs ZENworks to ensure all subsequent delta changes are automatically synchronized.

4.2.22 Satellite Authentication Role

Each Satellite Server in a ZENworks Management Zone can be configured with one or more roles for managed devices.

Table 4-2 *Satellite Roles*

Role	Description	Available on a Satellite Device
Content	Provides access to the ZENworks content repository.	YES
Collection	Provides an upload point for inventory and endpoint status information.	YES
Imaging	Provides a PXE boot server for imaging jobs.	YES
Authentication	Provides a service where user credentials intercepted on the managed device can be passed to ZENworks. This allows for bundles and policies to be assigned based on the identity and role of the user.	YES
Configuration	Provides a service where configuration information such as bundles and policy assignments can be refreshed.	NO

As shown in [Table 4-2, "Satellite Roles," on page 122](#), a majority of roles can be hosted by a Satellite device. The ZENworks Authentication role was previously restricted to ZENworks Primary Servers. However, the role has been available on Satellite devices from ZENworks 10 SP3 Configuration Management or later. Configuring the Authentication role on a Satellite device allows for additional connections to be made to an eDirectory or Active Directory user source through a device that is local to the devices at a given location. For example, a customer using eDirectory will most likely create partitions dedicated to the resources for a given site and store a replica of the partition on a local server.

If a remote site has a local Directory server with LDAP enabled, a Satellite device can be configured with the Authentication role so that the authentication process can occur locally on the LAN. The authentication process is as follows:

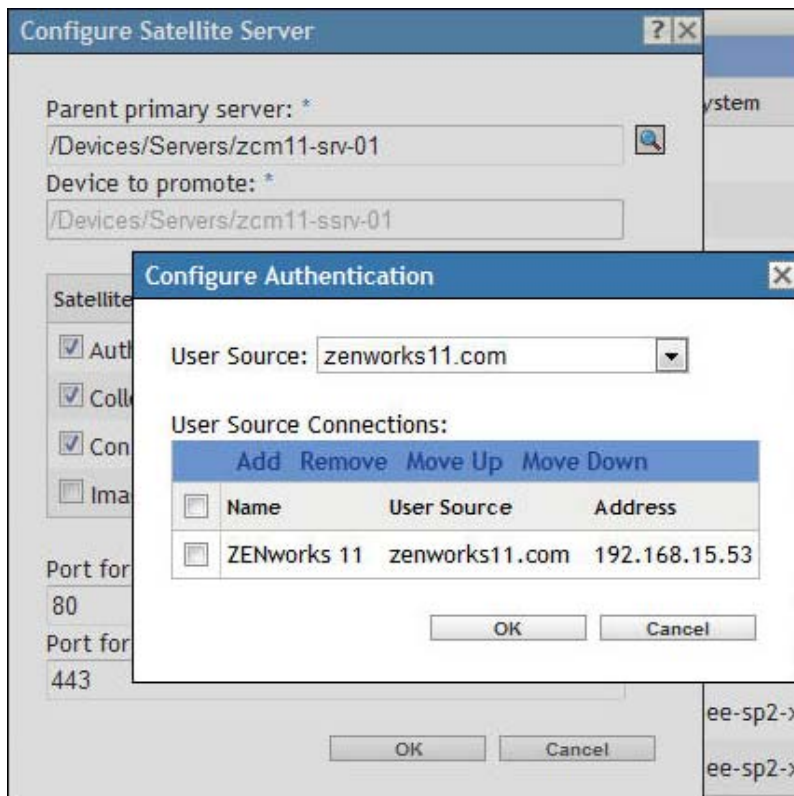
1. The user authenticates to eDirectory or Active Directory as part of the Windows logon process.

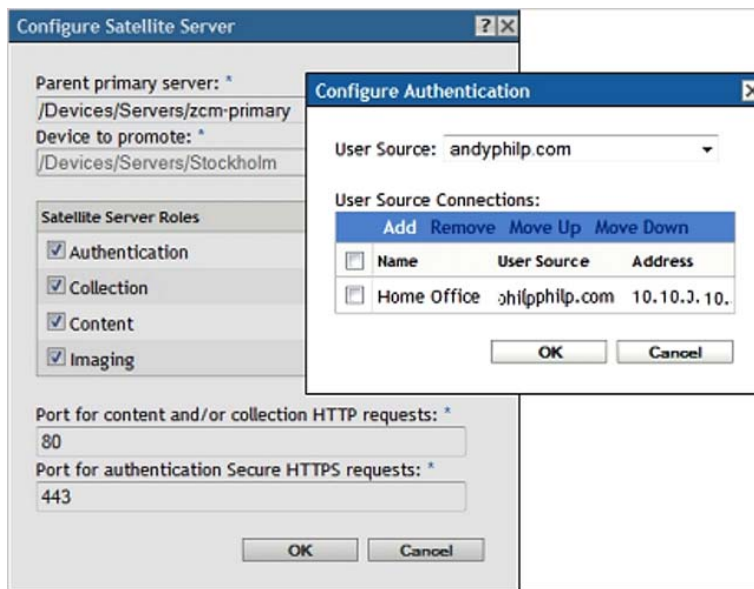
2. The credentials are intercepted and passed on to a ZENworks server hosting the Authentication role.
3. The Authentication Server searches for the user in the user source via LDAP(S). This information is used to determine what policy and bundles should be applied for users, based on their location in the directory and their group memberships.

The process of configuring local Satellite authentication is as follows:

1. Define an additional connection to the User Source.
2. Assign the User Source Connection to the Satellite device.

The following screen shot shows an example of a Satellite Authentication role, configured to connect to a local user source.





User Authentication Load-Balancing

The creation of additional user source connections that can be applied to Primary Servers or Satellite devices offers additional load-balancing capabilities for the authentication process. ZENworks provides authentication load balancing at two levels:

1. Closest Server rules define the Authentication Server to which a managed device sends its credentials. Typically, there are multiple Authentication servers in a zone; therefore, the authentication process can spread across those servers through Closest Server rules.
2. User Source Connections instruct Primary Servers and Satellites of additional servers that can be used to perform the LDAP(S) user lookups. If there are multiple eDirectory or Active Directory servers in a given location, the authentication load can also be balanced across multiple LDAP servers.

When you make decisions on infrastructure placement to support ZENworks services, ensure that the load is spread across the ZENworks servers first and the customer's Directory servers second.

4.3 Lab Testing and Validation

One of the key parts of the design phase is the testing and validation that is done in the organization's lab environment prior to any deployment being completed. This is your opportunity to do the following:

- ◆ Prove that the design and design decisions you made are accurate and correct, and meet the very specific requirements of the organization.
- ◆ Verify that software components are functioning properly, and that users are receiving the results that they should expect.
- ◆ Prove that the deployment will be successful.

The organization should use the lab to develop acceptance tests that are run by the project team and tracked for completion and success. The best way to do this is to document individual acceptance tests (a simple spreadsheet can be used if you want), and complete the tests according to the steps you need to take. After the individual tests have been run successfully and validated (proven successful), you can document this and move on until all tests have been completed.

If individual tests are unsuccessful, you need to make changes (this could also include your design), and run the test until it is successfully completed.

The idea is not to create more work for you, but to prove the overall design quality and increase the probability of a successful ZENworks Configuration Management deployment.

Your lab environment must reflect your existing infrastructure as closely as possible, and the ZENworks Configuration Management infrastructure in the lab must accurately reflect the design you are creating.

The lab should contain real-world layout (design) to ensure that the ZENworks Configuration Management design fits well within the existing environment. Things to include are:

- ◆ The design of directory services infrastructures, including Novell eDirectory and Microsoft Active Directory. If you can, replicate the directory services in the lab to ensure that the lab environment is isolated from the actual production systems. You want to avoid causing issues with the endpoints on the production network because of testing in the lab.
- ◆ Major network infrastructure components that need to be tested. This includes a replica of the main data center layouts, and the major classifications of remote sites that need to be tested for Satellite distributions and collections.
- ◆ An exact replica of the ZENworks Configuration Management infrastructure design that you are creating. This needs to be kept up-to-date. If any changes are made to the design, you need to immediately reflect these changes in the lab environment.
- ◆ You should test actual packages, content, collection, and so forth, and this needs to reflect the decisions made in the design phase. For example, you should test inventory collection based on the decisions you have made for inventory collection schedules. This is also true for all major components of ZENworks Configuration Management that are being deployed.
- ◆ You should perform all endpoint testing with actual base images that are being used in production. This includes a sample set of actual line-of-business applications and custom OS configurations.

It is beneficial to have a sample set of departmental devices to use here. For example, use a typical workstation you would find in Accounting, Human Resources, Engineering, IT, and so forth.

When building your lab, you do not need to build the entire lab with physical hardware. You are not testing the breaking point here. You are testing functionality and whether or not there are any major issues found with the overall design. You should use actual production hardware to test functionality at the device level, but the server infrastructure could be virtualized to save hardware costs. The idea is to reflect the design so you can prove that it is solid.

4.4 Documentation

Documentation is the most important aspect of the design phase. It is critical that you document all decisions that are made during the design phase and keep these items up-to-date. After the document has been finalized, it is important to keep it up-to-date to reflect all changes to both the ZENworks Configuration Management infrastructure that is in place, as well as the infrastructure and services that ZENworks Configuration Management relies on.

In addition to reflecting the infrastructure, the design document can prove to be a useful and powerful knowledge transfer document. As individuals within the organization move in and out of the IT Services division, they can use this document to better understand what was put in place, and how the system is connected and interconnected. It is a tool to provide insight into what was decided during the project and beyond.

We recommend that you store the design document in a documentation repository if you have one, and you should provide access to the document as required. However, you should limit who has write access to the document so that it is not updated by unauthorized personnel.

5 Deploying ZENworks Configuration Management

Deployment is the final stage of the implementation of Novell ZENworks Configuration Management across your enterprise. If you have planned and documented everything during the assessment and design phases, this stage of the project should be much easier.

The following sections explain the steps you should take when deploying ZENworks Configuration Management across the entire infrastructure. These steps should be followed closely regardless of the size of the organization.

This section also includes some scenarios to ensure that the basic principles of design are covered.

- ♦ [Section 5.1, “New ZENworks Customer,” on page 127](#)
- ♦ [Section 5.2, “Migrating from a Previous Version of ZENworks,” on page 133](#)
- ♦ [Section 5.3, “Pre-Deployment Planning,” on page 139](#)
- ♦ [Section 5.4, “Pre-Deployment Documentation,” on page 139](#)
- ♦ [Section 5.5, “Deployment Rules of Thumb,” on page 140](#)
- ♦ [Section 5.6, “Pre-Deployment Testing,” on page 144](#)
- ♦ [Section 5.7, “Pilots,” on page 144](#)
- ♦ [Section 5.8, “Migration,” on page 145](#)
- ♦ [Section 5.9, “Wider Deployment,” on page 147](#)
- ♦ [Section 5.10, “Post-Deployment Documentation and Validation,” on page 147](#)

5.1 New ZENworks Customer

This scenario is the simplest deployment to plan. Because an existing ZENworks implementation is not in place, the pace of the deployment can be controlled very carefully without coordinating the decommissioning of previous ZENworks services. Administrative effort is simplified in this scenario because ZENworks Control Center is the only tool you need.

When you deploy ZENworks Configuration Management to a new customer, Novell recommends that you consider the following steps:

- ♦ [Section 5.1.1, “Building a Model Office Environment,” on page 128](#)
- ♦ [Section 5.1.2, “Planning a Deployment,” on page 130](#)
- ♦ [Section 5.1.3, “Deploying the Product,” on page 131](#)

5.1.1 Building a Model Office Environment

It is important to test the desired solution in an environment that accurately represents the customer environment. If a test or model office environment can be built, the ZENworks Adaptive Agent should be deployed to devices that accurately reflect the various configurations that are in the field. Customers often have multiple operating system configurations with different service packs, authentication mechanisms, and standard applications. Ensuring that your solution works in all of these configurations helps ensure a successful deployment in the live environment.

Another benefit of providing a model office environment is that groups of users can be invited to use the systems and provide feedback on how information and data is presented. A good example of this is the various methods for presenting application icons to the users. In some cases, you might prefer to use the Start menu, Quick Launch bar, or the ZENworks Application Window. Gathering feedback on these items early allows careful planning on how to best provide the users with the ZENworks Configuration Management functionality.

- ♦ [“Discovery and Deployment Methods” on page 128](#)
- ♦ [“Deploying and Testing Policies” on page 129](#)
- ♦ [“Deploying and Testing Applications” on page 129](#)
- ♦ [“Line of Business Applications” on page 129](#)
- ♦ [“Specialized Applications” on page 129](#)
- ♦ [“User Acceptance Testing” on page 129](#)

Discovery and Deployment Methods

A new ZENworks customer might not have a desktop management solution in place. In this scenario, the customer needs to try various methods for deploying the ZENworks Adaptive Agent to the new machines. ZENworks Configuration Management provides the ability to discover devices through IP or LDAP discovery routines and then to target remote deployments of the agent to these discovery devices. For remote agent deployment to function, a number of criteria must be in place, such as:

- ♦ Simple File Sharing is disabled.
- ♦ An administrative credential is provided.

If it is not possible to deploy devices through the built-in deployment tool, a number of other methods can be investigated. For each of the following methods, the process should be tested to ensure that it is acceptable to the end user and that the ZENworks Adaptive Agent can be successfully deployed.

- ♦ [“Login Scripts” on page 128](#)
- ♦ [“Manual Agent Download” on page 129](#)

Login Scripts

If the customer utilizes a directory, the Adaptive Agent can be deployed through login scripts.

NOTE: The user must have the necessary privileges to install the Adaptive Agent.

Manual Agent Download

The last resort for agent deployment is to manually download the agent from the ZENworks Control Center. Alternatively, customers can place agent installation on their own intranet pages to allow users to install the product.

Deploying and Testing Policies

After the ZENworks Adaptive Agent is deployed in the model office environment, the ZENworks policies can be tested to ensure that the desired result is achieved. Particular attention should be directed to the deployment of Group policies. Group policies in ZENworks Configuration Management are plural, allowing multiple policies to be stacked. It is important to test the different policy stacks.

Deploying and Testing Applications

Test all the applications that are to be made available on the first day of the production rollout. This testing should include standard applications that are made available to all the managed devices.

Typical examples of these are the following:

- ◆ Adobe Reader
- ◆ OpenOffice
- ◆ GroupWise e-mail client
- ◆ GroupWise Instant Messenger

Line of Business Applications

Different departments within the organization, such as Finance and Human Resources, might require different application sets. Ensure that these applications deploy successfully on each build type and that they interact with other applications.

Specialized Applications

Applications that are used by a small numbers of users should also be tested, such as applications designed for people with disabilities.

User Acceptance Testing

After the ZENworks Adaptive Agent has been deployed and all policies and applications have been tested for functionality, the next phase involves inviting representatives of the user base to test the end user experience. At this stage, it is valuable to receive feedback on a number of items, such as:

- ◆ The look and feel of the desktop.
- ◆ The method by which users can launch ZENworks Configuration Management delivered applications (Start menu, Quick Launch bar, notification area, and so forth).

Feedback received from users helps to ensure that the ZENworks desktop experience is acceptable. Another useful result of this activity is that requirements for additional training or marketing collateral are identified.

5.1.2 Planning a Deployment

Planning deployments is an important part of a successful project. After a robust design has been tested and evaluated in a model office environment, a number of steps should be followed before implementing ZENworks Configuration Management in a production environment.

- ♦ [“Identifying Groups of Users and Devices” on page 130](#)
- ♦ [“Creating Internal Documentation” on page 130](#)
- ♦ [“Scheduling Deployments” on page 131](#)

Identifying Groups of Users and Devices

An important part of any deployment is to identify which devices must be targeted and in which order. Novell recommends that logical groupings be made in the target environment before deploying the product. After ZENworks Adaptive Agents are deployed and represented in the ZENworks Control Center as managed objects, ZENworks groups can be created to reflect these groups. Groups can become important in the future when staging the rollout of system updates, applications, and patches.

The following list provides examples of how environments can be grouped:

- ♦ **Departments:** The IT organization is a good group of people to start with because the members tend to be technology-savvy and understand the need for reboots and testing.
- ♦ **Laptop Users:** Laptop users can help to identify and test the roaming capabilities of ZENworks Configuration Management. As devices roam inside the firewall, it is important that Closest Server Rules are configured in the Management Zone to ensure that devices connect to the most appropriate servers according to their physical locations.
- ♦ **Home workers and VPN users:** These users have devices that connect to the corporate firewall in a non-standard way. Testing these devices early ensures that the logon and connection process works to connect to the ZENworks Management Zone and refresh content.
- ♦ **Geographical locations:** You should establish a footprint at each major location in the testing process. This is to ensure that the Management Zone is configured correctly to spread the load of devices through Closest Server Rules.
- ♦ **VIP users:** You might want to manage the devices of CxOs and IT directors early, to ensure that these devices are working well. Grouping important devices together allows for quick remedial actions.

Creating Internal Documentation

Internal documents that can be shared with the user are an important part of any project that introduces technology that affects the desktop experience.

The following sections describe internal documentation that you could use:

- ♦ [“Internal Marketing Collateral” on page 130](#)
- ♦ [“Support and Issue Escalation Process Documents” on page 131](#)

Internal Marketing Collateral

Internal marketing is an important tool to inform the users of IT projects that affect them. This marketing is usually done in the form of intranet postings, internal promotions, and posters and so forth. You should use these actions to ensure effective management of the deployment are encouraged to use these actions to ensure effective management of the deployment process.

Support and Issue Escalation Process Documents

When you introduce a new product into a customer environment, it is important that the customer's support escalation process is well defined. In addition to this, it is vital that the support organization is well trained on ZENworks Configuration Management. The key members of the support team should attend workshops and training early in the project to ensure that they are familiar with the product, configuration, and troubleshooting methods. After the key members are trained, this knowledge can be cascaded to the other members of the team, as needed.

Scheduling Deployments

After the deployment groups have been defined, the next stage is to schedule when the deployments occur for each group within the organization. This process is typically associated with the process of starting change control requests. You should schedule deployments in small groups to begin with and then ramp up over time to ensure that the ZENworks Configuration Management architecture can be monitored effectively during peak periods of change.

5.1.3 Deploying the Product

Deploying ZENworks Configuration Management to managed devices is the most important part of any ZENworks project. At this stage, user productivity can become affected. You should use the following basic steps when deploying the product to a new environment:

- ♦ [“Deploying the First ZENworks Primary Server and Database” on page 131](#)
- ♦ [“Deploying the Initial Managed Devices” on page 132](#)
- ♦ [“Extending the Architecture” on page 132](#)
- ♦ [“Extending the Managed Device Footprint” on page 132](#)
- ♦ [“Analyzing, Reviewing, and Planning” on page 132](#)

Deploying the First ZENworks Primary Server and Database

Deploy the first ZENworks Primary Server and database, then ensure that the Management Zone is stable.

The first server in the Management Zone is often the certificate authority for the rest of the Zone. This server should be carefully managed and backed up regularly.

After the Management Zone is functional, the initial configuration should be defined as follows:

1. Create workstation folders, depending on how the customer wants to organize devices, such as departments, geographical locations, and project teams.
2. Create registration rules and keys to control the placement of devices in the Management Zone.
3. Create roles, then assign administration rights. If a user source is being used, configure existing users with the management rights necessary for their role. For more information, see the [ZENworks 11 SP2 System Administration Reference](#).
4. Configure Closest Server Rules. Ensure that the various network locations are reflected. For more information, see the [ZENworks 11 SP2 System Administration Reference](#).
5. Configure System Update. Ensure that the server can access the various Internet resources required to download system updates and product recognition updates. For more information, see the [ZENworks 11 SP2 System Administration Reference](#).

6. Configure user sources. Configure the link to the chosen user source and ensure that the user objects can be found by browsing the source. For more information, see the [ZENworks 11 SP2 System Administration Reference](#).
7. Configure Inventory scheduling. The default setting for all devices is to inventory monthly on the first day of each month. Create different schedules for each of the workstation folders that exist within the Management Zone.
8. Configure Remote Management to remotely control managed devices.
9. Create a policy to configure the system or application settings for Windows or Linux managed devices.
10. Create the required application bundles. When you use a staged approach, it is necessary to create only the standard bundles and the applications that are required by the first device stages.

Deploying the Initial Managed Devices

Use the chosen deployment methods to deploy the first devices to the Management Zone. After the devices have been deployed, ensure the following:

- ◆ Devices are in the correct location (Workstation folder).
- ◆ Devices have successfully created and uploaded the inventory.
- ◆ Devices can be remotely controlled.
- ◆ ZENworks Primary Servers and the ZENworks database are stable.
- ◆ Devices can be refreshed successfully and do not report errors.

After the customer is satisfied that the initial Management Zone configuration is stable with the first devices, the project can continue.

Extending the Architecture

According to the recommendations in this document, add more Primary Servers and Satellite devices. If possible, make sure all the servers are in place before introducing additional devices. This provides the opportunity for the servers to be patched appropriately and for the Content Repository to synchronize completely. If all of the servers cannot be deployed before the live devices are added, ensure that the deployment is staged in such a way that the servers are added before the relevant groups of devices are added.

Extending the Managed Device Footprint

Using the stages identified earlier, continue the managed device rollout to the rest of the organization.

Analyzing, Reviewing, and Planning

During the device rollout, it is vital that you closely monitor the performance of the back-end servers, databases, and managed devices by using tools such as Perfmon. The following items should be closely monitored:

- ◆ Disk utilization
- ◆ Memory
- ◆ Peak processor utilization

If the servers are highly utilized and struggling to cope with the load placed on them by the managed devices, you should review the Management Zone configuration and the number of Primary Servers and Satellite devices.

5.2 Migrating from a Previous Version of ZENworks

In addition to the topics described in the previous section, a number of key factors should be taken into consideration when migrating from a previous version of ZENworks to ZENworks Configuration Management:

- ♦ [Section 5.2.1, “Application Deployment Strategy,” on page 133](#)
- ♦ [Section 5.2.2, “Application and Policy Migration,” on page 134](#)
- ♦ [Section 5.2.3, “Active Directory,” on page 134](#)
- ♦ [Section 5.2.4, “Repurposing Hardware Used by Previous ZENworks Products,” on page 134](#)
- ♦ [Section 5.2.5, “Introducing ZENworks Patch Management to an Existing ZENworks Zone,” on page 134](#)

5.2.1 Application Deployment Strategy

If a customer already has a mature deployment of ZENworks Desktop Management in place, it is likely that there is an extensive application repository. In many cases, the customer is using the Tiered Electronic Distribution component of ZENworks Server Management to tightly manage the distribution of application software code to the file servers needed to support deployment to users. In addition to these components, the customer might have already invested in the processes and workflows to facilitate application delivery and might be reluctant to start again with a new system.

ZENworks Configuration Management provides an encrypted data store known as the Content Repository, which stores delivery content for applications, patch remediations, and ZENworks system updates. When an application bundle is created, the delivery content is uploaded to the Management Zone, encrypted, and subsequently synchronized to all ZENworks Primary Servers. This process allows for applications to be delivered securely to devices by using HTTP, regardless of the physical location of the device.

However, it is possible to create application bundles that refer to application repositories that are external to ZENworks. For example, a customer might want to deliver applications with ZENworks Configuration Management but refer to the same application content (MSIs) that ZENworks Desktop Management is pointing to. This approach has several advantages:

- ♦ The existing repositories can be used.
- ♦ The existing processes for application management can be used. If a customer has heavily invested in these processes, this is a compelling case to use the existing methods.

This approach also has some disadvantages:

- ♦ The management of content is controlled outside of ZENworks Configuration Management, where the files reside. Therefore, the user rights to these locations must be managed outside of the ZENworks Configuration Management management tools.
- ♦ Using the standard file and print delivery mechanisms restricts content delivered to devices inside the firewall.

With the ZENworks Content Repository, the devices download content though HTTP, which allows the content to be made available to external users through a Primary Server location in the DMZ.

5.2.2 Application and Policy Migration

ZENworks Configuration Management ships with a migration utility designed to migrate applications, policies, and associations from a ZENworks Desktop Management system to ZENworks Configuration Management. When applications are migrated to ZENworks Configuration Management by using this tool, the data for the applications is automatically placed in the Content Repository. If a customer wants to use the existing application repositories, the migration tool should not be used for these applications.

For more information on the migration tool, see the [ZENworks 11 SP2 Configuration Management Migration Guide](#).

5.2.3 Active Directory

If the preferred server and directory platforms of your organization are Windows Server and Active Directory, and you are currently using ZENworks middle tier architecture and Identity Manager directory synchronization, ZENworks Configuration Management makes it possible to eliminate both of these stepping-stone technologies and interact directly with Active Directory for user authentication and content association. This can be done by simply configuring the ZENworks Configuration Management Zone to point directly at Active Directory as a user source.

5.2.4 Repurposing Hardware Used by Previous ZENworks Products

Customers commonly want to reuse hardware when possible. If a customer is migrating from the previous ZENworks technologies such as ZENworks Patch Management, ZENworks Asset Management, eDirectory, and ZENworks Desktop Management, the hardware utilized for this functionality can be repurposed.

In some instances, it might be beneficial to reuse the hardware to provide the additional ZENworks Primary Servers and ZENworks Satellite devices required by the migration project. Planning reprovisioning of hardware is an important step in a migration project and can help reduce the architecture costs for ZENworks Configuration Management deployment.

5.2.5 Introducing ZENworks Patch Management to an Existing ZENworks Zone

- ♦ [“Patch Management” on page 134](#)
- ♦ [“Discover Applicable Update Bundles” on page 135](#)
- ♦ [“Enabling ZENworks Patch Management in an Existing ZENworks Zone” on page 136](#)
- ♦ [“Deploying Patches to Remote Sites with ZENworks Patch Management” on page 137](#)

Patch Management

ZENworks 11 provides an integrated and common architecture for ZENworks Configuration Management, ZENworks Patch Management, ZENworks Asset Management, and ZENworks Endpoint Security Management. Conceptually, introducing one of these products into an existing ZENworks Zone is as simple as entering a license key. However, for ZENworks Patch Management, it is important to understand the implications of enabling the product so that the introduction of the product can be tightly controlled.

Discover Applicable Update Bundles

Discover Applicable Updates (DAU) bundles are created for each instantiation of the operating system, service pack, and CPU architecture that is currently under management in the ZENworks Zone. Each DAU bundle contains all of the patch signature files (.pls) in a ZIP file. When the signature collection for a given OS, SP, and CPU changes, such as when a new patch is released, the entire ZIP file is rebuilt, the bundle version is updated, and the entire payload is distributed to each managed device that needs it.



The screenshot shows a web-based interface for managing update bundles. At the top, there is a menu bar with options: New, Edit, Delete, Action, and Quick Tasks. Below the menu is a table with the following columns: Status, Name, Type, Category, Enabled, Version, and Has Sandbox. The table lists 12 bundles, including Linux Patch Bundles for Red Hat and SUSE, and Patch Bundles for Windows. Each bundle has a checkbox for selection, a status icon, and a name with a version number. The 'Enabled' column shows 'Yes' for all bundles, and the 'Has Sandbox' column shows 'No' for all bundles. The bottom of the interface shows a pagination control: '1 - 12 of 12 show 25 items'.

Status	Name	Type	Category	Enabled	Version	Has Sandbox
<input type="checkbox"/>	Discover Applicable Updates Linux-REDHAT-x86-en-ES-4.0	Linux Patch Bundle		Yes	43	No
<input type="checkbox"/>	Discover Applicable Updates Linux-REDHAT-x86-en-Server-5.0	Linux Patch Bundle		Yes	43	No
<input type="checkbox"/>	Discover Applicable Updates Linux-SUSE-x86_64-en-SLES-11.0	Linux Patch Bundle		Yes	42	No
<input type="checkbox"/>	Discover Applicable Updates Linux-SUSE-x86-en-SLED-10.0	Linux Patch Bundle		Yes	42	No
<input type="checkbox"/>	Discover Applicable Updates Linux-SUSE-x86-en-SLED-11.0	Linux Patch Bundle		Yes	42	No
<input type="checkbox"/>	Discover Applicable Updates Windows-x86_64-en-2003sp2	Patch Bundle		Yes	43	No
<input type="checkbox"/>	Discover Applicable Updates Windows-x86_64-en-2008R2sp0	Patch Bundle		Yes	43	No
<input type="checkbox"/>	Discover Applicable Updates Windows-x86_64-en-WIN7sp0	Patch Bundle		Yes	43	No
<input type="checkbox"/>	Discover Applicable Updates Windows-x86-en-2003sp2	Patch Bundle		Yes	43	No
<input type="checkbox"/>	Discover Applicable Updates Windows-x86-en-VISTAsp1	Patch Bundle		Yes	43	No
<input type="checkbox"/>	Discover Applicable Updates Windows-x86-en-WIN7sp0	Patch Bundle		Yes	43	No
<input type="checkbox"/>	Discover Applicable Updates Windows-x86-en-XPsp3	Patch Bundle		Yes	43	No

It is important to understand the implications of enabling ZENworks Patch Management for all devices at the same time, because each DAU bundle contains approximately 20 MB of data and each device requests its DAU bundle content on a set schedule. In addition to the requirement for delivering the DAU bundle to all devices that are to be patched, the DAU bundle is updated on a daily basis. Another point to bear in mind is that remote sites with satellites in place should have the latest DAU bundle in order for local devices to perform vulnerability scans.

If no additional signature files are present, the DAU ZIP file is rebuilt at the back end, but the checksum of the ZIP file should be the same. This means that the ZIP file should not be distributed to devices unless a new patch has been released.

When you configure Patch Management, the Subscription Download page has a number of important options. First, select only the languages of interest are selected to ensure that the patch repository is kept to the minimum size necessary. Next, make sure you understand the *Cache patch bundles to satellite servers* option. If this option is enabled, all bundles related to the patch are synchronized to all satellite servers. This option has the potential to drastically increase the network and storage requirements of ZENworks and should only be selected after careful consideration.

[Configuration](#) > Subscription Download ☰

Subscription Download ✕

Configure subscription download options

Subscription Download ⤴

Select the platforms to download

Windows Linux

Choose Windows your language options

These languages are for Operating Systems prior to Vista and other third party patches. For the best performance results select only the languages used by your organization.

<input checked="" type="checkbox"/> English	<input type="checkbox"/> Portuguese (Brazil)	<input type="checkbox"/> French	<input type="checkbox"/> Italian	<input type="checkbox"/> German
<input type="checkbox"/> Japanese	<input type="checkbox"/> Korean	<input type="checkbox"/> Traditional Chinese	<input type="checkbox"/> Simplified Chinese	<input type="checkbox"/> Hong Kong Chinese
<input type="checkbox"/> Spanish	<input type="checkbox"/> Dutch	<input type="checkbox"/> Swedish	<input type="checkbox"/> Finnish	<input type="checkbox"/> Czech
<input type="checkbox"/> Danish	<input type="checkbox"/> Hungarian	<input type="checkbox"/> Norwegian	<input type="checkbox"/> Russian	

Select the option below to combine all languages into each Discover Applicable Updates Assignment. (Not Recommended)

Mix Multiple Languages

Specify whether to use a secure channel when communicating with the Patch Subscription

SSL

Specify whether patch bundle content will automatically replicate to other servers

Cache patch bundles to satellite servers

Cache patch bundles to primary servers

Enabling ZENworks Patch Management in an Existing ZENworks Zone

Because of the DAU bundles and the potential for causing network disruption, you should follow these steps when enabling ZENworks Patch Management in an existing ZENworks Zone:

- 1 In ZENworks Control Center, enter the license key to enable the Patch Management features. ZENworks Control Center should show Patch Management in the left pane and in the Configuration page.
- 2 At the Zone level, in *Configuration > Device Management > ZENworks Agent*, disable the Patch Management agent module.

Agent Features		
Policy Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Remote Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Asset Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Image Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
User Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Bundle Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Patch Management	<input checked="" type="checkbox"/> Installed	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Endpoint Security Management	<input checked="" type="checkbox"/> Installed	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

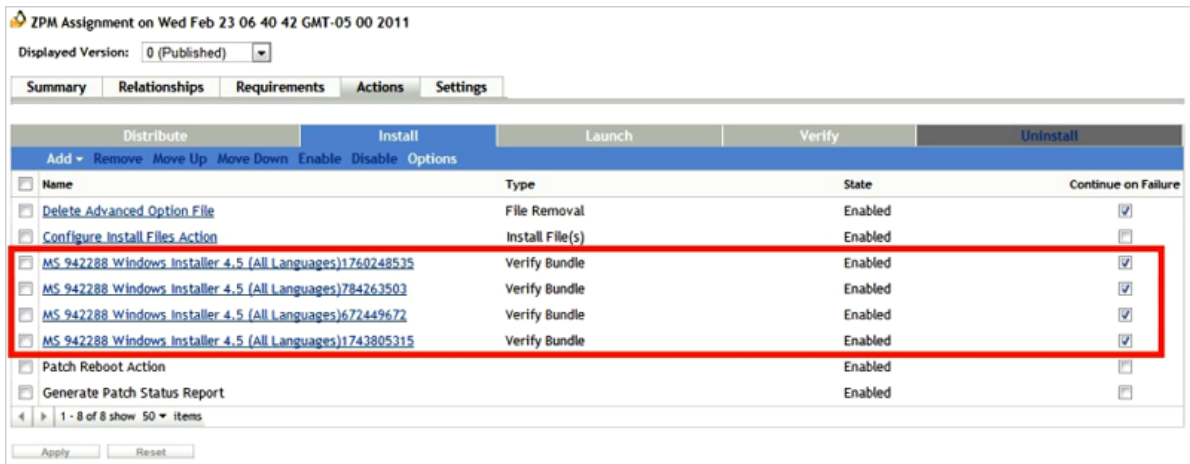
- 3 Connect the devices to the Zone and receive this configuration before proceeding.
- 4 When you are ready to start, choose the Primary Server that is responsible for downloading patches and assign it to the Patch Management role. This server needs Internet access.
- 5 In *Configuration Management > Patch Management > Subscription Download*, choose the subscription settings for language and platforms.

IMPORTANT: Select *Cache patch bundles to satellite servers* only if you are sure that you want to do this.

- 6 If you are patching LINUX go to *Configuration Management > Patch Management > Patch Subscription Credentials*, and configure the credentials to be used for Novell Customer Center and Red Hat Network access.
- 7 After the Patch Subscription process runs, the Zone is populated with vulnerabilities and patch management bundles.
- 8 Enable the Patch Management agent module on test devices either through folder or device settings.
This step overwrites the Zone level settings to disable Patch Management.
- 9 Use folders to control the introduction of Patch Management by enabling the agent module in a controlled manner.

Deploying Patches to Remote Sites with ZENworks Patch Management

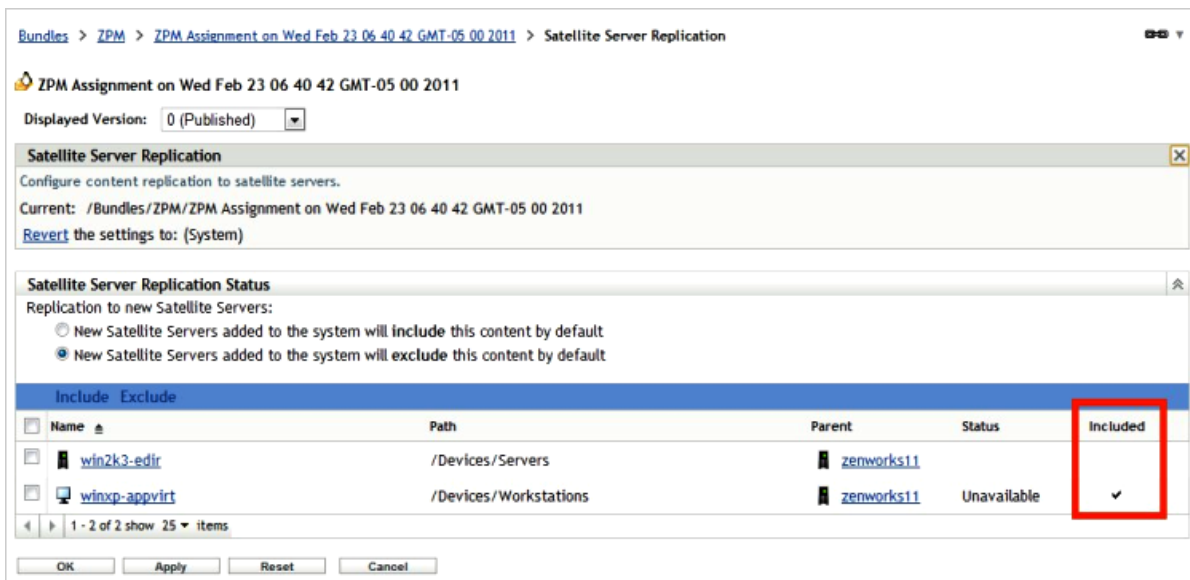
When you deploy a patch remediation, ZENworks creates a deployment bundle that delivers each of the patch bundles for that deployment bundle. As shown below, each patch bundle to be distributed is automatically configured as an Install action of the patch deployment bundle.



If several patches need to be deployed to a remote location with Content Satellite devices, each of these patch bundles needs to be configured so that they are available on the remote Satellite device. To address this, you have three options:

- ♦ Automatically synchronize all patch content to all satellites.
- ♦ Identify each patch bundle individually, then set the content synchronization behavior.
- ♦ Define the content synchronization behavior on the deployment bundle.

The third option is preferred because it requires the least amount of administration and also ensures that only the required patch data is synchronized to remote locations. If the content synchronization behavior is configured on a patch deployment bundle, ZENworks automatically applies this to the child bundles, or to the bundles that are configured as Install actions. The following example shows how the content synchronization behavior can be set on a Patch Management deployment bundle.



When you manage patch remediation content this way, it is important to ensure that the remediation schedule is set well in advance such that the content can be synchronized to the relevant remote locations. The patch remediation schedule should be based on a number of factors:

- ♦ Whether the patch content synchronization is daily, weekly, or hourly.
- ♦ For how long the schedule is open and how often it is repeated.

- ♦ The available bandwidth.
- ♦ Whether bandwidth throttling is enabled.

Finally, remember that patches of different severities can have different settings.

5.3 Pre-Deployment Planning

The first step in the process of deployment is planning the actual deployment. The following are recommendations on how to plan this process:

- ♦ Contact departmental leaders and inform them about the deployment.
- ♦ Make suggestions on how you want to roll out the ZENworks Adaptive Agent to the endpoints, including which departments are going to be targeted by date and time. Make sure you line this up with your planned deployment schedule in your project plan. Ensuring that everyone knows that this is a deliverable of the organization makes it much easier to line up the departments, sites, or groups for deployment.
 - ♦ Identify and notify individuals that are part of the pilot phase of the deployment.
 - ♦ Emphasize that feedback is key to the success of this project. Individuals who are part of the pilot and more wider-scale deployment should provide feedback directly to the IT organization or to the Service Desk.
- ♦ Make sure your teams are well informed of the deployment. This includes:
 - ♦ Departmental leaders.
 - ♦ Employees of the organization.
 - ♦ The organization's Service Desk (staff members should have the full documented schedule posted everywhere so everyone onsite knows what is going on, and when). This also includes everyone involved in Incident and Problem Management processes.
 - ♦ The entire IT department, including desktop support, network services, and other operational groups.
 - ♦ Change Management.
 - ♦ Security services groups, they need to be well informed that this is a planned organizational initiative.

5.4 Pre-Deployment Documentation

Documentation is key to the success of every aspect of the project, including how you plan to deploy the services and agents. Everyone directly involved in the actual deployment, should have documentation that they can reference at all times, eliminating the chance of error.

Documentation regarding the deployment processes needs to be completed during the design phase, and while you are testing the deployment in your test lab facilities. After you have proven the concept and included deployment activities in the design document, you should create a Deployment Assistance Guide that can be used by the individuals who are involved. You might not need to share the entire design document with everyone involved in the deployment of the product. Use your best judgment here.

5.5 Deployment Rules of Thumb

The following scenarios depict the rules of thumb to be followed for deploying ZENworks 11:

- ♦ [Section 5.5.1, “Scenario 1: One Major Location with 1, 500 Devices,” on page 140](#)
- ♦ [Section 5.5.2, “Scenario 2: One Major Location with Several Remote Locations and More Than 1,500 Devices,” on page 140](#)
- ♦ [Section 5.5.3, “Scenario 3: ZENworks 7 Migration to ZENworks 11,” on page 142](#)

5.5.1 Scenario 1: One Major Location with 1, 500 Devices

Consider a scenario consisting of only one major location with 1,500 devices. To deploy ZENworks Configuration Management in this scenario, you should consider two Primary Servers to provide fault tolerance and load balancing, and any of the supported databases. Even though the External Sybase database is sufficient for your requirements, you can choose Microsoft SQL Server or Oracle, especially if growth is a future consideration.

In this scenario, there is no need for Satellite servers or configured locations (unless you want to create locations based on departments, or floors, etc.) but you must carefully monitor the overall system performance and add Primary Servers, if necessary.

5.5.2 Scenario 2: One Major Location with Several Remote Locations and More Than 1,500 Devices

Consider a scenario consisting of one major location, several remote locations, and more than 1,500 devices. To deploy ZENworks Configuration Management in this scenario, you must consider the following:

- ♦ A minimum of three Primary Servers. You must plan to initially deploy three Primary Servers to provide a robust core infrastructure. If necessary, you can scale it back at a later time.
- ♦ Enterprise-ready database infrastructure, based on either Microsoft SQL Server or Oracle.
- ♦ Satellite Servers deployed to remote sites. Based on the size of the sites and Satellite roles, you can host the Satellite services on server class or workstation class devices. If User Sources are used, it is recommended to enable and configure the Authentication Role at the Satellite Server and have the server point to a local replica or domain for user and group object information.
- ♦ Configure and use Locations, then configure Closest Server Rules at the Locations level. This will allow you to be in full control of where devices will go to perform functions as they travel around your network (ie Roaming Users). Otherwise the only option you have is the Default Closest Server Rule, and that is simply not flexible enough for this scenario.

Now let's take it a step further and provide some additional details so we can formulate a design.

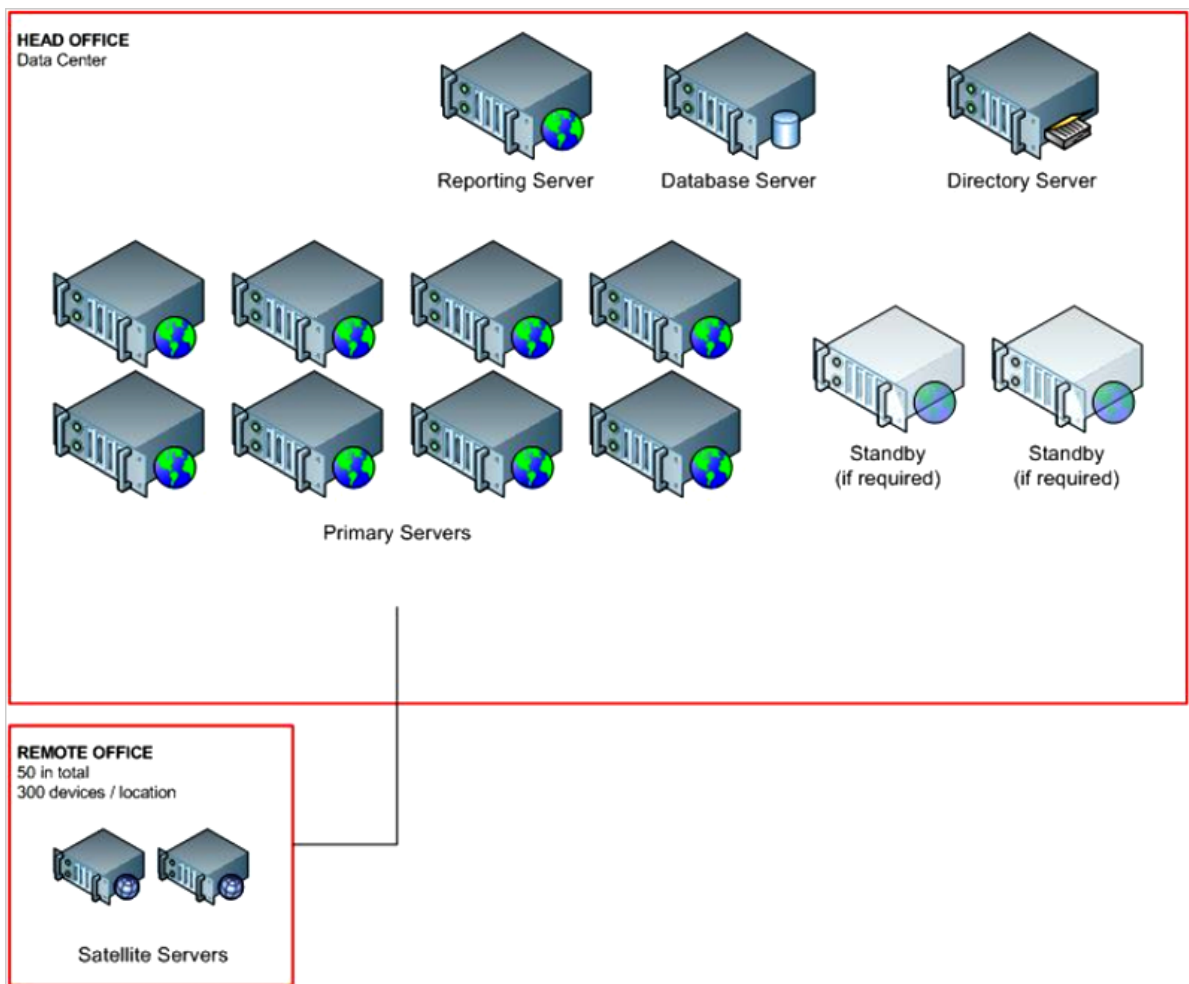
- ♦ One (1) major datacenter location
- ♦ Fifty (50) remote locations
- ♦ 25,000 devices require management - 10,000 at main office, and 300 at each remote location (on average)
- ♦ Will use all functions of ZENworks including ZENworks Reporting Server
- ♦ Everything will be virtualized including the Database Server

Based on what we've outlined as best practices, this means that the first of design elements would be:

- ◆ The Database Server and all Primary Servers would be located in the major datacenter location.
- ◆ The database would be either Microsoft SQL Server or Oracle. In this case we will choose Microsoft SQL Server 2008, and run the database in Microsoft SQL Server 2005 compatibility mode.
- ◆ Based on the number of devices that require management, we would initially make a recommendation for 8 Primary Servers that will be part of the Closest Server Rules, and paired up with Satellite Servers.
- ◆ A 9th Primary Server dedicated to running the ZENworks Reporting Server, and excluded from the Closest Server Rules.
- ◆ Two (2) Satellite Server at each location is recommended to provide fault tolerance, and balancing of load (mainly imaging).
- ◆ Satellite Servers paired with the 8 Primary Servers evenly (ie. 25 per Primary Server).
- ◆ A Location set up and configured for each of the physical locations (50). Along with this, you need to define each location using Network Environments. When set up, you are ready to configure the Closest Server Rules for each Location.

There is a lot of additional thought that needs to go into building the design, but as you can see it is easy to start envisioning what the overall design will look like from an infrastructure perspective. Scalability and service placement are the most important aspects of the design, everything else is work that you can accomplish in the lab or by discussing the topic with your teams.

Now that we have put together some of the basics, let's see what it looks like in graphical format:



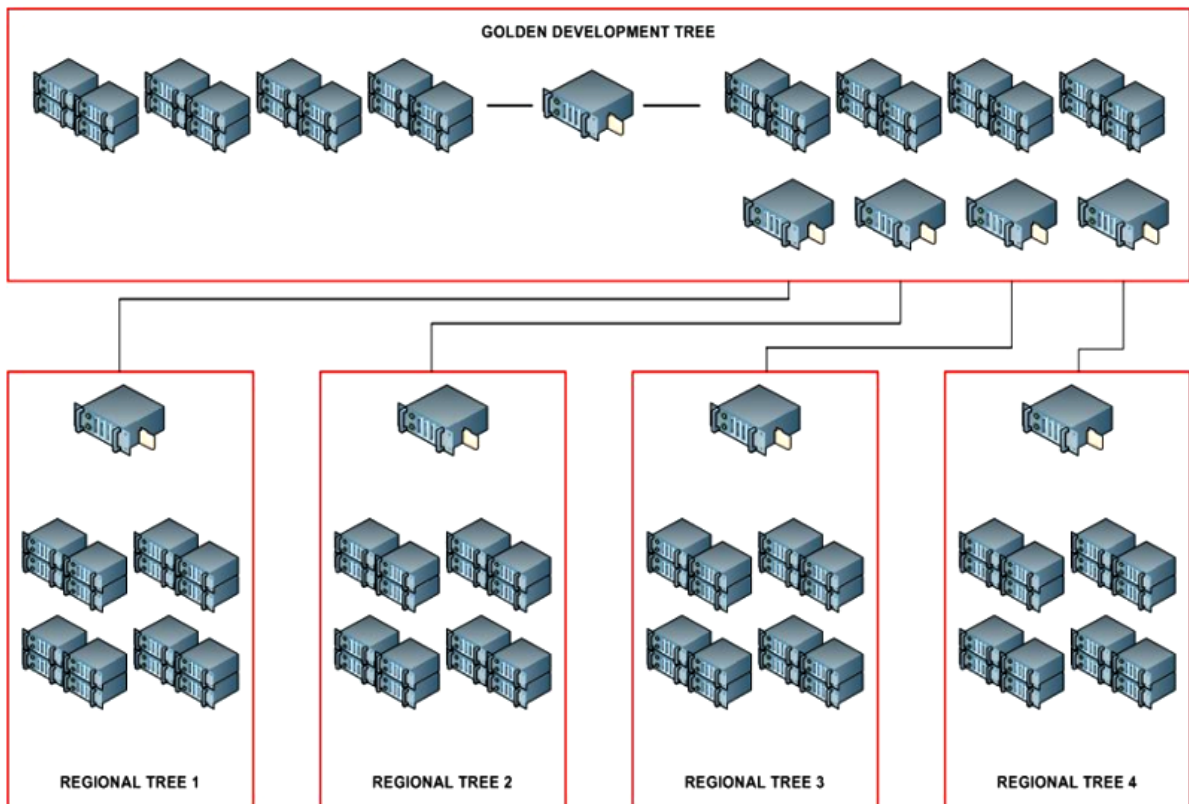
5.5.3 Scenario 3: ZENworks 7 Migration to ZENworks 11

This scenario looks at the process of moving from ZENworks 7 to ZENworks 11 Configuration Management.

Assume the following specifics:

- ◆ One tree for the development of applications, policies, and images.
- ◆ Four regional production trees.
- ◆ ZENworks 7 Desktop Management across the entire organization.
- ◆ ZENworks 7 Server Management (Tiered Electronic Distribution) is used to replicate content between the development tree and regional trees.
- ◆ 20,000 devices are being managed (5,000 devices per regional tree).
- ◆ Each regional tree has a main datacenter and several remote locations. There are no remote locations with more than 200 devices that require management.

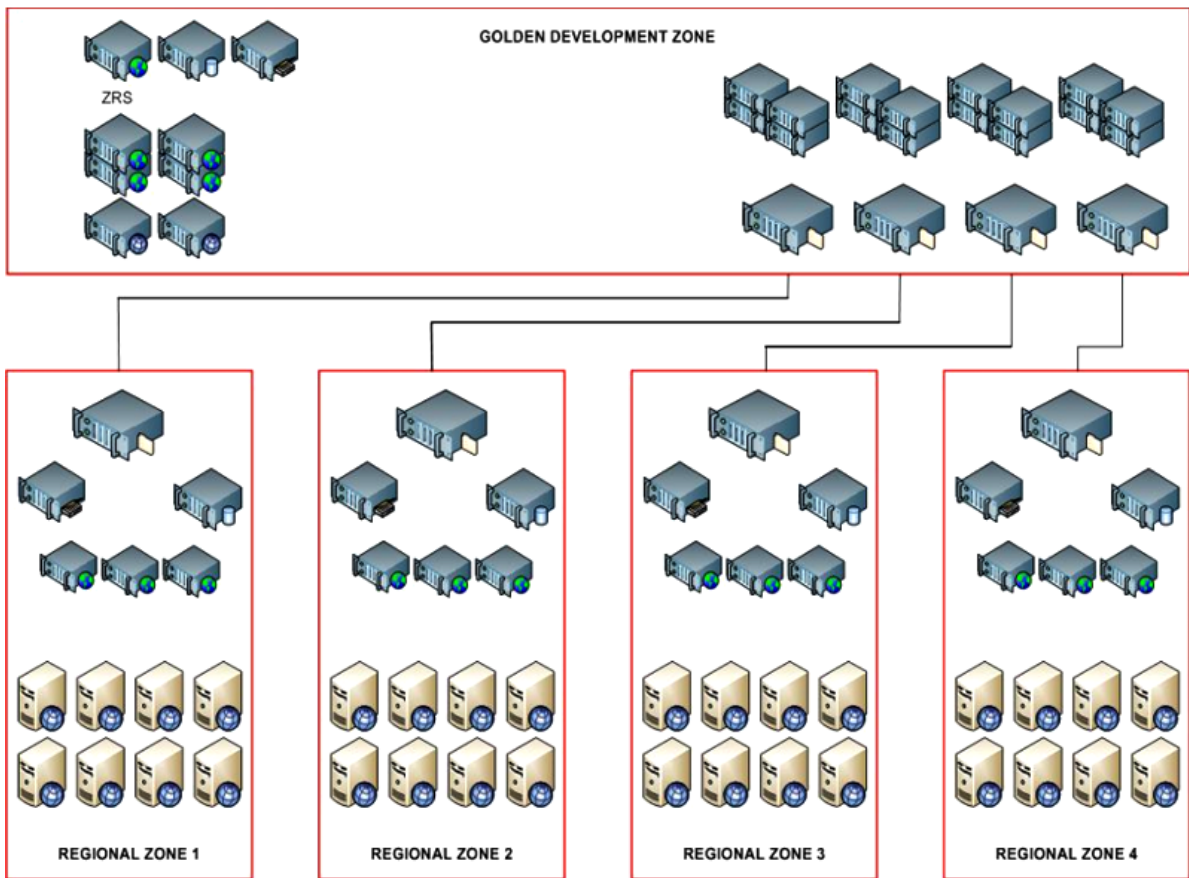
The following diagram shows the customer's existing infrastructure:



Based on what we have outlined as best practices, this means that the first of design elements would be:

- ◆ Five zones in total - One development zone, and four production (regional) zones.
- ◆ The development zone would be configured to two testing facilities, which is accomplished by using folders for content, devices, and roles to restrict where administrators or testers can create or modify content.
- ◆ Each regional tree would include the following:
 - ◆ One database server running Microsoft SQL Server 2008 in the 2005 compatibility mode.
 - ◆ Three Primary Servers at the main regional datacenter.
 - ◆ Two Satellite Servers at each of the remote offices to mainly provide fault tolerance.
- ◆ Content is still synchronized from the datacenter to datacenter by using ZENworks 7 Server Management. When the content is replicated to the regional datacenter, it is imported manually into the zone by the local administration team. In the future, ZENworks 7 Server Management will be replaced by the ZENworks Configuration Management content share/subscribe software.
- ◆ An eDirectory infrastructure will still be a part of this overall design, and the User Sources will be configured to point to the local replica servers, which include both Primary Servers and remote Satellite Servers.

According to these design decisions, the infrastructure for this customer looks similar to the following diagram. With all designs, minor adjustments might need to be done to ensure that the designs meet all of the requirements for all devices and locations. These changes can be worked out in the lab and documented accordingly.



5.6 Pre-Deployment Testing

We recommend that you set aside some time before you perform your pilots to further prove your deployment by running some last-minute tests. Allow enough time so that any adjustments can be made and documented prior to deployment.

Perform the test in your lab facilities, using three or four sample workstations with a sample of line-of-business applications installed. This can be a replica of tests done during your full testing phase.

5.7 Pilots

The first phase of the actual deployment is the pilots. This is where you deploy the ZENworks Adaptive Agent to those members that you identified and notified as part of the pilot phase. You are looking for feedback from these individuals, and this can be done through a feedback form, e-mail, or face-to-face meetings.

Do not perform the pilots all at once. Use a rolling approach to this phase. If something goes wrong with the deployment, you want to limit the number of people that are impacted. After you are confident that the deployment is going as planned, you can increase the number of devices you deploy to.

5.8 Migration

If your deployment involves a migration from an existing ZENworks infrastructure, you should have gone through a pre-staging process, but your actual process for deploying to the end user communities should not be different. You still need to pilot and deploy in the same way as if this is a new deployment of ZENworks Configuration Management.

You should use the ZENworks Migration Wizard to perform the pre-staging activities, which includes migration of the following resources:

- ♦ Application objects and source content. This includes all AOT/AXT-based objects and content, MSI-based objects and content, and Simple objects.
- ♦ Image objects and image files.
- ♦ Policy objects and applicable policy files (for example, Group Policy files).
- ♦ Imported workstation objects.
- ♦ All associations for application objects and policy packages.

The Migration Wizard can be found at the following locations:

```
%zenworks_home%\install\downloads\tools  
https://servername/zenworks-setup/
```

It is important to note that if you are migrating from an eDirectory infrastructure (for user sources) to an Active Directory environment, you should take advantage of the migration capabilities built into the Migration Wizard for migrating associations. This allows you to migrate your existing eDirectory associations to Active Directory users, groups, and folders.

In addition, if you are migrating workstation objects, the wizard allows you to avoid the need for discovery of devices. After you have migrated your workstation objects into the ZENworks Configuration Management Zone, you can target them directly from there. In fact, we recommend that all existing ZENworks customers migrate their workstation objects even if they are associating applications and policies only to users in the user source. If workstations are not migrated, and you deploy the ZENworks Adaptive Agent to the existing ZENworks workstations, all applications and policies within ZENworks Configuration Management redeploy.

Some additional best practice recommendations for using the ZENworks Desktop Management Migration Wizard include:

- ♦ If you migrate traditional ZENworks application objects as MSI files through the Migration Utility running on a Windows Vista device, the performance might degrade. For improved performance, run the Migration Utility on a Windows XP SP2 device.
- ♦ While migrating applications that require the content to be uploaded to the content server, the migration might fail. Ensure that the port specified in the *File Upload Http Port* option while logging in to the migration destination zone matches the port configured during installing the ZENworks Configuration Management Server.
- ♦ While migrating large applications that should be uploaded to the content server, the connection to the server might be lost, resulting in failure of the migration. Ensure that the *Get response timeout* option in the Web Client Configuration is set to *None* in order to establish a persistent connection with the server.
- ♦ While migrating applications, deselect the *Upload to content server* option if you do not want to upload the applications to the content server. Deselecting the option migrates the MSI applications as Install Network MSI, which installs the MSI from a network path. By default, the *Upload to content server* option is enabled.

- ♦ If you use the Snapshot Manager in traditional ZENworks to create complex application objects with multiple changes such as Registry, INI, and File Copy, you should migrate the applications as MSI by disabling the *Migrate distribution options as individual actions* option.
- ♦ If you use the Snapshot Manager in traditional ZENworks to create application objects with single changes such as Registry, INI, or File Copy, or if the application object must be edited later, you should migrate the application as actions by enabling the *Migrate distribution options as individual actions* option.
- ♦ If an application is dependent on other applications, review the applications on which the dependency exists and migrate them as MSI or as actions dependent on the requirements, then migrate the dependent applications.
- ♦ If the traditional ZENworks application objects use files that are hosted on the network share, you should map the network share on the device hosting the migration tool.
- ♦ By default, the applications are uploaded to the content server during the migration. If the application files are located on a shared network and you want to continue using the network files, deselect the *Upload to content server* option.
- ♦ If there are too many associations to be listed in the Migration Utility, select the *Either eligible or ineligible for migration (No warning)* option to reduce the time taken by the utility in listing the associations.
- ♦ Application objects that have the AppFsRights attribute set in eDirectory are not listed in the Migration Utility. To list such applications for the migration, remove the AppFsRights attribute. For more information on removing attributes, search for the LDAP Attribute Remover article at the [ZENworks Cool Solutions Community \(http://www.novell.com/communities/coolsolutions/zenworks\)](http://www.novell.com/communities/coolsolutions/zenworks).

In addition to the ZENworks 7 Migration Wizard, ZENworks 11 Configuration Management also includes a migration tool that can be used to migrate data from an existing ZENworks Linux Management infrastructure. The tool can also be downloaded from the same setup page as the migration tool for ZENworks 7.

The ZENworks Linux Management migration utility helps ZLM customers migrate their ZENworks Linux Management zone to an existing ZENworks 11 zone. This involves migration of bundles, policies, devices and associations for devices to bundles and policies. As there is no concept of Catalogs in ZENworks 11, we you be migrating ZENworks Linux Management Catalogs as either Linux Bundles or Linux Dependency Bundles in ZENworks 11. In addition, you will be migrating ZENworks Linux Management policies (Remote Execute/Text File) as ZENworks 11 bundles with install actions as run script/edit text file actions.

It is important to note that you should always test your migration(s) in a lab environment first, before you begin your production migrations. You should also test everything that you want to migrate as well, it doesn't hurt and it can save you a lot of time when it comes time to touch the production environment. When it is time to perform your production migration, we suggest doing things in phases, and take it one manageable step at a time.

The ZENworks Linux Management object migration wizard migrates RPM/File/Image Bundles, Remote Execute Policy and Text File Policy, Settings, Devices and Assignments.

In short, the user experience with the migration tools that Novell provides are very similar, and accomplish what is required to get existing content and settings from one infrastructure to your new ZENworks 11 infrastructure.

5.9 Wider Deployment

After you have completed the pilot deployments, you can move on to a wider deployment. Continuing to use the deployment plan that you have documented. You should execute against your project plan until you have completed the rollout to all remaining workstations on your network.

5.10 Post-Deployment Documentation and Validation

After you have completed the deployment, you should document all steps you took to deploy across your entire infrastructure. We recommend that you do this outside of the project plan, and include this in your documentation repository as either a separate document or as a part of your existing design document.

In addition, you should validate your success as much as possible. This can be done by doing the following:

- ◆ Perform physical spot checks wherever you can. Interview individuals briefly to see if they are experiencing any issues with the deployment, and more specifically with the addition of the ZENworks Adaptive Agent.
- ◆ Review error logs in ZENworks Control Center and investigate further from there. Visit workstations to find out more details if necessary.
- ◆ Monitor Service Desk activity throughout the duration of the deployment phase. Service Desk incidents reveal a lot of information. You are looking for spikes in activity and the details of the individual Service Desk requests.

6 Best Practices for Deploying ZENworks on a Citrix Server

This section describes the items you need to consider when deploying Novell ZENworks 11 on a Citrix server. This information is intended to supplement the online resources that Novell provides to give you a better understanding of the design-related topics and requirements when deploying a Novell ZENworks 11 solution on a Citrix server.

ZENworks Configuration Management is also supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the [ZENworks 11 SP2 documentation \(http://www.novell.com/documentation/zenworks11/index.html\)](http://www.novell.com/documentation/zenworks11/index.html).

The information in this document is organized as follows:

- ◆ [Section 6.1, “Understanding the Need for Integrating ZENworks and the Citrix Server,” on page 149](#)
- ◆ [Section 6.2, “Gathering Critical Information for Design Activities,” on page 150](#)
- ◆ [Section 6.3, “Performing Lab Tests and Validation,” on page 152](#)
- ◆ [Section 6.4, “Deploying the ZENworks Configuration Management Agent on Citrix Server,” on page 152](#)
- ◆ [Section 6.5, “ZENworks Configuration Management Tuning Parameters,” on page 152](#)

6.1 Understanding the Need for Integrating ZENworks and the Citrix Server

When ZENworks and the Citrix Server are properly integrated, these powerful solutions provide a functionally rich and manageable solution that is not possible when they are implemented in isolation. It is important to provide additional functionality without losing the functionality or reliability of either of the components.

By integrating Novell ZENworks Configuration Management and the Citrix Server, you achieve the following benefits:

- ◆ Improved application accessibility and manageability
- ◆ Strengthened security through Patch Management
- ◆ Improved compliance through Asset Management
- ◆ Improved remote access of applications that are on the Citrix server
Allows you to gain simple and one-click access to the applications on the Citrix server. Having all your local and remote software in one place allows you to reduce complexity and increase productivity.
- ◆ Management of the Citrix servers

- ◆ Patching of the Citrix servers and the applications hosted on the Citrix servers
- ◆ Load balancing of the Citrix servers
- ◆ Availability of support for the Citrix Server farm that has servers that are a part of an Active Directory forest or a workgroup

6.2 Gathering Critical Information for Design Activities

You need to gather information to help you design your specific implementation for deploying Novell ZENworks 11 on a Citrix Server.

Review the following sections:

- ◆ [Section 6.2.1, “Performing a Technical Assessment,” on page 150](#)
- ◆ [Section 6.2.2, “Factors Influencing Scalability,” on page 151](#)
- ◆ [Section 6.2.3, “Scale Numbers,” on page 151](#)
- ◆ [Section 6.2.4, “Ports Used by the ZENworks Agent,” on page 151](#)

6.2.1 Performing a Technical Assessment

You need to perform a technical assessment to review what you already have, identify what you need, and document your requirements.

You also need to have a good understanding of the existing infrastructure. To do this, you should hold a set of workshops or meetings to obtain all the information you need.

The two main results from a technical assessment are documentation on your findings, along with a set of tasks that you need to perform. Information that you should gather includes the following:

- ◆ Which version of Citrix Server should you use?

For more information on the supported versions of Citrix Server, see the [ZENworks 11 SP2 Server Installation Guide](#).

- ◆ What is the maximum number of user sessions per server that can be active on Citrix Server?

If the maximum number of user sessions per server is more than the recommended number, try adding more servers to the Citrix farm. We plan to provide such recommendations for the ZENworks 11 Configuration Management product after the product is released.

- ◆ Is user-based management used?

If it is used, a policy or bundle must be assigned to the users only if the policy or bundle is not applicable to all the users logging in to the server. However, if the policy or bundle is applicable to all the users logging in to the server, assign it to the device instead of assigning it to all the users.

For example, if there are 150 bundles that are assigned to the users and 50 bundles are common to all the users logging in to a device, assign these 50 bundles to the device instead of the user.

- ◆ Are servers available in the Citrix farm? If they are, how many servers are available and are these servers load balanced?

Make sure that no single server is overloaded. For information on load balancing mechanisms, see the [Citrix Web site \(http://www.citrix.com\)](http://www.citrix.com).

- ◆ Is the Novell Client installed on the Citrix server?

If the Novell Client is not installed on a Citrix server, the Citrix server session might crash during login. To avoid this issue, see “[Tasks to be Performed After Deploying the Agent on Citrix Servers](#)” on page 152.

- ◆ Do you plan to use the DLU policy? If you do, are the profiles volatile?

If there is more than one Citrix server in a farm, you must use the volatile DLU and Roaming Profile policies to enable the users and their profiles to exist on all the servers in the farm. If you do not use the volatile DLU and Roaming Profile policies, a profile synchronization issue might exist among the servers.

- ◆ Do you have a mechanism to handle idle and disconnected sessions? If you do, how often is it used?

The idle and disconnected sessions should be periodically logged out to enable the ZENWorks events such as memory release and policy unenforcement to happen. Otherwise, the server might have high memory consumption.

- ◆ Are the Citrix servers used only to distribute applications or they are also used as terminal servers?

You must deploy ZENworks 11 on Citrix Server only if you want the Citrix server to be used as a terminal server in addition to distributing applications. However, if you only intend to distribute applications, you can create thin client bundles and assign them to devices or users.

6.2.2 Factors Influencing Scalability

The main physical factor that govern the scalability of the Citrix servers is the RAM. The majority of operations are performed by three services: zenworksWindowsService, ZenNotifyIcon, and zenUserDaemon. The RAM consumption depends on the number of sessions and the number of effective assignments that each session has.

For the minimum hardware recommendations, refer to the [Citrix Web site \(http://www.citrix.com\)](http://www.citrix.com). If you can provide hardware that exceeds these recommendations, your system will perform better. Additional processing power and faster drives can make the systems more responsive.

The other factors that you need to consider include:

- ◆ Device refresh frequency
- ◆ Bundle schedules
- ◆ System requirements

6.2.3 Scale Numbers

The information will be available for ZENworks 11 Configuration Management product after the product is released.

6.2.4 Ports Used by the ZENworks Agent

For information on the ports used by the ZENworks Agent, see the [ZENworks 11 SP2 Server Installation Guide](#).

6.3 Performing Lab Tests and Validation

Before deploying ZENworks 11 on Citrix Server in a production environment, we recommend that you test ZENworks 11 on the Citrix servers with the exact load that needs to be in the production environment.

6.4 Deploying the ZENworks Configuration Management Agent on Citrix Server

For deploying the ZENworks Configuration Management Agent on Citrix Server, see the Deploying the ZENworks Adaptive Agent section in the [ZENworks 11 SP2 Discovery, Deployment, and Retirement Reference](#).

Tasks to be Performed After Deploying the Agent on Citrix Servers

After deploying the ZENworks Adaptive Agent on Citrix servers, do either of the following on the Citrix servers before launching a terminal session with the server:

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

IMPORTANT: If you fail to perform the preceding tasks, you will encounter ICA login session issues when you try to launch a terminal session with the Citrix server. For more information about the ICA login session issues, see “Unable to launch a terminal session with a Citrix Server that has ZENworks Adaptive Agent installed” in the [ZENworks 11 SP2 System Administration Reference](#).

6.5 ZENworks Configuration Management Tuning Parameters

This section provides information about the scenarios you might encounter if the parameters configured for a Citrix server are not appropriately tuned as per the deployment environment:

- ♦ [Section 6.5.1, “User Sessions on a Citrix Server Fail to Terminate,” on page 153](#)
- ♦ [Section 6.5.2, “High Utilization of Resources on a Citrix Server,” on page 153](#)
- ♦ [Section 6.5.3, “High Consumption of Memory on a Citrix Server,” on page 153](#)
- ♦ [Section 6.5.4, “Disabling Random Refresh Might Cause the ZENworks Adaptive Agent to Crash on a Citrix Server,” on page 153](#)
- ♦ [Section 6.5.5, “Logging in to the User Source on a ZENworks Server is Slow,” on page 154](#)

6.5.1 User Sessions on a Citrix Server Fail to Terminate

Terminating a thin client application that is running on a Citrix server might not close the user session on the server. Consequently, when the user logs out of the server, the roaming profile data for the user session is not saved.

To close the user session on the Citrix server, perform the following steps on the server:

- 1 Open the Registry Editor.
- 2 Go to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI`.
- 3 Change the value of `LogoffCheckSysModules` from `ZCMUMHelper.exe` to `ZenUserDaemon.exe`.
- 4 Reboot the device.

6.5.2 High Utilization of Resources on a Citrix Server

During a partial or general refresh of the ZENworks Adaptive Agent on a terminal session of a Citrix server, the agent simultaneously refreshes the sessions of all the users logged into the terminal server. If too many users have logged into the terminal server, this might cause high usage of system resources, and subsequently the ZENworks Adaptive Agent might take considerable time to refresh the terminal server.

To avoid high utilization of resources on the Citrix server:

- 1 Open the Registry Editor.
- 2 Go to `HKLM\Software\Novell\ZCM\`.
- 3 Create a string called `EnableBatchRefresh` and set its value to 1. By default, the number of user sessions that can be simultaneously refreshed is 5.
- 4 (Optional) If you want to change the default number of user sessions that must be simultaneously refreshed, create a string called `maxUserRefreshThreads` and set the desired value.

6.5.3 High Consumption of Memory on a Citrix Server

On a Citrix server or a terminal server, if a user disconnects a session without logging out from it, the session exists in the disconnected state. This might cause high memory consumption of the agent service.

To avoid high consumption of memory on the Citrix server, do one of the following:

- ♦ Ensure that the users log out from a session instead of just disconnecting the session.
- ♦ Set a time limit to automatically log out from a disconnected session. For detailed information, see the [Microsoft Knowledgebase \(http://support.microsoft.com/kb/186566\)](http://support.microsoft.com/kb/186566).

6.5.4 Disabling Random Refresh Might Cause the ZENworks Adaptive Agent to Crash on a Citrix Server

If Random Refresh for the ZENWorks Adaptive Agent is disabled and if multiple users log in to the Citrix server at the same time, then all the sessions try to refresh at the same time. This can cause resource contention, and subsequently causes the agent to crash because the cache access is not synchronized. To avoid this, Random Refresh must be enabled for the ZENWorks Adaptive Agent.

6.5.5 Logging in to the User Source on a ZENworks Server is Slow

Logging in to the user source on a ZENworks Server from the managed device might take some time because the login process executes the device refresh synchronously.

To speed up the login process, perform the following steps to execute the device refresh asynchronously:

- 1 Open the Registry Editor.
- 2 Go to `HKEY_LOCAL_MACHINE\Software\Novell\ZCM`
- 3 Create a string called `ZENLoginUserRefreshAsync` and set its value to `TRUE`.
- 4 Log in to the device again.

IMPORTANT: If you change the login process to execute the device refresh asynchronously, the latest policies might not be immediately available. With this change, you make the login performance more important than the accuracy of the policies.

A ZENworks Services

This section explains some of the Novell ZENworks Configuration Management services in greater detail, and also provides some useful information regarding logging, backing up, and restoring the Certificate Authority.

- ♦ [Section A.1, “ZENworks Services,” on page 155](#)
- ♦ [Section A.2, “Useful URLs,” on page 158](#)
- ♦ [Section A.3, “Critical File Locations,” on page 158](#)
- ♦ [Section A.4, “Logging Information,” on page 161](#)
- ♦ [Section A.5, “Backing Up and Restoring the ZENworks Certificate Authority,” on page 162](#)

A.1 ZENworks Services

On a Windows ZENworks Primary Server, the services reside in the `\novell\zenworks\bin` directory. On a Linux ZENworks Primary Server, they reside in the `/etc/init.d` directory.

- ♦ [Section A.1.1, “Checking the Status of a ZENworks Service,” on page 155](#)
- ♦ [Section A.1.2, “Starting a ZENworks Service,” on page 155](#)
- ♦ [Section A.1.3, “Stopping a ZENworks Service,” on page 156](#)
- ♦ [Section A.1.4, “Restarting a ZENworks Service,” on page 156](#)
- ♦ [Section A.1.5, “ZENworks Services,” on page 156](#)
- ♦ [Section A.1.6, “Web Services Test Pages,” on page 157](#)
- ♦ [Section A.1.7, “Agent Log Files,” on page 157](#)
- ♦ [Section A.1.8, “Server Log Files,” on page 158](#)

A.1.1 Checking the Status of a ZENworks Service

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

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

Replace *servicename* with the name of the service as listed in [Section A.1.5, “ZENworks Services,” on page 156](#).

A.1.2 Starting a ZENworks Service

To start a ZENworks service on a Windows ZENworks Primary Server:

- 1 Click *Start > Administrative Tools > Services*.
- 2 Select the service you want to start, then click *Start*.

To start a ZENworks service on a Linux ZENworks Primary Server:

- 1 Enter the following command at the server console prompt:

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

Replace *servicename* with the name of the service as listed in [Section A.1.5, “ZENworks Services,” on page 156](#).

To start all services:

- 1 Enter the following command at the server console prompt:

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

A.1.3 Stopping a ZENworks Service

To stop a ZENworks service on a Windows Primary Server:

- 1 Click *Start > Administrative Tools > Services*.
- 2 Select the service you want to stop, then click *Stop*.

To stop a ZENworks service on a Linux ZENworks Primary Server:

- 1 Enter the following command at the server console prompt:

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

Replace *servicename* with the name of the service as listed in [Section A.1.5, “ZENworks Services,” on page 156](#).

A.1.4 Restarting a ZENworks Service

To restart a service that is already running on a Windows Primary Server:

- 1 Click *Start > Administrative Tools > Services*.
- 2 Select the service you want to start, then click *Restart*.

To restart a service that is already running on a Linux Primary Server:

- 1 Enter the following command at the server console prompt:

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

Replace *servicename* with the name of the service as listed in [Section A.1.5, “ZENworks Services,” on page 156](#).

A.1.5 ZENworks Services

Table A-1 ZENworks Services, Service Names, and Descriptions

Service	Service Name	Description
Proxy DHCP Service	novell-proxydhcp	Used with a standard DHCP server to inform PXE-enabled devices of the IP address of the Novell TFTP server.

Service	Service Name	Description
TFTP Service	novell-tftp	Used by PXE-enabled devices to request files that are needed to perform imaging tasks.
ZENworks Agent Service	zenworkswindowsservice novell-zmd	Used to enable the server as a managed device.
ZENworks Datastore	dbsrv10	Embedded database used for storing ZENworks objects and resources.
ZENworks Loader	zenloader	Used for loading and controlling the Java services that perform ZENworks Server tasks.
ZENworks Preboot Policy Service	novell-zmgprebootpolicy	Used by PXE-enabled devices to check for assigned preboot policies and work.
ZENworks Preboot Service	novell-pbserv	Used to provide imaging services to a device. This includes sending and receiving image files, discovering assigned Preboot bundles, acting as session master for multicast imaging, and so forth.
ZENworks Remote Management	nzrwinvnc	Used to enable remote management of the server.
ZENworks Server	zenserver	Used for communicating with the ZENworks Agent.
ZENworks Services Monitor	zenwatch	Used to monitor the status of the ZENworks services.
ZENworks Imaging Agent	ziswin	Used to save and restore image-safe data on the server (as a managed device). Only runs when launched by the ZENworks Agent.

A.1.6 Web Services Test Pages

Most web services on the Primary Server provide details regarding the services, and can be used for test purposes after the servers have been installed. This ensures that the services are up and running prior to any deployment of the Adaptive Agent into the infrastructure, and there are no problems with the services themselves.

The three common interfaces are:

- ♦ https://Primary_Server_IP_address_or_FQDN/zenworks-useradmin
- ♦ https://Primary_Server_IP_address_or_FQDN/zenworks-coreadmin
- ♦ https://Primary_Server_IP_address_or_FQDN/zenworks-ping
- ♦ https://Primary_Server_IP_address_or_FQDN/zenworks (ZCC)

A.1.7 Agent Log Files

The following log files help that are available at the device level help you to troubleshoot issues pertaining to managed devices:

- ♦ `zmd-messages.log` - Contains logging information of the agent.
- ♦ `nwgina.log` - Contains information related to GINA startup and login.

- ♦ `zenlgn.log` - Contains information regarding the login process.
- ♦ `casaauthtoken.log` - Contains information regarding CASA connection to the CASA servlet.
- ♦ `nalshell.txt` - Contains information related to the ZENworks Explorer shell extension.
- ♦ `system-update.log` - Contains information regarding the progress and errors related to installing a System Update.

A.1.8 Server Log Files

The following log files help that are available for Primary Servers help you to troubleshoot issues pertaining to server activities.

- ♦ `services-messages.log` - Contains messages from all of the ZENworks servlets.
- ♦ `loader-messages.log` - Contains messages from all registered ZENworks loader modules and the queue (important).
- ♦ `ats.log` - Contains information related to CASA connections to the agent and to the LDAP user source.
- ♦ `zcc.log` - Contains output information from the ZENworks Control Center servlet. It helps you to troubleshoot issues that might occur while working in ZENworks Control Center.
- ♦ `catalina.out` - Tomcat logs.

A.2 Useful URLs

- ♦ [Section A.2.1, “Discovery,” on page 158](#)
- ♦ [Section A.2.2, “Deployment,” on page 158](#)

A.2.1 Discovery

`https://Primary_Server/zenworks-discovery`

`https://Primary_Server/zenworks-discoveryadmin`

`https://Primary_Server/zenworks-fileupload`

A.2.2 Deployment

`https://Primary_Server/zenworks-deployment`

`https://Primary_Server/zenworks-deploymentadmin`

`https://Primary_Server/zenworks-downloads`

A.3 Critical File Locations

ZENworks Configuration Management uses the following directories:

- ♦ [Section A.3.1, “Installation Directories,” on page 159](#)
- ♦ [Section A.3.2, “The ZENworks Content Repository,” on page 159](#)

A.3.1 Installation Directories

ZENworks Configuration Management uses the installation directories listed here. It is important to keep this in mind and be aware of where ZENworks Configuration Management is storing files. This is useful when you are troubleshooting specific functionality in ZENworks Configuration Management:

Windows installation directories:

- ♦ *Installation_directory*/ZENWORKS

Linux Installation directories:

- ♦ /opt/novell/zenworks/
- ♦ /etc/opt/novell/zenworks
- ♦ /var/opt/novell/zenworks
- ♦ /var/opt/novell/log/zenworks/

For best performance, you should use separated disks and logical drives for the OS and the installation directory. In addition, the database (if it is embedded) and log file size can increase very quickly, so it is better to have them on separate partitions.

A.3.2 The ZENworks Content Repository

The content repository is found in the following location on a Windows server:

installation_path\zenworks\work\content-repo

You should specify a different disk drive to be your content repository. This is based on best practices that Novell outlines for ZENworks Configuration Management. In Windows, this is done by mounting the drive. Mounting is simply pointing an existing path to a hard drive partition without the use of mapped drive letters.

In the following steps, you mount the default content repository location to a disk drive partition, which becomes the new content repository:

- 1 Make sure that the disk drive you want to use is attached to the server and is properly formatted as NTFS. This disk drive can be an existing drive or new drive for the machine. The hardware must be recognized by the server. However, do not specify a drive letter if you are adding a new disk drive to the machine. Windows does not allow mounting to a drive letter.
- 2 Because an empty *content-repo* directory must exist in the default location (*installation_path*\zenworks\work\content-repo) to be the pointer to the new Content Repository location, do one of the following to make sure that there is no content in the default location:
 - ♦ If you need to save the content that is now in this directory, rename the existing directory and create a new directory named *content-repo*.
You can then copy the content from this renamed directory to the new Content Repository location.
 - ♦ If you do not need any of the content in the existing *content-repo* directory, delete the directory and re-create it.
 - ♦ If the *content-repo* directory is not present in the path given above, create the path and directory.
- 3 Click *Start*, right-click the *My Computer* icon, then click *Manage*.

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

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

The disk drive you selected during the beginning of these steps should be displayed in the right pane.

- 5 (Conditional) If a driver letter is associated with the partition that you want to use as the new content repository location, do the following:

- 5a In the Computer Management dialog box, right-click the drive's partition.

- 5b Select *Change Drive Letter and Paths*.

- 5c Select the drive letter.

- 5d Click *Remove*, then click *Yes* to confirm.

- 6 Right-click the partition of the disk drive that you want to use as your content repository, then click *Change Drive Letter and Paths*.

This is the disk drive that you will mount to the `content-repo` directory later in this procedure.

- 7 Click *Add*.

This displays the Add Drive Letter or Path dialog box.

- 8 Select *Mount in the Following Empty NTFS Folder*, browse for and select the default `content-repo` directory, then click *Next*.

The default directory is `installation_path\zenworks\work\content-repo`.

This mounts the default path to the hard drive partition that you selected previously.

If necessary, format the drive as NTFS using the Computer Management feature in Windows.

- 9 Click the buttons as necessary to exit and save the configuration change.

- 10 Copy the files from the old renamed `content-repo` directory to the new `content-repo` directory.

From this point on, all ZENworks Configuration Management data is written directly to the new Content Repository location on the selected hard drive partition.

For Linux servers, you might want the `/opt` directory to be located on a large partition. This is where the database (if embedded) and content repository are stored.

The minimum disk configuration is required as follows:

Table A-2 *Disk Setup for Windows*

Partitions	Size	Contains
Boot (C:)	20 GB	Windows System
Install (D:)	40 GB and larger	<i>Installation directory</i> /ZENWORKS
Content	40 GB and larger	Mounted to <i>Installation directory</i> /ZENWORKS/work/content-repo

Table A-3 *Disk Setup for Linux*

Partitions	Size	Contains
/boot	300 Mb	Linux boot / ext2

Partitions	Size	Contains
/swap	4 GB	Linux swap
/root	20 GB	Linux system / ext3
Content	40 GB and larger	Mounted to /var/opt/novell/zenworks/content-repo

A.4 Logging Information

The Message Logger component of Novell ZENworks 10 Configuration Management lets the other ZENworks components such as zenloader and web services, ZENworks Management Daemon (ZMD), Remote Management, and Policy Enforcers log messages to different output targets. The output targets include the system log, local log, database, SMTP, SNMP trap, and UDP. For more information, see *Message Logging* in the [ZENworks 11 SP2 System Administration Reference](#).

Message Logger performs the following functions:

- ♦ Writes messages to local log files.
- ♦ Writes messages to a system log or event log.
- ♦ Writes messages to the Management console.
- ♦ Sends messages to the Management server.
- ♦ Sends messages as SMTP mail to SMTP servers from the Primary Server.
- ♦ Sends messages as SNMP traps to remote or local machines from the Primary Server.
- ♦ Sends messages as UDP packets to UDP destinations.
- ♦ Writes messages to the ZENworks database.
- ♦ Automatically purges database entries from the ZENworks database.
- ♦ Automatically acknowledges the messages in the ZENworks database.

The following sections contain more information:

- ♦ [Section A.4.1, “Local Log File,” on page 161](#)
- ♦ [Section A.4.2, “Installation Log File,” on page 162](#)
- ♦ [Section A.4.3, “Registration Log File,” on page 162](#)

A.4.1 Local Log File

On a managed device, the location of the local log file is:

```
novell\zenworks\logs\localstore\zmd-messages.log
```

On a ZENworks Server, the location of the local log file is:

- ♦ ZENworks Services:

Linux: /var/opt/novell/log/zenworks/services-messages.log

Windows: novell\zenworks\logs\services-messages.log

- ♦ ZENloader and its modules:

Linux: /var/opt/novell/log/zenworks/loader-messages.log

Windows: novell\zenworks\logs\loader-messages.log

A message is an event that is generated by different components and modules. These events can be exceptions such as errors, warnings, information to a user, or a debug statement for a module.

Messages are classified based on the following severity levels:

- ♦ **Error:** Indicates that an action cannot be completed because of a user or system error. These messages are critical and require immediate attention from an administrator.
- ♦ **Warning:** Indicates an exception condition. These messages might not be an error but can cause problems if not resolved. These messages do not require immediate attention from an administrator.
- ♦ **Information:** Provides feedback about something that happened in the product or system that is important and informative for an administrator.
- ♦ **Debug:** Provides debug information to troubleshoot and solve problems that might occur. The debug messages are stored only in the local file.

For additional information related to message logging, see *Message Logging* in the [ZENworks 11 SP2 System Administration Reference](#).

A.4.2 Installation Log File

The log file related to the installation of ZENworks can be found at the following location, for both the Linux and Windows platforms:

```
Install_Path\logs\ZENworks_Install_date.log.xml
```

A.4.3 Registration Log File

The log files related to registration can be found in the following locations:

Server Log File

Linux: /var/opt/Novell/logs/zenworks/service-messages.log

Windows: /Novell/ZENWorks/logs/service-messages.log

Agent Log File

```
Novell/ZENworks/logs/LocalStore/zmd-messages.log
```

A.5 Backing Up and Restoring the ZENworks Certificate Authority

When you install ZENworks Configuration Management for the first time you are prompted to either create an internal Certificate Authority (CA) or provide the appropriate certificate information for an external CA. If you are using the built-in CA, it is important to keep in mind that the CA can be backed up and restored if you require this as part of a set of troubleshooting procedures.

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

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

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

This command exports the key-pair credentials of the zone certificate authority to a file.

- 2 Enter the username and password of the administrator of the Management Zone.
- 3 Enter a passphrase for the file encryption.

The passphrase is used in the encryption of the backed-up file.

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

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

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

This command imports the key-pair credentials of the zone certificate authority from a file.

- 2 Enter the username and password of the administrator of the Management Zone.
- 3 Enter the file encryption passphrase you specified when you backed up the Certificate Authority files

B The ZENworks Configuration Management Architecture

The following sections are intended to be a reference for the Novell ZENworks Configuration Management architecture and should be used for education purposes. Because the architecture for ZENworks Configuration Management has changed dramatically from that of ZENworks 7 and previous versions, it is important to have a better understanding of these changes and how the system components interact.

- ♦ [Section B.1, “ZENworks Architecture Reference,” on page 165](#)
- ♦ [Section B.2, “Detailed ZENworks Components Diagram,” on page 170](#)

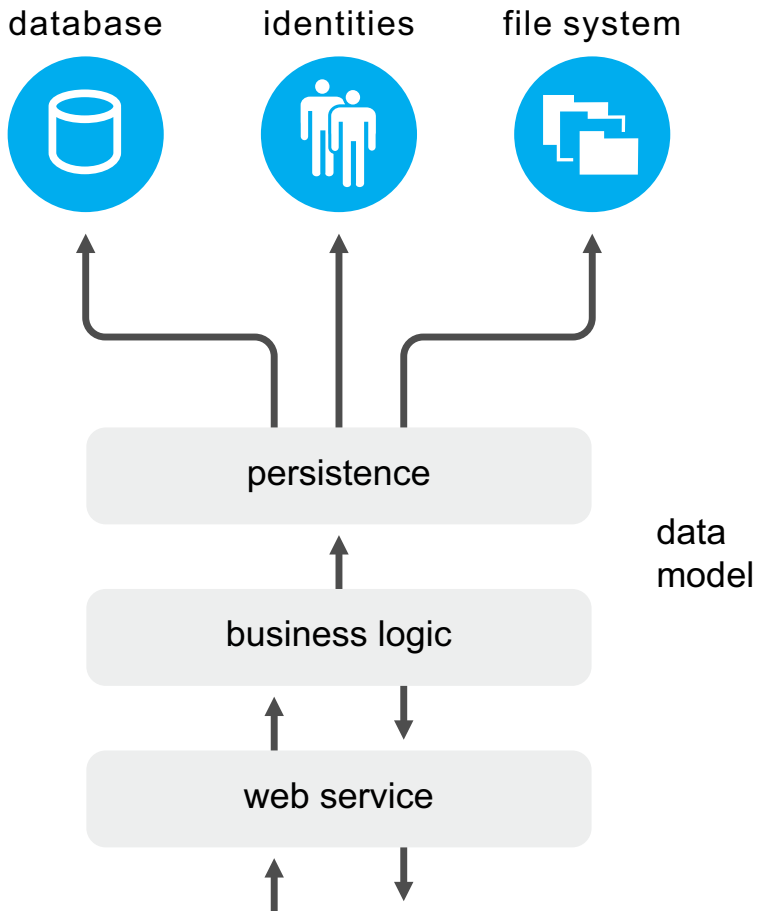
B.1 ZENworks Architecture Reference

Out of the box, ZENworks Configuration Management provides a standards-based, three-tier, services-oriented architecture that allows you to manage devices over the Internet without disrupting your network infrastructure. Separating components into different tiers makes it easier to change business logic or add new modules without affecting other tiers of the architecture.

The server-side infrastructure consists of two tiers. The first tier provides Web services, including object-to-relational mapping and data-model APIs. The second tier comprises the file system for storing actual files, the database for storing ZENworks information, and the optional identity store (eDirectory or Active Directory) for performing user-based resource management. The third tier consists of the ZENworks Adaptive Agent on managed devices.

The following diagram is a visual representation of the three-tier web services architecture (including the optional connection to a user source) of ZENworks Configuration Management.

Figure B-1 Web Services Architecture



Because it is a fully Web-based application, ZENworks Configuration Management uses Web services as the primary mechanism for communications between management servers, managed clients, identity and object stores, and the management console. No proprietary protocols are used.

The following sections contain more information:

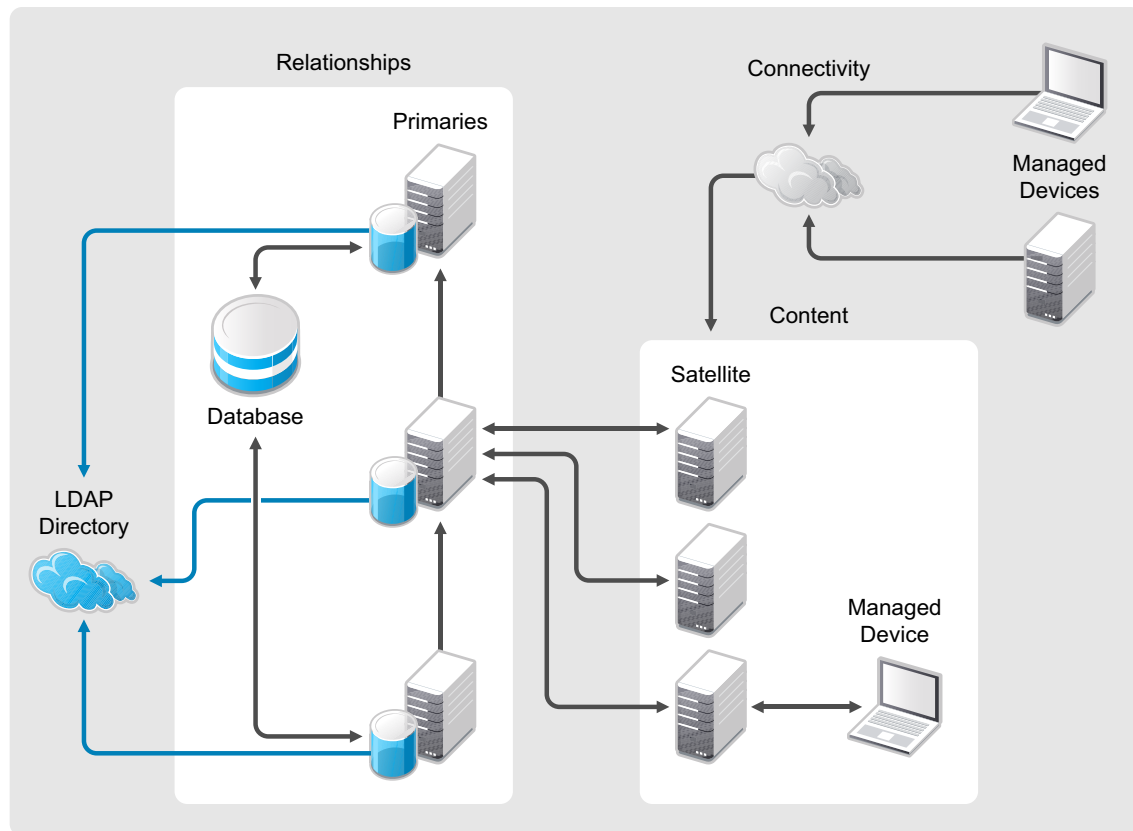
- ♦ [Section B.1.1, “Standard Protocols,” on page 166](#)
- ♦ [Section B.1.2, “ZENworks Primary Server Architectural Components,” on page 167](#)
- ♦ [Section B.1.3, “Agent Architecture,” on page 169](#)
- ♦ [Section B.1.4, “Agent Communication,” on page 169](#)

B.1.1 Standard Protocols

- ♦ **HTTP or HTTPS:** Used for communication from managed clients to the server.
- ♦ **SOAP over HTTPS:** Used for communication from the server to the ZENworks Adaptive Agent on managed devices.
- ♦ **LDAP:** Used for integration with eDirectory or Active Directory identity stores.
- ♦ **SOAP:** Used for zone administration win zman.
- ♦ **SSL:** Used for secure communications with managed devices and the management console. This allows devices located anywhere to be managed from anywhere, even beyond the corporate firewall.

The following graphic illustrates this:

Figure B-2 ZENworks System Diagram



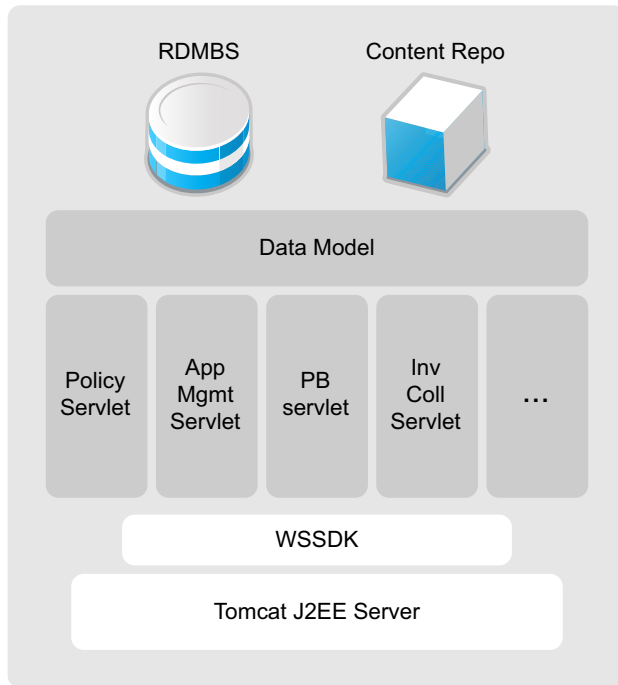
B.1.2 ZENworks Primary Server Architectural Components

A ZENworks Primary Server delivers the back-end infrastructure of ZENworks Configuration Management. The following items are the components of the ZENworks primary server:

- ◆ Apache Tomcat is a servlet container that provides Web serving, Java servlet hosting, and SSL encryption and authorization.
- ◆ Extend WSSDK provides the core SOAP infrastructure.
- ◆ Java servlets implement feature-specific functionality.
- ◆ The data model abstracts the storage layer from the Web services.
- ◆ The database stores relationships, configuration management data, and inventory.
- ◆ The Content Repository contains images, files, and other bundle content.

The following diagram is a visual representation of the Primary Server (ZENServer) architecture:

Figure B-3 Primary Server Architecture



Advantages of this simplified architecture include:

Time to value: The new architecture allows you to install ZENworks Configuration Management with just a few mouse-clicks. Very little administrator input is required to install a Primary Server, and it typically takes only 35 minutes from the time you drop the CD into the tray until you can actually be discovering and managing devices on your network. The ZENworks Adaptive Agent is installed and managed from the central management console, eliminating the need for IT to touch each individual device. The system connects non-disruptively to your identity stores - Active Directory and Novell eDirectory - requiring no changes to your security policies. Because it's based on more than two years of human factors research and input from users, the user interface works the way you work, so you can be productive almost immediately.

Deployment flexibility: Configuration management tool should be deployed in a manner that harmonizes with the existing IT infrastructure. The architecture of ZENworks Configuration Management is designed with this requirement in mind, providing the flexibility to deploy the solution in a wide range of IT environments with minimal change management barriers. For example, it can be deployed as a departmental solution or enterprise-wide, without requiring new operating systems, database administration skills, or non-standard communication protocols.

Reduced wire traffic: Metadata is retrieved in a single request or response by using SOAP calls. This minimizes the network traffic devoted to management, in contrast to architectures that must make multiple calls to retrieve raw data for business logic located on the client.

A single client agent: Legacy management practices have created a need for multiple agents, which must be installed, updated, and patched individually, to handle various management tasks. The new ZENworks Configuration Management architecture features a single ZENworks Adaptive Agent that requires just one installation, then dynamically "shrinks" or "expands" according to specific management needs.

B.1.3 Agent Architecture

The ZENworks Adaptive Agent consists of the following components:

- ♦ [“Primary Agent” on page 169](#)
- ♦ [“Core Plug-Ins” on page 169](#)
- ♦ [“Feature-Specific Plug-Ins” on page 169](#)
- ♦ [“Policy Enforcers” on page 169](#)

Primary Agent

The primary agent is responsible for maintaining connectivity to the ZENworks Primary Servers and listening for requests from the server. This component is implemented as a Windows service and is started at system startup time.

Core Plug-Ins

A core set of plug-ins provides common services required by most features. These plug-ins include the trigger and event scheduling system (TESS) components, caching components, components to implement features such as system shutdown and reboot.

Feature-Specific Plug-Ins

Other features are also implemented by plug-ins to the ZENworks Adaptive Agent. These plug-ins include the Bundle plug-in, Policy plug-in, Inventory plug-in, Remote Management plug-in, and Patch Management plug-in. These plug-ins leverage the core plug-ins and the primary agent to retrieve information from the Primary Server. For instance, the Bundle plug-in is responsible for installing of Windows, File, and Directive bundles.

Policy Enforcers

The Policy plug-in is also divided into multiple components. These components are the Policy Manager, which identifies the effective policies, and the Policy Enforcers, which are platform-specific components that understand how to implement policies.

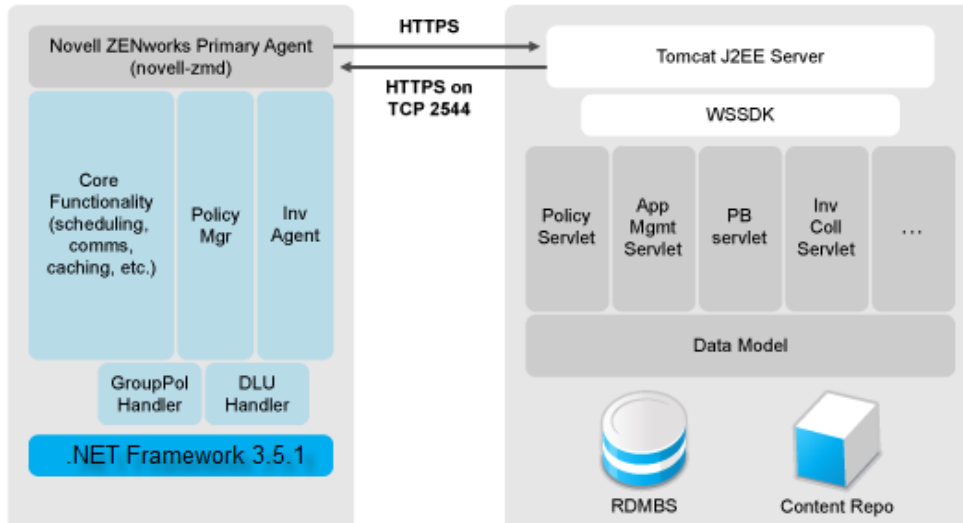
During Adaptive Agent installation, all the components are installed on the managed device and are activated as needed.

B.1.4 Agent Communication

The communication between the ZENworks Adaptive Agent and the ZENworks Primary Server is generally implemented as a standard Web session. Unlike previous versions of ZENworks, the Adaptive Agent does not maintain a session with the Primary Server. Instead, it makes an HTTPS request, receives information it needs, and then disconnects from the Server. The Adaptive Agent also includes an HTTPS listener that is implemented on TCP port 2544. The purpose of this listener is to allow a Primary Server to initiate partial or full refreshes remotely. The result of a refresh is the immediate initiation of task on the device.

The following graphic depicts the ZENworks Adaptive Agent architecture and how the Server and Agent pieces interact with each other:

Figure B-4 ZENworks Adaptive Agent Architecture



Modular three-tier services oriented architecture: Standard protocols are used for IT over public and private networks, as well as for communications between the solution's three tiers:

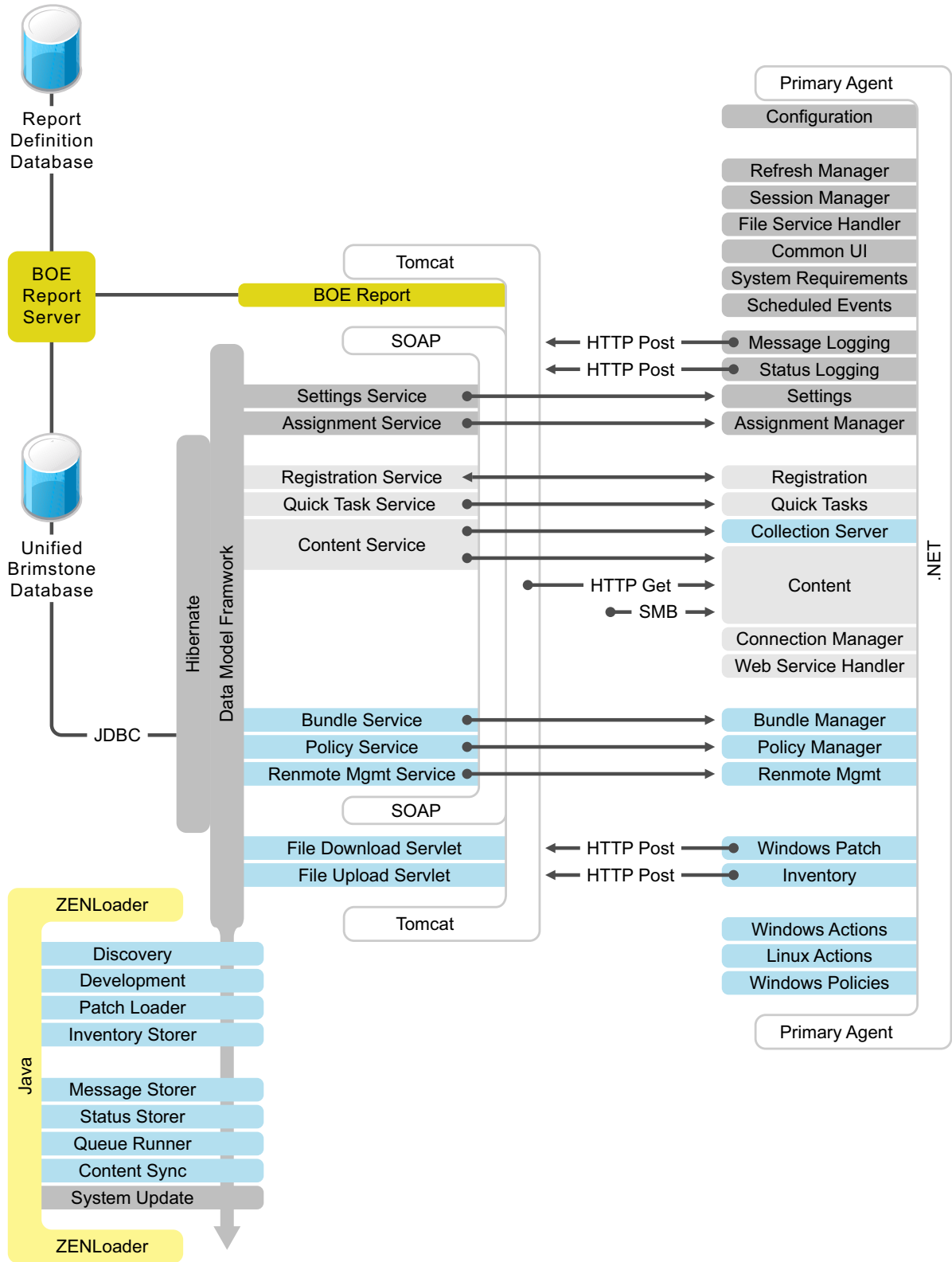
- ♦ All general business logic resides on the server, allowing complete flexibility in system-wide updates and keeping client-specific updates to a minimum.
- ♦ The single agent is tailored in size and functionality for the specific managed device, enabling the most efficient delivery and policy enforcement.
- ♦ An SQL database provides an industry-standard method for integrating the solution with IT and business systems.

Management Zones: Users and devices can be grouped together to form management zones, which provide a single, authoritative source for all configuration information applicable to the members of the Management Zone. All managed devices are registered to a single ZENworks Management Zone.

B.2 Detailed ZENworks Components Diagram

The following diagram is a visual representation of how the individual components of both the ZENworks Server and the ZENworks Adaptive Agent interact with each other at a component-by-component level, and where the processes are initiated. This is a full view of the ZENworks Configuration Management architecture.

Figure B-5 ZENworks Configuration Management Architecture



C Reference Materials

This section contains references to useful information that is found online at the Novell Web site, as well as information that you can use to create your own Business Requirements and Technical Requirements surveys.

The following sections contain more information:

- ♦ [Section C.1, “Online Documentation,” on page 173](#)
- ♦ [Section C.2, “Sample Business Requirements Survey Questions,” on page 173](#)
- ♦ [Section C.3, “Sample Technical Requirements Survey Questions,” on page 175](#)
- ♦ [Section C.4, “Extended Port Chart Including Port Usage,” on page 176](#)

C.1 Online Documentation

This section includes a number of links to help customers plan, deploy, and manage their ZENworks Configuration Management infrastructure. These documents should be reviewed prior to the kickoff of the implementation or migration project. It is important to be familiar with the product, its features, and capabilities before you start your assessments and design, and it is especially important before ZENworks Configuration Management goes live. We suggest that you either reference these documents in your own briefings, or print and deliver these documents prior to the start of the project.

C.2 Sample Business Requirements Survey Questions

The following sample survey is a good starting point for you to develop a survey that you can use as you begin to discuss the ZENworks Configuration Management deployment project. You should modify the survey according to your specific needs. Each customer environment is different and each survey requires a different set of questions.

Please answer the following questions to the best of your abilities, based on the information that you have on hand.

1. Is this a global organization? How many locations do you have? Where are they specifically?
2. How many people work for your organization? Where are they located based on your answer to the first question? Do you support multiple languages? Do you have a list of departments and internal organizations that you can provide? What is the percentage breakdown of full-time employees, part-time employees, and contractors or consultants?
3. How many total users do you want to manage?
4. How many total devices do you want to manage? What types of devices (laptops, desktops, handhelds)? What platforms are they?
5. In terms of your people and locations, please provide some metrics for the following:
 - ♦ How many data centers do you operate? Where are they specifically?

- ♦ What are the size breakdowns of your remote, typically lower bandwidth locations (for example, 10-50 users, 50-250 users, 250-1,000 users, etc.)?
 - ♦ What is the bandwidth to your data center and to your remote locations? Best case? Worst case?
 - ♦ Do you typically have servers at your remote locations? And if so, which platforms?
 - ♦ Where are your departments located? What do you mean by departments? Did you mean remote locations again?
 - ♦ Do you have employees that roam from site to site on a regular basis?
 - ♦ What percentage of your employee population is considered “mobile employees”?
 - ♦ Do you have employees who work from home?
6. Do you have an ITIL initiative in place or under way? If so, which disciplines are you currently utilizing or plan to utilize?
 7. Does your organization have Service Level Agreements in place with other internal and external organizations, suppliers, or vendors?
 8. What other projects are currently under way at your organization? For example, SAP implementation, Service Desk implementation, Identity Management, Security Management, etc.
 9. Are there times during each month or quarter where blackouts to implement changes are in effect?
 10. How often are changes implemented? Do you have a regular schedule? As needed? Are the changes and change windows tightly controlled?
 11. Do you have a Change Control Board? If so, who are the members of this board and where are they located? How are changes proposed, reviewed, tracked, and ultimately managed?
 12. Do you always have a test environment for each critical system? And if so, are these environments persistent or only available during deployment?
 13. Do you have a Security department? If so, who are the leaders of this department and where are they located?
 14. Is security managed centrally? Does this include both physical and logical security? Do you have an empowered security officer (CSO, Director, etc.)?
 15. Do you have any type of endpoint security in place? For example, USB controls, encryption (full disk or file level), WiFi controls, VPN, or VPN enforcement?
 16. Do you have a Service Desk in place? Is it centralized or decentralized? Is this a 24x7 operation? Who manages the Service Desk operations? What service desk are you running (commercial package or homegrown)?
 17. Do you have a configuration/change management database system? If so, is this a commercial package (and if so what?) or homegrown?
 18. Do you have a Project Management Office in place? Do you typically allocate Project Managers to your internal projects, or is this something that is normally outsourced?
 19. Does the organization have any growth plans or expectations (that can be shared) for the upcoming two or three years where you would be expanding outside of your existing location base? What quantity of growth do you expect from a user or device perspective?

C.3 Sample Technical Requirements Survey Questions

The following sample survey is a good starting point for you to develop a survey that you can use as you begin to discuss the ZENworks Configuration Management deployment project. You should modify the survey according to your specific needs. Each customer environment is different and requires a different set of questions.

Please answer the following questions to the best of your abilities, based on the information that you have on hand.

1. Can you provide a diagram of your network infrastructure, including network hardware, placement, and link speeds?
2. What are the desktop operating systems that you support in your environment?
3. What are the server operating systems that your support in your environment? Do you anticipate leveraging any of your existing server infrastructure to host ZENworks services?
4. How many people will be supported with the ZENworks solution? Do you have initial thoughts on how quickly you would like to deploy this? What is your estimated project completion date?
5. Do you currently support mobile users? Will you begin, or continue, to support mobile users with the new ZENworks implementation?
6. Do you host your own DNS infrastructure? Can you provide details on how your DNS is currently set up?
7. Can you provide details on how your DHCP infrastructure is set up? Can you provide a list of subnets by site (IP subnet design diagram)?
8. Are you currently leveraging any form of Network Access Control (NAC)? If so, which solution is in place?
9. Are you currently leveraging any form of endpoint security management at the desktop and server levels? If so, which solution is in place?
10. How do roaming users access your corporate infrastructure from remote locations (VPN, Access Management, etc.)?
11. Which directory services technologies do you have in place (Novell eDirectory, Microsoft Active Directory, Sun Directory Services, etc.)? Are you able to provide diagrams that show the physical structures of each of the individual directory services that you are currently leveraging?
12. Do you have any existing Identity Management software in place? If so, which product are you currently using?
13. Are you currently utilizing any other systems management products to perform any form of desktop management? If so, provide details around each of the individual point technologies that you are currently leveraging. This would include areas such as:
 - ◆ Software deployment
 - ◆ Desktop policy management
 - ◆ Desktop and server OS provisioning
 - ◆ Patch management
 - ◆ Hardware inventory collection
 - ◆ Software inventory collection
 - ◆ Reporting
 - ◆ License compliance
 - ◆ Usage tracking
 - ◆ Contract management

- ◆ Endpoint Security Management
- ◆ Remote control
- ◆ Other forms of remote diagnostics
- ◆ Thin-client solutions
- ◆ Application virtualization
- ◆ Other forms of advanced scripting capabilities
- ◆ Homegrown processes (provide as much detail as possible on each of the homegrown applications you are currently using for systems management)

NOTE: The parameters listed above are applicable for both the Windows and the Linux platforms.

14. Are you also performing a hardware refresh at this time? If not, when will you be performing the next one? If so, when will it be complete?
15. What is your turnaround time when it comes to hardware acquisition (desktop and server)?

C.4 Extended Port Chart Including Port Usage

The following table shows the individual ports required to be open, the description of each port, etc.

This is an extended version of the information in [Section 3.6, “Ports Used by ZENworks Components,”](#) on page 63.

Table C-1 ZENworks Ports Usage

Port	Type	From	To	Description	Initiated By	Duration
80	TCP	ZENworks Adaptive Agent	Primary Server or Satellite	Used to download content from Primary Server or Satellite. Used to upload inventory, message data, patch results, etc to a Satellite. Used to download content from Primary Server to Satellite during content replication. Used to roll up the collection data from Satellite to Primary Server.	ZENworks Adaptive Agent	HTTP listener is active until the ZENServer service runs. Active until the completion of the HTTP GET or PUT request.

Port	Type	From	To	Description	Initiated By	Duration
443	TCP	ZENworks Adaptive Agent Management workstation Imaging Satellite	Primary Server or Authentication Satellite	Used mostly for agent communication with the server including authentication, configuration requests, assignments, and registration. Used to send authentication requests to the Satellite server. Hosts ZENworks Control Center. Used by zman to communicate to the administrative Web services on the server.	ZENworks Adaptive Agent or Management workstation	HTTPS listener is active until the ZENServer service runs Active only when an authentication request occurs.
2645	TCP	ZENworks Adaptive Agent	Primary Server	Used for authentication when CASA servlet is not available on 443. This occurs if the ZENServer instance of Tomcat is busy to service the CASA authentication token requests.	Agent (CASA Authentication Token Service)	Listener is active until the CASA instance of Tomcat runs. Active only when an authentication request occurs.
67/4011	UDP	Device that is PXE booted	DHCP Sever and Primary Server or Imaging Satellite	The DHCP port is used to request for DHCP and PXE boot information. 4011 is used only if the DHCP server is the ZENworks server as well.	PXE Boot ROM	Listener is active if the Proxy DHCP service is running on the Primary Server or Satellite. Listens for all broadcasts.
69	UDP	Device that is PXE booted	Primary Server or Imaging Satellite	The TFTP port is used to download PXE boot files and other imaging files as described in bundles.	PXE Boot ROM ZENworks Network Boot Program ZENworks Imaging Engine WindowsPE Boot Loader WindowsPE ZENworks Work To Do application	Listener is active if the TFTP service is running on the Primary Server or Satellite. Active only when GET or PUT requests are received from the agent.

Port	Type	From	To	Description	Initiated By	Duration
1333 1	UDP	Device that is PXE booted and finds ZENworks Boot program	Primary Server or Imaging Satellite	Preboot Services lookup port. Used by the PXE boot program as a proxy to the Imaging server. This is required because PXE ROM can communicate only through UDP.	ZENworks Network Boot Program on PXE booted device	Listener is active if the ZENworks Preboot Policy service is running.
998	TCP / UDP	Device that requests for the imaging work		Used to identify the imaging work that needs to be performed and when images are to be sent or received. Generally, the request is from the device that is imaged to the Imaging server. In the case of Preboot Services, forwarding a server in Zone 1 would contact a server in Zone 2 specified in the forwarding list. UDP is used while performing multicast imaging operations.	ZENworks Imaging Distribution Windows PE ZENworks Work To Do application From Primary Server in Zone 1 to Primary Server in Zone 2.	Listener is active until the Novell Preboot Service runs. Active only during the imaging operations or work to do.
5950	TCP	Management Workstation Remote Management Proxy	ZENworks Adaptive Agent			
5550	TCP	Managed Device	Management Workstation	Remote Management listener on the Management workstation. This allows users at managed devices to request assistance from the administrator on the Management workstation.	ZENworks Remote Management requester	Listener is active after installed. Connection is active when a user requests assistance.

Port	Type	From	To	Description	Initiated By	Duration
5750	TCP	Management Workstation	Remote Management Proxy	Remote Management proxy listener. This allows a user connecting through NAT to remote manage a device that can be accessed by the proxy. The Management workstation connects to the proxy on 5750 and the proxy connects to the managed device on 5950.	ZENworks Control Center when initiating a remote management connection through a Remote Management proxy.	Listener is active on the device where you install the Remote Management proxy component. The connection is active from the time the administrator initiates a connection until the connection ends.
7628	TCP	Primary Server	ZENworks Adaptive Agent			
1433	TCP	Primary Server	Microsoft SQL Database	JDBC connection established from Primary Servers to MS SQL.	ZENworks Server and ZENworks Loader services maintain database connections.	Connection is active until the ZENworks Server or Loader runs.
2638	TCP	Primary Server	Sybase Database	JDBC connection established from Primary Servers to Sybase.	ZENworks Server and ZENworks Loader services maintain database connections.	Connection is active until ZENworks Server or Loader runs.
1521	TCP	Primary Server	Oracle Database	JDBC connection established from Primary Servers to Oracle.	ZENworks Server and ZENworks Loader services maintain database connections.	Connection is active until ZENworks Server or Loader runs.
1761	UDP			Used to forward subnet-oriented broadcast magic packets for Wake-On-LAN		

D Understanding the Performance and the ZENworks Login Process

The ZENworks Configuration Management Superlab tests conducted across the releases of ZENworks 11 and ZENworks 11 SP1 have enabled Novell to improve the ZENworks Configuration Management login times significantly as compared to previous versions. In some cases, login times have improved by as much as 150 seconds. However, some users still experience slow logins, and you as an administrator need to address their concerns.

There are many different causes for slow logins. This section discusses some of the most common causes, and suggests best practices and configuration changes that you can make to enhance the login experience for users:

- ♦ [Section D.1, “Supported Authentication Mechanisms,” on page 181](#)
- ♦ [Section D.2, “Supported Directories for Authentication,” on page 181](#)
- ♦ [Section D.3, “The Login Process,” on page 182](#)
- ♦ [Section D.4, “Best Practices to Optimize ZENworks User Login Times,” on page 184](#)
- ♦ [Section D.5, “Registry Keys and Configuration Files,” on page 186](#)
- ♦ [Section D.6, “ZENworks Configuration Management Policies,” on page 187](#)
- ♦ [Section D.7, “ZENworks Configuration Management Bundles,” on page 188](#)
- ♦ [Section D.8, “Logging in to a Terminal Server or Citrix Environment,” on page 188](#)
- ♦ [Section D.9, “Troubleshooting Login Issues,” on page 189](#)

D.1 Supported Authentication Mechanisms

ZENworks Configuration Management supports the following authentication mechanisms:

- ♦ **Password:** Active Directory, eDirectory, DSfW (Domain Services For Windows)
- ♦ **Kerberos:** Active Directory and DSfW
- ♦ **Shared Secret:** eDirectory (smart card authentication)

D.2 Supported Directories for Authentication

ZENworks Configuration Management supports three types of directories as LDAP user sources:

- ♦ Novell eDirectory
- ♦ Microsoft Active Directory
- ♦ DSfW (Domain Services For Windows)

The login times are not dependent on the type of directory used for the purpose of authentication. However, if multiple user sources are configured and seamless login is enabled, users might experience longer login times because all of the user sources are searching for matching user credentials.

D.3 The Login Process

- ♦ [Section D.3.1, “Windows Login Process,” on page 182](#)
- ♦ [Section D.3.2, “ZENworks Configuration Management Login Process,” on page 183](#)

D.3.1 Windows Login Process

Winlogon starts the Local Security Authority Subsystem Service (LSASS) and Service Control Manager (SCM), which in turn start all the Windows services that are set to auto-start. Winlogon is also responsible for responding to the Secure Attention Sequence (SAS), loading the user profile on logon, and optionally locking the computer when a screen saver is running.

The logon process is as follows:

1. Winlogon calls GINA (Graphical Identification and Authentication).
2. GINA displays the Logon prompt.
3. The user presses the secure attention sequence (Control+Alt+Delete).
4. GINA displays the Logon dialog box.
5. The user enters the credentials (username, password, and domain).
6. GINA passes the credentials back to Winlogon.
7. Winlogon passes the credentials to LSASS, which determines which account database is to be used:
 - ♦ Local SAM
 - ♦ Domain SAM
 - ♦ Active Directory
8. LSASS enforces the Local Security Policy (checking user permissions, creating audit trails, issuing security tokens, and so forth).
9. After a user has successfully logged in to the machine, Winlogon does the following:
 - a. Updates the control sets.
 - b. Applies the User and Computer Group Policy settings.
 - c. Starts the shell program (typically `Explorer.exe`).
 - d. Runs the Startup programs from the following locations:
 - ♦ `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`
 - ♦ `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run`
 - ♦ `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
 - ♦ `HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load`
 - ♦ `HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run`
 - ♦ `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`
 - ♦ `HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce`

- ♦ %ALLUSERSPROFILE%\Start Menu\Programs\Startup\
- ♦ %USERPROFILE%\Start Menu\Programs\Startup\

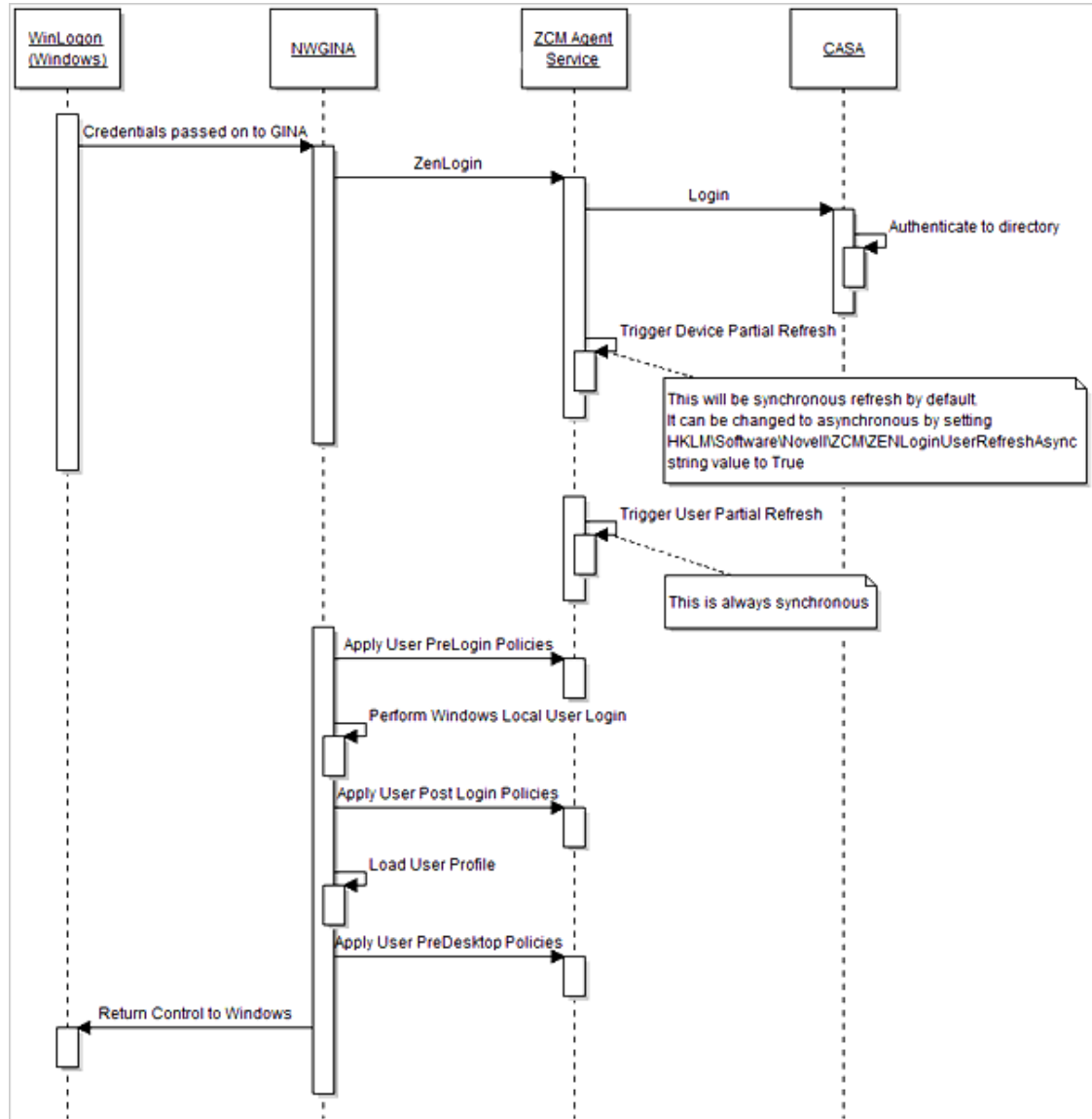
D.3.2 ZENworks Configuration Management Login Process

The ZENworks Configuration Management login sequence is as follows:

1. The ZENLgn interface displays a dialog box for the user to enter credentials.
2. ZMD (ZENworks Management Daemon) sends the Obtain an Auth Token call to the CASA client.
3. The CASA client sends the Get Auth Policy call to the ATS server on the ZENworks Configuration Management Authentication server.
The Get Auth Policy call is made to identify the authentication mechanisms that have been configured on the ZENworks Configuration Management server.
4. The Get Auth Policy call sends the mechanisms configured on the ZENworks Configuration Management server back to the CASA client.
5. The Authenticate call is sent from the CASA client to the ATS server.
6. The credentials are validated with eDirectory, Active Directory, or Domain Services for Windows, and a reply is returned from the directory, indicating whether the credentials are correct.
7. This reply is sent to the ATS server, which creates a session token.
8. The session token is sent to the CASA client. It succeeds if the credentials are valid or sends error messages for a failure.
9. The CASA client creates Get Auth Token requests to identify attributes such as Grace Login and restrictions for changing password for that particular user.
The Grace Login attribute was added in ZENworks 11 SP1.
10. The details are sent back to the CASA client.

The ZENworks Configuration Management Login flow of events is depicted in the following diagram:

Figure D-1 ZENworks Configuration Management Authentication Sequence



D.4 Best Practices to Optimize ZENworks User Login Times

- ◆ For beginner guidelines for troubleshooting slow login issues, see [TID 7007583](http://www.novell.com/support/search.do?usemicrosite=true&searchString=7007583) (<http://www.novell.com/support/search.do?usemicrosite=true&searchString=7007583>).
- ◆ For more information on configuration of recommended antivirus exclusions that can reduce login times, see [TID 7007545](http://www.novell.com/support/search.do?usemicrosite=true&searchString=7007545) (<http://www.novell.com/support/search.do?usemicrosite=true&searchString=7007545>).
- ◆ Perform a routine health check on all of the authentication servers and user sources, because any non-functional server that is configured in the Closest Server rules might add to login time delays.
- ◆ Verify that the ZENworks Configuration Management Primary Servers and the configured user sources can communicate properly.

- ♦ Verify that all the replicas of user sources associated with a given authentication server (Primary or Satellite) are functional and working properly.
- ♦ Verify that the replicas or user sources associated with all of the authentication servers in the Closest Server rules are reachable. Non-functional user sources can cause delays in login times.
- ♦ When you configure connections for a Primary or authentication Satellite Server, use only those user sources or replicas that are easy to reach.
- ♦ Configure the list of connections for every authentication server, in the order of how easy it is to reach them.
- ♦ Wherever possible, configure local authentication satellites and local directory servers or their replicas for authentication purposes.
- ♦ Configure the Default location with only one authentication server if possible.
- ♦ Ensure that time is synchronized for servers, satellites, managed devices, databases, and directory servers. For more information, see [Section D.9.2, “Time Synchronization,” on page 190](#).
- ♦ Ensure that DNS resolution is working across Primary Servers, Satellites, managed devices, and user sources.
- ♦ Ensure that the external (2645) and internal (443) CASA services are functional.
- ♦ Ensure that the certificates are valid and have not expired. For more information, see [Section D.9.3, “Checking Certificates,” on page 190](#).
- ♦ Where possible, avoid configuring multiple Group policies with multiple settings. For details, see [Section D.6.1, “Group Policy,” on page 188](#).
- ♦ Group policies with security settings enabled might cause delays to login times. You should use a combination of bundles and Windows secedit (security configuration editor) to achieve the desired results.
- ♦ Do not set multiple bundles to be launched at login. Use On Device Refresh or other appropriate schedules to reduce the user login times. For more information, see [Section D.7, “ZENworks Configuration Management Bundles,” on page 188](#).
- ♦ Do not assign multiple bundles with multiple system requirements to be triggered at user login. For details, see [Section D.7, “ZENworks Configuration Management Bundles,” on page 188](#).
- ♦ Enable Random Refresh in the Management Zone and configure the time window according to your users’ needs. Setting the time window to be too small might impact login times.
- ♦ When there are multiple user sources configured in the Management Zone, configure a default realm to improve boot login times.
- ♦ Do not use a combination of Default Realm and Seamless Login registry settings.
- ♦ Configure NALWIN in the Run section of the registry (HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run) instead of launching it as a bundle in a user login event HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run.
- ♦ Configure NALWIN in the SHELL registry key instead of Explorer for cases where NAL is required but Explorer is not required. The registry key is located at

```
/HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
```
- ♦ Disable NALVIEW if the NAL icons do not need to be displayed on the desktop, Quick Launch, startup menu or notification area. For more information, see [Section D.5.1, “Using Registry Keys to Reduce Login Time,” on page 186](#).
- ♦ Set the registry key to enable asynchronous device refresh during user login. For details, see [Section D.5.1, “Using Registry Keys to Reduce Login Time,” on page 186](#).

- ♦ Enable login status messages on the managed device (10.3.x) to view the complete login sequence.
- ♦ Enable batch refresh on terminal servers to improve the user login times when users log in simultaneously to access terminal server sessions. Create a Dword type registry key named EnableBatchRefresh and set the value to 1 at HKLM\Software\Novell\ZCM\.

D.5 Registry Keys and Configuration Files

In general, ZENworks login times do not differ much when the user logs in for the first time and when the user logs in after a device logout. However, users might experience certain tangible delays because various services take time during the Windows boot sequence. Loading various modules can cause a slowdown. Security and antivirus operations that are configured to run at startup, such as a disk scan configured to run on Windows startup, might also add to the perceived login delays. The following registry keys and application configuration files can reduce the user login times.

- ♦ [Section D.5.1, “Using Registry Keys to Reduce Login Time,” on page 186](#)
- ♦ [Section D.5.2, “Using Configuration Files to Reduce Application Startup Times,” on page 187](#)

D.5.1 Using Registry Keys to Reduce Login Time

Registry Key Name and Path	Description
Delete Nalview HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Registry Key Type: String Registry Key Value: %ZENworks_home%\bin\nalview.exe Use this key to disable Nalview (Novell Application Launcher) in environments where NAL icons do not need to be loaded such as the Desktop, Start menu, Quick Launch, taskbar, or Windows Explorer.
Delay HKLM\Software\NetWare\NAL\1.0	Registry Key Type: Dword Registry Key Value: In seconds Use this key to have NAL (Novell Application Launcher) read the icon's information with a delay equal to the value for this key. This helps the system's resources to handle non-ZENworks Configuration Management services or applications.
ZENLoginUserRefreshAsync HKLM\Software\Novell\ZCM\	Registry Key Type: String Registry Key Value: True Use this key to allow the ZENworks user login to happen simultaneously with the boot time device refresh that is asynchronously performed in the background.

Registry Key Name and Path	Description
Desired User Source	Registry Key Type: String
/HKLM/Software/Novell/ZCM/ZenLgn/	Registry Key Value: User Source Name
	Use this key to specify the ZENworks user source name.

D.5.2 Using Configuration Files to Reduce Application Startup Times

When assemblies are signed by Authenticode, the signed assemblies need to be verified by the certificate authority (CA). If the CA certificate is not on the same machine, the assemblies require network or Internet access. If the signed assemblies are installed on a device and if the CA certificate is not on the same device, then the .NET thread might time out while waiting to connect when there is no network or Internet access.

- ♦ [“Improving Application Startup Time in 10.3.x” on page 187](#)
- ♦ [“Improving Application Startup Time in 11.x” on page 187](#)

NOTE: Ensure that the device has the following configuration files for improved startup times.

Improving Application Startup Time in 10.3.x

- 1 Create the `ZenUserDaemon.exe.config`, the `ZenworksWindowsService.exe.config`, and the `ZenWindowsDaemon.exe.config` files in the `%ZENworks_Home%\ZENworks\bin` folder.
- 2 Copy the following content into all three files:

```
<configuration>
<runtime>
<generatePublisherEvidence enabled="false"/>
</runtime>
</configuration>
```

Improving Application Startup Time in 11.x

- 1 Create the `ZenUserDaemon.exe.config`, `ZenworksWindowsService.exe.config`, and `ZenWindowsDaemon.exe.config` files in the `%ZENworks_Home%\bin` folder.
- 2 Copy the content of the `ZESService.Exe.config` file that is located in the `%ZENworks_Home%\esm` folder into all three files.

D.6 ZENworks Configuration Management Policies

Some of the ZENworks Configuration Management policies are enforced in the pre-login, post-login and pre-desktop processes. Multiple policies and settings can lead to perceived slowness in ZENworks login times.

- ♦ [Section D.6.1, “Group Policy,” on page 188](#)
- ♦ [Section D.6.2, “DLU or Roaming Profile Policy,” on page 188](#)
- ♦ [Section D.6.3, “Printer Policy,” on page 188](#)
- ♦ [Section D.6.4, “LFR Policy,” on page 188](#)

D.6.1 Group Policy

Multiple Device or User Assigned Group policies might lead to slow logins. This is because the Group Policy settings of the policies are merged and the effective set of attributes to be enforced on the device is calculated in the pre-login process.

D.6.2 DLU or Roaming Profile Policy

- ♦ Any of the DLU and Roaming Profile policies or a combination of both of these policies can cause certain slow login experiences, especially when they are configured to be volatile.
- ♦ When you use DLU policies, you should configure non-volatile user profiles, if users must use the same device for a long period of time.
- ♦ When you use Roaming Profile policies, you should ensure that the shared profile path is reachable and that the profiles are uploaded and retrieved faster.

D.6.3 Printer Policy

Many Printer policies can make the end user feel that login is slow because it takes time to install all of the printers.

D.6.4 LFR Policy

A wrongly configured LFR (Local File Rights) policy (for instance, an LFR policy configured to set rights or permissions on a non-existent file or folder) can cause login delays. You need to consider this when you configure your LFR policies.

D.7 ZENworks Configuration Management Bundles

ZENworks Configuration Management bundles can cause slow logins under certain circumstances:

- ♦ If a large number of bundles is assigned, triggering considerable content metadata to be pushed in the initial refresh.
- ♦ If a large number of system requirements are associated with the bundles. The system requirements are evaluated to identify which bundle needs to be enforced on the device.
- ♦ If a large number of bundles are assigned to the device or user and are configured to be launched on login.
- ♦ If NALWIN is launched when the user logs in.

D.8 Logging in to a Terminal Server or Citrix Environment

ZENworks Configuration Management login in a Terminal server or a Citrix environment can be slow under the following circumstances:

- ♦ If there are more than 25 users logging in simultaneously, and each user has bundles configured to launch at login.
- ♦ If NAL is set to launch on user login in a terminal server environment

- If Random Refresh is disabled on the terminal server.
- If the Batch Refresh feature is not used. For information on batch refresh, see [Section D.4, “Best Practices to Optimize ZENworks User Login Times,”](#) on page 184

D.9 Troubleshooting Login Issues

Use the information in the following sections to troubleshoot login and authentication issues.

- [Section D.9.1, “Enabling the CASA Server and Client Logs,”](#) on page 189
- [Section D.9.2, “Time Synchronization,”](#) on page 190
- [Section D.9.3, “Checking Certificates,”](#) on page 190
- [Section D.9.4, “Checking ATS Status,”](#) on page 191

D.9.1 Enabling the CASA Server and Client Logs

- [“Capturing the ats.log and ats.trace on Authentication Servers”](#) on page 189
- [“Capturing the casaauthtoken.log on Managed Devices”](#) on page 189

Capturing the ats.log and ats.trace on Authentication Servers

1 Edit the `log4j.properties` file.

Windows Primary Server: The locations are:

`<%ZENworks_HOME%>\share\tomcat\conf\log4j.properties` (internal CASA)

`<%ZENworks_HOME%>\share\ats\etc\svc\log4j.properties` (external CASA)

Windows Satellite Server: The location is:

`<%ZENworks_HOME%>\ share\ats\etc\svc\log4j.properties`

Linux Primary Server: The locations are:

`\opt\novell\zenworks\share\tomcat\conf\log4j.properties` (internal CASA)

`etc\CASA\auttoken\svc\log4j.properties` (external CASA)

Linux Satellite Server: The location is:

`/etc/opt/novell/zenworks/conf/casa/log4j.properties`

2 Set the log mode to debug, and restart the ATS (Authentication Token Service).

NOTE: The names of the services are specified in [“Checking the CASA Service Status”](#) on page 191.

Capturing the casaauthtoken.log on Managed Devices

- 1 Create a folder. For example: `c:\logfolder`
- 2 Modify `<%ZENworks_HOME%>\casa\etc\auth\client.conf` to set the values of `DebugLevel` to 3 and `DebugLogFolderPath` to the desired log location. For example, `c:\logfolder`.
- 3 Restart the ZENworks Agent Service.

D.9.2 Time Synchronization

If the time on the managed device is not synchronized with the ZENworks Server, the managed device does not trust the certificate presented by the server. Ensure that devices are always time-synchronized. Also, ensure that you check the time synchronization with the eDirectory servers.

D.9.3 Checking Certificates

- ♦ [“Checking the Authentication Satellite Server’s DNS Suffix” on page 190](#)
- ♦ [“Importing the ATS Certificate” on page 190](#)
- ♦ [“Checking casa_crypto.properties” on page 190](#)
- ♦ [“Checking Certificate Properties” on page 191](#)

Checking the Authentication Satellite Server’s DNS Suffix

Ensure that the authentication Satellite Server has a primary DNS suffix specified prior to promoting the server. Generally the certificates are created against the device's (Satellite or Primary) FQDN or DNS name.

Importing the ATS Certificate

Ensure that the ATS (Authentication Token Service) certificate of a Satellite Server is imported into the trust store of the Primary Server by issuing the following commands:

- ♦ On the Windows Primary Server:

```
keytool -list -keystore "c:\program  
files\novell\zenworks\conf\security\trusted-ats-jks-store" -storepass secret
```

- ♦ On the Linux Primary Server:

```
keytool -list -keystore "/etc/opt/novell/zenworks/security/ trusted-ats-jks-  
store " -storepass secret
```

Checking casa_crypto.properties

Ensure that the `casa_crypto.properties` file, available at the locations specified below, is updated to show the correct keystore path. The trusted ATS keystore entry should map to the ZENworks keystore.

Windows Internal CASA

```
<%ZENworks_HOME%>\share\tomcat\webapps\CasaAuthTokenSvc\WEB-  
INF\classes\casa_crypto.properties
```

Windows External CASA

```
<%ZENworks_HOME%>\share\ats\catalinabase\webapps\CasaAuthTokenSvc\WEB-  
INF\classes\casa_crypto.properties
```

Linux Internal CASA

```
/opt/novell/zenworks/share/tomcat/webapps/CasaAuthTokenSvc/WEB-INF/classes/  
casa_crypto.properties
```

Linux External CASA

```
/srv/www/casaats/webapps/CasaAuthTokenSvc/WEB-INF/classes/casa_crypto.properties  
(/etc/opt/novell/zenworks/security/ trusted-ats-jks-store)
```

Ensure that the right certificates are present in the server store and the trusted store.

Checking Certificate Properties

- ◆ Ensure that the subject name in the server certificate matches the server host name or the server IP.
- ◆ Ensure that the certificate has not expired.

D.9.4 Checking ATS Status

- ◆ [“ATS Configuration Files” on page 191](#)
- ◆ [“Checking the CASA Service Status” on page 191](#)
- ◆ [“Checking the ATS Servlet” on page 192](#)
- ◆ [“Checking the Authentication Satellite” on page 192](#)
- ◆ [“Checking the User Source” on page 192](#)

ATS Configuration Files

Ensure that the ATS (Authentication Token Service) configuration files are present in the following locations:

- ◆ On Linux (Primary and Satellite): `\etc\CASA\authtoken\svc`
- ◆ On Windows (Primary and Satellite): `<%ZENworks_HOME%>\share\ats\etc\svc`

Ensure that the `iarealms.xml` file exists and verify whether the configured tee and search root are updated.

Ensure that the `auth.policy` files for the configured services are created under the `Enabled_Services` folder. If these files are missing, reconfigure the user source or restart the ZenLoader Service.

Checking the CASA Service Status

Ensure that the CASA services are up and running. On Windows, launch `services.msc`. On Linux, go to `/etc/init.d` and check the status of the service.

- ◆ **Primary Server External CASA ATS:** `casaAuthTokensvc` (Windows); `casa_atd` (Linux)
- ◆ **Primary Server Internal CASA ATS:** `novell-zenserver` (Linux); `Novell ZENworks Server` (Windows)
- ◆ **Windows Satellite:** `Novell ZENworks Authentication server`
- ◆ **Linux Satellite:** On Linux satellites, the authentication service runs within the ZMD (ZENworks Management Daemon) service.

If the CASA service has not started on the Linux server, verify that the PID file exists in: `/var/lib/CASA/authtoken/svc/casaatsd.pid`. If it exists, manually delete the file, and start the service again.

Checking the ATS Servlet

Ensure that the ATS servlet is listening on the configured ports by issuing the following command on the managed device:

```
https://<server_ip>:<port>/CasaAuthTokenSvc/Rpc
```

on the Managed Device.

If you receive a 400 error, this indicates that the servlet is listening but the browser has not formed the request in the required format.

Checking the Authentication Satellite

Ensure that the authentication Satellite (if it is configured) is accessible by typing `https://<server_ip>:<port>/zenworks-ping` in the browser. The browser should display Zenworks-Ping or Pong.

Checking the User Source

Verify that there is communication between CASA-ATS and the configured user source and ensure that you can browse through the users of the configured user source. Also, ensure that the LDAP server is not overloaded and server utilization is normal. LDAP server responses might directly impact login times.

E Documentation Updates

This section contains information on documentation content changes that were made in this *System Planning, Deployment, and Best Practices Guide* for Novell ZENworks 11 SP2. The information can help you to keep current on updates to the documentation.

The documentation is provided on the Web in two formats: HTML and PDF. The HTML and PDF documentation are both kept up-to-date with the documentation changes listed in this section.

If you need to know whether a copy of the PDF documentation you are using is the most recent, the PDF document contains its publish date on the front title page.

The documentation was updated on the following date:

- ◆ [Section E.1, “May 17, 2012: ZENworks 11 SP2,” on page 193](#)

E.1 May 17, 2012: ZENworks 11 SP2

Updates were made to the following sections:

Location	Update
Chapter 1, “ZENworks Configuration Management: A Single Solution for Systems Management,” on page 9.	Added a new section: Section 1.4, “Additional ZENworks Products,” on page 13.
Chapter 3, “Gathering Critical Information for Design Activities,” on page 21.	Added a new section: Section 3.2.4, “Tuning the JVM and Tomcat,” on page 31.
Chapter 4, “Performing Design Activities,” on page 69.	<ul style="list-style-type: none">◆ Added a new section: Section 4.2.2, “Tuning Adaptive Agent Parameters for Slow Links,” on page 75.◆ Added the following topics in Section 4.2.5, “User Sources,” on page 81:<ul style="list-style-type: none">◆ “Single Context:” on page 83◆ “Multiple Contexts:” on page 83◆ Added a new section in section “Macintosh Agent Install Packages” on page 96 in Section 4.2.10, “Adaptive Agent Deployment,” on page 95.
Appendix D, “Understanding the Performance and the ZENworks Login Process,” on page 181	Added a new appendix.
