ZENworks 2017 Update 4

Primary Server and Satellite Reference

January 2019

Legal Notice

About This Guide

This *ZENworks Primary Server and Satellite Reference* provides information about managing ZENworks Primary Servers and configuring devices to function as Satellites. The guide includes the following sections:

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 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 documentation Web site (http://www.novell.com/documentation/zenworks2017).

Contents

ZENworks Server

The ZENworks Server is the backbone of the ZENworks system. It communicates with the ZENworks Agent on managed devices to perform management tasks. It stores content to be delivered to devices and images to be used for imaging devices. It communicates with other ZENworks Servers and ZENworks Satellites to replicate or receive content, software and hardware inventory, and messages throughout the Management Zone.

The following sections provide additional information about the ZENworks Server:

1 ZENworks Services on a Windows Server

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

Table 1-1 *ZENworks Services on Windows*

Service	Service Name	Description
Novell Identity Store	micasad	Used by CASA(Common Authentication Service Adapter) to encrypt and store credentials entered by users. These credentials can be used to authenticate to additional network services.
Novell TFTP Service	novell-tftp	Used by PXE-enabled devices to request files that are needed to perform imaging tasks.
Novell ZENworks Agent Service	ZenworksWindowsService	Novell ZENworks primary agent provides application management and policy related services for managed desktops and servers.
Novell ZENworks Embedded Datastore	dbsrv12	Embedded database used for storing ZENworks objects and resources.
Novell ZENworks Embedded Datastore for Auditing	dbsrv12	Embedded datastore used for storing ZENworks Audit objects and resources.
Novell ZENworks ISD Service	novell-zisdservice	Used for synchronizing image-safe data with OS information.
Novell ZENworks Join Proxy	ZENJoinProxy	Allows ZENworks components to work with managed devices in a private network.
Novell ZENworks Loader	zenloader	Used for loading and controlling the Java services that perform ZENworks Server tasks.
Novell ZENworks Preboot Policy Service	novell-zmgprebootpolicy	Used by PXE-enabled devices to check for assigned preboot policies and work.
Novell 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.

Service	Service Name	Description
Novell ZENworks Remote Management powered by VNC	nzrwinvnc	Used to enable remote management of the server.
Novell ZENworks Server	zenserver	Used for communicating with the ZENworks Agent. An Apache Tomcat WebServer/Servlet engine that is used for hosting ZENworks web services and the ZENworks Control Center
Novell ZENworks Services Monitor	zenwatch	Used to monitor the status of critical ZENworks services and to restart them in case of failure.
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.
ZENworks Endpoint Security Service	zesservice	Used to support location awareness in the ZENworks Agent.
ZENworks Imaging Agent	ziswin (on Windows XP and Windows Server 2003) zisd (on Windows Vista, Windows Server 2008, Windows Server 2008 R2, Windows 7)	Used to save and restore image-safe data on the server (as a managed device). Only runs when launched by the ZENworks Agent.

The services reside in the `\novell\zenworks\bin` directory on a ZENworks Server. Refer to the following sections for instructions to help you control the ZENworks services:

- “Checking the Status of a ZENworks Service” on page 14
- “Starting the ZENworks Services” on page 14
- “Stopping the ZENworks Services” on page 15
- “Restarting the ZENworks Services” on page 15

Checking the Status of a ZENworks Service

1 On the server, click **Start**, select **Administrative Tools** > **Services**, then review the status of the services listed in Table 1-1 on page 13.

Starting the ZENworks Services

Do one of the following:

- Start the ZENworks services from the Services windows:
  1. Click the desktop **Start** menu.
  2. Click **Settings** > **Control Panel.**
  3. Double-click **Administrative Tools** > **Services**.
  4. Select the service you want to start (see Table 1-1 on page 13), then click **Start.**

- Start the ZENworks services from the command prompt:
  1. Execute the following command:

     `novell-zenworks-configure -c Start`

     By default, all the services and the `Start` option are selected.
  2. To start a specific service, specify the number next to the service, then press Enter.

     or

     To start all the services, press Enter.

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

Stopping the ZENworks Services

Do one of the following:

- Stop the ZENworks services from the Services windows:
  1. Click the desktop **Start** menu.
  2. Click **Settings** > **Control Panel.**
  3. Double-click **Administrative Tools** > **Services**.
  4. Select the service you want to stop (see Table 1-1 on page 13), then click **Stop.**
- Stop the ZENworks services from the command prompt:
  1. Execute the following command:

     `novell-zenworks-configure -c Start`
  2. To stop a specific service, specify the number next to the service you want to stop followed by the number next to the `Stop` action by using comma (,) as the delimiter, then press Enter.

     or

     To stop all the services, specify the number next to the `Stop` action, then press Enter.

Restarting the ZENworks Services

Do one of the following:

- Restart the ZENworks services from the Services windows:
  1. Click the desktop **Start** menu.
  2. Click **Settings** > **Control Panel.**
  3. Double-click **Administrative Tools** > **Services**.
  4. Select the service you want to restart (see Table 1-1 on page 13), then click **Restart.**
- Restart the ZENworks services from the command prompt:
  1. Execute the following command:

     `novell-zenworks-configure -c Start`

2. To restart a specific service, specify the number next to the service you want to restart followed by the number next to the `Restart` action by using comma (,) as the delimiter, then press Enter.

   or

   To start all the services, specify the number next to the `Restart` action, then press Enter.

2 ZENworks Services on a Linux Server

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

Table 2-1 *ZENworks Services on Linux*

Service	Service Name	Description
Novell TFTP Service	novell-tftp	Used by PXE-enabled devices to request files that are needed to perform imaging tasks.
Novell ZENworks Agent Service	novell-zenworks-xplatzmd	Used to enable the server as a managed device. Also used to support location awareness in the ZENworks Agent.
Novell ZENworks Embedded Datastore	sybase-asa	Embedded datastore used for storing ZENworks objects and resources.
Novell ZENworks Embedded Datastore for Auditing	`sybase-audit-asa`	Embedded datastore used for storing ZENworks Audit objects and resources.
Novell ZENworks Imaging Agent	novell-zislnx	Used to save and restore image-safe data on the server (as a managed device). Only runs when launched by the ZENworks Agent.
Novell ZENworks Join Proxy	`novell-zenjoinproxy`	Allows ZENworks components to work with managed devices in a private network.
Novell ZENworks Loader	novell-zenloader	Used for loading and controlling the Java services that perform ZENworks Server tasks.
Novell ZENworks Preboot Policy Service	novell-zmgprebootpolicy	Used by PXE-enabled devices to check for assigned preboot policies and work.
Novell 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.
Novell ZENworks Server	novell-zenserver	Used for communicating with the ZENworks Agent.
Novell ZENworks Services Monitor	novell-zenmntr	Used to monitor the status of the ZENworks services.

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.

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

- “Checking the Status of a ZENworks Service” on page 18
- “Starting the ZENworks Services” on page 18
- “Stopping the ZENworks Services” on page 18
- “Restarting the ZENworks Services” on page 19

Checking the Status of a ZENworks Service

1 At the console prompt, enter the following command:

`/etc/init.d/servicename status`

Replace *servicename* with the name of the service as listed in Table 2-1 on page 17.

Starting the ZENworks Services

- To start a ZENworks service, do one of the following:
  - Enter the following command at the console prompt:

    `/etc/init.d/servicename start`

    Replace *servicename* with the name of the service as listed in Table 2-1 on page 17.
  - At the console prompt, execute `/opt/novell/zenworks/bin/novell-zenworks-configure -c Start`, specify the number next to the service you want to start, then press Enter.
- To start all the ZENworks services:
  1. Execute the following command at the server prompt:

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

     By default, all the services and the `Start` option are selected.
  2. Press Enter.

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

Stopping the ZENworks Services

- To stop a service, do one of the following:
  - Enter the following command at the console prompt:

    `/etc/init.d/servicename stop`

Replace *servicename* with the name of the service as listed in Table 2-1 on page 17.

- At the console prompt, execute `/opt/novell/zenworks/bin/novell-zenworks-configure -c Start`, specify the number next to the service you want to stop, then press Enter.

- To stop all the ZENworks services:
  1. Execute the following command at the server prompt:

     `/opt/novell/zenworks/bin/novell-zenworks-configure -c Start`
  2. Enter the number next to the `Stop` action.

Restarting the ZENworks Services

- To restart a service that is already running, do one of the following:
  - Enter the following command at the console prompt:

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

    Replace *servicename* with the name of the service as listed in Table 2-1 on page 17.
  - At the console prompt, execute `/opt/novell/zenworks/bin/novell-zenworks-configure -c Start`, specify the number next to the service you want to restart, then press Enter.
- To restart all the ZENworks services:
  1. Execute the following command at the server prompt:

     `/opt/novell/zenworks/bin/novell-zenworks-configure -c Start`
  2. Enter the number next to the `Restart` action.

3 Configuring Additional Access to a ZENworks Server

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

Addressing Non-Detectable IP Address Conditions

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

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

   IP Address: Standard dotted-decimal notation. For example, `192.168.0.1`.
3. Click **Add** to add the address to the list.
4. Repeat Step 1 to Step 3 to add additional IP addresses.
5. If necessary, use the **Move Up** and **Move Down** buttons to reorder the list.

   The IP addresses are used in the order listed, from top to bottom.
6. When you are finished adding addresses, click **Apply** or **OK** to save the addresses.

Addressing Non-Detectable DNS Name Conditions

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

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

To add a DNS name:

1. In ZENworks Control Center, click **Devices** in the left pane, select **Servers** in the Devices panel, select a server object, click the **Settings** tab, click **Infrastructure Management**, then select **Additional DNS Names**.
2. In the **List of Server DNS Names** field, specify the DNS name for the IP address of the server (such as a proxy server) that the devices can access.
3. Click **Add** to add the DNS name to the list.
4. If necessary, use the **Move Up** and **Move Down** buttons to reorder the list.

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

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

4 Configuring Restricted Access to a ZENworks Server

You can configure a list of IP addresses for the ZENworks server that should not be visible to the registration agent.

NOTE: The Restrict IP Addresses page is available only for Primary Servers and Satellite Servers.

To automatically move the newly added IP addresses to the **Restricted IP Addresses** list:

1. In ZENworks Control Center, click **Devices** in the left pane, select **Servers** in the Devices panel, select a server object, click the **Settings** tab, click **Infrastructure Management**, then select **Restricted IP Addresses**.
2. Select the **Restrict new IP addresses by default** option. The newly added IP addresses will be invisible to the ZENworks agent.

To restrict IP addresses:

1. In ZENworks Control Center, click **Devices** in the left pane, select **Servers** in the Devices panel, select a server object, click the **Settings** tab, click **Infrastructure Management**, then select **Restricted IP Addresses**.
2. Click the address in the Visible IP Addresses list, then click > to move that IP address to the Restricted IP Addresses list.

To make a restricted IP address visible to the registration agent:

1. In ZENworks Control Center, click **Devices** in the left pane, select **Servers** in the Devices panel, select a server object, click the **Settings** tab, click **Infrastructure Management**, then select **Restricted IP Addresses**.
2. Click the address in the Restricted IP Addresses list, then click < to move that IP address to the **Visible IP Addresses** list.

IMPORTANT: If there is only one IP address in the **Visible IP Addresses** list, do not move it to the **Restricted IP Addresses** list. Otherwise, the ZENworks agent cannot see the IP address of the server. The ZENworks agent should be able to see at least one IP address of the server.

5 Determining the ZENworks Software Version Installed on Servers

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

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

1. In ZENworks Control Center, click the **Devices** tab.
2. Click **Servers**, then click the desired Primary Server.
3. View the version number in the **ZENworks Configuration Management Version**, **ZENworks Asset Management Version**, **ZENworks Patch Management Version**, **ZENworks Endpoint Security Management** and **ZENworks Full Disk Encryption** rows.
4. (Optional) Click the underlined version number next to **ZENworks Configuration Management Version** to see a list of installed packages.

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

1. In ZENworks Control Center, click the **Configuration** tab.
2. In the Server Hierarchy panel, view the version information in the **ZCM Version**, **ZAM Version**, **ZPM Version**, **ZESM Version** and **FDE Version** columns for each server.

6 Uninstalling a ZENworks Server

Instructions for uninstalling a ZENworks Server are provided in the *ZENworks Uninstall Guide*.

7 Deleting a ZENworks Primary Server

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

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

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

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

If you remove a Primary Server on which the Patch Management subscription service is configured to run, you must reset the Patch Management settings before deleting the server. For more information on how to reset the Patch Management settings, see "Viewing and Configuring the Subscription Service" in the *ZENworks 2017 Patch Management Reference*.

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

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

To remove a ZENworks Primary Server from your Management Zone:

1. In ZENworks Control Center, click the **Configuration** tab.
2. In the Server Hierarchy section, select the check box next to the Primary Server (you can select multiple devices).
3. Click **Action** > **Delete ZENworks Server**.

8 Troubleshooting ZENworks Server

Server installation will fail on a Windows server if the free space is less than 20 GB

Source: ZENworks, ZENworks Server

Explanation: Server installation fails on a Windows server, if you select a drive which has free space less than 20 GB.

Action: Re-initiate the installation process and select another drive that has at least 20 GB of free space.

The ZENworks Application Window (ZAPP) might not work when you upgrade a server from Windows 2008 to 2012 and then you upgrade to ZENworks 2017

Source: ZENworks, ZENworks Server

Explanation: The ZENworks Application Window (ZAPP) might not work, when you upgrade the Primary Server from ZENworks 11.4.x to ZENworks 2017 after upgrading the operating system from Windows Server 2008 to Windows Server 2012.

Action: After upgrading the operating system, manually install the latest .NET Framework (4.5.x), and then upgrade the Primary Server.

When a second Primary Server is added to the zone, an out of memory error message might be displayed

Source: ZENworks; ZENworks Server

Explanation: When a second Primary Server is added to the zone, though the installation is successful, you might receive an error message indicating that the installation failed due to insufficient memory.

Action: None, Ignore the message.

The casa_atsd service on a Linux server fails to start

Source: ZENworks; ZENworks Server

Explanation: On a Linux server, if you choose to manually start the `casa_atsd service` that is in the unused state, the service fails to start.

Action: If the `casaatsd.pid` file exists within the `/var/lib/CASA/authtoken/svc/` directory, delete the file and then restart the service.

Unable to start the ZENworks Services on a Windows Primary Server

Source: ZENworks; ZENworks Server

Explanation: After you reboot or restart a Windows Primary Server, the ZENworks Services fail to start. If you choose to manually start the services, the following error message is displayed: `Error 1609: The service did not start due to a logon failure.`

Possible Cause: A group policy setting, applied on the server, has revoked the `log on as a service` right for the specified user account.

NOTE: Most of the ZENworks Services run as a privileged user account. This account can be identified based on the following naming convention: `__z_x_y__`, where *x* and *y* are the last two digits of the IP address of the server, added at the time of installation.

Action 1 (Mandatory): Configure the applied group policy setting to add the user account to the list of accounts that possess the `log on as a service` right.

Action 2 (Optional): If the ZENworks Services do not start after performing Action 1, perform the following steps:

1. Start the `Local Security Settings MMC` snap-in.
2. Expand **Local Policies**, and then click **User Rights Assignment**.
3. In the right pane, right-click **Log on as a service**, and then click **Security**.
4. Add the user to the policy, and then click **OK**.
5. Close the `Local Security Settings MMC` snap-in.

9 ZENworks SWEET32 Vulnerability

Primary and Satellite Servers are vulnerable to SWEET32.Perform the steps provided in the following ZENworks Servers to overcome the SWEET32 Vulnerability:

On Primary Servers:

1. Backup the server.xml in the following location:
   - **On Windows:** `%ZENworks_HOME%/share/tomcat/conf/`
   - **On Linux:** `/opt/novell/zenworks/share/tomcat/conf/`
2. In the server.xml file, remove the following ciphers attribute in the Connector element:
   - `SSL_RSA_WITH_3DES_EDE_CBC_SHA`
   - `TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA`
   - `TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA`
   - `TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA`
   - `TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA`
3. Restart the services by running the `novell-zenworks-configure -c Start` command.

NOTE: If the zone is upgraded to 2017 Update 1 or later versions, then these steps are not required.

On Appliance Primary Server:

1. Backup the jetty-ssl.xml file available in the /opt/novell/jetty8/etc/ location.
2. Under the Call element in the jetty-ssl.xml file, move the following ciphers from **IncludedCipherSuites** to **ExcludedCiphers**:
   - `SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA`
   - `SSL_RSA_WITH_3DES_EDE_CBC_SHA`
   - `TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA`
   - `TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA`
   - `TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA`
   - `TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA`
3. 3.Restart the services by running the `novell-zenworks-configure -c Start` command.

NOTE

- In addition to performing these steps, perform the steps mentioned in “On Primary Servers:” on page 33.

On Satellite Servers

To address the SWEET32 vulnerability on the Satellite Servers, exclude the following set of ciphers in the `zenworks-ssl.conf` file. Manually create the `zenworks-ssl.conf` file in the following locations:

- **On Windows:** `ZENworks install path/novell/zenworks/conf/`
- **On Linux:** `/etc/opt/novell/zenworks/conf/`

Add the *ExcludeCipherSuites* key name in the `zenworks-ssl.conf` file. The key name should not be modified:

```
ExcludeCipherSuites=SSL_RSA_WITH_3DES_EDE_CBC_SHA,
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
```

NOTE: By default ciphers are not excluded to address the SWEET32 vulnerability, as the communication breaks between agents with Windows XP and Satellite Servers.

IMPORTANT: Fixing the SWEET32 vulnerability requires to remove weak ciphers. This causes older Windows versions to have less or no common ciphers to establish communication with the server. Hence, fixing SWEET32 vulnerability issue breaks communication from Windows XP or Windows 2003 devices.

10 Configuring a Primary Server as an MDM Server

This feature is applicable for mobile devices only. For more information, see Configuring an MDM Server.

11 Firewall Rules and Exceptions

Ensure that the firewall rules allow outbound connections to the following addresses as you might not be able to download System Update, PRU, Patches and ZENworks NEWS.

- Primary Server performs the ZENworks System Update Entitlement registration or activation over HTTPS (port 443) using the secure-www.novell.com (https://secure-www.novell.com) website. This rule can be turned off after successfully completing the entitlement activation.
- ZENworks System Update, PRU (Checks and Downloads) and ZENworks NEWS are shared over HTTPS (port 443) using the nu.novell.com (https://nu.novell.com) website.

For more information on list of Patch provider websites that requires outbound connectivity to download patches, see Patches are unavailable because of connectivity or firewall issues.

For more information of TCP and UDP ports used by ZENworks Primary Servers, see TCP and UDP Ports Used by ZENworks Primary Servers.

Satellites

A Satellite is a managed device that can perform some of the roles that a ZENworks Primary Server normally performs, including authentication, information collection, content distribution, and imaging. A Satellite can be any managed Windows or Linux device (server or workstation), but not a Primary Server. For more information, see Managed Device Requirements" in the *ZENworks 2017 Update 4 System Requirements* and "Deploying the ZENworks Agent" in the *ZENworks Discovery, Deployment, and Retirement Reference*.

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

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

NOTE: For information about Satellites from the perspective of an end user using the ZENworks Agent, see "Satellite Roles" in the *ZENworks Agent Guide*.

The following sections contain more information:

12 Understanding the Satellite Roles

A Satellite is a device that can perform some of the roles that a ZENworks Primary Server normally performs, including authentication, information collection, content distribution, and imaging. The following sections contain more information about each role:

Understanding the Authentication Role

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

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

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

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

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

Understanding the Collection Role

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

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

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

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

To redirect collection roll-up from the satellite to a different server, configure the PreferredCollectionRollUpServer registry key. This will re-route the collection roll-up to an alternate Primary Server that you can rely on temporarily instead of the configured Parent Primary server.To assign a different primary server for collection roll-up, create the PreferredCollectionRollUpServer registry key. This key specifies the alternate server that will be used for collection roll-up. For more information, see PreferredCollectionRollUpServer in the *ZENworks Registry Keys Reference*.

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

Understanding the Content Role

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

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

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

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

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

Understanding the Imaging Role

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

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

On the managed device, the Imaging module is inactive until you promote the managed device to be a Satellite with the Imaging role or until the Imaging role is added to an existing Satellite. This activates the Imaging services on the device, and enables you to perform the Imaging operations in auto and maintenance mode. The Imaging services installed on the device include TFTP, Preboot policy, pbserv, and proxy DHCP. All services, except for proxy DHCP, are automatically started. You can manually start or stop the proxy DHCP service from ZENworks Control Center.

Understanding the Join Proxy Role

Join Proxy is a Primary Server or a Satellite with the Join Proxy role that acts as a proxy by accepting and maintaining connections from Windows managed devices that are in a private network.

Join Proxy when used for remote management operations joins two connections together. The first connection being the one that the managed device maintains with the proxy server while the second one is the connection that comes from the viewer machine of the administrator.

In ZENworks, Join Proxy is a role that is by default assigned to the Primary Servers while you can also assign this role to Satellites. If you choose a Primary Server for the Join Proxy role, there is no need to further configure the server. If you choose a Satellite, then you need to assign the Join Proxy role to the Satellite server.

When a Join Proxy is used, the ZENworks Agent first connects to the Join Proxy server if its location is configured with a Join Proxy server. The agent then initiates a TCP connection to the Join Proxy Server and then periodically checks in to keep the connection alive. The ZENworks administrator will be able to remotely manage the device only If the Join Proxy server is reachable by both the ZENworks administrator and the managed device.

For example, if a device is located in a hotel room behind a NAT (Network Address Translation) the administrator cannot directly contact the machine. In this context, the administrator can only use the Join Proxy to reach the managed device.

13 Adding and Configuring Satellite Devices

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

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

- The ZENworks version installed on the managed device must be the same as that of the Primary Server.

  NOTE

  Ensure that you update the Satellite Server to the latest version of ZENworks before you promote to any role.

- You cannot promote the following devices as a Satellite:
  - A managed device that has a previous version of ZENworks Agent (version 10.*x* or 11.x) installed.
  - A ZENworks 11.*x* test device.
- You cannot change the Satellite roles and settings for the existing Satellites until you upgrade the Satellites to ZENworks. For more information on how to upgrade Satellites to ZENworks, see "Updating Satellites and Managed Devices to ZENworks 2017" in the *ZENworks Upgrade Guide*.
- For a MAC device that has been promoted as a Satellite, only the Collection and Content roles are available.

The following sections contain more information:

Tasks for Adding and Configuring Satellites

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

or

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

You can only configure one Satellite at a time.

or

To configure an existing Satellite from the device view, in ZENworks Control Center, click the **Devices** tab, then on the **Managed** tab, click either **Servers** or **Workstations**. In the Servers or Workstations panel, select the check box for the Satellite that you want to configure, click **Action**, then click **Configure Satellite Server**.

You can only configure one Satellite at a time.

Depending on whether you are adding a new Satellite device or configuring an existing device, the title of the dialog box is different (Add Satellite Server or Configure Satellite Server). The settings and options on each page are similar.

You can also use the `zman satellite-server-create (ssc)` command to add or configure roles for a Satellite. For more information, see "Satellite Commands" in the *ZENworks Command Line Utilities Reference*.

2 Click the **General** tab to specify the basic information about the satellite server, including the roles of the server. (Conditional) To remove Satellite roles from a device, deselect the desired role in the Satellite Server Roles section, then click **OK**.

You can also use the `zman satellite-server-delete (ssd)` command to remove roles from a Satellite. For more information, see "Satellite Commands" in the *ZENworks Command Line Utilities Reference*.

3 (Conditional) To add a role to a Satellite, select the desired role in the **Satellite Server Roles** section.

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

See the following sections for more information about each role:

- "Authentication Role" on page 47
- "Collection Role" on page 49
- "Content Role" on page 49
- "Imaging Role" on page 51

4 Click the **Server Settings** tab to view the default port and throttle rate settings. You can changethese default values if required.

Port for Content and/or Collection HTTP Requests: In this field specify the port number (Optional). The default port is 80. Content and Collection servers share the same Web server and the same port. Make sure that the specified port is not in use.

Port for authentication Secure HTTPS requests: In this field, specify the port number. The default port is 443. This is the port on which the Satellite device listens while communicating with the managed devices. Make sure that the specified port is not in use.

Satellite Server Output Throttle Rate (in kbps): In this field, specify the rate at which the Satellite server should send the content to other devices requesting the content. These devices could be either other content satellite servers or managed devices. Satellite server calculates different throttle rates in the following scenarios:

- A Single content request with the Content type throttle
- A Single content request without the Content type throttle

- Multiple requests without the Content type throttle
- Multiple requests with the Content type throttle

For more information, see “Satellite Server Output Throttle Rate Calculations” on page 55.

5 Click the **Content Replication** tab to select one of the listed content replication methods.

A satellite with the Content role replicates content from other satellite content servers by using one of the following methods:

Use Parent Primary Server Only: This is the default content replication method. The satellite replicates content only from its parent primary server (as configured during the satellite promotion.

Use Closest Content Servers First: Select this option if you want the Satellite server to look for a content repository hosted in the CIFS location (if it is configured) or closest content servers first, to replicate the content.

If the CIFS location is not configured or if content is not found in the CIFS location, the Satellite Server checks the closest content servers for content replication before trying to use the parent Primary Server.

The CIFS share or the closest servers will be determined by the Location or the Network environment that is effective on the Satellite.

Use Closest Content Servers Only: Select this option if you want the Satellite Server to look for a content repository hosted in the CIFS location (if it is configured) or closest content servers only to replicate the content. If the CIFS location is not configured or if content is not found in the CIFS location, the Satellite Server checks the closest content servers for content replication. If content is not found on the closest servers as well, the replication will fail.

The CIFS share or the closest servers will be determined by the Location or the Network environment that is effective on the Satellite.

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

7 Repeat the previous steps to configure other Satellites.

8 Specify the devices that need to use this Satellite for the Collection Roll-Up, Content, Authentication and Imaging roles.

9 To configure the Location Closest Server for this Satellite:

9a On the **Configuration** page, click the **Locations** tab.

9b In the **Locations** panel, click the location for which you want to configure the Closets Servers rules.

9c Click the **Severs** tab.

9d Configure the location closest servers.

Authentication Role

This role helps speed the authentication process by spreading the workload among various devices and by performing authentication locally to managed devices.

- “Prerequisites to Configure the Authentication Role on a Satellite” on page 48
- “Configuring the Authentication Role on a Satellite” on page 48

Prerequisites to Configure the Authentication Role on a Satellite

If you have installed ZENworks with external certificates, you must complete the following tasks on the Satellite before configuring the Authentication role on a Satellite:

1. Ensure that the Satellite has its own individual server certificate and private key.

   For detailed information on how to create to an external certificate, see "Creating an External Certificate" in the *ZENworks Server Installation Guide*.

2. Import the external certificate by using the `zac iac` command on the Satellite.

   For more information about zac, view the zac man page (man zac) on the Satellite or see the *ZENworks Command Line Utilities Reference*.

NOTE: You must import the external certificate each time you promote the Satellite to Authentication role.

Configuring the Authentication Role on a Satellite

1. (Optional) To configure the Authentication role on a Satellite, select the check box next to **Authentication**, click **Configure** to display the Configure Authentication dialog box.
2. Specify the authentication port.
3. Select a user source from the User Source drop-down list.
4. Click **Add** to display the Add User Source Connections dialog box.

   Fill in the fields:

   Connection Name: (Optional) Specify all or part of the name for the connection to the LDAP directory, then click **Filter** to display the list of connections that match the criteria.

   If you have many connections in your ZENworks Management Zone, you can use the **Connection Name** field to display only those connections that match the criteria. For example, to display all connections that contain the word "London," type `London` in the **Connection Name** field, then click **Filter**.

   Connection Address: (Optional) Specify part of the IP address or DNS hostname of the connection to the LDAP directory, then click **Filter** to display all connections with that IP address.

   If you have many connections in your ZENworks Management Zone, you can use the **Connection Address** field to display only those connections that match the criteria. For example, to search for and display all connections that have an IP address starting with 172, type 172 in the **Connection Address** field, then click **Filter**.

   User Source Connections: Select the check box next to the connection you want to add.
5. Click **OK** to return to the Configure Authentication dialog box.
6. (Optional) Reorder the connections in the User Source Connection list by selecting a connection's check box, then clicking **Move Up** or **Move Down**.

   The device uses the connections in the order they are listed to authenticate the device to the ZENworks Management Zone.
7. Click **OK** to return to the Add Satellite Server or Configure Satellite Server dialog box.
8. Continue with Step 4 on page 46.

NOTE

Any change made to an Authentication satellite server in the Zone will trigger a device refresh through the Quick Task feature. If the Authentication satellite is modified, it will cause all the Authentication satellite servers in the Zone to refresh. This may lead to the creation of excessive Quick Tasks, resulting in the clogging of database.

To prevent the creation of excessive Quick Tasks, you can configure the Quick Task refresh interval by editing the `quicktask_trigger_interval` field in the file named `quicktask.properties`. This file can be accessed from the following location:

- **On Windows:** `ZENworks_installation_path\novell\zenworks\conf\quicktask`
- **On Linux:** `/etc/opt/novell/zenworks/conf`

By default, the Quick Task refresh interval value is set as 600 minutes (10 hours).If changes are made to the satellite server within the predefined refresh interval, a new Quick Task will not be created. The new changes will get reflected on the managed devices when the next system refresh is performed.

Collection Role

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

1. Select the check box next to **Collection**, then click **Configure**.
2. Fill in the field:

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

   The Collection Roll-Up schedule determines how often the collected inventory information is rolled up to the parent Primary Server for inclusion in the ZENworks database. When the information is in the database, it is viewable in ZENworks Control Center.
3. Click **OK**.
4. Continue with Step 4 on page 46.

Content Role

This role enables the managed device to distribute content (bundles, policies, system updates, and patches) to other devices.

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

1. Select the check box next to **Content**, click **Configure**, then click **Add**.

   Fill in the fields:

   Content Type: Select a Content Type (for example, **Policy**, **Non-Patch Bundles**, or **System Update** Server).

   NOTE

If you choose **Imaging** as the **Content Type** and configure the settings to replicate the Imaging content, these settings are automatically reflected in the Configure Imaging Content Replication dialog box invoked while configuring the Imaging role to the device. Similarly, the Imaging content replication settings configured while configuring the Imaging role to a device are automatically reflected in the Configure Content Type Replication dialog box invoked while configuring the Content role with the Imaging content type to the device.

Throttle (in KB/sec): Select the throttle rate. This rate specifies the maximum rate at which content (in kilobytes per second) is replicated. The actual rate can be lower, depending on other factors, including the number of downloads.

NOTE: The specified throttle speed only controls the rate at which ZENworks delivers content, it does not control the rate at which the NIC sends data to other applications. Thus the total bandwidth used by the server's NIC may be greater than the throttle speed set.

To view the traffic from ZENworks alone, you need to filter on the ports configured for your server. For example 80 and 443.

Duration: Click the up-arrow or down-arrow to set the content update duration period in minutes. Depending on the Schedule Type and its options you select, you need to be aware of the following:

- The **End Time** setting in all three scheduling types (**Days of the Week**, **Month**, and **Fixed Interval**) is not the true end time when the content update stops processing. The end time specifies the end of the time period during which an update can start. For Fixed Interval replication in a newly promoted Satellite Server, the replication starts with a minimum delay of 1 day.

  If you select **Days of the Week** or **Month** and set a random start and end time, the update starts between these times and continues for the specified duration. For example, if the **Duration** is set at the default of 60 minutes and the update starts 10 minutes before the specified end time, content is updated for the entire 60 minutes. The same concept applies for the **Fixed Interval** schedule. If **Duration** is set at the default of 60 minutes and the end time does not allow enough time for the specified duration, content is updated for the entire 60 minutes.

- If the Primary Server contains too much content to update during the specified duration, the update continues at the next regularly scheduled time. Content that already exists on the Satellite device is not updated again. Content that was not updated during the previous update and any new content added to the Primary Server is updated.

After the completion of content replication, if there is no content to replicate when the satellite queries for the missing content on the primary server, you can add more time in between the content replication retries in a given content replication duration. This will reduce the load on the primary server and the database.

If there is no content to replicate, the satellite content query interval doubles each time. By default the first wait is 10 minutes. For instance, the first query interval would be at 10 minutes, the next at 20, then 40, 80, 160, and so on until the interval has reached the maximum wait time of 1440 minutes. At any point of time, if the content for replication is found, then the query interval is reset to 10 minutes.

You can configure the initial wait time with the following registry key:

For Windows:

```
HKLM\SOFTWARE\Novell\ZCM: CDPRestartInterval (Reg_SZ): Seconds to wait
```

For Linux:

`/etc/opt/novell/zenworks/conf/xplatzmd.properties CDPRestartInterval=Seconds to wait`

Schedule Type: Select a schedule for how often you want the Satellite's content to be updated from the parent Primary Server:

- **No Schedule:** If you select **No Schedule**, content is never automatically updated from the parent Primary Server. To manually replicate the content run the `zac wake-cdp (cdp)` command on the Satellite.
- **Recurring:** Select **Days of the Week**, **Monthly**, or **Fixed Interval**, then fill in the fields. For more information, see "Recurring" on page 135.

  You should also consider the following:

  - We recommend you to set the schedule to 12 hours.
  - When you change the default Zone level Content Replication Schedule, the new schedule is not applied to the existing Satellite Servers that have been promoted to the Content role. For the new Content Replication Schedule to be applied to the promoted Satellite Servers, you can either demote and then promote the Satellite Servers to the Content role or you can edit the default Content Replication Schedule for each promoted Satellite Server.

Be aware that the cleanup action for content occurs every night at midnight.

If you do not set a schedule for a particular type of content, the **<Default>** schedule applies to all content of that type.

2. Click **OK** twice to return to the Add Satellite Server or Configure Satellite Server dialog box.
3. Continue with Step 4 on page 46.
4. (Optional) Specify the content to host on the Content Server. For more information, see "Including or Excluding Content" on page 106.

   If you want to specify the content that the Satellite hosts, you can include or exclude content from being replicated to it.

   If you want to include content that its parent Primary Server does not have, you must first add the content to the parent Primary Server.

Imaging Role

Selecting this option installs the Imaging services and adds the Imaging role to the device. With this role, the device can be used as an Imaging server to perform all the Imaging operations, such as taking an image, applying an image, and multicasting an image. However, the ZENworks images are not replicated from the Primary Server to Imaging Satellites.

NOTE: The Imaging role is tied to the state of your ZENworks Configuration Management license. If your license state is deactivated, the Imaging role is disabled. For example, if you have a licensed copy of ZENworks Asset Management and you are evaluating ZENworks Configuration Management, the Imaging role is disabled if your ZENworks Configuration Management license expires. For more information, see "Possible License State Changes" in the *ZENworks Product Licensing Reference*.

---

1. Select the check box next to **Imaging**, then click **Configure**.
2. (Conditional) Select the check box next to **Enable PXE Services** to automatically start the Proxy DHCP service on the device to which the Imaging Server role has been assigned.

To check whether the Proxy DHCP service has been started on the device, review the message log of the device (**Devices** tab > **Workstations** folder > click the workstation > **Summary** > Message Log panel).

3 (Conditional) Select the check box next to **Delete Image Files from the Server if Imaging Role is Removed** if you want the ZENworks image files to be automatically deleted from the device when the Imaging role is removed from the device.

The messages are logged in the Message Log panel if the severity level of the local file and the system log is set to **Information and Above** on the Local Device Logging page. (**Configuration** tab > **Device Management** > **Local Device Logging**).

This option is available only when you want to remove the Imaging Server role from the device.

4 Click **Options** next to **Configure Imaging Content Replication** to launch the Configure Imaging Content Replication dialog box.

The Configure Imaging Content dialog box lists a default configuration that applies to the imaging content, with a fixed interval schedule of every five minutes, no throttling, and a 60-minute content replication period.

5 Configure the Imaging content replication settings.

5a Select a throttle rate (in KB/sec). This rate specifies the maximum rate at which content (in kilobytes per second) is replicated. The actual rate can be lower, depending on other factors, including the number of downloads.

5b Select the duration of the content replication.

When you set the duration, be aware of the following:

- The **End Time** setting in all three scheduling options in the Recurring schedule type (**Days of the Week**, **Month**, and **Fixed Interval**) is not the end time when the content stops replicating. The start and end time settings specify the time period during which a replication can start.

  If you select **Days of the Week** or **Month** and set a random start and end time, the replication starts between these times and continues for the specified duration. For example, if the **Duration** is set at the default of 60 minutes and replication starts 10 minutes before the specified end time, content is replicated for the entire 60 minutes. The same concept applies for the **Fixed Interval** schedule. If **Duration** is set at the default of 60 minutes and the end time does not allow enough time for the specified duration, content is replicated for the entire 60 minutes.

- If the Primary Server contains too much content to replicate during the specified duration, the replication continues at the next regularly scheduled time. Content that already exists on the Satellite device is not replicated again. Content that was not replicated during the previous replication session and any new content added to the Primary Server is replicated.

5c Select a schedule (**No Schedule** or **Recurring**).

The Imaging Content Replication schedule determines how often the imaging content is sent down from the parent Primary Server to its child Satellite. Be aware that the cleanup action for content occurs every night at midnight.

If you do not set a schedule, the **<Default>** schedule applies to the Imaging content.

5d Click **OK** to save the changes.

NOTE: You can also configure the Imaging content replication settings while configuring the Content role to a device. These settings are automatically reflected in the Configure Imaging Content Replication dialog box invoked while configuring the Imaging role to the device. Similarly, the Imaging content replication settings configured while configuring the

Imaging role to a device are automatically reflected in the Configure Content Type Replication dialog box invoked while configuring the Content role with Imaging content type to the device.

6 Click **OK**.

7 (Conditional) If you configure the Imaging role, the role is immediately added to the device. If the role is not immediately added, it is added only during the next device refresh schedule. If you want to immediately apply the role to the device, manually refresh the device in one of the following ways:

- In the ZENworks Control Center, click the **Configuration** tab > the **Server Hierarchy**, select the check box next to the devices you want to refresh, then click **Action** > **Refresh Device**.
- On a managed device, do one of the following:
  - Right-click the icon, then click **Refresh**.
  - Execute the `zac ref` command from the console prompt.

To check whether the Proxy DHCP service has been started on the device, review the message log of the device (**Devices** tab > **Workstations** folder > click the workstation > **Summary** > Message Log panel or **Devices** tab > **Servers** folder > click the server > **Summary** > Message Log panel).

The messages are logged in the Message Log panel only if the severity level of the local file and the system log is set to **Information and Above** on the Local Device Logging page. (**Configuration** tab > **Device Management** > **Local Device Logging**).

8 (Conditional) If the Linux Satellite has the Imaging role configured, turn off the firewall on the device before performing imaging operations.

IMPORTANT: Imaging content refers to files present in the TFTP folder and the imaging content does not include images available in the server.

TFTP folder location:

- **On Windows:** `%ZENWORKS_HOME%\share\tftp`
- **On Linux** `/srv/tftp`

Join Proxy Role

If you want to remotely connect a managed device that is in a private network or on the other side of a firewall or router that is behind NAT (Network Address Translation), a remote management proxy server should be installed on the same NAT environment that the device is in. For this, an interface machine is required.

Finding the interface machine is difficult in cases where the Managed device is moved out of the zone to home. As each individual home is a NAT environment, one remote management proxy is required for each home to remotely control the device in home. There is no single remote management proxy for devices across many NAT environments. Different remote management proxy servers are required for different NAT environments.

However you can use the Join Proxy Satellite server that allows multiple devices to connect to it for remote management operations. The devices will connect to the Join Proxy based on the locations configured for them, so an interface machine is not required. You can easily promote a device to and demote a device from the Join Proxy role.

You can add Join Proxy role to a ZENworks 11.3 or later version of a Windows or Linux managed device to make it a Join Proxy server for performing remote management operations on Windows managed devices that are in a private network.

NOTE: Primary servers by default have a Join Proxy role. If you select a Primary Server for the Join Proxy role, there is no need to further configure the server in ZENworks Control Center. However, you can reconfigure the Join Proxy configuration settings by manually editing the joinproxy.properties file on the Primary Server device in the following location:

`ZENWORKS_HOME\conf\`

Configuring Join Proxy Closest Server rules for the location and network environment helps the managed devices to connect to the closest Join Proxy servers defined for them in the location. For more information, see "Creating Closest Server Rules for a Location" and "Creating Closest Server Rules for a Network Environment " in *ZENworks Location Awareness Reference*.

Example 13-1 *For example:*

For Join Proxy services, a device receives the following server list from the ZENworks system. It attempts to connect to the first server in the list, then the second, and so on until it is successfully connected.

- Server4 (network environment)
- Server5 (network environment)
- Server3 (location)

For more information, see"Creating Closest Server Rules for a Location" in *ZENworks Location Awareness Reference*.

NOTE: You can promote only ZENworks 11.3 or later versions of Windows or Linux managed devices to the Join Proxy Satellite role. Using the Join Proxy Satellite Server, you can perform remote management operations only on Windows managed devices that are in a private network.

To configure the Join Proxy role:

1. First identify the ZENworks Windows or Linux managed device in the demilitarized zone (DMZ).
2. In ZENworks Control Center, select the check box next to **Join Proxy**, then click **Configure**.
3. In the Join Proxy Role Settings dialog box, specify the port on which the Join Proxy listens for connection. The default port number is 7019.
4. Specify the maximum number of devices to be allowed to connect to the Join Proxy. The default value is 1000, but you can change it to any value up to 1000. Because satellite servers are dedicated to join proxy service, they allow more such connections without being overloaded.

   NOTE: For a Primary server, the default value is 100.To manually increase this limit, update the `joinproxy.properties` file and restart the Join Proxy service. Increasing the join proxy connection limit on a Primary server might overload it when more devices start connecting to the Primary server.

   Though the range for maximum number of connections is from 1- 65535, if you specify a number greater than 1000, the following message is displayed:

   ```
   Maximum number of connections exceeding 1000 may impact the performance of Join Proxy adversely. Do you want to continue anyway?
   ```

5 Specify the frequency interval at which the Join Proxy should check if the devices are still connected to it or not. The default value is one minute.

NOTE: Based on the frequency specified here, Join Proxy will send packets to all the managed devices connected to it to detect the connection status and update it in the database. This enables remote operators to connect to managed devices through Join Proxy for performing remote sessions on Windows managed devices that are in a private network.

If you specify a lower value in this field, status updates are quicker in the database. However, this might result in higher traffic on the network, depending upon the number of devices connected to the Join Proxy.

6 Click **Ok** to return to the Add Satellite Server dialog box.

7 Configure any additional roles as desired, then click **OK**.

8 Create locations and assign Join Proxy devices to them.

For more details, see "Creating Closest Server Rules for a Location"*ZENworks Location Awareness Reference*. You can have multiple Join Proxies configured for a single location. You can include even Primary Servers in the Closest Server rules for the Join Proxy.

Double - click the Z icon of the Join Proxy server to view the Join Proxy Server's configuration details.

NOTE: Linux or Mac devices cannot connect to Join Proxy. However you might find Join Proxy listed as the Closest Server in Zicon Properties page of Linux or Mac devices when they are moved to a location that has Join Proxy.

Satellite Server Output Throttle Rate Calculations

When you assign the Content role to a Satellite Server, you need to specify the output throttle rate for it.The Satellite server output throttle rate is the rate at which the Satellite Server should send the content to other devices requesting content. These devices could be either other content Satellite Servers or managed devices.

While sending content to other devices, the Satellite Server calculates the throttle rate in the following manner:

For a Single Content Request with a Content Type Throttle: If you specified the Satellite Server output throttle rate as 500, and if the content type throttle is set to 200, then the final throttle rate will be smaller of the two.

For a Single Content Request with No Content Type Throttle: If you specified the Satellite Server output throttle rate as 500, and if there is no content type throttle configured for the content type, then the throttle rate for a single content request is 500.

For Multiple Requests without the Content Type Throttle: The sender Satellite Server divides the Satellite Server output throttle rate by the number of requests to find the final throttle rate.

For Multiple Requests with the Content Type Throttle: First, the sender Satellite divides the Satellite Server output throttle rate by the number of requests. Next, the sender Satellite considers the rate that is set for the content type throttle. The sender Satellite then uses the smaller of the two rates as the final throttle rate.

For information about content type throttle, see"Throttle (in KB/sec):" on page 50.

Example 13-2 *Example:*

The following table describes how the Satellite Server calculates the final throttle rate when you have specified 500 as the Satellite Server output throttle rate:

No. of Requests	Content Type Throttle (A)	Satellite Server Output Throttle Rate after Dividing (B)	Final Throttle Rate (Minimum of A and B)
5	100	500/5=100	100
10	100	500/10=50	50
2	200	500/2=250	200
1	600	500/1=500	500

14 Refreshing a Satellite

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

1. Select the check box next to the Satellite that you want to refresh.
2. Click **Action** > **Refresh Device**.

   The QuickTask Status box is displayed while the action is in progress.
3. (Optional) To close the status dialog box, click **Hide**.

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

15 Removing the Roles from a Satellite

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

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

To remove one or more roles from a Satellite:

1. In ZENworks Control Center, click the **Configuration** tab.
2. In the Server Hierarchy panel, select the check box next to the Satellite from which you want to remove the role.
3. Click **Actions** > **Configure Satellite Server**.
4. In the Configure Satellite Server dialog box, deselect the check box next to the Satellite role you want to remove.
5. Click **OK**.

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

When you demote a Satellite Server in ZENworks Control Center, the icon of the device changes only after a successful demotion is acknowledged by the device to the Server. If during demotion, the managed device or the agent on the manage device is not reachable, the demotion task does not complete successfully and the Satellite icon does not change on the Server.

16 Removing Satellites from the Server Hierarchy

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

When you remove a Satellite, the managed devices that used it must be reconfigured to use another server for content, collection, imaging and authentication purposes. For more information, see "Adding Closest Servers to Locations" in the *ZENworks Location Awareness Reference*.

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

To remove a Satellite:

1. For the Satellite that you want to remove, make a note of all devices that are using it for authentication, content, imaging, or collection information roll-up.
2. In ZENworks Control Center, click the **Configuration** tab.
3. In the Server Hierarchy panel, select the check box next to the Satellite that you want to remove from the zone.
4. Click **Action** > **Remove Satellite Server**.
5. To confirm the removal, click **OK**.
6. As necessary, reconfigure the managed devices that used the Satellite so that they can continue to receive content and roll up collection information.

   For more information, see "Adding Closest Servers to Locations" in the *ZENworks Location Awareness Reference*.
7. (Conditional) The Imaging role is immediately removed from the device. If the role is not immediately removed, it is removed only during the next device refresh schedule. If you want to immediately remove the role from the device, manually refresh the device in one of the following ways:
   - In the ZENworks Control Center, click the **Configuration** tab > the **Server Hierarchy**, select the check box next to the devices you want to refresh, then click **Action** > **Refresh Device**.
   - On a managed device, do one of the following:
     - Right-click the icon, then click **Refresh**.
     - Execute the `zac ref` command from the console prompt.

17 Specifying Content to be Hosted

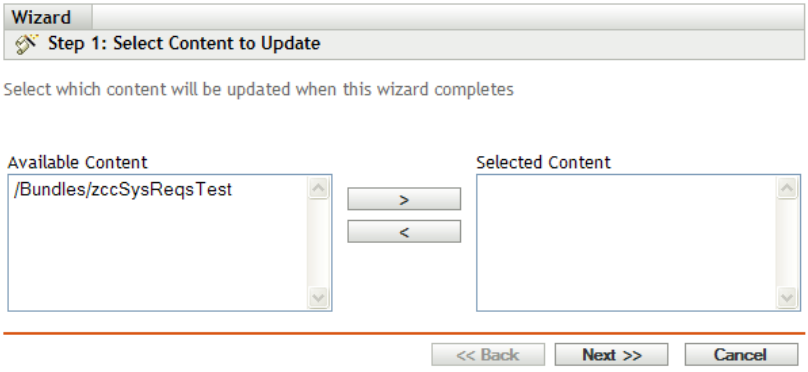
Because Content role devices retrieve their content from their parent Primary Servers, any content that you want hosted on a Satellite must also be hosted on its parent Primary Server.

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

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

To specify the content to be hosted:

1. In ZENworks Control Center, click the **Configuration** tab. In the Server Hierarchy section, select the check boxes next to the Satellites with the Content role that you want to designate as the hosts for one or more pieces of content.
2. Click **Action > Specify Content** to launch the Select Content to Update Wizard.



3. In the **Available Content** list, select the desired content.

   You can use Shift+click and Ctrl+click to select multiple bundles or policies.
4. Click > to move the selected content to the **Selected Content** list.
5. Click **Next**.
6. Click **Finish** to create the relationships between the content and the content servers.

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

18 Manually Replicating Content from a Primary Server to Satellite Devices

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

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

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

You cannot manually export content from one ZENworks Primary Server and then import that content into another Primary Server. For information about replicating content between Primary Servers, see Section 31, "Content Replication," on page 103.

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

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

1. In ZENworks Control Center, click the **Configuration** tab.
2. In the Server Hierarchy panel, select the check box next to the Satellite that you want to move, then click **Move**.
3. Select the Primary Server you want to be the Satellite's new parent, then click **OK**.

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

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

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

installation_path\zenworks\work\content-repo

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

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

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

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

   - If the content-repo directory is not present in the path given above, create the content-repo directory in that path.
   - If you need to save the content that is now in this directory, rename the existing directory and create a new empty directory named content-repo.

     You can later copy the content from the renamed directory to the new content repository location (see Step 9).
   - If you do not need any of the content in the existing content-repo directory, delete the directory and re-create the content-repo directory.

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

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

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

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

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

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

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

6. Click **Add**.

   This displays the Add Drive Letter or Path dialog box.

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

   installation_path\zenworks\work\content-repo

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

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

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

21 Specifying a Different Repository for Content Role Satellite (Linux Only)

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

`/var/opt/novell/zenworks/content-repo/`

To change the default path to another location accessible to the server, use one of the following ways:

- If you want to move the content repository to a different location on a different device, create a NFS volume on the device, mount the content-repo directory on the volume, and make the root user as the owner of the directory with Read, Write, and Execute permissions.
- If you want to move the content repository to a different location on the same Linux Satellite, mount the repository on a different volume that has sufficient disk space by using Soft Link.
- If you want to move the content repository to a OES device, create a NSS volume (CIFS share) on the device, mount the content-repo directory on the volume, and make the root user as the owner of the directory with Read, Write, and Execute permissions.

For more information, see “Changing the Location of the Content Repository on a Linux Server” on page 95.

22 Promoting an RHEL 6 device as a Content or Collection Role Satellite

To promote an RHEL 6 device as a Content or Collection Role Satellite, the firewall needs to allow communication over the HTTP port. However, due to SELinux policy rules, certain `iptables` commands such as `iptables-save` are denied write-access to the `iptables` configuration, due to which the firewall rules are not enforced.

To promote an RHEL 6 device as a Content or Collection Role Satellite:

1. Enable the permissive state for the security domain `iptables_t` using the following command:

   ```
   # semanage permissive -a iptables_t
   ```

2. Promote the device to a Content or Collection Role Satellite.

As an alternative workaround, you can also restart the ZENworks Agent service using the following command, before promoting a device to a Content or Collection Role Satellite:

```
/etc/init.d/novell-zenworks-xplatzmd restart
```

23 Promoting a Macintosh Device to Be a Content Role Satellite Server

1. Log in to ZENworks Control Center.
2. Click **Configuration**.
3. In the **Server Hierarchy** panel, select the Primary Server you want to promote.
4. Click **Action > Add Satellite Server** to display the **Add Satellite Server** dialog box.
5. In the **Device to promote** option, browse for and select a Macintosh device that is registered inthe Management Zone, then click **OK**.
6. In the **Satellite Server Roles** panel, select **Content**.
7. Click **OK**.

On the Macintosh managed device:

1. Log in to the managed device as `root`.
2. Refresh the device.
3. Right-click the ZENworks icon and click **Show Properties**. The Macintosh device is promoted to the **Content** role.

24 Promoting a Macintosh Device to Be a Collection Role Satellite Server

1. Log in to ZENworks Control Center.
2. Click **Configuration**.
3. In the **Server Hierarchy** panel, select the Primary Server you want to promote.
4. Click **Action > Add Satellite Server** to display the **Add Satellite Server** dialog box.
5. In the **Device to promote** option, browse for and select a Macintosh device that is registered inthe Management Zone, then click **OK**.
6. In the **Satellite Server Roles** panel, select **Collection**.
7. Click **OK**.

On the Macintosh Managed Device:

1. Log in to the managed device as `root`.
2. Refresh the device.
3. Right-click the ZENworks icon and click **Show Properties**. The Macintosh device is promoted to the **Collection** role.

25 Troubleshooting Satellites

The following section provides solutions to the problems you might encounter while working with Satellites:

Linux managed device promoted as a Satellite server with authentication role, the Jetty service hangs

Explanation: When you promote a Linux managed device as a satellite server with authentication role, the Jetty service hangs.

Action: Set a system variable `RegenerateJettyKeystore` for the satellite server and refresh the agent.

Unable to add a Satellite with the Imaging role to a Windows managed device by using the zman ssc command

Source: ZENworks; Satellite.

Action: To promote a Windows managed device to be a Satellite with the Imaging role, use the `zman ssaimg` command.

For more information about the `zman ssaimg` command, view the zman man page (`man zman`) on the ZENworks Server or see "Satellite Commands" in the *ZENworks Command Line Utilities Reference*.

Unable to remove a Satellite with the Imaging role from a Windows device by using the zman ssd command

Source: ZENworks; Satellite.

Action: To remove the Imaging Satellite role from a Windows managed device, use the `zman ssrimg` command.

This command does not remove other Satellite roles such as Content or Collection if they are assigned to the device.

For more information about the `zman ssrimg` command, view the zman man page (`man zman`) on the ZENworks Server or see “Satellite Commands” in the *ZENworks Command Line Utilities Reference*.

The managed device is not promoted to the Imaging Satellite role even though the role has been assigned to it

Source: ZENworks; Satellite.

Possible Cause: The managed device is unable to contact the Primary Server because of the firewall settings configured on the managed device.

Action: Do the following on the managed device:

1. Disable the firewall settings.
2. Ping the Primary Server to make sure that the managed device can contact the server.
3. Refresh the information on the  icon by right-clicking the icon, then clicking **Refresh**.

Updated Imaging statistics are not displayed on the ZENworks icon when a Windows Vista SP2 managed device is promoted to be a Satellite with the Imaging role

Source: ZENworks; Satellite.

Explanation: When you promote a Windows Vista SP2 managed device to be a Satellite with the Imaging role, any updated Imaging statistics are not displayed on the  icon (**Show Properties** > **Satellite** > **Imaging**)

Action: To view the latest Imaging statistics on the Satellite:

1. At the console prompt, go to *ZENworks_installation_directory*`\novell\zenworks\bin\preboot`.
2. Run the following command:

   `zmgmcast -status -i` *`Satellite_IP_address`*

Server Hierarchy

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

26 Primary Servers: Peer Versus Parent/ Child Relationships

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

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

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

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

We do not recommend having a Primary Server across a WAN link from the ZENworks database because this causes increased traffic across the network. We recommend that you use a Satellite device across a WAN link. For more information, see Section 27, “Satellite Role Relationships,” on page 85.

27 Satellite Role Relationships

A Satellite is a device that can perform certain roles that a ZENworks Primary Server normally performs. A Satellite can be any managed Windows or Linux device (server or workstation), but not a Primary Server. The ZENworks version installed on the managed device must be same as that of the Primary Server. When you configure a Satellite, you specify which roles it performs (Authentication, Collection, Content or Imaging). A Satellite can also perform roles that might be added by third-party products that are snap-ins to the ZENworks framework. For more information about the tasks you can perform on Satellites, see Chapter II, “Satellites,” on page 39.

The following sections contain more information:

Authentication Role Sever Relationships

An Authentication role identifies a managed device that is able to authenticate devices to the ZENworks Management Zone. When you set up a device to function with a Authentication role, you must specify a Primary Server as its parent.

Content Role Server Relationships

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

Collection Role Server Relationships

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

Imaging Role Server Relationships

An Imaging role causes a managed device to take and restore images within as well as across subnets by using unicast or multicast imaging.

Join Proxy Role Server Relationship

A Satellite with the Join Proxy role acts as a Join Proxy server Join Proxy helps to connect to Windows devices that are in a private network. Remote Management is one of those operations performed using Join Proxy.

28 Changing the Parent-Child Relationships of Primary Servers

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

Making a Primary Server a Child

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

To make a Primary Server a child of another server:

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

Making a Primary Server a Peer

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

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

1. In ZENworks Control Center, click the **Configuration** tab.
2. In the Server Hierarchy panel, select the check box next to the Primary Server you want to make a peer.
3. Click **Move** to display the **Move Device** dialog box.
4. Do one of the following:
   - Select **None** to move it up to the first level of servers in the listing.
   - Select another Primary Server to be the parent server.
5. Click **OK**.

IV Content

The following sections provide information to help you ensure that content is replicated correctly among the devices in your ZENworks Management Zone:

Each ZENworks Server contains a content repository. The content repository stores all bundle, policy, Patch Management, Product Recognition Update (PRU) and system update content that has been replicated to the server and any images that have been captured and stored to the server.

29 Replicated Content

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

Each ZENworks Server contains a content repository. The content repository stores all bundle, policy, Patch Management, Product Recognition Update (PRU) and system update content that has been replicated to the server and any images that have been captured and stored to the server.

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

30 Content Repository

Each ZENworks Server contains a content repository. The content repository stores all bundle, policy, Patch Management, Product Recognition Update (PRU) and system update content that has been replicated to the server and any images that have been captured and stored to the server.

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

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

If necessary, you can move the content repository to a different location. The following sections provide instructions:

Changing the Location of the Content Repository on a Windows Server

The content repository is found in the following location on a Windows server:

`installation_path\zenworks\work\content-repo`

You can specify a different disk drive to be your content repository. 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 or new one 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. Stop all ZENworks Services.

3 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 later copy the content from this renamed directory to the new content repository location (see Step 11).
- 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.

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

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

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

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

6 (Conditional) If a driver letter is associated with the partition that you want to use as the new content repository location, do the following:

6a In the Computer Management dialog box, right-click the drive's partition.

6b Select **Change Drive Letter and Paths**.

6c Select the drive letter.

6d Click **Remove**, then select **Yes** to confirm.

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

This is the disk drive that you will mount to the `content-repo` directory in Step 9.

8 Click **Add**.

This displays the Add Drive Letter or Path dialog box.

9 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 in Step 7.

If necessary, format the drive as NTFS using the Computer Management feature in Windows.

10 Click the buttons as necessary to exit and save the configuration change.

11 (Conditional; see Step 3) Copy the files from the old renamed `content-repo` directory to the new `content-repo` directory.

12 Start all ZENworks Services.

From this point on, all ZENworks data is written directly to the new content repository location on the selected hard drive partition.

Changing the Location of the Content Repository on a Linux Server

You can store your data on a local mount or on a network share such as NFS, SMB, or CIFS and mount the share in your `content-repo` directory to access your data.

You can also create a symbolic link on your local hard drive if you want to store your data elsewhere on your local device. However, the existing `content-repo` directory must be deleted.

1. (Optional) Run the following command to move the content from the `content-repo` directory to a new directory on the disk to which you want to create the symbolic link:

   ```
   mv /var/opt/novell/zenworks/content-repo/* another-local-directory-on-device
   ```

2. Run the following command to delete the `content-repo` directory:

   ```
   rm -rf /var/opt/novell/zenworks/content-repo/
   ```

3. Run the following command to create the symbolic link to the new directory where you want to store the data:

   ```
   ln -s another-local-directory-on-device /var/opt/novell/zenworks/content-repo
   ```

   See the ln(1) man page for more information about how to symbolically link directories.

   NOTE: You do not need to perform Step 4 if you are trying to configure the content repository on a Linux Satellite Server.

   ---

4. ZENworks requires that the ZENworks user has complete ownership rights on the directory to which you have created the symbolic link. Run the following command to make the ZENworks user the owner of this directory:

   ```
   chown zenworks:zenworks -R /var/opt/novell/zenworks/content-repo/
   ```

   See the chown(1) man page for more information about how to change ownership of directories.

The following sections provide information on managing content repository locations on Linux.

- “Mounting a Share” on page 95
- “Unmounting a Share” on page 96
- “Creating a Permanent Mount” on page 96
- “Moving Existing Content to the New Repository” on page 96

Mounting a Share

After configuring a share on a remote machine, you can mount it from `/var/opt/novell/zenworks/content-repo`. Stop all ZENworks Services before mounting the share.

Use the following command to mount the share:

```
mount -t cifs -o username=username //example.machine.com/share_name /var/opt/novell/zenworks/content-repo
```

In the command, *`//example.machine.com/share-name`* is the share to mount and `/var/opt/novell/zenworks/content-repo` is the mount point.

If you only need to store the data from part of your content repository on another share, you can also do that. For example, if you need to store your ZENworks image files on another share, you can use the following command:

```
mount -t cifs -o username=username //example.machine.com/share_name /var/opt/
novell/zenworks/content-repo/images
```

Or, to store bundle and policy content on another share, you can use the following command:

```
mount -t cifs -o username=username //example.machine.com/share_name /var/opt/
novell/zenworks/content-repo/content
```

Start all ZENworks Services after the share is mounted.

Unmounting a Share

The mount that you created in “Mounting a Share” on page 95 is temporary; the share is unmounted when the operating system is shut down or rebooted. You can also use the following command to manually unmount the share:

```
umount /var/opt/novell/zenworks/content-repo
```

Stop all ZENworks Services before unmounting the share and start all ZENworks Service after the share is unmounted.

Creating a Permanent Mount

Stop all ZENworks Services before creating a permanent mount and start all ZENworks Service after the permanent mount is created.

To ensure that the mount occurs each time the Linux server starts, you must add the following entry to your `/etc/fstab` configuration file:

```
//example.machine.com/share_name /var/opt/novell/zenworks/content-repo cifs
credentials=path_to_credentials_file 0 0
```

The credentials file listed in the command contains a username and password. For more information, see the `mount.cifs(8)` man page. The format of the credentials file is:

```
username=value
```

```
password=value
```

Moving Existing Content to the New Repository

After you change the location of a content repository by mounting a new share, any content in the old location is no longer available. To make it available, you must move it to the new repository. Stop all ZENworks Services before moving existing content to the new repository and start all ZENworks Service after the existing content is moved.

Mounting the Content Repository on a Linux Server to an NSS Volume

You can mount the `content-repo` directory on a Linux server on to an NSS Volume.

Before you begin, ensure that the following prerequisites are met:

- The NSS volume is set up and mounted in the `/media/nss/NSSVOL/` directory of the server.

- The Samba service is installed and configured to run as `root` on the server. To verify this, run the following command and ensure that the value in UID column is `root`, especially for the processes with PPID = 1.

  ```
  ps -Alf | grep samba
  ```

To mount the `content-repo` directory:

1. Go to the `/etc/init.d/` directory and stop the `novell-zenserver`, `novell-zenloader`, and `novell-zenmntr` services.
2. Run the following command to move the content from the `content-repo` directory to a temporary directory on the disk so that the `content-repo` directory is empty:

   ```
   mv /var/opt/novell/zenworks/content-repo/* another-local-directory-on-device
   ```
3. Go to the `/media/nss/NSSVOL` directory, and create a `zencontent` subdirectory within it.
4. Use YaST to add the newly created subdirectory to the list of Samba shares (for example, `zenshare`) on the server.
5. Restart the Samba service.
6. (Conditional) Run the following command to add a Samba `root` user if the Samba `root` user does not already exist:

   ```
   smbpasswd -a root
   ```

   For security reasons, you must specify a `root` password that is different from the login password.
7. (Optional) To test if the newly created share is accessible over the Samba protocol, access the share from a Windows device by providing the Samba `root` user credentials
8. Run the following command to mount the `zenshare` share:

   ```
   mount //localhost/zenshare /var/opt/novell/zenworks/content-repo -t cifs -o username=root
   ```
9. Restore the backed-up content to the `/var/opt/novell/zenworks/content-repo` directory. The content is now stored on the NSS volume.
10. Go to the `/etc/init.d/` directory and restart the `novell-zenserver`, `novell-zenloader`, and `novell-zenmntr` services.
11. (Conditional) To ensure that the share is automatically mounted every time the server reboots, add the following line in the `/etc/fstab` file:

    ```
    //localhost/zenshare /var/opt/novell/zenworks/content-repo cifs username=root,password=rootpass 0 0
    ```

Changing the Location of the Temporary Location on a Windows Server

Creating bundles that contain content temporarily requires up to twice the amount of disk space as the original files. The bundle creation process uploads copies of the original files from the local machine to a temporary directory on the ZENworks content server. The process then packages those files as encrypted, compressed ZENworks content files. After the ZENworks content files are created, the original uploaded files are automatically deleted.

When the bundle is created in ZENworks Control Center, the temporary files are stored in the *installation_path*`\zenworks_home\share\tomcat\temp` location.

If the space on the default temporary location is insufficient, you can specify a different disk drive to be the location of temporary files.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 temporary location to a disk drive partition, which becomes the new temporary location:

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 or new one 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. Stop all ZENworks Services.
3. Click **Start**, right-click the **My Computer** icon, then select **Manage**.

   You can also click **Start**, then enter `compmgmt.msc` at the **Run** command line.
4. Select **Disk Management** under the **Storage** section in the left pane.

   The disk drive you selected in Step 1 should be displayed 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 select **Yes** to confirm.
6. Right-click the partition of the disk drive that you want to use as your temporary location, then select **Change Driver Letter and Paths**.

   This is the disk drive that you will mount to the `temporary location` directory in Step 9.
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 `temporary location` directory, then click **Next**.

   The default directory is *`installation_path`*`\zenworks_home\share\tomcat\temp`.

   This mounts the default path to the hard drive partition that you selected in Step 7.

   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. Start all ZENworks Services.

From this point on, all ZENworks data is written directly to the new temporary location on the selected hard drive partition.

Changing the Location of the Temporary Location on a Linux Server

You can store your data on a local mount or on a network share such as NFS, SMB, or CIFS and mount the share in your `temporary` directory to access your data.

You can also create a symbolic link on your local hard drive if you want to store your data elsewhere on your local device. However, the existing temporary location directory must be deleted.

1. Run the following command to create the symbolic link to the new directory where you want to store the data:

   ```
   ln -s another-temporary-directory-on-device /var/temp/
   ```

   See the ln(1) man page for more information about how to symbolically link directories.

2. ZENworks requires that the ZENworks user has complete ownership rights on the directory to which you have created the symbolic link. Run the following command to make the ZENworks user the owner of this directory:

   ```
   chown zenworks:zenworks -R /var/temp/
   ```

   See the chown(1) man page for more information about how to change ownership of directories.

The following sections provide information on managing content repository locations on Linux.

- “Mounting a Share” on page 99
- “Unmounting a Share” on page 99
- “Creating a Permanent Mount” on page 100

Mounting a Share

After configuring a share on a remote machine, you can mount it from `/var/temp/`. Stop all ZENworks Services before mounting the share

Use the following command to mount the share:

```
mount -t cifs -o username=username //example.machine.com/share_name /var/temp/
```

In the command, *`//example.machine.com/share-name`* is the share to mount and `/var/temp/` is the mount point.

Start all ZENworks Services after the share is mounted.

Unmounting a Share

The mount that you created in “Mounting a Share” on page 95 is temporary; the share is unmounted when the operating system is shut down or rebooted. You can also use the following command to manually unmount the share:

```
umount /var/temp/
```

Stop all ZENworks Services before unmounting the share and start all ZENworks Service after the share is unmounted.

Creating a Permanent Mount

Stop all ZENworks Services before creating a permanent mount and start all ZENworks Service after the permanent mount is created.

To ensure that the mount occurs each time the Linux server starts, you must add the following entry to your `/etc/fstab` configuration file:

```
//example.machine.com/share_name /var/temp/ cifs
credentials=path_to_credentials_file 0 0
```

The credentials file listed in the command contains a username and password. For more information, see the `mount.cifs(8)` man page. The format of the credentials file is:

```
username=value
```

```
password=value
```

Configuring NSS Volume as a Content Repository on an OES Satellite Server

Any server in a remote location can be used to host ZENworks Satellite and Content Repository on an NSS Volume. This enables optimization of hardware resources and network bandwidth.

- OES 2017 SP1 as Satellite Server

Prerequisites

1. The OES Server is running.
2. NSS volumes are mounted on the OES Server.
3. ZENworks Primary Server is running.
4. Few bundles are created and are available on the ZENworks Primary Server.

ZENworks Primary Server Configurations

Discover and deploy ZENworks Agent on an OES Server by using ZENworks Configuration Management. To add the OES Server as a Satellite:

1. Log in to ZENworks Control Center.
2. Click **Server Hierarchy** > **Action** > **Configure Satellite Server**.
3. Browse for and select the OES Server to be added as a Satellite Server.
4. Select **Content** from the Satellite Server Roles list.
5. Click **Configure**.
6. In the Settings tab, change the port number from 80 to any other port which is not used for content and/or collection HTTPS requests. (Port 80 is used by the OES services).
7. In the Content Replication tab, select the **Use Parent Primary Server Only** as the content replication method and save the changes.

   NOTE: You can also create a Closest Server Rule (Network Environment/Location) for agents to receive content from the Satellite Server.

   ---

8. Click **Configuration** and select the Satellite Server that has been configured.

9 Click **Details** and navigate to the Content tab.

10 Select the bundles and policies which need to be included for content replication.

11 In **Server Hierarchy**, click the arrow icon to navigate to the Satellite Server.

12 Select the Satellite Server, click **Actions** and select **Configure Satellite Server**.

13 In the Satellite Server Roles panel, click the **Configure** link for **Content**.

14 In the Configure Content Role panel, click **Edit** to configure the interval for content replication or create a new schedule by adding a new interval.

15 Click **Edit** to configure interval, throttle rate, duration, and schedule type for content.

Verifying content replication on OES Server

1 Check the privileges of the `content repo` folder in the default location.

2 Navigate to the following directory to verify if the content is replicated successfully from the Primary Server to the Satellite Server:

```
/var/opt/novell/zenworks/content-repo/content # ls –lrt
```

Satellite Server (OES Server) Configurations

1 Stop the ZENworks Agent on the Satellite Server by running the following command:

```
# /etc/init.d/novell-zenworks-xplatzmd stop
```

2 Create a user defined content repo under NSS mounted volume. For example:

```
/media/nss/VOL1/zendata/content-repo/
```

3 Copy the content data from the default location to the mounted volume as follows by running the following command:

```
cp /var/opt/novell/zenworks/content-repo/media/nss/VOL1/zendata
```

4 Rename the `content-repo` directory path to `/var/opt/novell/zenworks/content-repo-backup`.

5 Create a soft link by using the following command:

```
ln -s /media/nss/VOL1/zendata/content-repo/ /var/opt/novell/zenworks/content-repo
```

6 Start the ZENworks Agent on the Satellite Server by running the following command:

```
# /etc/init.d/novell-zenworks-xplatzmd start
```

7 Assign the bundle to any managed device.

Verifying content replication on a managed device

Check the `zmd-message` logs to ensure that the content is replicated successfully from the Satellite Server to the managed device. You can find the logs in the following location for a Windows managed device:

```
C:\Program Files (x86)\Novell\ZENworks\logs\LocalStore
```

31 Content Replication

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

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

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

Content Replication settings can be inherited from the following locations:

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

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

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

Content replication settings let you:

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

For information about performing these tasks, see the following sections:

- “Configuring Content Replication at the Management Zone Level” on page 104
- “Replicating Content to New Content Servers” on page 105
- “Manually Replicating Content from a Primary Server to Satellite Devices” on page 106
- “Including or Excluding Content” on page 106

- "Replicating Content to Primary Servers" on page 109
- "Cleaning up Content from the Primary Server" on page 109

Configuring Content Replication at the Management Zone Level

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

2 In the Management Zone Settings panel, click **Content** > **Content Replication**.

3 Fill in the fields:

Primary Server Recurring Content Replication Schedule: Use the **Days**, **Hours**, and **Minutes** fields to set the schedule.

You can use any combination of the fields. For example, to specify every 30 hours, you can enter 30 hours or 1 day, 6 hours.

NOTE:

- We recommend you to set the schedule to 12 hours.
- If a Satellite device is at the end of a very slow link (for example, a 128K WAN), you might want to disable the content replication schedule so that content can be manually replicated by using the `zac wake-cdp (cdp)` command. For more information about the zac wake-cdp command, see "Content Distribution Commands in the *ZENworks Command Line Utilities Reference*".

  To disable the content replication schedule on a Satellite device set the Schedule Type to No Schedule. For more information on setting the schedule type, see "Understanding the Content Role" on page 42.

Primary Server Output Throttling in KB/Sec: Select the throttling rate you want to use.

This rate applies to all ZENworks Servers in your zone. You cannot set individual throttling rates.

The content replication throttling rate determines the maximum amount of content (in kilobytes per second) that a ZENworks Server transfers when replicating content to other content servers or when distributing content to managed devices.

By default, no throttling rate is imposed, which means that a ZENworks Server uses all available bandwidth.

Agent Content Checksum: Specify whether the ZENworks Agent on managed devices computes the checksum of downloaded content and compares that checksum to the stored checksum for that content on the ZENworks Primary Server.

Comparing checksums helps to ensure that no errors were introduced during the downloading of the content and that the content was not altered.

Under normal conditions, you should use the default of **On**. If your ZENworks System has serious performance issues, you can set this setting to **Off** to increase performance.

Satellite Content Checksum: Specify whether the ZENworks Agent on Satellite devices computes the checksum of downloaded content and compares that checksum to the stored checksum for that content on the ZENworks Primary Server.

Comparing checksums helps to ensure that no errors were introduced during content replication and that the content was not altered.

Under normal conditions, you should use the default of **On**. If your ZENworks System has serious performance issues, you can set this setting to **Off** to increase performance.

4 Click **Apply** or **OK** to save the changes.

Manually Configuring the Web Service Timeout Advanced Content Replication Setting

You can adjust the Web Service Timeout value to suit your needs. For example, if a Satellite device is across a slow WAN link and there is missing content, the default 240-second timeout value might not be long enough to make the Web service call.

To modify the Web Service Timeout on a Satellite device:

For Windows, create the following string value in the registry on the Satellite device:

`HKEY-LOCAL-MACHINE\SOFTWARE\Novell\ZCM\CDPWebCallWaitTimeout` and set the value to the desired number of milliseconds.

For Linux, in the `/etc/opt/novell/zenworks/conf/xplatzmd.properties` file on the Satellite device, add the following line:

CDPWebCallWaitTimeout=*xxx*

where *xxx* is the desired timeout value in milliseconds.

Replicating Content to New Content Servers

By default, when a new ZENworks server is added to the zone, all bundle and policy content is replicated to that ZENworks server. You can, however, choose not to replicate a specific bundle or content policy. If a new content Satellite Server is added to the zone, no content is replicated on the satellite server, unless specified.

For example, assume that you have a bundle for Microsoft Office. You've included it on specific content servers and don't want it replicated to additional servers. To keep this from happening, you modify the Microsoft Office bundle's replication settings to exclude replication to new content servers.

1. In ZENworks Control Center, go to the details page for the object (bundle, policy, or folder) whose replication setting you want to modify, then click the **Settings** tab.
2. To configure the settings on a bundle, click **Bundle Management**, then click **Primary Server Replication** or **Satellite Server Replication**.

   or

   To configure the settings on a policy, click **Policy Management**, then click **Primary Server Replication** or **Satellite Server Replication**.

   or

   To configure the settings on a bundle or policy folder, click **Content**, then click **Primary Server Replication** or **Satellite Server Replication**.
3. In the Primary Server Replication Status section, click the appropriate buttons to include or exclude new Primary Servers from hosting the content.
4. In the Satellite Server Replication Status section, click the appropriate buttons to include or exclude new Satellite Servers from hosting the content.
5. (Optional) In the **Search** option, type the string to be used to filter the Server (Primary or Satellite) then press **Enter**.

6 (Optional) If you are configuring settings on a bundle folder or policy folder, click **Force Inheritance** in the **Folder Task** list in the left navigation pane to ensure that all children (all subfolders as well as individual bundles and policies) inherit the settings. Be aware that settings configured on children are lost and that this action cannot be undone.

7 Click **OK** to save the changes.

Manually Replicating Content from a Primary Server to Satellite Devices

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

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

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

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

Including or Excluding Content

The default replication setting determines whether content is automatically replicated to new content servers (see "Replicating Content to New Content Servers" on page 105). You configure the setting for each bundle, policy, or folder. If you choose to include a bundle's or policy's content on new content servers, it is replicated to all new servers; likewise, if you choose to exclude the content, it is not replicated to any new servers.

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

- "Managing a Single Piece of Content on Multiple Content Servers" on page 107
- "Managing Content on the Folder Level" on page 107
- "Managing Multiple Pieces of Content on a Single Content Server" on page 108
- "Managing Multiple Pieces of Content on Multiple Content Servers" on page 108

Managing a Single Piece of Content on Multiple Content Servers

This section provides instructions for managing the replication of a single bundle's or policy's content to multiple content servers.

1. In ZENworks Control Center, go to the details page for the bundle or policy whose content replication you want to manage.
2. Click the **Settings** tab, click **Bundle Management** or **Policy Management**, then click **Primary Server Replication** or **Satellite Server Replication**.

   The **Primary Server Replication Status** panel and the **Satellite Server Replication Status** panel display all content servers in the zone. If the bundle or policy content is included on a content server, the **Included** column displays a ■ icon.
3. To change the replication status for a content server, select the check box next to the server, then click **Include** to include the content on the server, or click **Exclude** to exclude the content from the server.

   As you include or exclude content servers, be aware of the following replication rules:

   - If a ZENworks Server is the parent server for one or more Satellite devices, you can't exclude the content from the ZENworks Server without first excluding it from the Satellite devices.
   - If you have only one ZENworks Server in your Management Zone, you can't exclude the content from it.
   - You can't include a Satellite devices without first including the Satellite devices's parent ZENworks Server.
4. Click **Apply**, then click **OK**.

Managing Content on the Folder Level

This section provides instructions for managing the replication of the content in a bundle or policy folder.

1. In ZENworks Control Center, go to the details page for the bundle or policy folder whose content replication you want to manage.
2. Click the **Settings** tab, then click **Content**.
3. Click **Primary Server Replication** or **Satellite Server Replication**.

   The **Primary Server Replication Status** panel and the **Satellite Server Replication Status** panel display all content servers in the zone. If the bundle or policy content is included on a content server, the **Included** column displays a ■ icon.
4. To change the replication status for a content server, select the check box next to the server, then click **Include** to include the content on the server, or click **Exclude** to exclude the content from the server.

   As you include or exclude content servers, be aware of the following replication rules:

   - If a ZENworks Server is the parent server for one or more Satellite devices, you can't exclude the content from the ZENworks Server without first excluding it from the Satellite devices.

- If you have only one ZENworks Server in your Management Zone, you can't exclude the content from it.
- You can't include a Satellite devices without first including the Satellite devices's parent ZENworks Server.

5 (Optional) Click **Force Inheritance** in the **Folder Task** list in the left navigation pane to ensure that all children (all subfolders as well as individual bundles and policies) inherit the settings.

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

Managing Multiple Pieces of Content on a Single Content Server

This section provides instructions for managing the replication of the content for multiple bundles or policies to a single content servers.

1 In ZENworks Control Center, go to the details page for the content server whose content replication you want to manage.

2 Click the **Content** tab.

The Replication Settings panel displays all bundles and policies in the zone. If the bundle or policy content is included on the content server, the **Included** column displays a ■ icon.

3 To change the replication status for a bundle or policy, select the check box next to the bundle or policy, then click **Include** to include its content on the server, or click **Exclude** to exclude its content from the server.

As you include or exclude content from the server, be aware of the following replication rules:

- If a ZENworks Server is the parent server for one or more Satellite devices, you can't exclude the content from the ZENworks Server without first excluding it from the Satellite devices.
- If you have only one ZENworks Server in your Management Zone, you can't exclude the content from it.
- You can't include a Satellite devices without first including the Satellite devices's parent ZENworks Server.

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

Managing Multiple Pieces of Content on Multiple Content Servers

You can use the Specify Content Wizard to include multiple pieces of content on multiple content servers. For example, you might have four bundles that you want included on two of your four content servers. Rather than managing the replication for the individual bundles (see "Managing a Single Piece of Content on Multiple Content Servers" on page 107) or the individual content servers (see "Managing Multiple Pieces of Content on a Single Content Server" on page 108), you can use the wizard to manage the replication for all four bundles and content servers at one time.

1 In ZENworks Control Center, click the **Devices** tab, then click the **Servers** folder to open it.

2 Select one or more servers on which you want to manage the content.

3 Click Action > **Specify Content.**

or

In the **Server Tasks** list in the left navigation pane, click **Specify Content** to launch the wizard.

4 On the Select Content to Update page, select the content and move it from the Available Content list to the Selected Content list.

5 Click **Finish**.

You can also launch the Specify Content Wizard from the following location: **Configuration page> Server Hierarchy** panel.

If you need more information about a wizard page, click the **Help** button.

Replicating Content to Primary Servers

You can replicate a bundle's or policy's content to a Primary Server immediately without waiting for the scheduled content replication.

1 In ZENworks Control Center, click the **Devices** tab on the left, select one of the Primary Servers and click Content.

2 In the Replication settings panel under the Content tab, select the content (bundle or policy) you want to replicate immediately to the selected Primary Server.

3 Click **Actions** > **Replicate Now**.

The selected bundle or policy content will be included on a content server and the **Included** column displays a check mark

4 If you click **Advanced**, the **Status** column displays the content as Available, based on the content size. Once marked as available, the content will be available in the repository of the selected Primary Server.

NOTE: The Replicate Now option is applicable only for the Primary Servers and not for the Satellite Servers.

Cleaning up Content from the Primary Server

You can cleanup a bundle's or policy's content from a Primary Server immediately without waiting for the scheduled content cleanup.

1 In ZENworks Control Center, click the **Devices** tab on the left, select one of the Primary Servers and click Content.

2 In the Replication Settings panel under the Content tab, select the check box for the content (bundle or policy) you want to cleanup immediately from the selected Primary Server.

3 Click **Actions** > **Cleanup Now**.

The content will be removed from the **Included** column. The content will be removed also from the repository of the selected Primary Server.

NOTE: The Cleanup Now option is applicable only for the Primary Servers and not for the Satellite Servers. The content will not be cleaned up if that is the only Primary server where the content is hosted.

---

32 Content Delivery

Content delivery, or distribution, refers to the process of transferring bundle and policy content from a content server (ZENworks Primary Server or Satellite with the Content role) to a managed device.

There are a variety of settings you can use to determine how content is delivered to managed devices, such as setting up Closest Server rules, setting delivery blackout dates for when content can't be downloaded, and setting how often you want managed devices to look for new content to download.

For information about performing these tasks, see the following sections:

- "Setting Up Location Closest Server Rules" on page 111
- "Scheduling Delivery Blackout Dates" on page 111
- "Setting the Device Refresh Schedule" on page 112

Setting Up Location Closest Server Rules

When you have multiple content servers, you can use the Closest Server rules to determine from which content server a managed device receives its content. By associating content servers with locations, you can ensure that a device accesses the closest content server even when the device changes location. The Closest Server rules for a location let you map devices to content servers based on many network parameters (DNS names, IP addresses, Gateways, and so forth).

For more information, see "Adding Closest Servers to Locations" in the *ZENworks Location Awareness Reference*.

Scheduling Delivery Blackout Dates

If there are times when you don't want managed devices to download content, you can create a content blackout schedule. Schedules can be defined at the following levels:

- **Management Zone:** The schedule is inherited by all devices.
- **Device Folder:** The schedule is inherited by all devices within the folder and its subfolders. It overrides the Management Zone blackout schedule.
- **Device:** The schedule applies only to the device for which it is defined. It overrides any schedules set at the Management Zone and folder levels.

A blackout schedule can include one or more time periods.

NOTE: The Content Blackout Schedule setting lets you prevent managed devices from downloading content from a content source during the blackout period. This setting, however, does not affect content replication. For this reason, a Satellite device with the Content role can still replicate content from its parent primary server during the blackout period.

To create a content blackout schedule:

1. Launch ZENworks Control Center.
2. Do one of the following:
   - To create a content blackout schedule for your Management Zone, click the **Configuration** tab, then click **Content** (in the Management Zone Settings panel) > **Content Blackout Schedule**.
   - To create a content blackout schedule for a device folder, open the folder's details page, then click **Settings** > **Content** (in the Settings panel) > **Content Blackout Schedule**.
   - To create a content blackout schedule for a device, open the device's details page, click **Settings** > **Content** (in the Settings panel) > **Content Blackout Schedule**.
3. If you are creating content blackout schedules for a device or device folder, click **Override settings** to activate the Content Blackout Schedule panel.
4. Click **Add** to display the Specify Blackout Time Period dialog box, then fill in the following fields:

   Start Date: Select the first date you want to include in the schedule.

   End Date: Select the last date you want to include in the schedule. The blackout time period (specified by the start and end times) occurs on each day from the start date to the end date.

   Start Time: Select the hour you want the blackout time period to start each day.

   End Time: Select the hour you want the blackout time period to end each day. If you want the blackout time period to extend for 24 hours, select the same time as the start time.
5. Click **OK** to save the blackout period.
6. Repeat Step 4 to create additional blackout periods.
7. When you are finished, click **OK** or **Apply** to save the schedule.

Setting the Device Refresh Schedule

At device startup, the ZENworks Agent on a device contacts a ZENworks Server to refresh its information. If information changes after startup, the ZENworks Agent must refresh its information again before the changes can show up on the device.

If the refreshed information indicates that there is new content to be downloaded, the ZENworks Agent contacts its content server and begins the download process.

You can use the device refresh schedule to determine how often a device contacts a ZENworks Server to update bundle, policy, configuration, and registration information. Schedules can be defined at the following levels:

- **Management Zone:** The schedule is inherited by all devices.
- **Device Folder:** The schedule is inherited by all devices within the folder and its subfolders. It overrides the Management Zone schedule.
- **Device:** The schedule applies only to the device for which it is defined. It overrides any schedules set at the Management Zone and folder levels.

To create a device refresh schedule:

1. Launch ZENworks Control Center.
2. Do one of the following:
   - To create a device refresh schedule for your Management Zone, click the **Configuration** tab, then click **Device Management** (in the Management Zone Settings panel) > **Device Refresh Schedule**.
   - To create a device refresh schedule for a device folder, open the folder's details page, then click **Settings** > **Device Management** (in the Settings panel) > **Device Refresh Schedule**.
   - To create a device refresh schedule for a device, open the device's details page, then click **Settings** > **Content** (in the Settings panel) > **Device Refresh Schedule**.
3. If you are creating a device refresh schedule for a device or device folder, click **Override settings** to activate the Device Refresh Schedule panel, then choose from the following schedules:

   Manual Refresh: If you want a device refreshed only when its user manually initiates the refresh, select **Manual Refresh,** then click **Apply**. Users can initiate a refresh by clicking the ZENworks icon located in the desktop's notification area (system tray).

   Timed Refresh: Select **Timed Refresh** if you want to establish a refresh schedule. You can use a Full Refresh Schedule or a Partial Refresh Schedule:

   - **Full Refresh Schedule:** Defines how often you want a device to update all of its information from the ZENworks Server, including bundle, policy, setting, and registration information. Use the following fields to create the full refresh schedule:
     - **Days, Hours, Minutes:** Specifies the amount of time between refreshes. For example, to set a refresh interval of 8.5 hours, you would specify 0 Days, 8 Hours, 30 Minutes. The default is 12 hours.
     - **Random Time to Wait:** Select this option to ensure that multiple devices with the same refresh schedule do not all initiate their refresh at the same time. For example, if you have 1000 devices with the same refresh schedule, you might overburden your ZENworks Server. By selecting this option, the device waits a randomly generated amount of time before initiating its refresh. Use the **Minimum** and **Maximum** fields to specify the range (in seconds) for the randomly generated time.
   - **Partial Refresh Schedule:** Defines how often you want a device to update its policy, configuration setting, and registration information from the ZENworks Server. Bundle information is not updated.

     In the **Days**, **Hours**, and **Minutes** fields, specify the amount of time between refreshes. For example, to set a refresh interval of 3 hours, you would specify 0 Days, 3 Hours, 0 Minutes. The default is 2 hours.

   The **Timed Refresh** setting is applicable to both the full and partial refreshes.

   The refresh interval is not reset until the device refresh is complete. For example, assume you set a refresh interval of 8 hours. The device's first refresh occurs at 6:00 p.m. and takes 13 seconds to complete. The second refresh occurs at 2:00:13 a.m. (8 hours after the refresh was completed at 6:00:13). If the second refresh takes 15 seconds to complete, the third refresh occurs at 10:00:28 a.m.
4. When you are finished, click **OK** or **Apply** to save the schedule.

33 Content Sharing

Content sharing helps you leverage your existing file sharing infrastructure and download the content to managed devices.

NOTE: Managed devices download the content from the content repository by using the HTTP protocol. They can additionally download the content by using the CIFS protocol.

For information about sharing content, see the following sections:

Sharing the content-repo Directory on the Primary Server

On the ZENworks Primary Server, you need to configure the content repository as a file system share that can be accessed as an anonymous read-only share. You must configure the content repository as read-only for preventing anonymous users from manipulating the data and causing security issues.

Sharing the Content Repository on a SUSE Linux Server

1. Install Samba.

   For more information on how to install Samba, see the *Samba Administration Guide*.

2. Launch YaST Control Center.
3. In the **Filter** field, type `Samba Server`.

   The Samba Server configuration process is initialized.
4. Click **Next**.

   The Samba Installation window is displayed.
5. In the **Workgroup or Domain Name** field, specify the workgroup or domain name, then click **Next**.
6. In the **Samba Server Type** option, select one of the following:
   - Primary Domain Controller (PDC)
   - Backup Domain Controller (BDC)
   - Not a Domain Controller

7 Click **Next**.

The Samba Configuration window is displayed.

8 In the **Start-Up** tab, select how you want the Samba Server to start:

- During Boot
- Manually

9 Click **OK**.

The Password dialog box is displayed.

10 Specify the Samba root password, verify the password, then click **OK**.

11 Select the settings for the new share.

11a Click **Shares** > **All users** > **Edit**.

The New Share window is displayed.

11b Specify the share name, then provide a short description of the share.

11c Select the **Directory** option to share the folder.

11d Click **Browse** to display the Browse for Folder dialog box. Browse to and select the path that you want to share. For example, `%zenworks_home%\work\content-repo`

11e Select the **Read-Only** check box to only read the files that are shared.

11f Select the **Inherit ACLS** check box to make new files inherit the default ACLs from the containing folder.

11g Click **OK**.

12 In the Share content-repo window, click **Edit**.

13 In the **Selected Option** drop-down list, select **guest ok**, then click **OK**.

14 Click **OK**.

Sharing the Content Repository on Windows

You can perform the following tasks in the order listed:

1. Enable simple file system sharing.

Windows 2003

a. Click **Start** > **All Programs** > **Accessories** > **Windows Explorer**.

b. Expand **My Computer**, then locate the shared folder or drive to that you want to share.

c. Right-click the folder or drive, then click **Properties**.

The Properties dialog box is displayed.

d. Click the **Sharing** tab.

e. Select the **Share this folder** option.

f. Specify the share name and a brief description about the folder.

g. Click **Apply** > **OK**.

Windows 7

a. Open Windows Explorer, then locate the shared folder or drive to that you want to share.

b. Right-click the folder or drive, then click **Properties**.

The Properties dialog box is displayed.

c. Click **Sharing** > **Share**.

d. In the Advanced Sharing panel, click **Advanced Sharing**.

The Advanced Sharing dialog box is displayed.

e. Select the **Share this folder** check box.

The Settings panel is enabled.

f. Specify the share name.

g. Click **Apply** > **OK**.

2. Use the `gpedit.msc` method to configure the group policy settings:

a. From the desktop Start menu, click **Run**.

b. In the Open option, type `gpedit.msc`, then click **OK**.

The Local Group Policy Editor window is displayed.

c. Double-click **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **Security Options**.

d. Select the **Network access: Let Everyone permissions apply to anonymous users** option.

e. In the **Local Security Setting** tab, select **Enabled**.

f. Click **Apply** > **OK**.

g. Select the **Network access: Shares that can be accessed anonymously** option.

h. In the Local Security Setting tab, add the content-repo setting to the list of shares.

i. Click **Apply** > **OK**.

j. Restart the Server service from the Service Manager.

Sharing the content-repo directory on a Satellite Server

To share the content repository on a Satellite Server, you must follow the procedures in "Sharing the content-repo Directory on the Primary Server" on page 115.

In addition, if the Satellite Server is a promoted Satellite Server, you must configure the settings for allowing the user to access the `content-repo` directory anonymously.

For Windows:

1. Open the Registry Editor.
2. Go to `HKLM/Software/Novell/ZCM`.
3. In the right pane, right-click **New,** then click **String Value**.
4. Rename the string value as `AllowAnonymousAccessToContentRepo`.
5. Double-click `AllowAnonymousAccessToContentRepo`.

   The Edit String dialog box is displayed.
6. In the **Value data** field, specify the value of the string as `True`, then Click **OK**.

For Linux:

In the `/etc/opt/novell/zenworks/conf/xplatzmd.properties` file, set the value of the AllowAnonymousAccessToContentRepo string as `True`.

Configuring the Settings on a Managed Device

For managed devices to download the content repository by using a CIFS share, you need to configure the following settings on every device:

For Windows:

Create the following string value in the registry on the managed device:

`HKEY-LOCAL-MACHINE\SOFTWARE\Novell\ZCM`

Specify the value name as `PreferredContentRepo`. Set the value of the string as `\\<ip address>\\content-repo\`.

For example, `PreferredContentRepo = \\164.99.137.82\content-repo\`.

For Linux:

In the `/etc/opt/novell/zenworks/conf/xplatzmd.properties` file on the managed device, set the value of the PreferredContentRepo string as `smb://<ip address>>/<content-repo>/`.

"The imaging content is replicated according to the default content replecation schedule even if you change the schedule after promoting a managed device to an Imaging Satellite" on page 126.

Configuring the SMB Protocol

To configure the SMB protocol in ZENworks, a new registry key PreferredSMBProtocol has been introduced. Using this registry key, you can choose the preferred SMB protocol. The valid values are SMBv1 and SMBv2.

By default, ZENworks is configured to use the SMBv2 protocol. However, if you prefer to use SMBv1 protocol, perform the following:

On Windows managed device: Create the PreferredSMBProtocol registry key, and set the value of the string as SMBv1.

On Linux managed device: In the `/etc/opt/novell/zenworks/conf/xplatzmd.properties` file, add PreferredSMBProtocol key and set the value of the string as SMBv1.

Configuring Windows CIFS share

To make Windows CIFS share accessible, you must create a null session share. Perform the steps according to your device:

- "Setting up a null session share on an NT-based device" on page 118
- "Setting up a null session share on a Windows 2003 Server" on page 119
- "Setting up a null session share on Windows 2008 Server" on page 119

Setting up a null session share on an NT-based device

1. From the **Start** menu, Run the program `regedt32`.
2. In the **Registry Editor** window, search the `HKEY_LOCAL_MACHINE on Local Machine` window.
3. Navigate to `HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/lanmanserver/` parameters.

4. Open the multi string value `NullSessionShares` and add the share name from the selected folder. Enter the value on a new line in the registry value.
5. Close the **Registry Editor** window.
6. Under **Administrative Tools**, select **Services**.
7. Right-click the **Server** service and select **Restart** to restart the service.

Setting up a null session share on a Windows 2003 Server

If the system where you are creating the null session share is running Windows 2003 Server, you must enable the Group Policy "Network access: Let Everyone permissions apply to anonymous users". You must perform the steps mentioned in “Setting up a null session share on an NT-based device” on page 118, then perform the following steps:

1. Click the **Start** menu.
2. Click **Run**.
3. Specify `gpedit.msc`.
4. Go to the following location: `Local Computer Policy\Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options`.
5. Double-click **Network access: Let Everyone permissions apply to anonymous users**.
6. Select **Enable** and press **Enter**.

Setting up a null session share on Windows 2008 Server

If the system where you are creating the null session share is running Windows 2008 Server, you must enable the Group Policy "Network access: Shares that can be accessed anonymously". You must perform the steps mentioned in “Setting up a null session share on an NT-based device” on page 118, and “Setting up a null session share on a Windows 2003 Server” on page 119, then perform the following steps:

1. Click the **Start** menu.
2. Click **Run**.
3. Specify `gpedit.msc`.
4. Go to the following location: `Local Computer Policy\Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options`.
5. Double-click **Network access: Shares that can be accessed anonymously**.
6. Select **Enable** and press **Enter**.

To test your setup, use the `net use` command to connect to your resource using an anonymous login and null password. From a command prompt, execute the following:

```
net use \\servername\sharename "" /user:""
```

(Where `\\servername\sharename` is replaced by the UNC of the null share.)If you already have a connection to the server, you must clear the connection to the server prior to executing the above command, or it will instead attempt to map the device using the previously successful connection parameters.

The response **The command completed successfully** indicates that the device mapped successfully, while errors such as **System error 5 has occurred. Access is denied** indicates a failure and you must verify your setup.If you have successfully mapped the device, then copy files to or from the resource `\\servername\sharename` to ensure that you have the required access.

Shared Content Repository

This feature enables you to share the content repository among multiple Primary Servers in the same zone. In prior releases of ZENworks, every Primary Server had its own content repository. This section includes the following:

Pre-requisites

Before you configure the shared repository, you need to ensure that the following prerequisites are met in the following scenarios:

ZENworks running as a Primary Server on a Linux device

- Ensure that the ZENworks user has read/write access to the shared volume.
- Ensure that shared volume path is configured in the `/etc/fstab` file. This will ensure that during the reboot of the machine, the administrator does not have to remount the shared volume on the Primary Servers.

  The following command is an example of the shared volume path configuration when the shared repository is hosted on an separate OES Server as CIFS Share, on an NSS volume:

  ```
  <IP address of the OES server>/<Shared Volume>/var/opt/novell/zenworks/content-repo cifs username=zenworks,password=<password>,uid=zenworks,gid=zenworks 0 0
  ```

  In this command:

  - Replace <*IP address of the OES server*> with the IP address of the OES Server on which the content repository is hosted.
  - Replace <*Shared Volume*> with the NSS volume configured on the OES Server, with CIFS share enabled.
  - `/var/opt/novell/zenworks/content-repo` is the path of the content repo folder.
  - `username` is the name of the zenworks user, created on the OES Server, which is also LUM (Linux User Management) enabled.

  The following command is an example of the shared volume path configuration when the NFS Share is hosted on a separate SLES Server:

  ```
  <IP address of the SLES Server>:<Shared volume> /var/opt/novell/zenworks/content-repo nfs rw,sync,hard,intr 0 0
  ```

  In this command:

  - Replace <*IP address of the SLES server*> with the IP address of the SLES Server on which the content repository is hosted.
  - Replace <*Shared Volume*> with the NSS volume that is configured on the SLES Server, with NFS share enabled.
  - `/var/opt/novell/zenworks/content-repo` is the path of the content repo folder.

ZENworks running as a Primary Server on a ZENworks Appliance

- Ensure that the ZENworks user has read/write access to the shared volume.
- Ensure that shared volume path is configured in the `/etc/fstab` file. This is to ensure that during the reboot of the machine, the administrator does not have to remount the shared volume on the Primary Servers.

  The following command is an example of the shared volume path configuration when the shared repository is hosted on an OES Server as CIFS Share, on an NSS volume:

  ```
  <IP address of the OES server>/<Shared Volume>/vastorage/var/opt/novell/
  zenworks/content-repo cifs
  username=zenworks,password=<password>,uid=zenworks,gid=zenworks 0 0
  ```

  In this command:

  - Replace <*IP address of the OES server*> with the IP address of the OES Server on which the content repository is hosted.
  - Replace <*Shared Volume*> with the NSS volume configured on the OES Server, with CIFS share enabled.
  - `/vastorage/var/opt/novell/zenworks/content-repo` is the path of the content repo folder.
  - `username` is the name of the zenworks user, created on the OES Server, which is also LUM (Linux User Management) enabled.

NOTE: If NFS Share is configured on the appliance, ensure that you install the `nfs-client` RPM. This RPM is not installed by default along with the appliance.

ZENworks running as a Primary Server on a Windows Server Class device

When ZENworks is running as a Primary Server on a Windows device, the user account with which the ZENworks Loader process is running should have read/write access to the shared repository, before the shared repository is configured.

This section explains how to configure the shared content repository for an anonymous user. The ZENworks user account can be obtained by opening the ZENworks Loader process from the `services.msc` application and navigating to the **Log on** tab. Configuring stricter access permissions is beyond the scope of ZENworks. You will need to contact your File System administrator for further assistance.

The following command is an example for a scenario in which the shared content repository is hosted on an OES Server as CIFS Share, on an NSS volume:

```
C:\Program Files (x86)\Novell\ZENworks\work>mklink /D content-repo \\<ip address of
the OES Server>\<Shared Volume Eg: WIN_VOL>
```

In this command, `WIN_VOL` is the CIFS Share created on the OES Server, with anonymous access.

Configuring the Shared Content Repository for Multiple Primary Servers

1 Stop the ZENworks Loader and ZENworks Server services only on those Primary Servers for which you want to configure the shared content repository.

For example, if there are three Primary Servers in a zone (PS1, PS2 and PS3) and the shared content-repo needs to be configured for PS1 and PS2, then the services need to be stopped only on PS1 and PS2.

2 To back up the existing content, if it is locally mounted, rename the existing `/var/opt/novell/zenworks/content-repo` file to `/var/opt/novell/zenworks/content-repo.bak`.

3 Mount the shared content repo either by configuring the `/etc/fstab` file or by using the `mount` command on a Linux or Windows server. For more information, see the “Pre-requisites” on page 120 section.

4 Repeat steps 1 to 3 to mount each of the Primary Servers to the shared content repository.

5 Execute the configure action only on those Primary Servers that are configured for the shared content repository. This is to let them know that the content repository is shared among them. To execute the configure action, run the following command on all the Primary Servers that are configured for shared content or run the command from any one of the Primary Servers by providing the path details of all the other Primary Servers that share the same content repository in the zone:

```
novell-zenworks-configure -c
"com.novell.zenworks.configure.actions.SharedContentRepoConfigureAction" -
Daction=add
```

or

Add the path details of all the other Primary Servers that share the content repository, from one Primary Server, by running the following command:

```
novell-zenworks-configure -c
"com.novell.zenworks.configure.actions.SharedContentRepoConfigureAction" -
Daction=add -Dservers=/devices/Servers/<Primary Server 1>:<Primary Server
2>....
```

In this command:Replace <*Primary Server 1*> with the full path of the first Primary Server, replace<*Primary Server 2*> with the full path of the second Primary Server, and so on.

6 Copy or move the existing data from the `/var/opt/novell/zenworks/content-repo.bak` file to the `/var/opt/novell/zenworks/content-repo` file.

7 Restart the ZENwork Loader and ZENworks Server services only on those Primary Servers for which the shared content is configured.

NOTE

1. If you plan to add a new Primary Server to an existing zone and then configure the Shared Content Repo for this server, the Primary Server should initially be configured with its own local content repository. Once the server is installed, ensure that there is a long delay in the content replication interval so that content replication does not happen to the local repository. You need to follow steps 1 to 7 that are listed above, to configure the new Primary Server to the shared content repo.
2. If you want the shared content to be available for all the Primary Servers immediately, run the `Replicate Now` action.

Revoking the Sharing of the Content Repository

This scenario will enable you to revoke the sharing of the content repository that is mounted to a Primary Server.

1. Stop the ZENworks Loader and ZENworks Server services on those Primary Servers for which the shared content repository needs to be revoked.
2. Use the following command to revoke the shared content repository:

   ```
   novell-zenworks-configure -c
   "com.novell.zenworks.configure.actions.SharedContentRepoConfigureAction" -
   Daction=remove -Dservers=<Primary Server>
   ```

   In this command, replace *<Primary Server>* with the full path of the Primary Server on which the shared content repository is located.
3. Once the shared content repo folder is revoked successfully, you need to copy the content from the shared content repo to the local content repo.
4. Restart the ZENworks Loader and ZENworks Server services on those Primary Servers for which the shared content repository is revoked.

34 Troubleshooting

The following sections provide solutions to the issues you might encounter during content replication.

Files that have been deleted from the database are still present in the Content Repository

Source: ZENworks

Explanation: Files that have been deleted from the database still exist in the content repository.

Action: Perform the following steps:

IMPORTANT: You cannot retrieve content after you run the Delete command. We strongly recommend that you run the `novell-zenworks-configure -c CheckContentSystem` command first, to identify inconsistencies in the content. This command is applicable only for Primary Servers. After you verify the content, run the command and use the appropriate switch (delete or sync).If you have any queries, contact Technical Support for assistance.

1. Run the following command to sync the database with the content repository:

   ```
   novell-zenworks-configure -c CheckContentSystem -
   Dzenworks.configure.syncDb="true"
   ```

2. To identify content that is available in the content repository, but not in the database, select the `Look for content in the content-repo, not in the database` option.

   Files that are in the content repository and whose content sync status is not updated in database are updated. Any corruption of content in the content repository is reported if the checksum does not match the database.

3 To delete the files that are in the content respository but not in the database run the following command:

```
novell-zenworks-configure -c CheckContentSystem -
Dzenworks.configure.deleteFiles="true"
```

Content in the database is not available in the content repository

Source: ZENworks

Explanation: After you perform an upgrade, some files that are in the database are not available in the content repository.

Action: Perform the following steps:

IMPORTANT: It is strongly recommended to run the `novell-zenworks-configure -c CheckContentSystem` command first, to identify inconsistencies in the content.This command is applicable only for Primary Servers. After you verify the content, run the command and use the appropriate switch (sync). If you have any queries, contact Novell Support for assistance.

1 Run the following command to sync the database with the content repository:

```
novell-zenworks-configure -c CheckContentSystem -
Dzenworks.configure.syncDb="true"
```

2 To identify content that is available in the database, but not in the content repository, select the `Look for content in the database, not in the content-repo` option.

Files that are not available in the content repository are marked as `Unavailable`.

3 Perform the content replication procedure to replicate the files to the content repository.

Removing the Content role from a Satellite does not remove the device from the Closest Server Default Rule and Closest Server Rules

Source: ZENworks

Explanation: If you remove the Content role from a Satellite device, the device is not automatically removed from the Closest Server Default Rule and the Closest Server Rules.

Action: Remove the Satellite device from the Server Hierarchy list. In ZENworks Control Center, click the Configuration tab > select the check box next to the Satellite device, click Action, then click Remove Satellite Server.).

The imaging content is replicated according to the default content replecation schedule even if you change the schedule after promoting a managed device to an Imaging Satellite

Source: ZENworks

Explanation: If you change the Imaging content replication schedule for an Imaging Satellite, the imaging content is replicated from the Primary Server to the Satellite while promoting the managed device to the Imaging Satellite, by using the default schedule and not the revised schedule.

NOTE: ZENworks images are not replicated from one Primary Server to other Primary or Satellite Servers.

Action: To change the imaging content schedule after promoting a managed device to an Imaging Satellite:

1. Remove the Imaging role from the Satellite.

   For detailed information on how to demote a Satellite to a managed device, see Section 15, “Removing the Roles from a Satellite,” on page 59.

2. Add the Imaging role to the Satellite, then configure the desired imaging content replication schedule while configuring the role.

   For detailed information on how to add the Imaging role to a Satellite, see “Understanding the Imaging Role” on page 42..

Join Proxy connection might not work and displays incorrect port information on the Z icon page of the Join Proxy server

Source: ZENworks

Explanation: When a managed device tries to connect to a Primary server for Join Proxy service, the connection might fail. To verify the connection status if you click Servers in the Z icon page of the Join Proxy server, the port information displayed along with the host name might be incorrect. For example, port number could be 80 instead of the default port number 7019.

Action: Update the incorrect Join Proxy settings:

1. Execute `novell-zenworks-configure -c AddJoinProxyRole` on the Join Proxy server that has the incorrect Join Proxy settings
2. Execute `zman lrr -f` on the Primary server to recalculate the closest server rules.

When no content is available, content replication does not work based on the defined schedule

Source: ZENworks; Content Replication

Explanation: When there is no content available for replication, the content replication schedule does not follow the defined schedule or the CDP restart schedule.

Action: You need to configure the `DisableCDPRestartIntervalDoubling` setting, which has been introduced in ZENworks 11 SP4, to `True` or `False`.

- `True`: The CDP restart interval will get reset to the initial value (governed by `CDPRestartInterval` setting) and remain constant till the setting is changed to `False`.
- `False`: The CDP restart interval will double if no content is available.

NOTE: By default, this setting is set to `False`.

To configure the `DisableCDPRestartIntervalDoubling` setting:

- On Linux and Mac operating systems, configure the setting in the `/etc/opt/Novell/zenworks/conf/xplatzmd.properties` file.
- On a Windows operating system, use the Registry Editor and configure the registry key: `HKLM\SOFTWARE\Novell\ZCM: DisableCDPRestartIntervalDoubling=true`

  OR

  `HKLM\SOFTWARE\Novell\ZCM: DisableCDPRestartIntervalDoubling=false`

V Appendixes

The following sections provide information related to ZENworks Primary Servers:

A Support for L4 Switches

Layer 4 (L4) is used to make switching decisions, which means that a switch considers the information in Layer 4 when routing a packet. For example, an L4 switch can decide where to send the packet based on the port numbers. Layer 4 information is used to direct application sessions to different servers and prioritize and queue certain packet types, such as database or application server traffic. An L4 switch requires every device along its path to be together. These switches are useful for WAN and LAN/WAN boundaries.

Each L4 switch has a slightly different method and terminology for the sticky bit or persistence bind, which allows a client that has established a session to be directed to the same Primary Server for all requests sent during the session.

If you choose to deploy Primary Servers behind a L4 switch;

- Ensure that all such Primary servers are running on the same HTTP and HTTPS ports.
- And if you have specified DNS name for L4 switch in ZCC, ensure that the specified DNS name is resolvable by all the Primary servers behind L4.

For pull deployment in ZENworks to work efficiently, you must enable the sticky bit with the sticky age set to 30 minutes. After the deployment task is finished, the sticky bit configuration is not required and can be removed.

The following table lists supported and unsupported scenarios if L4 switching is used in ZENworks:

Supported	Not Supported
Pull deployment (Sticky bit set)	Push deployment
Regular managed device activity (Bundles and policy assignments, remotely controlling the devices, etc.)	Content Satellite
Authentication to user sources	Collection Satellite
	Authentication Satellite

NOTE: System updates of managed devices, Patch Management, and Imaging scenarios have not been tested.

Predeployment Tasks

Before you begin to use the pull deployment method to deploy the ZENworks Agent, perform the following tasks:

1 Create an L4 definition:

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

1b In the Management Zone Settings panel, click **Infrastructure Management**, then click **Closest Server Default Rule** to display the Closest Server Default Rule page.

1c Click **L4 Switch** > **Create Empty L4 Switch Definition**.

1d In the Create Empty L4 Switch Definition dialog box, specify the IP address or DNS name of the L4 switch.

1e Click **OK**.

2 Add Primary Server to the L4 switch:

2a Select the Primary Server that you want to add to the L4 switch, then click **L4 Switch** > **Add To L4 Switch Definition**.

2b In the Add to Existing/New L4 Switch Definition dialog box, specify the L4 IP address or DNS name for a new L4 switch definition or select an existing L4 definition from the drop-down list, then click **OK**.

2c Click **OK**.

3 (Optional) Add an L4 switch definition to a location:

3a Click **Configuration** > **Locations**.

3b Select the location that you want to add to the L4 switch, then click **Servers** tab.

3c Click **L4 Switch** > **Add L4 Switch**.

3d In the Add Existing L4 Switch Definition dialog box, select an existing L4 definition from the drop-down list, then click **OK**.

3e Click **Apply**.

4 Edit the deployment package to add the L4 switch IP address.

For more information on how to edit the deployment package, see "Customizing Packages" in the *ZENworks Discovery, Deployment, and Retirement Reference*.

5 On the L4 switch console, enable the sticky bit or persistent bind with the stick age set to 30 minutes.

For more information on how to enable the sticky bit, refer to your L4 switch vendor documentation.

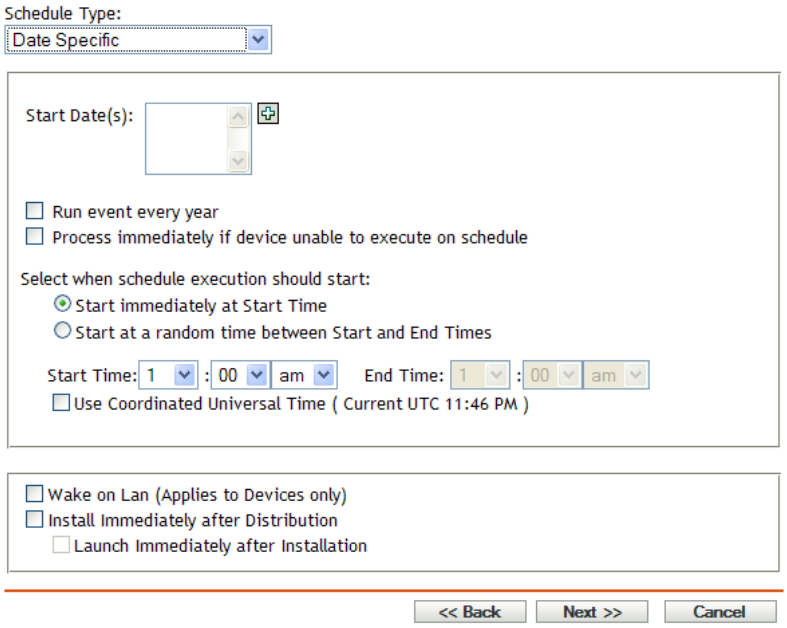
B Schedule Types

You can schedule to run ZENworks components based on your requirements. The following schedules are available:

Date Specific

The Date Specific scheduling option lets you specify one or more dates on which to run the event.

Figure B-1 *Date Specific Schedule*



Start Dates: Click to display a calendar you can use to select a date for the event. You can add multiple dates one at a time.

Run Event Every Year: Select this option to run the event every year on the dates shown in the **Start Date(s)** list.

Process Immediately if Device Unable to Execute on Schedule: Any event is considered past due if a bundle is not executed on the configured schedule for some reason. If you select this option, the past due event is executed during the immediate device refresh.

NOTE: The event is executed immediately after device refresh because the configured schedule which is passed does not recur.

Select When Schedule Execution Should Start: Select one of the following options:

- **Start Immediately at Start Time:** Starts the event at the time you specify in the **Start Time** field.
- **Start at a Random Time between Start Time and End Time:** Starts the event at a randomly selected time between the time you specify in the **Start Time** and **End Time** fields. You can use this option to avoid possible network overload from concurrently scheduled events.

Use Coordinated Universal Time (UTC): The Start Time is converted to Universal Coordinated Time (UTC). Recommended, if the management zone is across geographical locations. Select this option to indicate that the Start Time you entered is already in Coordinated Universal Time and should not be converted. For example, suppose you are in the Eastern time zone. If you enter 10:00 a.m. and select this option, the Start Time is scheduled for 10:00 UTC. If you don't select this option, the Start Time is scheduled for 14:00 UTC because Eastern time is UTC - 4 hours.

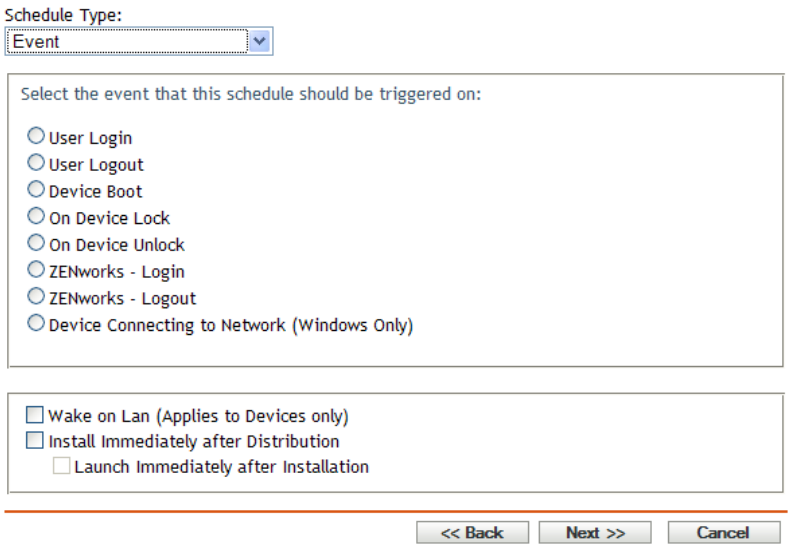
Event

This scheduling option lets you specify the event you want, to trigger the scheduled action.

NOTE

- User management is supported only on Windows platforms.
- Event Schedule type is not supported for Inventory Scans.
- Event Schedules are not supported on Linux and Macintosh devices.

Figure B-2 *Event Schedule*



Select from the following triggers:

User Login: A user logs in to the device's operating system.

User Logout: A user logs out of the device's operating system. This is not applicable if a user shuts down, or reboots the system.

Device Boot: The device powers on.

On Device Lock: The device's operating system is locked.

On Device Unlock: The device's operating system is unlocked.

ZENworks Login: A user logs in to the ZENworks Management Zone.

ZENworks Logout: A user logs out of the ZENworks Management Zone.

Device Connecting to Network (Windows Only): The disconnected device detects a new wired or wireless network connection.

NOTE

At device startup, the ZENworks Agent contacts a ZENworks Server according to the device's refresh schedule to refresh its bundle, policy, configuration, and registration information. If information changes, the ZENworks Agent must refresh its information before the changes can show up on the device, even if one of the event triggers occur. By default, devices refresh randomly between 300 and 360 seconds after device startup with a full refresh every 12 hours.

For example, if you create a bundle and schedule it to launch when the device connects to the network, the device must be manually refreshed or refreshed according to schedule before the ZENworks Agent can upload or launch the bundle, even if the device connects to the network.

Now

Select this option to run the event immediately. For this schedule to be effective during bundle assignment, ensure that the number of devices to which you want to assign a bundle does not exceed 30. If you select more than 30 devices with the distribution schedule set to Now, the following error message is displayed:

```
Distribution Schedule can be set to 'Now' only for bundle assignments to devices
not exceeding 30.
```

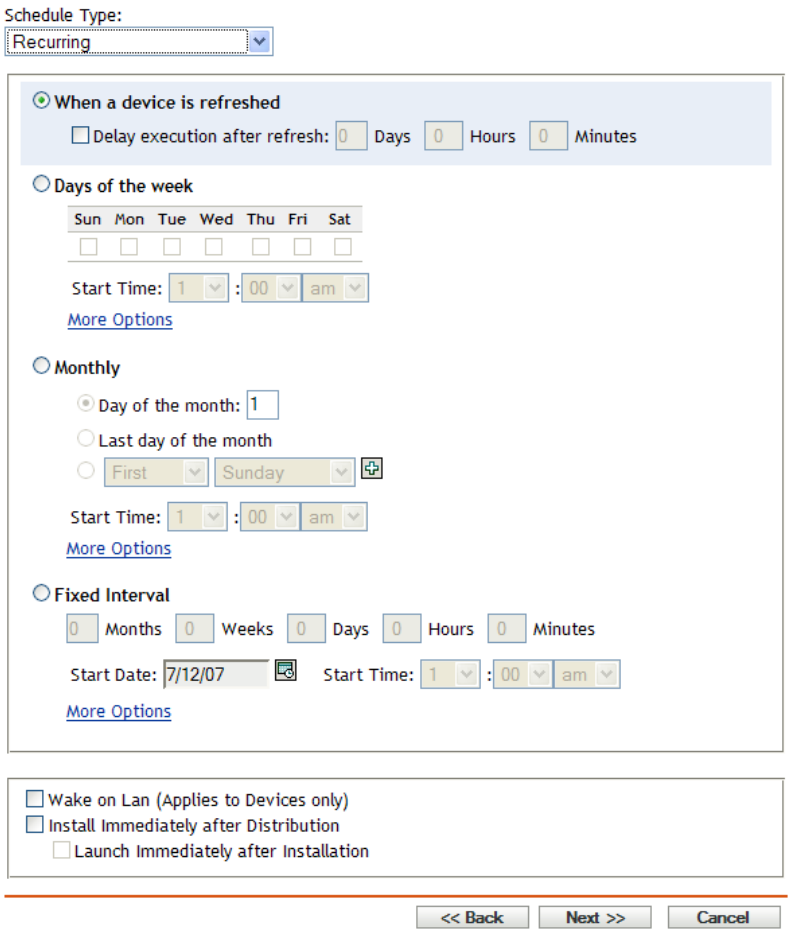
To assign bundles, policies, WOL tasks randomly to more than 30 devices, use the **Quick Tasks** option in ZENworks Control Center. For more information, see Initiating a Quick Task in the *ZENworks Control Center Reference*.

Recurring

The Recurring scheduling option lets you repeat the event at a specified interval.

NOTE: The following sections describe all of the Recurring schedule options. Depending on the event or action you are scheduling, some options might not be available.

Figure B-3 *Recurring Schedule*



When a Device Is Refreshed: This schedule causes the event to occur each time the ZENworks Agent performs a refresh on the device. If you want to delay the event so that it does not happen immediately upon refresh, select the **Delay execution after refresh** option and specify the number of days, hours, or minutes you want to delay the event.

Days of the Week: This schedule lets you specify the days during the week that you want the event to run. The event is run on these same days each week.

Select **Days of the Week**, then fill in the following fields:

- **Sun... Sat:** Specifies the days of the week you want to run the event.
- **Start Time:** Specifies the time you want to run the event.
- **Process Immediately if Device Unable to Execute on Schedule:** Any event is considered past due if a bundle is not executed on the configured schedule for some reason. If you select this option:
  - A past due bundle is executed immediately after the device refresh if the bundle has flown down to the agent on or before the configured schedule.
  - A past due bundle is executed in the next recurring schedule if the bundle has not flown down to the device on or before the configure schedule.
- **Use Coordinated Universal Time:** The Start Time is converted to Universal Coordinated Time (UTC). Recommended, if the management zone is across geographical locations. Select this option to indicate that the Start Time you entered is already in Coordinated Universal Time and

should not be converted. For example, suppose you are in the Eastern time zone. If you enter 10:00 a.m. and select this option, the Start Time is scheduled for 10:00 UTC. If you don't select this option, the Start Time is scheduled for 14:00 UTC because Eastern time is UTC - 4 hours.

- **Start at a Random Time between Start Time and End Time:** Starts the event at a randomly selected time between the time you specify in the **Start Time** and **End Time** fields. You can use this option to avoid possible network overload from concurrently scheduled events.
- **Restrict Schedule Execution to the Following Date Range:** Limits running the event to the time period specified by the starting and ending dates.

Monthly: This schedule lets you specify one or more days during the month to run the event.

Select **Monthly**, then fill in the following fields:.

- **Day of the Month:** Specifies the day of the month to run the event. Valid entries are 1 through 31. If you specify 29, 30, or 31 and a month does not have those days, the event is not run that month.
- **Last Day of the Month:** Runs the event on the last day of the month, regardless of its date (28, 30, or 31).
- ***First Sunday*:** Specifies a specific day of a week. For example, the first Monday or the third Tuesday. Click  to add multiple days.
- **Start Time:** Specifies the time you want to run the event.
- **Process Immediately if Device Unable to Execute on Schedule:** Any event is considered past due if a bundle is not executed on the configured schedule for some reason. If you select this option:
  - A past due bundle is executed immediately after the device refresh if the bundle has flown down to the agent on or before the configured schedule.
  - A past due bundle is executed in the next recurring schedule if the bundle has not flown down to the device on or before the configure schedule.
- **Use Coordinated Universal Time:** The Start Time is converted to Universal Coordinated Time (UTC). Recommended, if the management zone is across geographical locations. Select this option to indicate that the Start Time you entered is already in Coordinated Universal Time and should not be converted. For example, suppose you are in the Eastern time zone. If you enter 10:00 a.m. and select this option, the Start Time is scheduled for 10:00 UTC. If you don't select this option, the Start Time is scheduled for 14:00 UTC because Eastern time is UTC - 4 hours.
- **Start at a Random Time between Start Time and End Time:** Starts the event at a randomly selected time between the time you specify in the Start Time and End Time boxes. You can use this option to avoid possible network overload from concurrently scheduled events.
- **Restrict Schedule Execution to the Following Date Range:** Limits running of the event to the time period specified by the starting and ending dates.

Fixed Interval: This schedule lets you specify an interval between days to run the event. For example, you can run the event every 14 days.

Select **Fixed Interval**, then fill in the following fields:.

- **Months, Weeks, Days, Hours, Minutes:** Specifies the interval between times when the event is run. You can use any combination of months, weeks, days, hours, and minutes. For example, both *7 days, 8 hours* and *1 week, 8 hours* provide the same schedule.
- **Start Date:** Specifies the initial start date for the interval.

NOTE: For a newly promoted Satellite Server, by default, the replication starts with a delay of 1 day.

- **Start Time:** Specifies the initial start time for the interval.
- **Process Immediately if Device Unable to Execute on Schedule:** Any event is considered past due if a bundle is not executed on the configured schedule for some reason. If you select this option:
  - A past due bundle is executed immediately after the device refresh if the bundle has flown down to the agent on or before the configured schedule.
  - A past due bundle is executed in the next recurring schedule if the bundle has not flown down to the device on or before the configure schedule.
- **Use Coordinated Universal Time:** The Start Time is converted to Universal Coordinated Time (UTC). Recommended, if the management zone is across geographical locations. Select this option to indicate that the Start Time you entered is already in Coordinated Universal Time and should not be converted. For example, suppose you are in the Eastern time zone. If you enter 10:00 a.m. and select this option, the Start Time is scheduled for 10:00 UTC. If you don't select this option, the Start Time is scheduled for 14:00 UTC because Eastern time is UTC - 4 hours.
- **Restrict Schedule Execution to the Following Date Range:** Limits running of the event to the time period specified by the start date, end date, and end time.

No Schedule

The No Schedule option is selected if you do not want to run the event automatically.

C Understanding Communication between ZENworks Components in Multi-Locale Environment

If you choose to run the ZENworks Primary Server, ZENworks Control Center, and ZENworks Agent on operating systems with different locales, review the following points to understand the communication behavior between ZENworks components:

- ZENworks extends support to the following languages:
  - Single-byte languages: English, French, German, Italian, Portuguese, and Spanish
  - Double-byte languages: Chinese-Traditional, Chinese-Simplified, and Japanese
- ZENworks Primary Server is language independent. It can render messages in all the languages supported by ZENworks.
- It is recommended to launch ZENworks Control Center in the same locale as the operating system locale of the management console.

  For example, if the operating system locale of the management console is German, you must launch ZENworks Control Center in German.

  You can choose to launch ZENworks Control Center in a locale different from the operating system of the management console only if the device has the necessary language support packs installed.
- ZENworks uses UTF-8 encoding for ZENworks textual messages and local encoding for standard Windows messages. If ZENworks Control Center is launched in a locale that is different from the operating system locale of the ZENworks Agent, the ZENworks messages that are sent by the agent are only translated and displayed in the ZENworks Control Center locale. The standard Windows messages are displayed in the operating system locale of the management console.

  For example, assume that the operating system locale of the ZENworks Agent is German and the operating system locale of the management console is French. If you choose to launch ZENworks Control Center in French, the ZENworks messages from the agent are displayed in French and not in German in ZENworks Control Center. The Windows messages sent from the agent are displayed in French.
- During Remote Management sessions and Remote Management operations that are triggered by the ZENworks Icon, all messages and user prompts are displayed on the managed device in the language of its operating system locale. During a Remote Management session, the keystrokes are translated according to the management console keyboard; the agent simulates the virtual key codes it receives from the viewer.

  If the operating system locale of the managed device is a single-byte locale supported by ZENworks, you can choose to launch Remote Viewer in any single-byte locale supported by ZENworks. For example, if the locale of the operating system of the managed device is French, you can launch the Remote Viewer in any of the following locales: English, French, German, Italian, Portuguese, or Spanish.

If the operating system locale of the managed device is a double-byte locale supported by ZENworks, you must launch ZENworks Control Center in the same double-byte locale as the operating system locale of the management console, or in English. For example, if the locale of the operating system of the managed device is Japanese, you must launch the Remote Viewer in either Japanese or English.

Table C-1 *Supported Compatibility Matrix between the Operating System Locale of the Managed Device and ZENworks Control Center Locale*

Operating System Locale of the Managed Device	Remote Viewer Locale
English, French, German, Italian, Portuguese, or Spanish	English, French, German, Italian, Portuguese, or Spanish
Chinese-Simplified	Chinese-Simplified or English
Chinese-Traditional	Chinese-Traditional or English
Japanese	Japanese or English

D RPMs for Linux Primary Servers

Server	RPM
SLES 11, 64-bit	bash.x86_64, coreutils.x86_64, diffutils.x86_64, fillup.x86_64, glibc.x86_64, grep.x86_64, insserv.x86_64, logrotate.x86_64, perl-base.x86_64, sed.x86_64, tcpd.x86_64, libxml2.x86_64, licenses.noarch, libavahi-client3.x86_64, libavahi-common3.x86_64, libjpeg.x86_64, libopenssl0_9_8.x86_64, xorg-x11-libX11.x86_64, xorg-x11-libXext.x86_64, xorg-x11-libXfixes.x86_64, xorg-x11-libs.x86_64, zlib.x86_64, glibc-32bit.x86_64, libjpeg-32bit.x86_64, zlib-32bit.x86_64, libbz2-1.x86_64, libexpat1.x86_64, libglib-2_0-0.x86_64, libgmodule-2_0-0.x86_64, libgobject-2_0-0.x86_64, libsqlite3-0.x86_64, rpm.x86_64, dbus-1.x86_64, hal.x86_64, net-tools.x86_64, util-linux.x86_64, gdbm.x86_64, libncurses5.x86_64, libreadline5.x86_64, perl.x86_64, gawk.x86_64, pwdutils.x86_64, findutils.x86_64, coreutils-lang.x86_64, info.x86_64, libacl.x86_64, libattr.x86_64, libselinux1.x86_64, pam.x86_64, filesystem.x86_64, bzip2.x86_64, cron.x86_64, popt.x86_64, xorg-x11-libXau.x86_64, xorg-x11-libxcb.x86_64, fontconfig.x86_64, freetype2.x86_64, xorg-x11-libICE.x86_64, xorg-x11-libSM.x86_64, xorg-x11-libXmu.x86_64, xorg-x11-libXp.x86_64, xorg-x11-libXpm.x86_64, xorg-x11-libXprintUtil.x86_64, xorg-x11-libXrender.x86_64, xorg-x11-libXt.x86_64, xorg-x11-libXv.x86_64, xorg-x11-libfontenc.x86_64, xorg-x11-libxkbfile.x86_64, glib2.x86_64, pcre.x86_64, permissions.x86_64, aaa_base.x86_64, ConsoleKit.x86_64, PolicyKit.x86_64, dbus-1-glib.x86_64, libgcc43.x86_64, libsmbios2.x86_64, libstdc++43.x86_64, libusb-0_1-4.x86_64, libuuid1.x86_64, libvolume_id1.x86_64, parted.x86_64, pciutils.x86_64, pm-utils.x86_64, pmtools.x86_64, setserial.x86_64, audit-libs.x86_64, libblkid1.x86_64, libsepol1.x86_64, util-linux-lang.x86_64, terminfo-base.x86_64, libdb-4_5.x86_64, mono-core.x86_64, libldap-2_4-2.x86_64, libnscd.x86_64, libxcrypt.x86_64, openslp.x86_64, pam-modules.x86_64, libzio.x86_64, cracklib.x86_64, glib2-branding-SLES.noarch, glib2-lang.x86_64, cpio.x86_64, login.x86_64, mingetty.x86_64, ncurses-utils.x86_64, psmisc.x86_64, sles-release.x86_64, udev.x86_64, libgthread-2_0-0.x86_64, pam-config.x86_64, device-mapper.x86_64, libreiserfs.x86_64, pciutils-ids.noarch, sysvinit.x86_64, cyrus-sasl.x86_64, cracklib-dict-full.x86_64, cpio-lang.x86_64, sles-release-DVD.x86_64, update-alternatives.noarch, postfix.x86_64, netcfg.noarch, openldap2-client.x86_64, jpackage-utils.x86_64

Server	RPM
SLES 12, 64 bit	bash-4.2-82.1.x86_64, bind-libs-9.9.9P1-49.1.x86_64, bind-utils-9.9.9P1-49.1.x86_64, btrfsprogs-4.1.2-7.1.x86_64, bzip2-1.0.6-29.2.x86_64, cdrkit-cdrtools-compat-1.1.11-24.15.x86_64, coreutils-8.22-9.1.x86_64, cpio-2.11-29.1.x86_64, cracklib-2.9.0-7.1.x86_64, cracklib-dict-full-2.8.12-63.17.x86_64, cron-4.2-58.3.x86_64, cronie-1.4.11-58.3.x86_64, cups-libs-1.7.5-12.4.x86_64, curl-7.37.0-31.1.x86_64, dbus-1-1.8.22-22.2.x86_64, dbus-1-x11-1.8.22-22.2.x86_64, diffutils-3.3-5.40.x86_64, dirmngr-1.1.1-4.1.x86_64, ethtool-3.12.1-5.1.x86_64, file-5.19-9.1.x86_64, filesystem-13.1-11.13.x86_64, fillup-1.42-270.64.x86_64, findutils-4.5.12-7.1.x86_64, fipscheck-1.2.0.9.3.x86_64, gawk-4.1.0-3.663.x86_64, glib2-tools-2.38.2-5.12.x86_64, glibc-2.19-38.2.x86_64, gnu-unifont-bitmap-fonts-20080123-83.182.noarch, grep-2.16-3.1.x86_64, gtk2-tools-2.24.24-3.1.x86_64, iceauth-1.0.6-3.59.x86_64, icedax-1.1.11-24.15.x86_64, icewm-1.3.8-5.3.x86_64, identity-abstraction-0.1.620-24.noarch, info-4.13a-37.229.x86_64, initviocons-0.5-101.62.x86_64, input-utils-2007.06.22-179.70.x86_64, insserv-compat-0.1-13.1.noarch, iotop-0.6-3.10.noarch, iproute2-3.12-12.2.x86_64, iptables-1.4.21-2.10.x86_64, iputils-s20121221-2.19.x86_64, jakarta-commons-lang-2.0-22.4.noarch, jakarta-commons-logging-1.0.4-21.2.noarch, javapackages-tools-2.0.1-6.10.x86_64, kbd-1.15.5-8.7.1.x86_64, keyutils-1.5.9-3.29.x86_64, kpartx-0.5.0-55.1.x86_64, less-458-5.13.x86_64, libacl1-2.2.52-6.1.x86_64, libadns1-1.4-101.65.x86_64, libaio1-0.3.109-17.15.x86_64, libao4-1.2.0-1.13.x86_64, libao-plugins4-1.2.0-1.13.x86_64, libapparmor1-2.8.2-45.1.x86_64, libapr1-1.5.1-2.7.x86_64, libapr-util1-1.5.3-1.77.x86_64, libasm1-0.158-6.1.x86_64, libasound2-1.0.27.2-11.10.x86_64, libassuan0-2.1.1-3.217.x86_64, libatk-1_0-0-2.10.0-1.84.x86_64, libattr1-2.4.47-3.143.x86_64, libaudiofile1-0.3.6-4.4.x86_64, libaudit1-2.3.6-3.103.x86_64, libaugeas0-1.2.0-10.1.x86_64, libavahi-client3-0.6.31-23.1.x86_64, libavahi-common3-0.6.31-23.1.x86_64, libblkid1-2.25-37.1.x86_64, libbz2-1-1.0.6-29.2.x86_64, libcairo2-1.12.16-16.3.x86_64, libcamgm100-1.0.7-1.4.x86_64, libcap2-2.22-13.1.x86_64, libcap-ng0-0.7.3-4.125.x86_64, libcloog-isl4-0.18.1-1.124.x86_64, libcom_err2-1.42.11-7.1.x86_64, libconfuse0-2.7-4.1.x86_64, libcrack2-2.9.0-7.1.x86_64, libcroco-0_6-3-0.6.8-6.62.x86_64, libcryptsetup4-1.6.4-2.10.x86_64, libcurl4-7.37.0-31.1.x86_64, libdb-4_8-4.8.30-27.206.x86_64, libdbus-1-3-1.8.22-22.2.x86_64, libdcerpc0-4.2.4-26.2.x86_64, libdcerpc-binding0-4.2.4-26.2.x86_64, libdnet1-1.12-20.57.x86_64, libdrm_intel1-2.4.52-2.12.x86_64, libdrm_nouveau2-2.4.52-2.12.x86_64, libdrm_radeon1-2.4.52-2.12.x86_64, liboggkate1-0.4.1-20.65.x86_64, libopenssl1_0_0-1.0.1i-52.1.x86_64, libp11-kit0-0.20.3-7.1.x86_64, libpango-1_0-0-1.36.3-4.14.x86_64, libparted0-3.1-19.3.1.x86_64, libpcap1-1.5.3-6.1.x86_64, libpci3-3.2.1-7.1.x86_64, libpciaccess0-0.13.2-5.1.x86_64, libpcre16-0-8.39-7.1.x86_64, libpcre1-8.39-7.1.x86_64, libpixman-1-0-0.32.6-1.13.x86_64, libply2-0.9.0-25.1.x86_64, libply-boot-client2-0.9.0-25.1.x86_64, libply-splash-core2-0.9.0-25.1.x86_64, libply-splash-graphics2-0.9.0-25.1.x86_64, libpng16-16-1.6.8-11.1.x86_64, libpopt0-1.16-26.128.x86_64, libprocps3-3.3.9-7.1.x86_64, libproxy1-0.4.11-11.2.x86_64, libpth20-2.0.7-139.67.x86_64, libpulse0-5.0-2.7.x86_64, libpython2_7-1_0-2.7.9-24.2.x86_64, libqrencode3-3.4.3-1.31.x86_64, libQt5Core5-5.5.1-6.1.x86_64, libQt5DBus5-5.5.1-6.1.x86_64, libQt5Gui5-5.5.1-6.1.x86_64, libQt5Network5-5.5.1-6.1.x86_64, libQt5Widgets5-5.5.1-6.1.x86_64, libQt5X11Extras5-5.5.1-3.2.x86_64, libreadline6-6.2-82.1.x86_64, libreiserfscore0-3.6.24-5.47.x86_64, libruby2_1-2_1-2.1.2-12.3.x86_64, libsamba-credentials0-4.2.4-26.2.x86_64, libsamba-hostconfig0-4.2.4-26.2.x86_64, libsamba-passdb0-4.2.4-26.2.x86_64, libsamba-util0-4.2.4-26.2.x86_64, libsamdb0-4.2.4-26.2.x86_64, libsasl2-3-2.1.26-7.1.x86_64, libSDL-1_2-0-1.2.15-14.1.x86_64, libseccomp2-2.1.1-5.1.x86_64, libselinux1-2.3-4.6.x86_64, libsemanage1-2.3-1.340.x86_64, libsensors4-3.3.5-1.22.x86_64, libsepol1-2.3-1.476.x86_64, libSM6-1.2.2-3.59.x86_64, libsmartcols1-2.25-37.1.x86_64, libsmbclient-raw0-4.2.4-26.2.x86_64, libsmbconf0-4.2.4-26.2.x86_64, libsmbldap0-4.2.4-26.2.x86_64, libsmi-0.4.8-18.63.x86_64, libsmi2-0.4.8-18.63.x86_64, libsndfile1-1.0.25-25.1.x86_64, libsoftokn3-3.21.3-50.1.x86_64, libsolv-tools-0.6.23-2.34.1.x86_64, libspeex1-1.1.999_1.2rc1-22.64.x86_64, libsqlite3-0-3.8.10.2-3.1.x86_64,

Server	RPM
	libssh2-1-1.4.3-19.1.x86_64, libstdc++6-6.2.1+r239768-2.4.x86_64, libstorage6-2.25.35.1-3.1.x86_64, libstorage-ruby-2.25.35.1-3.1.x86_64, libtalloc2-2.1.5-4.1.x86_64, libtasn1-3.7-11.1.x86_64, libtasn1-6-3.7-11.1.x86_64, libtdb1-1.3.8-4.1.x86_64, libtevent0-0.9.26-4.1.x86_64, libtevent-util0-4.2.4-26.2.x86_64, libtiff5-4.0.6-31.1.x86_64, libtirpc1-0.2.3-12.3.x86_64, libts-1_0-0-1.0-7.44.x86_64, libudev1-210-116.3.3.x86_64, libunwind-1.1-9.8.x86_64, libusb-0_1-4-0.1.13-29.13.x86_64, libusb-1_0-0-1.0.18-2.6.x86_64, libustr-1_0-1-1.0.4-31.197.x86_64, libutempter0-1.1.6-5.114.x86_64, libuuid1-2.25-37.1.x86_64, libvmtools0-10.0.5-3.1.x86_64, libvorbis0-1.3.3-8.23.x86_64, libvorbisenc2-1.3.3-8.23.x86_64, libvorbisfile3-1.3.3-8.23.x86_64, libwbclient0-4.2.4-26.2.x86_64, libwicked-0-6-0.6.31-26.1.x86_64, libwrap0-7.6-886.3.x86_64, libX11-6-1.6.2-11.1.x86_64, libX11-6-32bit-1.6.2-11.1.x86_64, libX11-data-1.6.2-11.1.noarch, libX11-devel-1.6.2-11.1.x86_64, libX11-xcb1-1.6.2-11.1.x86_64, libx86emu1-1.5-1.2.x86_64, libxatracker2-1.0.0-100.1.x86_64, libXau6-1.0.8-4.58.x86_64, libXau6-32bit-1.0.8-4.58.x86_64, libXau-devel-1.0.8-4.58.x86_64, libXaw7-1.0.12-4.1.x86_64, libxcb1-1.10-3.1.x86_64, libxcb1-32bit-1.10-3.1.x86_64, libxcb-composite0-1.10-3.1.x86_64, libxcb-damage0-1.10-3.1.x86_64, libxcb-devel-1.10-3.1.x86_64, libxcb-dpms0-1.10-3.1.x86_64, libxcb-dri2-0-1.10-3.1.x86_64, libxcb-dri3-0-1.10-3.1.x86_64, libxcb-glx0-1.10-3.1.x86_64, libxcb-icccm4-0.4.0-1.16.x86_64, libxcb-image0-0.3.9-8.60.x86_64, libxcb-keysyms1-0.3.9-8.54.x86_64, libxcb-present0-1.10-3.1.x86_64, libxcb-randr0-1.10-3.1.x86_64, libxcb-record0-1.10-3.1.x86_64, libxcb-render0-1.10-3.1.x86_64, libxcb-render-util0-0.3.8-8.52.x86_64, libxcb-res0-1.10-3.1.x86_64, libxcb-screensaver0-1.10-3.1.x86_64, libxcb-shape0-1.10-3.1.x86_64, libxcb-shm0-1.10-3.1.x86_64, libxcb-sync1-1.10-3.1.x86_64, libxcb-util1-0.3.9-10.54.x86_64, libxcb-xevie0-1.10-3.1.x86_64, libxcb-xf86dri0-1.10-3.1.x86_64, libxcb-xfixes0-1.10-3.1.x86_64, libxcb-xinerama0-1.10-3.1.x86_64, libxcb-xkb1-1.10-3.1.x86_64, libxcb-xprint0-1.10-3.1.x86_64, libxcb-xtest0-1.10-3.1.x86_64, libxcb-xv0-1.10-3.1.x86_64, libxcb-xvmc0-1.10-3.1.x86_64, libXcomposite1-0.4.4-7.53.x86_64, libXcursor1-1.1.14-3.60.x86_64, libXdamage1-1.1.4-7.54.x86_64, libXdmcp6-1.1.1-8.59.x86_64, libxerces-c-3_1-3.1.1-12.3.x86_64, libXext6-1.3.2-3.61.x86_64, libXext6-32bit-1.3.2-3.61.x86_64, libXext-devel-1.3.2-3.61.x86_64, libXfixes3-5.0.1-5.2.x86_64, libXfont1-1.4.7-7.1.x86_64, libXfontcache1-1.0.5-10.55.x86_64, libXft2-2.3.1-9.32.x86_64, libXi6-1.7.4-17.1.x86_64, libXinerama1-1.1.3-3.55.x86_64, libxkbcommon0-0.4.1-3.1.x86_64, libxkbcommon-x11-0-0.4.1-3.1.x86_64, libxkbfile1-1.0.8-11.1.x86_64, libxml2-2-2.9.1-26.3.1.x86_64, libxml2-tools-2.9.1-26.3.1.x86_64, libxml-security-c17-1.7.3-2.2.x86_64, libXmu6-1.1.2-3.60.x86_64, libXmuu1-1.1.2-3.60.x86_64, libXpm4-3.5.11-3.60.x86_64, libXrandr2-1.4.2-5.2.x86_64, libXrender1-0.9.8-5.2.x86_64, libxshmfence1-1.1-1.28.x86_64, libxslt1-1.1.28-6.57.x86_64, libxslt-tools-1.1.28-6.57.x86_64, libXt6-1.1.4-3.59.x86_64, libxtables10-1.4.21-2.10.x86_64, libXtst6-1.2.2-5.2.x86_64, libXtst6-32bit-1.2.2-5.2.x86_64, libXxf86misc1-1.0.3-10.54.x86_64, libXxf86vm1-1.1.3-3.54.x86_64, libyaml-0-2-0.1.6-7.1.x86_64, libyui7-3.2.3-1.2.x86_64, libyui-ncurses7-2.47.4-1.2.x86_64, libyui-ncurses-pkg7-2.48.2-1.2.x86_64, libyui-qt7-2.46.21-1.3.x86_64, libz1-1.2.8-5.1.x86_64, libzio1-1.00-9.188.x86_64, linux-glibc-devel-3.12-6.54.noarch, logrotate-3.8.7-3.21.x86_64, make-4.0-4.1.x86_64, mcescan-1.0.0-11.noarch, ncurses-utils-5.9-40.124.x86_64, netcfg-11.5-27.1.noarch, net-tools-1.60-764.185.x86_64, openslp-2.0.0-17.1.x86_64, openssl-1.0.1i-52.1.x86_64, parted-3.1-19.3.1.x86_64, pciutils-3.2.1-7.1.x86_64, pciutils-ids-2016.04.04-11.1.noarch, perl-5.18.2-11.1.x86_64, permissions-2015.09.28.1626-13.1.x86_64, postfix-2.11.6-24.2.x86_64, procmail-3.22-267.12.x86_64, procps-3.3.9-7.1.x86_64, rpm-4.11.2-15.1.x86_64, sles-release-POOL-12.1-1.331.x86_64, systemd-210-116.3.3.x86_64, systemd-bash-completion-210-116.3.3.noarch.

E TCP and UDP Ports Used by ZENworks Primary Servers

The following table lists the default TCP and UDP ports that are used by ZENworks Primary Servers. These ports are opened automatically when installing a Primary Server.

Item	Requirement	Additional Details
Firewall Settings: TCP Inbound Ports	80 and 443	Port 80 is for Tomcat non-secure port and Port 443 is for Tomcat secure port. Port 443 is also used for CASA authentication. Opening this port allows ZENworks to manage devices outside of the firewall. It is a good practice to make sure that the network is configured to always allow communication on this port between the ZENworks Server and ZENworks Agents on managed devices. If other services are running on ports 80 and 443, such as Apache, the installation program asks you for new ports to use. If you plan to use AdminStudio ZENworks Edition, it requires that the Primary Server is using ports 80 and 443.
	998	Used by the Preboot Server (novell-pbserv). The Preboot Server (novell-pbserv) is used only with ZENworks Configuration Management.
	5223	Used by enrolled mobile devices to communicate with the ZENworks MDM Servers.
	7444	Used to view the system update status of servers and managed devices. **IMPORTANT:** This is a fixed port. During Installation and Upgrade ensure that this port is not blocked.

Item	Requirement	Additional Details
Firewall Settings: TCP Outbound Ports	80 and 443	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 Ivanti licensing server (novell.patchlink.com), the patch content and checksum data is retrieved from an AKAMAI hosted content distribution network (novell.cdn.lumension.com). You must make sure 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. Primary Server performs the ZENworks System Update Entitlement activation over HTTP (port 443) using the secure-www.novell.com (https://secure-www.novell.com) website. This rule can be turned off after successfully completing the entitlement activation. For more information, see the *ZENworks System Updates Reference*. Primary Server downloads system update related information and content over HTTP (port 443) using the nu.novell.com (https://nu.novell.com) website. For more information see "Managing Update Downloads" in the *ZENworks System Updates Reference*. **NOTE:** You must assign the Network Interface to the firewall zone. Firewall rules are applied to this zone for managing the ports used by ZENworks.
	2195 and 2196	Used by ZENworks MDM Servers to communicate with the Apple Push Notification service (APNs).

Item	Requirement	Additional Details
	2645	Used for CASA authentication. Opening this port allows ZENworks to manage devices outside of the firewall. It is a good practice to make sure that the network is configured to always allow communication on this port between the ZENworks Server and ZENworks Agents on managed devices.
	5550	Used by Remote Management Listener by default.You can change this port in the Remote Management Listener dialog box in ZENworks Control Center. Remote Management is used only with ZENworks Configuration Management.
	5750	Used by Remote Management proxy. Remote Management is used only with ZENworks Configuration Management.
	5950	Used by Remote Management service by default. You can change this port in the Remote Management Settings panel of the Remote Management Configuration page in ZENworks Control Center. Remote Management is used only with ZENworks Configuration Management.
	7019	Used by Join Proxy
	7628	Used by the ZENworks Agent for Quick Tasks. **IMPORTANT:** This is a fixed port.During Installation and Upgrade ensure that this port is not blocked.
	8005	Used by Tomcat to listen to shutdown requests. This is a local port, and cannot be accessed remotely.
	8009	Used by Tomcat AJP connector.

Item	Requirement	Additional Details
	9971	Used by AMT Hello Listener to discover the Intel AMT devices. **IMPORTANT:** This is a fixed port.During Installation and Upgrade ensure that this port is not blocked.
	61491	Used for Diagnostics of ZENworks Loader Service **IMPORTANT:** This is a fixed port.During Installation and Upgrade ensure that this port is not blocked.
	61492	Used for Diagnostics of ZENworks JoinProxy Service **IMPORTANT:** This is a fixed port.During Installation and Upgrade ensure that this port is not blocked.
	61493	Used for Diagnostics of ZENworks CASA Service **IMPORTANT:** This is a fixed port.During Installation and Upgrade ensure that this port is not blocked.
	61494	Used for Diagnostics of ZENworks Xplat Agent Service **IMPORTANT:** This is a fixed port. During Installation and Upgrade ensure that this port is not blocked.
	61495	Used for Diagnostics of ZENworks Server Service **IMPORTANT:** This is a fixed port. During Installation and Upgrade ensure that this port is not blocked.
Firewall Settings: UDP Ports	67	Used by proxy DHCP when it is not running on the same device as the DHCP server.
	69	Used by the Imaging TFTP, but will not work across firewall because it opens random UDP port for each PXE device. The Imaging TFTP is used only with ZENworks Configuration Management.

Item	Requirement	Additional Details
	997	Used by the Imaging Server for multicasting. The Imaging Server is used only with ZENworks Configuration Management.
	1761	Port 1761 on the router is used to forward subnet-oriented broadcast magic packets for Wake-On-LAN.
	4011	Used for proxy DHCP when it is running on the same device as the DHCP server. Make sure that the firewall is configured to allow the broadcast traffic to the proxy DHCP service.
	13331	Used by the zmgpreboot policy, but will not work across firewall because it opens random UDP port for each PXE device. The zmgpreboot policy is used only with ZENworks Configuration Management.