Disaster Recovery Reference

ZENworks® 11 Support Pack 3

July 2014

Novell.

About This Guide

This *ZENworks 11 SP3 Disaster Recovery Reference* explains the disaster recovery mechanisms available to help you protect the first Primary Server of a Management Zone if an organizational risk assessment identifies a need for such steps:

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 11 SP3 is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the ZENworks 11 SP3 documentation Web site (http://www.novell.com/documentation/zenworks113).

Contents

1 Backing Up and Restoring the ZENworks Server and Certificate Authority

The following sections provide more information about backing up and restoring a ZENworks Server and certificate authority:

1.1 Backing Up a ZENworks Server

Novell ZENworks 11 allows you to back up and restore the configuration files for a ZENworks Primary Server. This enables you to maintain a ZENworks Server's identity and configuration if a server fails or if you need to upgrade to new server hardware.

Server backup operation is version specific. When a Server is updated to a higher version, the backup data needs to be collected for the specific version.The backup saves only the configuration files. The following items must be backed up separately:

- The content repository (bundle, policy, and image files). You should do a separate backup for the content repository if you only have one Primary Server in the Management Zone. If you have two or more Primary Servers and you've replicated all content to both servers, they serve as backup copies to each other.

- The ZENworks database (if it resides on the ZENworks Server). Backing up the ZENworks Server and backing up the ZENworks database are two separate processes. If your ZENworks database resides on the same server as one of your ZENworks Servers, first back up the database and then back up the ZENworks Server. Because the ZENworks database changes frequently, you should back up the database on a regular schedule. For information about backing up the database, see the *ZENworks 11 SP3 Database Management Reference*.

When you back up a ZENworks Server using a zman command, all files in the `Novell\ZENworks\conf` directory on a Windows server or the `etc/opt/novell/zenworks/` directory on a Linux server are stored in an encrypted backup file in a location that you specify. For more information on the files that are stored as backup, see "List of files and folders stored as backup after running the zman zenserver-backup command" on page 8.

1 (Conditional) If the server you are backing up hosts the ZENworks database, manually back up the database file to a safe location.

For information about backing up the database, see the *ZENworks 11 SP3 Database Management Reference*.

2 At a command prompt on the ZENworks Server, enter the following command:

```
zman zenserver-backup path_to_backup_file_to_create
```

For example:

```
zman zenserver-backup c:\zcm_backups\zone_backup.bak
```

or

```
zman zenserver-backup /root/zcm_backups/zone_backup.bak
```

3 When prompted, enter a ZENworks administrator name and password.

4 When prompted, enter a passphrase (at least 10 characters) to be used for encrypting the backup file.

Make sure you remember this passphrase. You must enter it if you ever need to restore the server.

5 (Conditional) If this is your only Primary Server, or if this is the only Primary Server that contains all content defined in your Management Zone, manually back up your content repository to a safe location.

For information on the content repository, see "Content" in the *ZENworks 11 SP3 Primary Server and Satellite Reference*.

IMPORTANT: If this is the only Primary Server that contains all of your defined content for the Management Zone and you do not back up the content repository, you are not prepared for a full disaster recovery.

6 Repeat Step 1 and Step 5 on a regular basis.

The zman command documented in Step 2 through Step 4 only needs to be run once.

List of files and folders stored as backup after running the zman zenserver-backup command

Following files and folders are stored as backup for Windows:

- ActionHandlersRegistration.xml
- ActionUndoHandlersRegistration.xml
- components.properties
- database-migration.properties
- DeviceData
- DeviceGuid
- DLUPolicyHandlerRegistration.xml
- guid.txt
- initial-web-service
- ippman.conf
- LCPRegistration.xml
- logger-server-conf.xml

    logger-zman-conf.xml

- logger-zmd-conf.xml

    logger.xsl

    lpm-server.properties

    monitor.conf

    novell-rm-audit.xml

novell-rm-setting.ini

novell-zenworks-configure.properties

PolicyHandlersRegistration.xml/

zman/properties/

primary_server_version.dll

RMHandlerRegistration.xml

WGPRegistration.xml

ZenMemoryCache.config

ZenServerVersion.xml

zenworks.uninstall.logger.config

zenworks_database.conf

security/

datamodel/

casa/

fde/

loader/

loader-logging/

pmconfig/

preboot/

quicktask/

RMPolicy/

Satellite/

services

zman/properties/

server.xml

casa/server.xml

extcasa/WEB-INF/classes/casa_crypto.properties

casa/WEB-INF/classes/casa_crypto.properties

Following files and folders are not stored as backup on Windows:

- agentcomponents/

  datamodel/authsources

  datamodel/cache

  datamodel/default

  zman/resources/

  pru/

  resources/

  trusted-certs/

  LoggerConfiguration-windows.xml

Following files and folders are stored as a backup for Linux:

- components.properties

  zenworks.properties

  monitor.conf

  version.txt

  database-migration.properties

  initial-web-service

  ZenServerVersion.xml

  primary_server_version.txt

  DeviceData

  DeviceGuid

  ippman.conf

  zenworks_database.conf

  guid.txt

  lpm-server.properties

  logger-server-conf.xml

  novell-zenworks-configure.properties

  logger-zman-conf.xml

  zenworks.uninstall.logger.config

  security/

  datamodel/

  casa/

  fde/

  loader/

  loader-logging/

  preboot/

  puppet/

  quicktask/

  services/

  zman/properties/

  server.xml

  casa/server.xml

extcasa/WEB-INF/classes/casa_crypto.properties

casa/WEB-INF/classes/casa_crypto.properties

zentruststore/

Following files and folders are not stored as backup on Linux:

◆ agentcomponents/

datamode/lauthsources

datamodel/cache

datamodel/default

conf/

pru/

resources/

trusted-certs/

zman/resources

1.2 Restoring a ZENworks Server

This procedure assumes the following:

◆ You have a backup of the ZENworks Server's configuration information. See Section 1.1, "Backing Up a ZENworks Server," on page 7.

◆ If the ZENworks database resides on the ZENworks Server, you have a backup of the database. See "Backing Up the Embedded Sybase SQL Anywhere Database" in the *ZENworks 11 SP3 Database Management Reference*.

◆ The bundles and policies that are stored on the ZENworks Server have been replicated to other ZENworks Servers. If not, distribution of a policy or bundle from the restored ZENworks Server fails.

◆ The image files that are stored on the ZENworks Server are available on another ZENworks Server. If not, distribution of the image files from the restored ZENworks Server will fail.

IMPORTANT: When you restore the ZENworks Server and the database, you must first restore the ZENworks Server, then continue with restoring the latest backed-up ZENworks database.

To restore a ZENworks server:

1 Reinstall the ZENworks Server, using the same IP address and DNS name.

If you do not use the same IP address and DNS name, any devices that connect to the server need to reregister.

If you have only one Primary Server connected to an external database in a zone, reinstall the Primary server and create a dummy database during the installation. You do not need to create an internal database.

If you have more than one Primary server connected to an external database in a zone, reinstall the failed Primary server as a second Primary Server. You are not prompted to configure the database during the installation.

2 Ensure that you have read/write rights to the `Novell\ZENworks\conf` directory on a Windows server or the `etc/opt/novell/zenworks` directory on a Linux server.

3 At a command prompt on the ZENworks Server, enter the following command:

`zman zenserver-restore` *path_to_backup_file_to_restore*

For example:

`zman zenserver-restore c:\zcm_backups\zone_backup.bak`

or

`zman zenserver-restore /root/zcm_backups/zone_backup.bak`

4 When prompted, enter a ZENworks administrator name and password.

5 When prompted, enter the pass phrase (at least 10 characters) to be used for decrypting the backup file.

This is the same passphrase that was entered to encrypt the file when backing up the server.

6 (Conditional) If the database is located on the server, restore the database after the ZENworks Server information has been restored. For instructions, see "Restoring the Embedded Sybase SQL Anywhere Database" in the *ZENworks 11 SP3 Database Management Reference*.

7 (Conditional) If you have backups of the image files, restore the files to the `Novell\Zenworks\work\content-repo\images` directory on a Windows server or the `/var/opt/novell/zenworks/content-repo/images` directory on a Linux server.

8 Restart the ZENworks Server.

1.3 Backing Up the Certificate Authority

To back up the certificate authority files on the Primary Server that is configured to be the ZENworks internal certificate authority:

1 At the command prompt of the ZENworks Server, enter the following command:

`zman certificate-authority-export (certificate-authority-export/cae) [options] (file path)`

For example, `zman cae C:\temp\zenbackup\ca.bak` on Windows and in the `zman cae /tmp/zenbackup/ca.bak` on Linux.

This command exports the key-pair credentials of the zone certificate authority to a file. For more information about zman certificate authority commands, see "zman(1)"in the *ZENworks 11 SP3 Command Line Utilities Reference*.

2 Enter the username and password of the administrator of the Management Zone.

3 Enter a passphrase for the file encryption.

Make sure you remember this passphrase. You must enter it if you ever need to restore the server.

1.4 Restoring the Certificate Authority

To restore the certificate authority files on the Primary Server that is configured to be the ZENworks internal certificate authority:

1 At the command prompt of the ZENworks Server, enter the following zman command:

`zman certificate-authority-import (certificate-authority-import/cai) (file path)`

This command imports the key-pair credentials of the zone certificate authority from a file. For more information about zman certificate authority commands, see "zman(1)" in the *ZENworks 11 SP3 Command Line Utilities Reference*.

2   Enter the username and password of the administrator of the Management Zone.

3   Enter the file encryption passphrase you specified when you backed up the Certificate Authority files (Step 3 in Section 1.3, "Backing Up the Certificate Authority," on page 12).

4   Manually open the `CaConfig.xml` file, which is located in `ZENworks_installation_directory\conf\security\` directory on Windows and in the `/etc/opt/novell/zenworks/security/` directory on Linux, to ensure that the `<Keystore>` tag contains the correct path of `zenca.keystore`. The `zenca.keystore` file is located by default in the `ZENworks_installation_directory\conf\security\` directory on Windows and in the `/etc/opt/novell/zenworks/security/` directory on Linux.

5   (Conditional) If you edit the `zenca.keystore` path in the `CaConfig.xml` file in Step 4, you must restart the Novell ZENworks Server service:

    ◆ **On Windows:** Do the following:

        1.   From the Windows desktop Start menu, click *Settings > Control Panel*.

        2.   Double-click *Administrative Tools > Services*.

        3.   Restart *Novell ZENworks Server*.

    ◆ **On Linux:** At the console prompt, enter `/etc/init.d/novell-zenserver restart`.

1.5   Migrating the Internal Certificate Authority Role between Primary Servers across different OS Platforms

To migrate the internal Certificate Authority (CA) role on a source Windows Primary Server to a destination Linux Primary Server and vice-versa, perform the following steps:

1   Run the following database query to identify the Primary Server in the zone that has the internal CA role configured:

```
select zsr.id,z.name,zsr.Roles as CA_Role,z.path from zZenServerRoles zsr,
zZenObject z where zsr.id=z.zuid and zsr.id in (select zuid from zZenServer
where Type='Primary') and zsr.Roles='CertAuth'
```

2   Back up the configuration data of the source and destination Primary Servers by using the command `zman zsb <path_of_backup_file>` and note their pass phrases.

3   Copy the specific files of the CA roles (`zenca.keystore` and `caConfig.xml`) from the `security` folder located in the source Primary Server, installation path.

    ◆ **On Windows:** `%zenworks_home%\conf\security`

    ◆ **On Linux:** `/etc/opt/novell/zenworks/security`

4   Place the copied files from Step 3 into the `security` folder located in the destination Primary Server, installation path.

5   Open the `caConfig.xml` file located under the `security` folder on the destination Primary Server, to update the `<Keystore>` tag value for the `zenca.keystore` file and correct the existing local path.

    By default, the `zenca.keystore` file is located in the following path:

    ◆ **On Windows:** `%zenworks_home%\conf\security`

    ◆ **On Linux:** `/etc/opt/novell/zenworks/security`

6 Run the `zman card` command on the source Primary Server to disable the internal CA role. This removes the CertAuth that is the Certificate Authority role entry for the source Primary Server in the database.

(Optional) You can move the CA files `caConfig.xml` and `zenca.keystore` to a different path.

7 Run the `zman care` on the destination Primary Server to enable the CA role. This adds the CertAuth that is the Certificate Authority role entry for the source Primary Server in the database.

8 If the destination Primary Server is Linux, you must also run the `permission.sh` script to set the correct ownership and permissions for configuration files that are present under the `security` folder.

Ensure that the files are owned by ZENworks user and zmanusers group. Otherwise, run the command `chown zenworks:zmanusers zenca.keystore caConfig.xml` below the `security` folder to set the correct ownership.

9 Restart the services on the source and destination Primary Servers by using the command `novell-zenworks-configure –c Start`

10 Perform Step 1 to validate whether the internal CA role is moved to the correct Primary Server.

IMPORTANT: The steps above do not change the CA certificate. Therefore, new or existing managed devices in the zone use the same CA certificate minted by the source Primary Server for any communication with Primary Servers and Satellite Servers.

2 Replacing Primary Servers

2.1 Replacing the First Primary Server with the Second Primary Server

You can replace the first Primary Server in your Management Zone with an existing second Primary Server or with a new server. If you choose to replace the first Primary Server with a new server that has a different hostname and IP address, you must install ZENworks 11 SP3 on the new server in the same Management Zone. Consequently, the new server becomes the first Primary Server.

The first Primary Server and the second Primary Server must have the same version of the ZENworks 11 SP3 installed.

NOTE: This scenario is not supported on Windows to Linux and vice-versa platform combinations.

To replace the first Primary Server with the second Primary Server:

1 Before replacing the First Primary Server with the Second Primary Server, take a reliable backup of the following on all Primary Servers in the Management Zone:

   ◆ **Content-Repo Directory:** The `content-repo` directory is located by default in the `ZENworks_installation_directory\work` directory on Windows and in the `/var/opt/novell/zenworks/` on Linux.

      Ensure that the `images` directory located within the `content-repo` directory has been successfully backed up.

   ◆ **Certificate Authority:** For detailed information on how to back up the certificate authority, see Section 1.3, "Backing Up the Certificate Authority," on page 12.

   ◆ **Embedded Database:** For detailed information on how to back up the embedded database, see in "Backing Up the Embedded Sybase SQL Anywhere Database" in the *ZENworks 11 SP3 Database Management Reference*.

   ◆ **ZENworks Server:** For detailed information on how to back up the ZENworks Server, see Section 1.1, "Backing Up a ZENworks Server," on page 7.

2 Ensure that all the contents of the `content-repo` directory of the first Primary Server are replicated to the second Primary Server.

   The `content-repo` directory is located in the `ZENworks_installation_directory\work\` directory on Windows and in the `/var/opt/novell/zenworks/` directory on Linux.

3 (Conditional) If the first Primary Server has add-on images:

   3a In ZENworks Control Center for the second Primary Server, click the *Bundles* tab, then click the Imaging bundle.

      The *Summary* tab is displayed.

   3b Click *Edit* next to *Add-on Image File*.

      The Bundle Add-on Image wizard is displayed.

3c On the *Add Image Server Address* page, select the first Primary Server that is associated with the bundle, then click *Remove.*

3d Click *Add.*

3e Click 🖝 next to the *Servers* folder to navigate through the folders until you find the second Primary Server.

3f Select the second Primary Server to display its name in the *Selected* list, then click *OK.*

3g Click *Finish.*

The add-on image is associated with the second Primary Server, and the add-on image content is created on the second Primary Server.

3h In the *Summary* tab of the bundle, click the *Increment Version* underlined link for *Version*, then click *Yes* in the Confirm Version Increment dialog box.

4 (Conditional) If the first Primary Server has a ZENworks Imaging bundle, copy the bundle to the second Primary Server:

4a Manually copy all the files with the `.zmg` extension from the `/content-repo/images` directory of the first Primary Server to the `/content-repo/images` directory on the second Primary Server.

4b In ZENworks Control Center of the second Primary Server, click the *Bundles* tab, then click the Imaging bundle.

4c Click the *Actions* tab.

4d Click the ZENworks Image action.

The Edit Action dialog box is displayed.

4e In the *ZENworks Image* field, click 🔍.

The Server and Path Information dialog box is displayed.

4f In the *Server Object, IP or DNS* field, click 🔍 to browse for and select the second Primary Server.

4g In the *File Path on Server* field, click 🔍 to browse for and select the `image.zmg` file.

5 (Conditional) If the first Primary Server has ZENworks Reporting installed, take a reliable back-up of the reports.

For more information about backup of ZENworks reports, see "Managing the Export Settings" in the *ZENworks Reporting 5 System Reference*.

6 Export the certificate authority role.

6a Take a reliable backup of the certificate authority of the first Primary Server.

For detailed information on how to take a backup of the certificate authority, see Section 1.3, "Backing Up the Certificate Authority," on page 12.

IMPORTANT: You must use the `-d` option with the `zman certificate-authority-export` command to remove the certificate authority role of the local server.

6b Restore the backed-up certificate authority on the second Primary Server.

For detailed information on how to restore a backed-up certificate authority, see Section 1.4, "Restoring the Certificate Authority," on page 12.

7 In the default closest server rule at the Management Zone level, move the first Primary Server as the last entry in the servers list.

    7a In ZENworks Control Center, click the *Configuration* tab.

    7b In the Management Zone Settings panel, click *Infrastructure Management > Closest Server Default Rule*.

    7c In the *Collection Servers* list, select the check box next to the first Primary Server, then click *Move Down* until the server is the last entry in the list.

    7d In the *Content Servers* list, select the check box next to the first Primary Server, then click *Move Down* until the server is the last entry in the list.

    7e In the *Configuration Servers* list, select the check box next to the first Primary Server, then click *Move Down* until the server is the last entry in the list.

    7f Click *OK*.

8 (Conditional) If you have any additional closest server rules configured, remove the first Primary Server from the rules.

    8a In ZENworks Control Center, click the *Configuration* tab.

    8b In the Management Zone Settings panel, click *Infrastructure Management > Closest Server Rules*.

    8c Select a closest server rule, then click *Edit*.

       The Rule Construction dialog box is displayed.

    8d In the *Collection Servers* list, select the check box next to the first Primary Server, then click *Remove.*

    8e In the *Content Servers* list, select the check box next to the first Primary Server, then click *Remove*.

    8f In the *Configuration Servers* list, select the check box next to the first Primary Server, then click *Remove*.

    8g Click *OK* twice.

9 Refresh all the devices (Primary Serves, Satellites, and managed devices) in the Management Zone so that they get the new closest server rules.

10 (Optional) Reregister all the managed devices and Satellites to the new Primary Server.

> **NOTE:** You can choose not to perform this step because there is no loss in the functionality. However, the ZENworks icon and the `zac zone-config` command continue to display the IP address and the host name of the retired Primary Server.

To reregister the devices, perform the following tasks on all the devices:

    10a Unregister the device from the Management Zone by running the following command:

```
zac unr -f
```

    10b Register the device in the Management Zone by running the following command:

```
zac reg https://ZENworks_Server_DNS_name:port_number
```

       For more information about zac, view the zac man page (`man zac`) on the device or see the *ZENworks 11 SP3 Command Line Utilities Reference*.

11 (Conditional) Move the database to another device in any of the following scenarios:

- You are using an internal ZENworks database (embedded Sybase SQL Anywhere).

- You are using an external database installed on the device hosting the first Primary Server and you do not plan to use the device after uninstalling the Primary Server.

To move the database to another device:

11a (Conditional) If you are using an external database, ensure that you have a reliable backup of the database.

11b Obtain the credentials of the database.

To procure the credentials of the internal database, use one of the following commands:

```
zman dgc -U administrator_name -P administrator_password
```

or

```
zman database-get-credentials -U administrator_name -P
administrator_password
```

To obtain the credentials of the external database, contact the database administrator.

11c Remove the database role, MasterPrimary role, and CertAuth role from the first Primary Server (applicable for Embedded Sybase):

    11c1 Log into the database.

    11c2 In the SQL editor, execute the following SQL queries to remove the corresponding role entries for the first Primary Server from the zZENServerRoles table:

```
delete from zZENServerRoles where Roles='Database';
delete from zZENServerRoles where Roles='MasterPrimary';
delete from zZENServerRoles where Roles='CertAuth';
commit;
```

11d To add the database role to the Second Primary Server (applicable for Embedded Sybase):

    11d1 Log into the database.

    11d2 In the SQL editor, execute the following SQL commands to assign the database role, MasterPrimary role, and CertAuth role for the Second Primary Server:

```
Insert into zZENServerRoles (id, Roles, position) values (0x<second PS
GUID>, 'Database', (select max(position) from zZENServerRoles where
id=0x<second PS GUID>)+1);
```

```
Insert into zZENServerRoles (id, Roles, position) values (0x<second PS
GUID>, 'MasterPrimary', (select max(position) from zZENServerRoles
where id=0x<second PS GUID>)+1);
```

```
Insert into zZENServerRoles (id, Roles, position) values (0x<second PS
GUID>, 'CertAuth', (select max(position) from zZENServerRoles where
id=0x<second PS GUID>)+1);
```

    commit;

11e If the database is installed on the same device as that of the first Primary Server, move the database.

Internal Sybase: For detailed information on how to move the data from an internal Sybase database to an internal Sybase database, see "Moving the Internal Sybase Database from One Primary Server to Another Primary Server" in the *ZENworks 11 SP3 Database Management Reference*.

External Sybase: For detailed information on how to move the data from one external Sybase database to another external Sybase database, see "Moving the Data from One External Sybase Database to another External Sybase Database" in the *ZENworks 11 SP3 Database Management Reference*.

MS SQL: For detailed information on how to move the data to a new MS SQL database, see the MS SQL documentation. Later on, perform the steps described in "Configuring the ZENworks Server to Point to the New MS SQL Database Containing Data Moved from Another MS SQL Database" in the *ZENworks 11 SP3 Database Management Reference*.

Oracle: For detailed information on how to move the data from one Oracle database to another Oracle database, see the Oracle documentation. Later on, perform the steps described in "Configuring the ZENworks Server to Point to the New Oracle Database Containing Data Moved from Another Oracle Database" in the *ZENworks 11 SP3 Database Management Reference*.

12 Remove all Satellites under the first Primary Server from the Server Hierarchy.

For more information on how to remove the Satellites from the Server Hierarchy listing in ZENworks Control Center, see "Removing Satellites from the Server Hierarchy" in the *ZENworks 11 SP3 Primary Server and Satellite Reference*.

13 (Conditional) On the second Primary Server, install ZENworks Reporting, and restore the reports that you backed-up in Step 5.

For more information on how to install ZENworks Reporting, see *ZENworks Reporting 5 Installation Guide*.

For detailed information about restoring the ZENworks reports. See "Managing the Import Settings" in the *ZENworks Reporting 5 System Reference*.

14 After ensuring that all the operations in the Management Zone are working as expected, uninstall ZENworks Reporting on the first Primary Server.

For detailed information on how to uninstall ZENworks Reporting, see "ZENworks 11 SP3 Uninstall Guide".

15 After ensuring that all the operations in the Management Zone are working as expected, uninstall ZENworks 11 SP3 on the first Primary Server.

For detailed information on how to uninstall ZENworks 11 SP3, see "ZENworks 11 SP3 Uninstall Guide".

NOTE: If Multizone is configured for this server (which has got replaced with a new Primary Server) as Publisher, then all its subscribers must be updated with the new IP address and certificate of this server.

1. Log in to ZENworks Control Center (ZCC) of subscribers.

2. Navigate to *Subscribe And Share > Subscriptions > <subscription_name> > Remote Server > Base URL > Edit*.

3. Update the IP address with the new IP address of the Primary Server (Publisher).

To update the new certificate:

1. Navigate to *Subscribe And Share > Subscriptions > <subscription_name> > Remote Server > Update Certificate*.

2. Update the certificate.

2.2 Replacing an Existing Primary Server with a New Primary Server

If you have only one Primary Server in the Management Zone and if you want to replace the device hosting the Primary Server with a new device that has the same host name and IP address as the old device, you must move the Primary Server to the new device.

The existing Primary Server and the new Primary Server must have the same version of the ZENworks 11 SP3 installed.

NOTE: This scenario is not supported on Windows to Linux and vice-versa. It applies to platforms having the same network identity.

1 Take a reliable backup of the existing ZENworks Server.

For detailed information on how to take a backup of the ZENworks Server, see Section 1.1, "Backing Up a ZENworks Server," on page 7.

2 (Conditional) Take a reliable backup of the certificate authority of the Primary Server.

For detailed information on how to take a backup of the certificate authority, see Section 1.3, "Backing Up the Certificate Authority," on page 12.

During the ZENworks Server backup, certificates are backed up for Primary Servers having an internal Certificate Authority and the same network identity (IP, FQDN, and Cert). Also, during the ZENworks Server restore, the Certificate Authority is restored.

3 (Conditional) Take a reliable backup of database in any of the following scenarios:

- ◆ You are using an internal ZENworks database (embedded Sybase SQL Anywhere).
- ◆ You are using an external database installed on the device hosting the Primary Server and you do not plan to use the device after uninstalling the Primary Server.

For detailed information on how to take a backup of an internal database, see in "Backing Up the Embedded Sybase SQL Anywhere Database" in the *ZENworks 11 SP3 Database Management Reference*.

To take a backup of an external database, see the documentation for the database.

4 (Conditional) If the first Primary Server has ZENworks Reporting installed, take a reliable back-up of the reports.

For more information about backup of ZENworks reports, see "Managing the Export Settings" in the *ZENworks Reporting 5 System Reference*.

5 Stop all the ZENworks services on the Primary Server.

For detailed information on how to stop the ZENworks services on Windows, see "Stopping the ZENworks Services" in the *ZENworks 11 SP3 Primary Server and Satellite Reference*. For detailed information on how to stop the ZENworks services on Linux, see "Stopping the ZENworks Services" in the *ZENworks 11 SP3 Primary Server and Satellite Reference*.

6 Take a reliable backup of the `content-repo` directory of the Primary Server.

The `content-repo` directory is located in the `ZENworks_installation_directory\work\` directory on Windows and in the `/var/opt/novell/zenworks/` directory on Linux.

7 Disconnect the device from the network.

8 Install ZENworks 11 SP3 on the new server with the following settings that are same as that of the old Primary Server:

- ◆ Installation drive and path. For Windows, ensure that the installation path points to `C:\Program Files (x86)`.
- ◆ ZENworks Ports
- ◆ Management Zone name

For detailed information on how to install ZENworks 11 SP3, see "Installing a ZENworks Primary Server on Windows" in the *ZENworks 11 SP3 Server Installation Guide*.

9 Do the following on the new Primary Server:

9a Restore the backed-up ZENworks Server.

For detailed information on how to restore the ZENworks Server, see Section 1.2, "Restoring a ZENworks Server," on page 11.

9b (Conditional) Restore the backed-up database.

For detailed information on how to restore the internal ZENworks database, see in "Restoring the Embedded Sybase SQL Anywhere Database" in the *ZENworks 11 SP3 Database Management Reference*.

9c (Conditional) Restore the backed-up Certificate Authority.

For detailed information on how to restore the certificate authority, see Section 1.4, "Restoring the Certificate Authority," on page 12.

9d Re-create all the default and custom deployment packages.

Default Deployment Packages: At the server's command prompt, enter the following command:

```
novell-zenworks-configure -c CreateExtractorPacks -Z
```

Custom Deployment Packages: At the server's command prompt, enter the following command:

```
novell-zenworks-configure -c RebuildCustomPacks -Z
```

9e Copy the backed-up `content-repo` directory to the `ZENworks_installation_directory\work\` directory on Windows or to the `/var/opt/ novell/zenworks/` directory on Linux. If you have any issues in copying `content-repo` directory in Linux, then run `permissions.sh` command.

9f (Conditional) Run the following scripts:

- ◆ delete from zzenserverroles where Roles = 'ReportCMSServer' or Roles = 'ReportApplicationServer'
- ◆ delete from zopaquedata where name = 'boe.mysql.database.pwd'
- ◆ delete from zopaquedata where name like '%zone.configuration.reports%'

9g (Conditional) On the new Primary Server, install ZENworks Reporting.

For detailed information on how to install ZENworks Reporting, see *ZENworks Reporting 5 Installation Guide*.

9h (Conditional) If you install ZENworks Reporting on the new Primary Server, restore the reports that you backed-up in Step 4 by using the following zman command:

```
zman rpld (source folder)
```

For detailed information about the zman Report Commands, view the zman man page (`man zman`) on the server or see "zman(1)" in *ZENworks 11 SP3 Command Line Utilities Reference*.

10 Ensure that the new server is running correctly. Subsequently, uninstall ZENworks 11 SP3 from the old device. For detailed information on how to uninstall ZENworks 11 SP3, see *ZENworks 11 SP3 Uninstall Guide*.

WARNING: After the new Primary Server starts running, you must disconnect the old Primary Server from the network and uninstall ZENworks, or disable ZENworks services so that it cannot register back to the zone.

---

3 Changing the IP Address or DNS Name of Primary Servers

If you want to change the IP address or DNS Name of a Primary Server after installing ZENworks 11 SP3, review the following sections:

- Section 3.1, "Changing the IP Address of a Primary Server after Installing ZENworks 11 SP3," on page 23
- Section 3.2, "Changing the DNS Name or the IP Address and DNS Name of a Primary Server after Installing ZENworks 11 SP3," on page 24

3.1 Changing the IP Address of a Primary Server after Installing ZENworks 11 SP3

 If you want to change the IP address of the Primary Server after installing ZENworks 11 SP3, and if the CN of the certificate does not have the IP address configured, use the following steps to change the IP address of the Primary Server:

1 Before changing the IP address of the Primary Server, take a reliable backup of the following on all Primary Servers in the Management Zone:

- **Content-Repo Directory:** The `content-repo` directory is located by default in the `ZENworks_installation_directory\work` directory on Windows and in the `/var/opt/novell/zenworks/` on Linux.

    Ensure that the `images` directory located within the `content-repo` directory has been successfully backed up.

- **Certificate Authority:** For detailed information on how to back up the certificate authority, see Section 1.3, "Backing Up the Certificate Authority," on page 12.

- **Embedded Database:** For detailed information on how to back up the embedded database, see in "Backing Up the Embedded Sybase SQL Anywhere Database" in the *ZENworks 11 SP3 Database Management Reference*.

- **ZENworks Server Back up:** For detailed information on how to back up the ZENworks Server, see Section 1.1, "Backing Up a ZENworks Server," on page 7.

2 Change the IP address of the Primary Server.

IMPORTANT: Do not change the DNS name of the server.

---

3 Ensure that the new IP address of the server is correctly mapped to its existing DNS name on the DNS server.

4 Restart all the ZENworks services by running the following command at the server's command prompt:

`novell-zenworks-configure -c Start`

By default, all the services are selected. You must select *Restart* as the *Action*.

5 Re-create all the default and custom deployment packages:

- ◆ **Default Deployment Packages:** At the server's command prompt, enter the following command:

  ```
  novell-zenworks-configure -c CreateExtractorPacks -Z
  ```

- ◆ **Custom Deployment Packages:** At the server's command prompt, enter the following command:

  ```
  novell-zenworks- configure -c RebuildCustomPacks -Z
  ```

6 If the database is located on the Primary Server whose IP address you changed in Step 2.

1. Change the database server address on all the second Primary Servers. On all the second Primary Servers, change the value of database server address in the *ZENworks_Installation_Directory*\Novell\ZENworks\conf\datamodel\zdm.xml to point to the new IP address of the first Primary Server.

2. Change the audit database server address on all the second Primary Servers. On all the second Primary Servers, change the value of audit database server address in the *ZENworks_Installation_Directory*\Novell\ZENworks\conf\datamodel\zenaudit.xm l to point to the new IP address of the first Primary Server.

7 Restart the ZENworks Adaptive Agent.

8 Restart the Proxy DHCP services on all the Satellites.

NOTE: When you change the IP address of a ZENworks Primary Server on which a ZENworks Reporting is installed, you must not perform any additional steps to ensure that the ZENworks Reporting functions properly. However, if the database is also residing on the ZENworks Primary Server, then you must run ZENworks Reporting Configuration Tool, to point to the new IP address of the Database.

For more information, see "ZENworks Reporting Configuration Tool " in the *ZENworks Reporting 5 System Reference*.

---

9 (Conditional) If multizone is configured with this server (whose IP address is changed) as Publisher, then after replacing the First Primary Server with the Second Primary Server, update the new IP address of this server for all its Subscribers. Perform the following to update the new IP address:

1. Log in to ZENworks Control Center (ZCC) of subscribers.

2. Navigate to *Subscribe And Share > Subscriptions > <subscription_name> > Remote Server > Base URL>Edit*.

3. Update the IP address with new IP address of the Primary Server (Publisher).

3.2 Changing the DNS Name or the IP Address and DNS Name of a Primary Server after Installing ZENworks 11 SP3

If you want to change only the DNS name or if you want to change both the IP address and DNS name of the Primary Server after installing ZENworks 11 SP3, and if the certificate's CN has fully qualified DNS configured, use the following steps to change only the DNS name or to change both the IP address and DNS name of the Primary Server.

NOTE: This scenario has been tested only on the Windows Primary Server and the embedded Sybase database. In this setup, the DNS and DHCP servers are configured on the same device.

The following two scenarios are supported:

3.2.1 Scenario for a zone configured with external certificate

1 Take a reliable backup of the following on all the Primary Servers in the Management Zone:

- **Content-Repo Directory:** The `content-repo` directory is located by default in the `ZENworks_installation_directory\work` directory on Windows and in the `/var/opt/novell/zenworks/` on Linux.

  Ensure that the `images` directory located within the `content-repo` directory has been successfully backed up.

- **Certificate Authority:** For detailed information on how to back up the certificate authority, see Section 1.3, "Backing Up the Certificate Authority," on page 12.

- **Embedded Database:** For detailed information on how to back up the embedded database, see in "Backing Up the Embedded Sybase SQL Anywhere Database" in the *ZENworks 11 SP3 Database Management Reference*.

- **ZENworks Server:** For detailed information on how to back up the ZENworks Server, see Section 1.1, "Backing Up a ZENworks Server," on page 7.

2 Create a certificate signing request (CSR) by providing the host name of the Primary Server as the subject.

For more information on how to create a CSR, for Windows, see "Creating an External Certificate" and for Linux, see "Creating an External Certificate".

3 At the console prompt of a Primary Server, run the following command:

```
zman sacert Path_of_the_Primary_Server_in_ZENworks_Control_Center
Path_of_Primary_Server_Certificate
```

For more information about zman, view the zman man page (`man zman`) on the device or see the *ZENworks 11 SP3 Command Line Utilities Reference*.

This adds the certificate of the Primary Server that you specified in the command to the ZENworks database and certificate store.

NOTE: You must run the command for each device whose certificate you want to replace.

4 Refresh all the devices, including the Primary Servers, in the zone.

The Primary Server certificates that were imported in Step 3 are sent to the devices as configuration data.

5 Enforce the new certificates on the zone by running the following command on any Primary Server whose DNS name is changed:

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

Follow the prompts.

Restart ZENworks services by using the `novell-zenworks-configure -c Start` command and select the *Restart* option.

6 (Optional) Import the root certificate of the new certificate authority into the trusted store on all the devices in the zone through the `zac cert-info` command. You can choose to execute the command in one of the following ways:

- Manually run the following command on each Primary Server and managed device in the zone:

```
zac cert-info certificate_file_path -u zone_administrator_username -p
zone_administrator_password
```

For more information about zac, view the zac man page (`man zac`) on the device or see the *ZENworks 11 SP3 Command Line Utilities Reference*.

- ◆ Use a ZENworks bundle.

  For more information about bundles, see "Creating Bundles" in the *ZENworks 11 SP3 Software Distribution Reference*.

7 If the database is located on the Primary Server whose IP address you changed.

1. Change the database server address on all the second Primary Servers. On all the second Primary Servers, change the value of database server address in the `ZENworks_Installation_Directory\Novell\ZENworks\conf\datamodel\zdm.xml` to point to the new IP address of the first Primary Server.

2. Change the audit database server address on all the second Primary Servers. On all the second Primary Servers, change the value of audit database server address in the `ZENworks_Installation_Directory\Novell\ZENworks\conf\datamodel\zenaudit.xml` to point to the new IP address of the first Primary Server.

8 Restart all the ZENworks services on all the Primary Servers in the zone by running the following command at the console prompt of each Primary Server in the zone:

```
novell-zenworks-configure -c Start
```

By default, all the services are selected. You must select *Restart* as the *Action*.

9 Refresh all the Primary Server Agents, so that the new IP and DNS name of the first Primary Server will be updated on the other servers. Run the following commands:

zac retr -u *zone_administrator_username* -p *zone_administrator_password*

zac ref bypasscache

10 On the first Primary Server, run the following command `zac ref bypasscache`

The first Primary Server agent contacts the second Primary Server (Closest Server Rules) and gets the updated details of its new IP and Hostname.

11 Restart all the ZENworks Adaptive Agents.

12 Restart the Proxy DHCP services on all the Satellites.

13 Refresh all the devices in the zone.

If any device is not reachable during the refresh, you must first establish a connection with the device, then run the following command at the console prompt of each device to reestablish the trust between the device and the zone:

```
zac retr -u zone_administrator_username -p zone_administrator_password
```

14 Configure the Satellites with the new external certificates by entering the following command at the console prompt of each Satellite in the zone:

```
zac iac -pk private-key.der -c signed-server_certificate.der -ca signing-
authority-public-certificate.der -ks keystore.jks -ksp keystore-pass-phrase -a
signed-cert-alias -ks signed-cert-passphrase -u username -p password -rc
```

For more information about zac, view the zac man page (`man zac`) on the device or see the *ZENworks 11 SP3 Command Line Utilities Reference*.

15 Re-create all the default and custom deployment packages for all the Primary Servers:

- ◆ **Default Deployment Packages:** At the console prompt of each Primary Server in the zone, enter the following command:

  ```
  novell-zenworks-configure -c CreateExtractorPacks -Z
  ```

- **Custom Deployment Packages:** At the console prompt of each Primary Server in the zone, enter the following command:

  ```
  novell-zenworks- configure -c RebuildCustomPacks -Z
  ```

16 (Conditional) If your zone includes Intel AMT devices, unprovision and provision the devices.

For more information about unprovisioning and provisioning Intel AMT devices, see "Configuring Intel AMT Devices in Enterprise Mode" in the *ZENworks 11 SP3 Out-of-Band Management Reference*.

17 (Conditional) If Multizone is configured with this server (whose IP address and DNS name is changed) as Publisher, then after replacing the First Primary Server with the Second Primary Server, update the new IP address and DNS name of this server for all its Subscribers. Perform the following to update the new IP address and DNS name:

1. Log in to ZENworks Control Center (ZCC) of subscribers.

2. Navigate to *Subscribe And Share > Subscriptions > <subscription_name> > Remote Server > Base URL>Edit*.

3. Update the IP address or Hostname with new IP address or Hostname of the Primary Server (Publisher).

To update the new certificate:

1. Navigate to *Subscribe And Share > Subscriptions > <subscription_name> > Remote Server > Update Certificate*.

2. Update the certificate.

NOTE: When you change the IP address or DNS name of the ZENworks Primary Server on which a ZENworks Reporting is installed, you need not perform any additional steps to ensure that the ZENworks Reporting functions properly. However, if the database is also residing on the ZENworks Primary Server, then you must run ZENworks Reporting Configuration Tool, to point to the new IP address of the Database.

For more information, see "ZENworks Reporting Configuration Tool " in the *ZENworks Reporting 5 System Reference*.

3.2.2 Scenario for a zone configured with internal certificate

If you want to change only the DNS name or if you want to change both the IP address and the DNS name of the Primary Server after installing ZENworks 11 SP3, and if the certificates CN has fully qualified DNS configured, perform the following steps to change only the DNS name or to change both the IP address and the DNS name of the Primary Server.

1 Take a reliable backup of the following on all the Primary Servers in the Management Zone:

- **Content-Repo Directory:** The content-repo directory is located by default in the *ZENworks_installation_directory*\work directory on Windows and in the /var/opt/ novell/zenworks/ on Linux.

  Ensure that the images directory located within the content-repo directory has been successfully backed up.

- **Certificate Authority:** For detailed information on how to backup certificate authority, see Section 1.3, "Backing Up the Certificate Authority," on page 12.

- **Embedded Database:** For detailed information on how to back up the embedded database, see in "Backing Up the Embedded Sybase SQL Anywhere Database" in the *ZENworks 11 SP3 Database Management Reference*.

- **ZENworks Server:** For detailed information on how to back up the ZENworks Server, see Section 1.1, "Backing Up a ZENworks Server," on page 7.

2 Enforce the new certificates on the zone by running the following command on any Primary Server whose DNS name is changed:

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

Follow the prompts, then remint **only the server certificate not the CA certificate**.

Restart ZENworks services by using the `novell-zenworks-configure -c Start` command and select the *Restart* option.

3 If the database is located on the Primary Server whose IP address you changed.

   3a Change the database server address on all the second Primary Servers. On all the second Primary Servers, change the value of database server address in the *ZENworks_Installation_Directory*\Novell\ZENworks\conf\datamodel\zdm.xml to point to the new IP address of the first Primary Server.

   3b Change the audit database server address on all the second Primary Servers. On all the second Primary Servers, change the value of audit database server address in the *ZENworks_Installation_Directory*\Novell\ZENworks\conf\datamodel\zenaudit.xml to point to the new IP address of the first Primary Server.

4 Refresh all the Primary Server Agents, so that the new IP and DNS name of the first Primary Server will be updated on the other servers. Run the following commands:

zac retr -u *zone_administrator_username* -p *zone_administrator_password*

zac ref bypasscache

5 On the first Primary Server, run the following command `zac ref bypasscache`

The first Primary Server agent contacts the second Primary Server (Closest Server Rules) and gets the updated details of its new IP and Hostname.

6 Restart all the ZENworks Adaptive Agents.

7 Restart the Proxy DHCP services on all the Satellites.

8 Restart all the ZENworks services on all the Primary Servers in the zone by running the following command at the console prompt of each Primary Server in the zone:

```
 novell-zenworks-configure -c Start
```

By default, all the services are selected. You must select Restart as the Action.

9 Refresh all the devices in the zone.

If any device is not reachable during the refresh, you must first establish a connection with the device, then run the following command at the console prompt of each device to reestablish the trust between the device and the zone:

```
zac retr -u zone_administrator_username -p zone_administrator_password
```

10 Configure the Authentication Satellites with the new certificates by entering the following command at the Satellite's prompt:

On Windows: `zac authentication server reconfigure (asr) -t all`

On Linux: `zac remint-satellite-cert (rsc`)

11 Re-create all the default and custom deployment packages for all the Primary Servers.

Default deployment packages:

At the console prompt of each Primary Server in the zone, enter the following command:

```
novell-zenworks-configure -c CreateExtractorPacks -Z
```

Custom deployment packages:

At the prompt of each Primary Server in the zone, enter the following command:

```
novell-zenworks- configure -c RebuildCustomPacks -Z
```

12 (Conditional) If your zone includes Intel AMT devices, unprovision and provision the devices.

For more information about unprovisioning and provisioning Intel AMT devices, see "Configuring Intel AMT Devices in Enterprise Mode" in the *ZENworks 11 SP3 Out-of-Band Management Reference*.

13 (Conditional) If Multizone is configured with this server (whose IP address and DNS name is changed) as Publisher, then after replacing the First Primary Server with the Second Primary Server, update the new IP address and DNS name of this server for all its Subscribers. Perform the following to update the new IP address and DNS name:

1. Log in to ZENworks Control Center (ZCC) of subscribers.

2. Navigate to *Subscribe And Share > Subscriptions > <subscription_name> > Remote Server > Base URL>Edit*.

3. Update the IP address or Hostname with new IP address or Hostname of the Primary Server (Publisher).

To update the new certificate:

1. Navigate to *Subscribe And Share > Subscriptions > <subscription_name> > Remote Server > Update Certificate*.

2. Update the certificate.

NOTE: When you change the IP address or DNS name of the ZENworks Primary Server on which a ZENworks Reporting is installed, you need not perform any additional steps to ensure that the ZENworks Reporting functions properly. However, if the database is also residing on the ZENworks Primary Server, then you must run ZENworks Reporting Configuration Tool, to point to the new IP address of the Database.

For more information, see "ZENworks Reporting Configuration Tool " in the *ZENworks Reporting 5 System Reference*.

4 Reconfiguring a Zone Certificate Before It Expires

ZENworks prompts you to change your ZENworks zone certificate 90 days before the expiration of the certificate. The following warning message is displayed for each administrator once every 24 hours after the administrator logs in to ZENworks Control Center:

The certificate on *hostname_of_the_device* will expire in *number_of_days* days.

The message is displayed for every server and zone whose certificate is about to expire.

If you do not change your zone certificate before it expires, the communication between Primary Servers and managed devices breaks down, and the managed devices fail to receive new assignments and policies. You should re-create the certificate before it expires because recreating a certificate after it expires is a very cumbersome process that involves performing manual tasks on each device in the zone.

The information provided in this section is applicable for Windows and Linux platforms.

To re-create the zone certificate before it expires, review the following scenarios:

- Section 4.1, "Changing the Zone Certificate from Internal to External," on page 31
- Section 4.2, "Replacing an Internal Server Certificate with a New Internal Server Certificate," on page 34
- Section 4.3, "Replacing an External Server Certificate with a New External Server Certificate Issued by the Same Certificate Authority," on page 36
- Section 4.4, "Replacing an External Server Certificate with a New External Server Certificate Issued by a Different Certificate Authority," on page 38

IMPORTANT

ZENworks 11 SP3 currently does not support changing the external certificate to an internal certificate on Primary Servers.

4.1 Changing the Zone Certificate from Internal to External

To change your zone certificate from an internal certificate to an external certificate:

1 Take a reliable backup of the following on all Primary Servers in the Management Zone:
   - **Content-Repo Directory:** The `content-repo` directory is located by default in the `ZENworks_installation_directory\work` directory on Windows and in the `/var/opt/novell/zenworks/` on Linux.

     Ensure that the `images` directory located within the `content-repo` directory has been successfully backed up.
   - **Certificate Authority:** For detailed information on how to back up the certificate authority, see Section 1.3, "Backing Up the Certificate Authority," on page 12.

- **Embedded Database:** For detailed information on how to take a backup of the embedded database, see in "Backing Up the Embedded Sybase SQL Anywhere Database" in the *ZENworks 11 SP3 Database Management Reference*.

- **ZENworks Server:** For detailed information on how to back up the ZENworks Server, see Section 1.1, "Backing Up a ZENworks Server," on page 7.

2 Create a server certificate for each Primary Server in the zone by providing the fully qualified DNS (FQDN) of the Primary Server as the subject.

For more information on how to create a CSR, for Windows, see "Creating an External Certificate" and for Linux, see "Creating an External Certificate".

3 At the console prompt of a Primary Server, run the following command:

```
zman sacert Path_of_the_Primary_Server_in_ZENworks_Control_Center
Path_of_Primary_Server_Certificate
```

For more information about zman, view the zman man page (`man zman`) on the device or see "zman(1)" in the *ZENworks 11 SP3 Command Line Utilities Reference*.

This adds the certificate of the Primary Server that you specified in the command to the ZENworks database and certificate store.

NOTE: You must run the command for each Primary Server in the zone to replace the new Certificate Authority or Certificate.

---

4 Refresh all the devices, including the Primary Servers, in the zone.

The Primary Server certificates that were imported in Step 3 are sent to the devices as configuration data.

5 (Optional) If the device is not contacting the server, then import the root certificate of the new certificate authority into the trusted store on all the devices in the zone through the `zac cert-info` command. You can choose to execute the command in one of the following ways:

- Manually run the following command on each Primary Server and managed device in the zone:

```
zac cert-info certificate_file_path -u zone_administrator_username -p
zone_administrator_password
```

For more information about zac, view the zac man page (`man zac`) on the device or see the *ZENworks 11 SP3 Command Line Utilities Reference*.

- Use a ZENworks bundle.

For more information about bundles, see "Creating Bundles" in the *ZENworks 11 SP3 Software Distribution Reference*.

6 Enforce the new certificates on the zone by running the following command on any Primary Server:

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

Follow the prompts.

7 Restart all the ZENworks services on all the Primary Servers in the zone by running the following command at the console prompt of each Primary Server in the zone:

```
novell-zenworks-configure -c Start
```

By default, all the services are selected. You must select *Restart* as the *Action*.

8 Ensure that DNS is properly configured for the Primary Servers, so that server host names get resolved. For DNS resolution requirements, see "DNS Resolution" in the "ZENworks 11 SP3 System Requirements".

Run the following commands in the same sequence:

```
novell-zenworks-configure -Z -c MergeTruststore

novell-zenworks-configure -c EnableJMX

novell-zenworks-configure -c ZenProbe
```

9 Refresh all the devices, including the Primary Servers, in the zone.

10 (Conditional) If any device is not reachable during the refresh, you must first establish a connection with the device, then run the following command at the console prompt of each device to reestablish the trust between the device and the zone:

```
zac retr -u zone_administrator_username -p zone_administrator_password
```

11 Configure the Satellites with the new external certificates by entering the following command at the console prompt of each Satellite in the zone:

```
zac iac -pk private-key.der -c signed-server_certificate.der -ca signing-
authority-public-certificate.der -ks keystore.jks -ksp keystore-pass-phrase -a
signed-cert-alias -ks signed-cert-passphrase -u username -p password -rc
```

For more information about zac, view the zac man page (`man zac`) on the device or see the *ZENworks 11 SP3 Command Line Utilities Reference*.

12 Re-create all the default and custom deployment packages for all the Primary Servers:

- ◆ **Default Deployment Packages:** At the console prompt of each Primary Server in the zone, enter the following command:

```
novell-zenworks-configure -c CreateExtractorPacks -Z
```

- ◆ **Custom Deployment Packages:** At the console prompt of each Primary Server in the zone, enter the following command:

```
novell-zenworks- configure -c RebuildCustomPacks -Z
```

13 (Conditional) If your zone includes Intel AMT devices, unprovision and provision the devices.

For more information about unprovisioning and provisioning Intel AMT devices, see "Configuring Intel AMT Devices in Enterprise Mode" in the *ZENworks 11 SP3 Out-of-Band Management Reference*.

14 (Conditional) If multizone is configured with the server whose certificate has got replaced as the Publisher, then update the new certificate of this server for all its Subscribers. Perform the following to update the new certificate:

1. Log in to ZENworks Control Center (ZCC) of subscribers.

2. Navigate to *Subscribe And Share > Subscriptions > <subscription_name> > Remote Server > Update Certificate*.

3. Update the certificate.

NOTE: Because ZENworks and ZENworks Reporting does not use the same certificate, the ZENworks Reporting does not require any configuration changes if the ZENworks certificate is changed. However, if you want to replace the certificate of ZENworks Reporting with the new certificate, you must run ZENworks Reporting Configuration Tool.

For more information, see "ZENworks Reporting Configuration Tool "in the *ZENworks Reporting 5 System Reference*.

4.2 Replacing an Internal Server Certificate with a New Internal Server Certificate

If the internal server certificate of your Windows or Linux Primary Server has expired or if the server certificate key pair has been compromised, you can choose to replace the certificate with a new internal server certificate.

1 Before replacing an internal server certificate with a new internal server certificate, take a reliable backup of the following on all Primary Servers in the Management Zone:
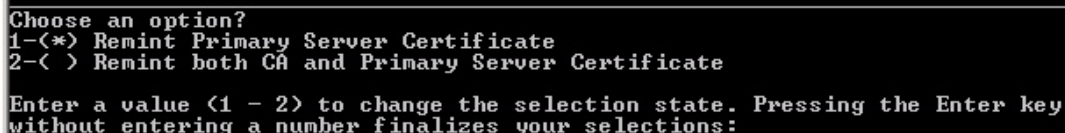
 * **Content-Repo Directory:** The `content-repo` directory is located by default in the *ZENworks_installation_directory*\work directory on Windows and in the `/var/opt/novell/zenworks/` on Linux.

    Ensure that the `images` directory located within the `content-repo` directory has been successfully backed up.

 * **Certificate Authority:** For detailed information on how to back up the certificate authority, see Section 1.3, "Backing Up the Certificate Authority," on page 12.

 * **Embedded Database:** For detailed information on how to back up the embedded database, see in "Backing Up the Embedded Sybase SQL Anywhere Database" in the *ZENworks 11 SP3 Database Management Reference*.

 * **ZENworks Server:** For detailed information on how to back up the ZENworks Server, see Section 1.1, "Backing Up a ZENworks Server," on page 7.

2 Enforce the new certificates on the zone by running the following command on the Primary Server with CA role:

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

```
Choose an option?
1-(*) Remint Primary Server Certificate
2-( ) Remint both CA and Primary Server Certificate

Enter a value (1 - 2) to change the selection state. Pressing the Enter key
without entering a number finalizes your selections:
_
```

Follow the prompts.

NOTE

 * If only the Server Certificate is expired, then select option 1 for reminting just the server certificate.

 * If both the Server Certificate and Certificate Authority are expired, then select option 2 for reminting both Certificate Authority and Primary Server certificates.

3 Restart all the ZENworks services on all the Primary Servers in the zone by running the following command at the console prompt of each Primary Server in the zone:

```
novell-zenworks-configure -c Start
```

By default, all the services are selected. You must select *Restart* as the *Action*.

4 Ensure that DNS is properly configured for the Primary Servers, so that server host names get resolved. For DNS resolution requirements, see "DNS Resolution" in the "ZENworks 11 SP3 System Requirements".

Run the following commands in the same sequence:

```
novell-zenworks-configure -Z -c MergeTruststore
```

```
novell-zenworks-configure -c EnableJMX

novell-zenworks-configure -c ZenProbe
```

5 Refresh all the devices, including the Primary Servers, in the zone.

If only one Primary Server certificate was changed, and if the CA certificate was not changed, and there is more than one Primary Server in the zone, refreshing the Server, Satellites, and managed devices will allow the agent to trust the new server certificate. Refreshes automatically on the next scheduled refresh.

If the CA certificate was changed or if there is only one Primary Server in the zone then the Primary Servers, Satellites, and managed devices need to run `zac retr` to reestablish the trust.

If any device is not reachable during the refresh, you must first establish a connection with the device, then run the following command at the console prompt of each device to reestablish the trust between the device and the zone:

```
zac retr -u zone_administrator_username -p zone_administrator_password
```

6 Configure the Authentication Satellites with the new certificates by entering the following command at the Satellite's prompt:

On Windows: `zac authentication server reconfigure (asr) -t all`

On Linux: `zac remint-satellite-cert (rsc)`

7 Re-create all the default and custom deployment packages for all the Primary Servers:

- ◆ **Default Deployment Packages:** At the console prompt of each Primary Server in the zone, enter the `novell-zenworks-configure -c CreateExtractorPacks -Z` command:

  Custom Deployment Packages: At the console prompt of each Primary Server in the zone, enter the `novell-zenworks- configure -c RebuildCustomPacks -Z` command

8 (Conditional) If your zone includes Intel AMT devices, unprovision and provision the devices.

For more information about unprovisioning and provisioning Intel AMT devices, see "Configuring Intel AMT Devices in Enterprise Mode" in the *ZENworks 11 SP3 Out-of-Band Management Reference*.

9 (Conditional) If multizone is configured with the server whose certificate has got replaced as the Publisher, then update the new certificate of this server for all its Subscribers. Perform the following to update the new certificate:

1. Log in to ZENworks Control Center (ZCC) of subscribers.

2. Navigate to *Subscribe And Share > Subscriptions > <subscription_name> > Remote Server > Update Certificate*.

3. Update the certificate.

NOTE: Because ZENworks and ZENworks Reporting does not use the same certificate, the ZENworks Reporting does not require any configuration changes if the ZENworks certificate is changed. However, if you want to replace the certificate of ZENworks Reporting with the new certificate, you must run ZENworks Reporting Configuration Tool.

For more information, see "ZENworks Reporting Configuration Tool " in the *ZENworks Reporting 5 System Reference*.

4.3 Replacing an External Server Certificate with a New External Server Certificate Issued by the Same Certificate Authority

1 Before replacing an external server certificate with a new external server certificate that is issued by the same certificate authority, take a reliable backup of the following on all Primary Servers in the Management Zone:

  ◆ **Content-Repo Directory:** The `content-repo` directory is located by default in the `ZENworks_installation_directory\work` directory on Windows and in the `/var/opt/novell/zenworks/` on Linux.

    Ensure that the `images` directory located within the `content-repo` directory has been successfully backed up.

  ◆ **Embedded Database:** For detailed information on how to back up the embedded database, see in "Backing Up the Embedded Sybase SQL Anywhere Database" in the *ZENworks 11 SP3 Database Management Reference*.

  ◆ **ZENworks Server:** For detailed information on how to back up the ZENworks Server, see Section 1.1, "Backing Up a ZENworks Server," on page 7.

2 Create a certificate signing request (CSR) by providing the hostname of the Primary Server as the subject.

   For more information on how to create a CSR, for Windows, see "Creating an External Certificate" and for Linux, see "Creating an External Certificate".

3 At the console prompt of a Primary Server, run the following command:

```
zman sacert Path_of_the_Primary_Server_in_ZENworks_Control_Center
Path_of_Primary_Server_Certificate
```

   For more information about zman, view the zman man page (`man zman`) on the device or see "zman(1)" in the *ZENworks 11 SP3 Command Line Utilities Reference*.

   This adds the certificate of the Primary Server that you specified in the command to the ZENworks database and certificate store.

   NOTE: You must run the command for each device whose certificate you want to replace.

4 Refresh all the devices, including the Primary Servers, in the zone.

   The Primary Server certificates that were imported in Step 3 are sent to the devices as configuration data.

5 Enforce the new certificates on the zone by running the following command on any Primary Server:

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

   Follow the prompts.

6 Restart all the ZENworks services on all the Primary Servers in the zone by running the following command at the console prompt of each Primary Server in the zone:

```
novell-zenworks-configure -c Start
```

   By default, all the services are selected. You must select *Restart* as the *Action*.

7 Ensure that DNS is properly configured for the Primary Servers, so that server host names get resolved. For DNS resolution requirements, see "DNS Resolution" in the "ZENworks 11 SP3 System Requirements".

   Run the following commands in the same sequence:

```
novell-zenworks-configure -Z -c MergeTruststore

novell-zenworks-configure -c EnableJMX

novell-zenworks-configure -c ZenProbe
```

8 Refresh all the devices, including the Primary Servers, in the zone.

9 (Conditional) If any device is not reachable during the refresh, you must first establish a connection with the device, then run the following command at the console prompt of each device to reestablish the trust between the device and the zone:

```
zac retr -u zone_administrator_username -p zone_administrator_password
```

10 Configure the Satellites with the new external certificates by entering the following command at the Satellite's prompt:

```
zac iac -pk private-key.der -c signed-server_certificate.der -ca signing-
authority-public-certificate.der -ks keystore.jks -ksp keystore-pass-phrase -a
signed-cert-alias -ks signed-cert-passphrase -u username -p password  -rc
```

For more information about zac, view the zac man page (`man zac`) on the device or see the *ZENworks 11 SP3 Command Line Utilities Reference*.

11 Re-create all the default and custom deployment packages for all the Primary Servers:

   ◆ **Default Deployment Packages:** At the console prompt of each Primary Server in the zone, enter the following command:

```
novell-zenworks-configure -c CreateExtractorPacks -Z
```

   ◆ **Custom Deployment Packages:** At the console prompt of each Primary Server in the zone, enter the following command:

```
novell-zenworks- configure -c RebuildCustomPacks -Z
```

12 (Conditional) If your zone includes Intel AMT devices, unprovision and provision the devices.

For more information about unprovisioning and provisioning Intel AMT devices, see "Configuring Intel AMT Devices in Enterprise Mode" in the *ZENworks 11 SP3 Out-of-Band Management Reference*.

13 (Conditional) If multizone is configured with the server whose certificate has got replaced as the Publisher, then update the new certificate of this server for all its Subscribers. Perform the following to update the new certificate:

   1. Log in to ZENworks Control Center (ZCC) of subscribers.

   2. Navigate to *Subscribe And Share* > *Subscriptions* > *<subscription_name>* > *Remote Server* > *Update Certificate*.

   3. Update the certificate.

NOTE: Because ZENworks and ZENworks Reporting does not use the same certificate, the ZENworks Reporting does not require any configuration changes if the ZENworks certificate is changed. However, if you want to replace the certificate of ZENworks Reporting with the new certificate, you must run ZENworks Reporting Configuration Tool.

For more information, see "ZENworks Reporting Configuration Tool " in the *ZENworks Reporting 5 System Reference*.

4.4 Replacing an External Server Certificate with a New External Server Certificate Issued by a Different Certificate Authority

1 If you want to change your zone certificate authority, take a reliable backup of the following on all Primary Servers in the Management Zone:

   - **Content-Repo Directory:** The `content-repo` directory is located by default in the `ZENworks_installation_directory\work` directory on Windows and in the `/var/opt/novell/zenworks/` on Linux.

     Ensure that the `images` directory located within the `content-repo` directory has been successfully backed up.

   - **Embedded Database:** For detailed information on how to back up the embedded database, see in "Backing Up the Embedded Sybase SQL Anywhere Database" in the *ZENworks 11 SP3 Database Management Reference*.

   - **ZENworks Server:** For detailed information on how to back up the ZENworks Server, see Section 1.1, "Backing Up a ZENworks Server," on page 7.

2 Create a server certificate by using the new certificate authority for each Primary Server in the zone by providing the fully qualified DNS (FQDN) of the Primary Server as the subject.

   For more information on how to create a CSR, for Windows, see "Creating an External Certificate" and for Linux, see "Creating an External Certificate".

3 At the console prompt of a Primary Server, run the following command:

   ```
   zman sacert Path_of_the_Primary_Server_in_ZENworks_Control_Center
   Path_of_Primary_Server_Certificate
   ```

   For more information about zman, view the zman man page (`man zman`) on the device or see "zman(1)" in the *ZENworks 11 SP3 Command Line Utilities Reference*.

   This adds the certificate of the Primary Server that you specified in the command to the ZENworks database and certificate store.

   NOTE: You must run the command for each Primary Server whose certificate you want to replace.

   ---

4 Refresh all the devices, including the Primary Servers, in the zone.

   The Primary Server certificates that were imported in Step 3 are sent to the devices as configuration data.

5 Import the root certificate of the new certificate authority into the trusted store on all the devices in the zone through the `zac cert-info` command. You can choose to execute the command in one of the following ways:

   - Manually run the following command on each Primary Server and managed device in the zone:

     ```
     zac cert-info certificate_file_path -u zone_administrator_username -p
     zone_administrator_password
     ```

     For more information about zac, view the zac man page (`man zac`) on the device or see the *ZENworks 11 SP3 Command Line Utilities Reference*.

   - Use a ZENworks bundle.

     For more information about bundles, see "Creating Bundles" in the *ZENworks 11 SP3 Software Distribution Reference*.

6 Enforce the new certificates on the zone by running the following command on any Primary Server:

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

Follow the prompts.

7 Restart all the ZENworks services on all the Primary Servers in the zone by running the following command at the console prompt of each Primary Server in the zone:

```
novell-zenworks-configure -c Start
```

By default, all the services are selected. You must select *Restart* as the *Action*.

8 Ensure that DNS is properly configured for the Primary Servers, so that server host names get resolved. For DNS resolution requirements, see "DNS Resolution" in the "ZENworks 11 SP3 System Requirements".

Run the following commands in the same sequence:

```
novell-zenworks-configure -Z -c MergeTruststore
```

```
novell-zenworks-configure -c EnableJMX
```

```
novell-zenworks-configure -c ZenProbe
```

9 Refresh all the devices, including the Primary Servers, in the zone.

10 (Conditional) If any device is not reachable during the refresh, you must first establish a connection with the device, then run the following command at the console prompt of each device to reestablish the trust between the device and the zone:

```
zac retr -u zone_administrator_username -p zone_administrator_password
```

11 Configure the Satellites with the new external certificates by entering the following command at the Satellite's prompt:

```
zac iac -pk private-key.der -c signed-server_certificate.der -ca signing-
authority-public-certificate.der -ks keystore.jks -ksp keystore-pass-phrase -a
signed-cert-alias -ks signed-cert-passphrase -u username -p password  -rc
```

For more information about zac, view the zac man page (`man zac`) on the device or see the *ZENworks 11 SP3 Command Line Utilities Reference*.

12 Re-create all the default and custom deployment packages for all the Primary Servers:

- ◆ **Default Deployment Packages:** At the console prompt of each Primary Server in the zone, enter the following command:

  ```
  novell-zenworks-configure -c CreateExtractorPacks -Z
  ```

- ◆ **Custom Deployment Packages:** At the console prompt of each Primary Server in the zone, enter the following command:

  ```
  novell-zenworks- configure -c RebuildCustomPacks -Z
  ```

13 (Conditional) If your zone includes Intel AMT devices, unprovision and provision the devices.

For more information about unprovisioning and provisioning Intel AMT devices, see "Configuring Intel AMT Devices in Enterprise Mode" in the *ZENworks 11 SP3 Out-of-Band Management Reference*.

14 (Conditional) If multizone is configured with the server whose certificate has got replaced as the Publisher, then update the new certificate of this server for all its Subscribers. Perform the following to update the new certificate:

1. Log in to ZENworks Control Center (ZCC) of subscribers.

2. Navigate to *Subscribe And Share > Subscriptions > <subscription_name> > Remote Server > Update Certificate*.

3. Update the certificate.

NOTE: Because ZENworks and ZENworks Reporting does not use the same certificate, the ZENworks Reporting does not require any configuration changes if the ZENworks certificate is changed. However, if you want to replace the certificate of ZENworks Reporting with the new certificate, you must run ZENworks Reporting Configuration Tool.

For more information, see "ZENworks Reporting Configuration Tool " in the *ZENworks Reporting 5 System Reference*.

5 Reconfiguring a Zone Certificate After It Expires

ZENworks prompts you to change your ZENworks zone certificate 90 days before the expiration of the certificate. The following warning message is displayed for each administrator once every 24 hours when the administrator logs in to ZENworks Control Center:

```
The certificate on hostname_of_the_device will expire in number_of_days days.
```

The message is displayed for every server and zone whose certificate is about to expire.

If you do not change your zone certificate before it expires, the communication between Primary Servers and managed devices breaks down, and the managed devices fail to receive new assignments and policies. To reestablish the communication, you have to re-create the certificate. ZENworks allows you to re-create the certificates in the following scenarios:

- Changing the zone certificate from internal to external. For more information, see Section 4.1, "Changing the Zone Certificate from Internal to External," on page 31.
- Replacing an internal server certificate with a new internal server certificate. For more information, see Section 4.2, "Replacing an Internal Server Certificate with a New Internal Server Certificate," on page 34.
- Replacing an external server certificate with a new external server certificate issued by the same certificate authority. For more information, see Section 4.3, "Replacing an External Server Certificate with a New External Server Certificate Issued by the Same Certificate Authority," on page 36.
- Replacing an external server certificate with a new external server certificate issued by a different certificate authority. For more information, see Section 4.4, "Replacing an External Server Certificate with a New External Server Certificate Issued by a Different Certificate Authority," on page 38.

You use the same procedure to re-create the certificates in all the scenarios.

Configure the Satellites with the renewed certificates by entering the following command at the console prompt of each Satellite in the zone:

```
zac iac -pk private-key.der -c signed-server_certificate.der -ca signing-authority-
public-certificate.der -ks keystore.jks -ksp keystore-pass-phrase -a signed-cert-
alias -ks signed-cert-passphrase -u username -p password -rc
```

For more information about zac, view the zac man page (`man zac`) on the device or see the *ZENworks 11 SP3 Command Line Utilities Reference*.

The information provided in this section is applicable for Windows and Linux platforms.

IMPORTANT: ZENworks 11 SP3 currently does not support changing the external certificate to an internal certificate on Primary Servers.

A Documentation Updates

This section summarizes the significant changes made to the *Disaster Recovery Reference* since the initial release of ZENworks 11 SP3.