www.novell.com/documentation

Audit Management Reference

ZENworks® 11 Support Pack 3

February 2014

Novell®

Legal Notices

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

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

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

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

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

Novell Trademarks

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

Third-Party Materials

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

Contents

About This Guide

This *Novell ZENworks 11 SP3 Audit Management Reference* includes information to help you successfully record and view activities that take place in your ZENworks system.

The information in this guide is organized as follows:

- Chapter 1, “Audit Management Workflow,” on page 7
- Chapter 2, “Audit Management Overview,” on page 9
- Chapter 3, “Prerequisites,” on page 13
- Chapter 4, “Working with Change Events,” on page 15
- Chapter 5, “Working with Agent Events,” on page 21
- Chapter 6, “Common Tasks,” on page 27
- Appendix A, “Troubleshooting,” on page 33

Audience

This document is intended for administrators or individuals who are concerned with the auditing and monitoring of all actions performed in the zone. To understand and perform the procedures described in this document, you should have a working knowledge of ZENworks and its various features.

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 website (http://www.novell.com/documentation/zenworks113/).

1 Audit Management Workflow

To audit changes that occur in the zone, complete the following tasks in the order listed:

	Task	Details
□	Review concepts important to the successful auditing of changes that occur in the zone.	For information, see “Audit Management Overview” on page 9.
□	Prior to commencing the workflow, ensure that all the prerequisite tasks are completed.	For information, see “Prerequisites” on page 13.
□	Understand the types of changes for which change and agent events can be generated.	You can audit two types of events: change events and agent events. Change events capture any configuration changes made to the zone through ZENworks Control Center. For information about change events, see “Change Event Categories” on page 15. Agent events capture actions that occur on the ZENworks managed devices. For information about agent events, see “Agent Event Categories” on page 21.
□	Enable the change events and agent events that you want to audit.	For information, see “Enabling a Change Event” on page 16 and “Enabling an Agent Event” on page 21.
□	View the generated event details in ZENworks Control Center.	For information about how to view a change event, see “Viewing a Generated Change Event” on page 17, and for information about how to view an agent event, see “Viewing a Generated Agent Event” on page 23.
□	Generate audit reports.	For information, see “Viewing and Generating Reports” on page 30.

2 Audit Management Overview

The Audit Management feature enables you to capture various events that occur in your zone. The details of a captured event can be used for security and compliance purposes, enabling you to identify who did what and on which system, when an important event occurs in your environment. Using this feature, you can centrally monitor activities related to Primary Servers, Satellite Servers, and managed devices.

The following sections provide information to help you understand ZENworks Audit Management:

- Section 2.1, “ZENworks Products That Include Auditing,” on page 9
- Section 2.2, “Types of Audit Events,” on page 9
- Section 2.3, “Audit Event Information,” on page 9
- Section 2.4, “Audit Management Process for Change Events,” on page 10
- Section 2.5, “Audit Management Process for Agent Events,” on page 11

2.1 ZENworks Products That Include Auditing

ZENworks 11 SP3 provides auditing for the following products: Configuration Management, Patch Management, Endpoint Security Management, and Full Disk Encryption.

2.2 Types of Audit Events

ZENworks audit events are of two types:

- **Change Events:** These events capture configuration changes made to the zone through ZENworks Control Center. You can capture a variety of changes ranging from bundle changes to ZENworks system changes. For example, you can configure an audit event that records the activity of an administrator assigning a bundle to a device. For information about the various change events, see Section 4.1, “Change Event Categories,” on page 15.
- **Agent Events** These events capture actions that occur on the ZENworks managed devices. They are also called Device events. For information about the various agent events, see Section 5.1, “Agent Event Categories,” on page 21.

Both change events and agent events can be enabled for all devices in the zone or for individual devices.

2.3 Audit Event Information

Each audit event captures the following information:

- **Initiator:** The individual who performed the action. This could be a ZENworks administrator, an end user, a program, or a service.
- **Target:** The target on which the action was performed. This could be a ZENworks object such as device, folder, bundle, or policy. A single audit event can capture the activity performed on multiple targets.

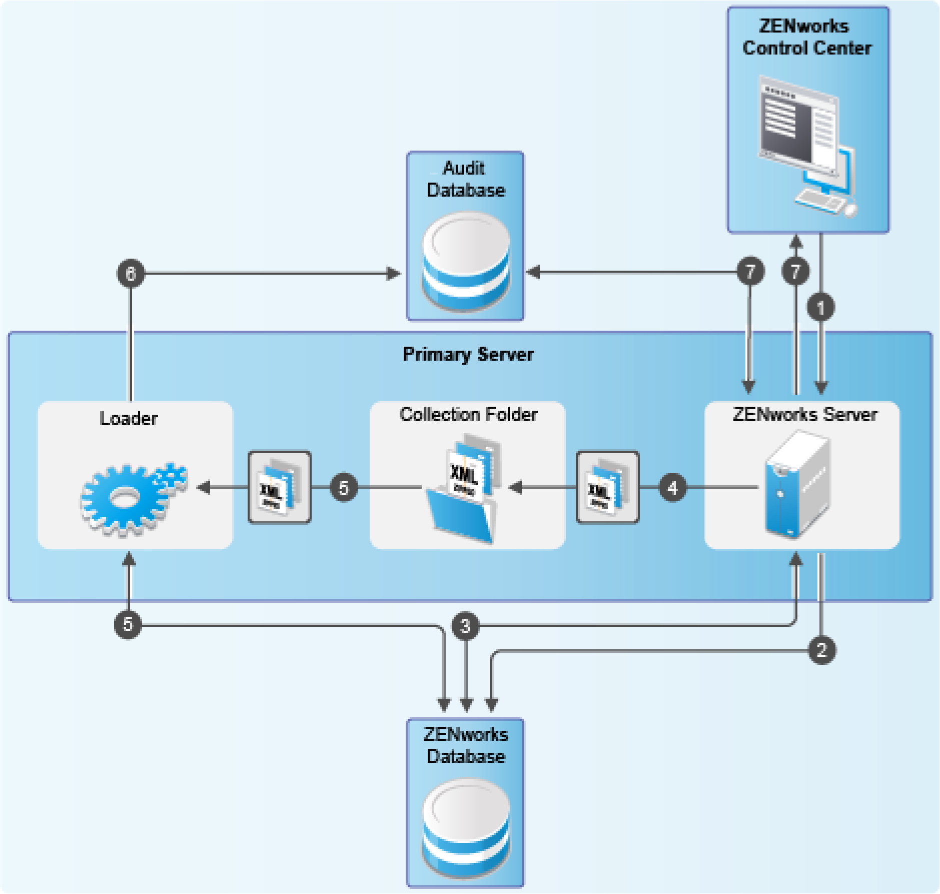
- **Time:** The time at which the action was performed.

You can view details of the generated ZENworks audit events in the ZENworks Control Center Dashboard, or you can generate reports using ZENworks Reporting. For information about the Dashboard, see Section 6.4, “Dashboard Details,” on page 31.

2.4 Audit Management Process for Change Events

Figure 2-1 provides an overview of how the Audit Management feature works for change events.

Figure 2-1 *Change Events*



The overall workflow to capture change events is as follows:

Step ❶ - Administrator enables the change events: The administrator logs in to ZENworks Control Center and enables the change events that need to be audited. For information about how to enable and configure change events, see Section 4.2, “Enabling a Change Event,” on page 16.

Step ❷ - ZENworks Primary Server saves the configuration information in the ZENworks database: After the administrator enables the change events, the ZENworks Primary Server stores this information in the ZENworks database.

Step ❸ - ZENworks Primary Server queries the ZENworks database: When a change occurs in the Management Zone, the ZENworks Primary Server queries the ZENworks database to identify whether the change needs to be audited.

Step ❹ - Change event information is sent as an XML file to the Collection folder: If the change needs to be audited, the Primary Server stores the change event details in the `Collection` folder.

Step ❺ - ZENLoader collects the XML file from the Collection folder: After the XML file is stored in the `Collection` folder, the ZENLoader collects the file from the folder. The ZENLoader also checks for additional information related to the generated change events in the ZENworks database.

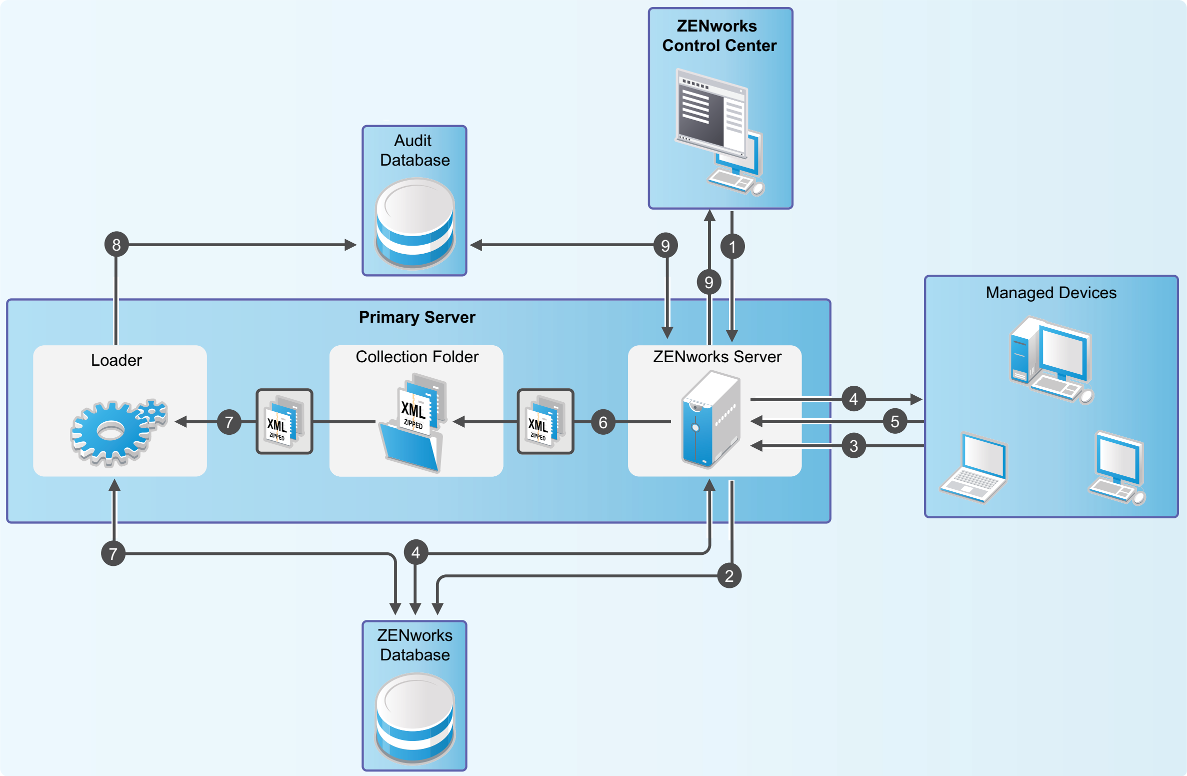
Step ❻ - ZENLoader stores the change event information in the audit database: The ZENLoader stores the change event information in the audit database.

Step ❼ - ZENworks Primary Server retrieves the generated change event details from the audit database and displays it in the Dashboard: The ZENworks Primary Server retrieves the details of the generated change events from the audit database and displays the details in the ZENworks Control Center Dashboard. For information about how to access the Dashboard, see Section 4.3, “Viewing a Generated Change Event,” on page 17.

2.5 Audit Management Process for Agent Events

Figure 2-2 provides an overview of how the Audit Management feature works for agent events.

***Figure 2-2** Agent Events*



The overall workflow to capture agent events is as follows:

Step ❶ - Administrator enables the agent events: The administrator logs in to ZENworks Control Center and enables the agent events that need to be audited. For information about how to enable and configure agent events, see Section 5.2, “Enabling an Agent Event,” on page 21.

Step ❷ - ZENworks Primary Server saves the configuration information in the ZENworks database: After the administrator enables the agent events, the ZENworks Primary Server stores this information in the ZENworks database.

Step❸ - Agent on the managed device refreshes and queries the ZENworks Primary Server: Based on the configuration settings, the agent on the managed device refreshes at regular intervals and queries the ZENworks Primary Server to identify whether the changes need to be audited.

Step ❹ - ZENworks Server queries the ZENworks Database: The ZENworks Primary Server queries the ZENworks database, and information related to the agent event configuration settings is passed back to the agent.

Step ❺ - Agent event information is sent as an XML file to the ZENworks Primary Server: If the agent event needs to be audited, the agent sends the agent events XML file to the Primary Server.

Step ❻- Agent event information is sent as an XML file to the Collection Folder: The Primary Server stores the agent events XML file in the `Collection` folder.

Step❼ - ZENLoader collects the XML file from the Collection folder: After the XML file is stored in the `Collection` folder, the ZENLoader retrieves the file from the folder. It also checks for additional information related to the generated agent events in the ZENworks database.

Step ❽ - ZENLoader stores the agent event information in the audit database: The ZENLoader stores the gathered agent event information in the audit database.

Step ❾ - ZENServer retrieves the generated agent event details from the audit database and displays it in the ZENworks Control Center Dashboard: The ZENworks Primary Server retrieves the details of the generated agent events from the audit database and displays them in the ZENworks Control Center Dashboard. For information about how to access the Dashboard, see Section 5.4, “Viewing a Generated Agent Event,” on page 23.

3 Prerequisites

Prior to using the Audit Management feature, ensure that the following requirements have been met:

- **Product Licensing:** To configure events related to a specific component, ensure that the component license is activated. For example, if you want to configure Patch Management events, Patch Management must be activated in the zone. For more information, see the *ZENworks 11 SP3 Product Licensing Reference*.
- **Audit Management Rights:** To perform activities related to Audit Management, such as configuring audit events, viewing audit logs, and viewing audit events, ensure that you have the appropriate Audit Management rights. For more information about these rights, see "Rights Descriptions" in the *ZENworks 11 SP3 Administrator Accounts and Rights Reference*.
- **Audit Reporting:** In addition to being able to view audit data in ZENworks Control Center from the Audit Log and Dashboard, you can also use ZENworks Reporting to report against the events in the database. To use the Audit Reporting feature, you must set up the ZENworks Reporting on a Windows or Linux server in your environment. For more information, see the *ZENworks Reporting 5 Installation Guide*.
- **Browser Setting for Firefox:** In a Firefox browser, when you try to scroll through the logged audit events in the Dashboard, or any Audit-related pages such as the Audit Event Configuration Settings tree, it does not scroll effectively like a normal web page. To resolve this issue, in the Firefox browser, navigate to the *Tools* > *Options* > *Advanced* > *General* tab, and in the *Browsing* section, deselect the *Use smooth scrolling* checkbox.

4 Working with Change Events

Change events capture configuration changes made to the zone through ZENworks Control Center. You can capture a variety of changes, ranging from bundle changes to ZENworks system changes. For example, you can configure an audit event that records the activity of an administrator assigning a bundle to a device.

The following sections provide information to help you configure and monitor change events:

- Section 4.1, “Change Event Categories,” on page 15
- Section 4.2, “Enabling a Change Event,” on page 16
- Section 4.3, “Viewing a Generated Change Event,” on page 17
- Section 4.4, “Searching for Events,” on page 18
- Section 4.5, “Generating Reports for Events,” on page 19
- Section 4.6, “Local Audit Logging,” on page 19

4.1 Change Event Categories

You can configure the following types of change events:

- **ZENworks Endpoint Security Management:** When an Endpoint Security policy is modified.
- **Full Disk Encryption:** When a Disk Encryption policy is modified.
- **ZENworks System:** When changes are made to the following objects:
  - **Settings:** When a zone setting or object setting is changed.
  - **User Source:** When User Sources and User Source Connections are added, removed, deleted, or modified.
  - **Administration:** For all actions related to ZENworks Control Center login, administrator and administrator groups, credential vault, roles, and registration.
  - **Location:** When Locations and Network Environments are created, deleted, or modified.
  - **System Update:** For the various stages of system update deployment.
  - **Licensing:** When products are activated or deactivated.
  - **Devices:** For all changes made to devices, device folders, device groups, and Satellite Servers.
  - **Bundles:** For all actions performed on bundles and bundle groups.
  - **Policies:** For all actions performed on policies, policy folders, and policy groups.
  - **Discovery Tasks and Deployment Tasks:** For all changes made to discovery and deployment tasks.
  - **Subscriptions:** For all changes made to subscriptions and subscription folders.
  - **Zone Sharing:** When zone sharing is suspended or changes are made.
  - **Patch:** When patches are enabled, disabled, created, or modified.

For information about how to configure change events, see Enabling a Change Event.

4.2 Enabling a Change Event

To audit a change event, you must first enable the event in ZENworks Control Center. You can enable the event at the zone or device level. An event that is enabled at the zone level applies to all devices in the zone, and an event that is enabled at the device level applies to only the selected device.

1 Log in to ZENworks Control Center.

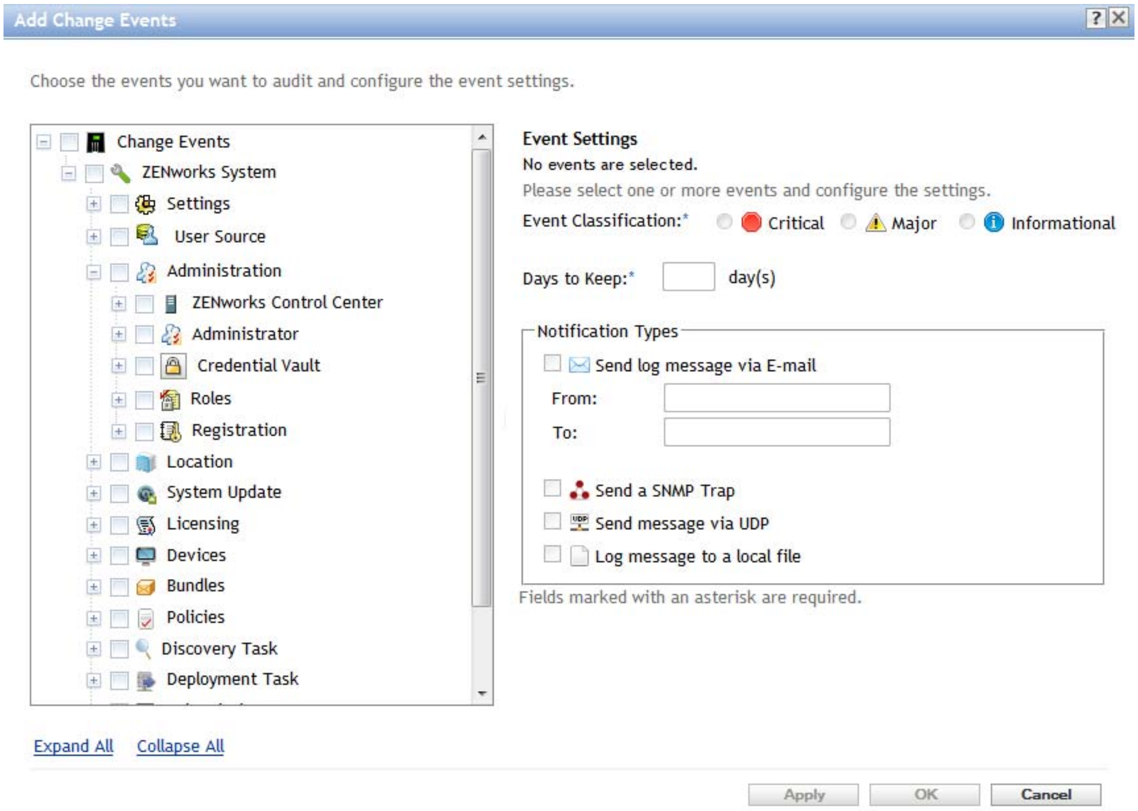
2 (Zone) To enable events at the zone, click *Configuration* > *Management Zone Settings* > *Audit Management*.

   or

   (Devices) To enable events at the device, click *Devices* > *Managed Devices*. Locate the device in the Servers or Workstations folders, click the device object to display its properties, then click *Settings* > *Audit Management*.

3 Click *Events Configuration* to display the Events Configuration dialog page.

4 In the *Change Events* tab, click *Add* to display the Add Change Events dialog box.



Add Change Events

Choose the events you want to audit and configure the event settings.

Event Settings

No events are selected.

Please select one or more events and configure the settings.

Fields marked with an asterisk are required.

For information about the change event categories, see Section 4.1, “Change Event Categories,” on page 15.

For this example, we are using the *Bundle Assignment Modified* event. However, depending on which event you want to enable, you can select the appropriate event category.

5 To select the *Bundle Assignment Modified* event, click *Change Events* > *ZENworks System* > *Bundles*.

6 Select the *Bundle Assignment Modified* check box.

7. Specify the following information for the *Event Settings*:

   - **Event Classification:** Based on the importance of the event, select *Critical*, *Major,* or *Informational*.
   - **Days to Keep:** Indicate the number of days to keep the event before purging it.

     For information about purging audit events, see Section 6.1, “Scheduling Audit Purge,” on page 27.
   - **Notification Types:** Specify whether the notification should be sent via email, SNMP Trap, UDP, or to a local file when the event occurs. If you select *Log message to a local file*, you must configure the local log file settings. For more information, see Section 4.6, “Local Audit Logging,” on page 19.

     Using the email option, you can send notifications to multiple email addresses. Each email address should be separated with a comma.

     You can also select multiple notification types. For more information, see “Using Message Logging”.

8. Click *OK* to add the event.

You can edit or delete an event by selecting the event in the Event Configuration page and clicking *Edit* or *Delete* from the menu bar. To select multiple events at a time, press *Ctrl* and click to select.

You can also search for events that have been enabled by using the Search field in the *Events Configuration* page. For more information about how to search for events, see Section 6.2, “Searching for Events,” on page 28.

4.3 Viewing a Generated Change Event

When an enabled change event has occurred, an audit event is generated. Hence, for the *Bundle Assignment Management* event used in this workflow, an audit event is generated when a bundle is assigned to a device. For information about how to assign a bundle to a device, see “Managing Bundle Assignments” in the *ZENworks 11 SP3 Software Distribution Reference*.

After an audit event is generated, you can access the details of the event from the following locations:

- **Dashboard:** You can view the audit data through the ZENworks Control Center Dashboard. The Dashboard has the following tabs:
  - **Dashboard:** From this tab you can see a summary of the audit events that have occurred in the zone. You can see key indicators about top events and impacted objects, and you can drill into the event log view in a filtered manner. By default, this dashboard shows you an overview of events in the last 4 hours. If you want to see more data, you can change the time period. For more information about the event details listed in the Dashboard, see Section 6.4, “Dashboard Details,” on page 31.
  - **Events (Audit Log):** This tab enables you to view all of the events that have occurred in the zone. The information is displayed in a format similar to the Events Configuration page. A count is displayed against those categories for which an event has been generated. For example, if a *Bundle Assignment Management* event has been generated, *1* is displayed against the Bundle Assignment Management category in the tree structure. When you click the event, the details of the event are displayed in the right pane.
- **Object Folders:** The *Audit* tab in the object folders (*Devices*, *Bundles*, *Polices* and *Users*) enables you to view the audit events that are generated for all objects within the selected folder. For example, you can view the events generated for all bundles within a bundles folder. Hence,

all bundle-related events can be viewed in the Bundles folder. The information is categorized similar to the *Events Configuration* page. You can browse through events that have occurred, and if you need more information, you can click the event to view the event details.

- **Objects:** You can also view the audit events for an object within the object folder. For example, if you select a particular bundle within a bundles folder, you can view the events generated for that specific bundle.

To view the generated event details (Example: *Bundle Assignment Management* event):

1. Log in to ZENworks Control Center.
2. (Dashboard) To view the events in the Dashboard, click *Dashboard* > *Events*.

   or

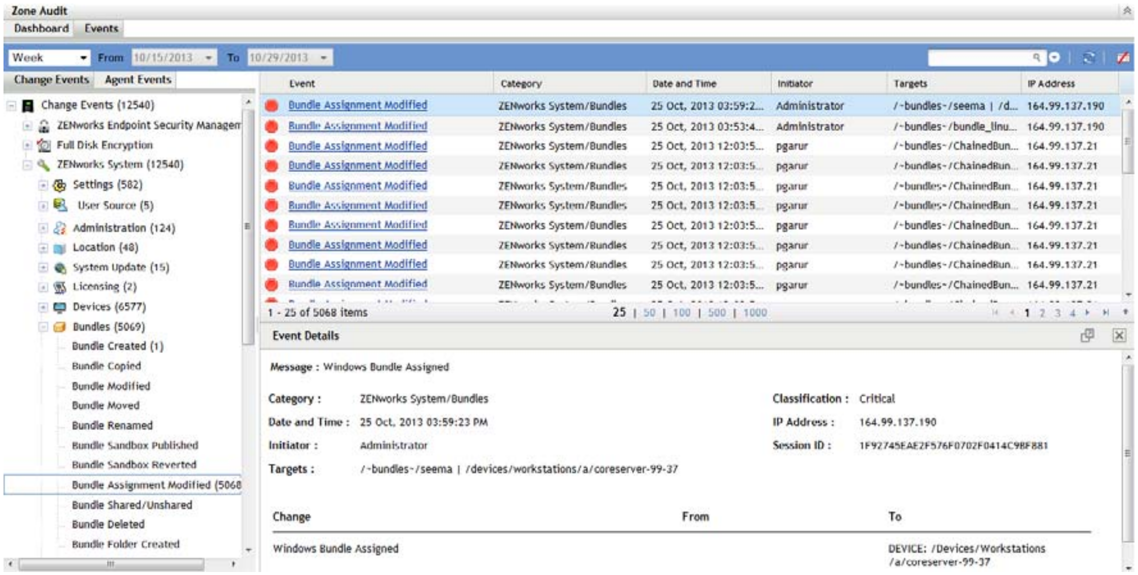
   (Object Folder) To view the events for all objects in a folder (for example, a device folder, bundles folder, or policy folder), click the folder's *Details* link, then click the *Audit* tab.

   or

   (Object) To view the events for a specific object (for example, a device, bundle, or policy), click the object, then click the *Audit* tab.
3. Click the *Change Events* tab.
4. In the tree structure, click *Change Events* and expand the *ZENworks System* category.

   Depending on the number of audit change events configured, the relevant count is displayed against the change event category.
5. Click *Bundles* > *Bundle Assignment Modified*.

   The details of the generated event are displayed in the right pane.



Event	Category	Date and Time	Initiator	Targets	IP Address
Bundle Assignment Modified	ZENworks System/Bundles	25 Oct, 2013 03:59:2...	Administrator	/~bundles~/seema | /d...	164.99.137.190
Bundle Assignment Modified	ZENworks System/Bundles	25 Oct, 2013 03:53:4...	Administrator	/~bundles~/bundle_linu...	164.99.137.190
Bundle Assignment Modified	ZENworks System/Bundles	25 Oct, 2013 12:03:5...	pgarur	/~bundles~/ChainedBun...	164.99.137.21
Bundle Assignment Modified	ZENworks System/Bundles	25 Oct, 2013 12:03:5...	pgarur	/~bundles~/ChainedBun...	164.99.137.21
Bundle Assignment Modified	ZENworks System/Bundles	25 Oct, 2013 12:03:5...	pgarur	/~bundles~/ChainedBun...	164.99.137.21
Bundle Assignment Modified	ZENworks System/Bundles	25 Oct, 2013 12:03:5...	pgarur	/~bundles~/ChainedBun...	164.99.137.21
Bundle Assignment Modified	ZENworks System/Bundles	25 Oct, 2013 12:03:5...	pgarur	/~bundles~/ChainedBun...	164.99.137.21
Bundle Assignment Modified	ZENworks System/Bundles	25 Oct, 2013 12:03:5...	pgarur	/~bundles~/ChainedBun...	164.99.137.21
Bundle Assignment Modified	ZENworks System/Bundles	25 Oct, 2013 12:03:5...	pgarur	/~bundles~/ChainedBun...	164.99.137.21
Bundle Assignment Modified	ZENworks System/Bundles	25 Oct, 2013 12:03:5...	pgarur	/~bundles~/ChainedBun...	164.99.137.21

1 - 25 of 5068 items 25 | 50 | 100 | 500 | 1000 1 2 3 4

Event Details

Message : Windows Bundle Assigned

Category : ZENworks System/Bundles
Date and Time : 25 Oct, 2013 03:59:23 PM
Initiator : Administrator
Targets : /~bundles~/seema | /devices/workstations/a/coreserver-99-37

Classification : Critical
IP Address : 164.99.137.190
Session ID : 1F92745EAE2F576F0702F0414C9BF881

Change	From	To
Windows Bundle Assigned		DEVICE: /Devices/Workstations /a/coreserver-99-37

NOTE: To view the details of the event in a new window, click

4.4 Searching for Events

You can search for specific events after they are generated. For information about how to search for an event, see Section 6.2, “Searching for Events,” on page 28.

4.5 Generating Reports for Events

In addition to viewing information about generated audit events in ZENworks Control Center, you can also view information and generate reports for events using ZENworks Reporting. For information about ZENworks Reporting, see Section 6.3, “Viewing and Generating Reports,” on page 30.

4.6 Local Audit Logging

The Local Audit Logging feature enables you to configure the local log file details. While configuring an event, if you select the Notification Type as *Log message to a Local file*, the configuration settings made in the Local Audit Logging page are used to create the files. This feature is available only for logging change events (not agent events). For more information about the *Log message to a Local file* option, see “Notification Types:” on page 17.

On a Windows Primary Server, the local files include the following:

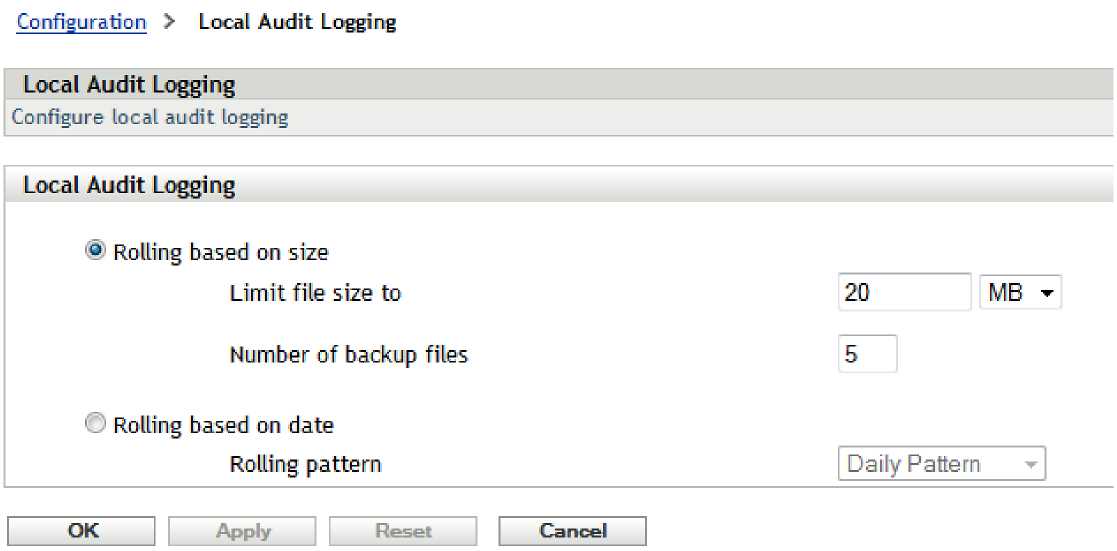
- `AuditLog.csv` located in `<%ZENworks_HOME%>\logs`

On a Linux Primary Server, the local files include the following:

- `AuditLog.csv` located in `/var/opt/novell/log/zenworks`

To configure the local audit logging settings:

1. In ZENworks Control Center, click *Configuration*.
2. In the *Management Zone Settings* section of the *Configuration* tab, click *Audit Management*.
3. Click *Local Audit Logging*.



Configuration > Local Audit Logging

Local Audit Logging
Configure local audit logging

Local Audit Logging

● Rolling based on size
Limit file size to: 20 MB
Number of backup files: 5

○ Rolling based on date
Rolling pattern: Daily Pattern

4. Specify the following details:
   - **Rolling Based on Size:** Closes the current audit event log file and starts a new one based on the file size:
     - **Limit File Size to:** Specify the maximum size of the audit event log file, in either kilobytes (KB) or megabytes (MB). The audit event log file is closed after reaching the specified size and a new one is started.

  - **Number of Backup Files:** Specify the number of closed files to be retained as backups. The maximum number of backup files is 13.
- **Rolling Based on Date:** Closes the current audit event log file and starts a new one based on the date. Based on the required frequency, you can use the *Daily Pattern* or *Monthly Pattern* options.

5 Working with Agent Events

Agent events capture actions that occur on the ZENworks managed devices. An example is an audit event that records the login activity of a ZENworks user on a managed device. The following sections provide information to help you configure and monitor agent events:

5.1 Agent Event Categories

You can configure the following types of agent events:

- **User Management:** For all actions related to user login, logout, and password change.

  NOTE: When the pass-through login fails and the user is prompted to enter the login credentials, if the user cancels the login prompt, a login failure event is still generated for the failed pass-through login.

- **Remote Management:** For all actions related to abnormal termination detection, authentication, intruder detection, remote sessions, and file transfer.
- **ZENworks Endpoint Security Management:** For all actions related to removable storage, and for all changes made to effective policies, locations, and network environments.
- **ZENworks Adaptive Agent:** For changes made to location or network environment parameters.

For information about how to configure agent events, see Enabling an Agent Event.

5.2 Enabling an Agent Event

To audit an agent event, you must first enable the event in ZENworks Control Center. You can enable the event at the zone or device level. An event that is enabled at the zone level applies to all devices in the zone; an event that is enabled at the device level applies only to the selected device. For this workflow, we have used the Remote Management, *File Transfer* event.

Remote Management events include tasks such as Remote Control, Remote View, File Transfer, Remote Execute, and Remote Diagnostics. Using the auditing capability, you can maintain a centralized log of who performed the operation and when was it performed. In the case of File

Transfer, Remote Execute, and Remote Diagnostics you will be able to capture what was done during the session. For more information on the Remote Management events, see the ZENworks 11 SP3 Remote Management Reference.

1 Log in to ZENworks Control Center.

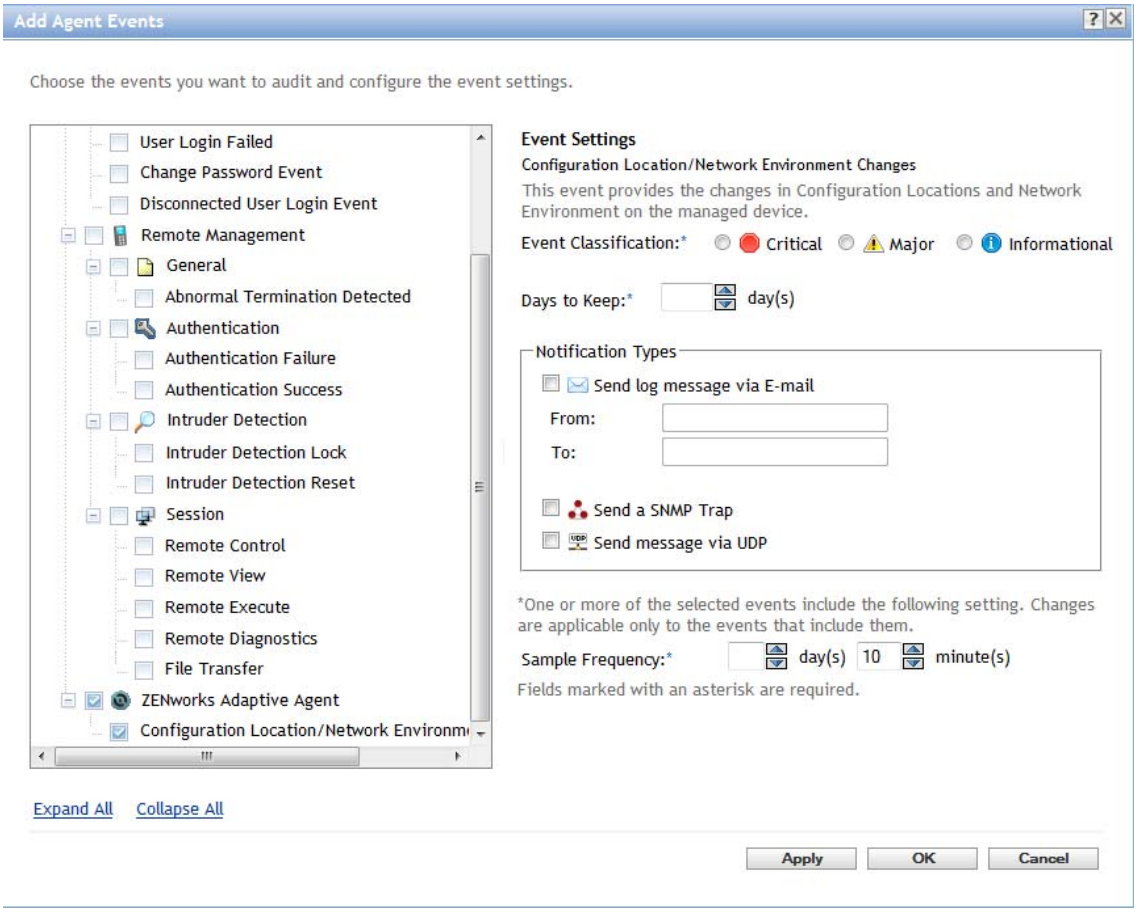
2 (Zone) To configure events at the zone, in the left pane, click *Configuration* > *Management Zone Settings* > *Audit Management*.

or

(Devices) To enable events at the device, click *Devices* > *Managed Devices*. Locate the device in the Servers or Workstations folders, click the device object to display its properties, then click *Settings* > *Audit Management*.

3 Click *Events Configuration* to display the Events Configuration page.

4 In the *Agent Events* tab, click *Add* to display the Add Agent Events dialog box.



Add Agent Events

Choose the events you want to audit and configure the event settings.

- □ User Login Failed
- □ Change Password Event
- □ Disconnected User Login Event
- □ Remote Management
  - □ General
    - □ Abnormal Termination Detected
  - □ Authentication
    - □ Authentication Failure
    - □ Authentication Success
  - □ Intruder Detection
    - □ Intruder Detection Lock
    - □ Intruder Detection Reset
  - □ Session
    - □ Remote Control
    - □ Remote View
    - □ Remote Execute
    - □ Remote Diagnostics
    - □ File Transfer
- ☑ ZENworks Adaptive Agent
  - ☑ Configuration Location/Network Environm

Event Settings

Configuration Location/Network Environment Changes

This event provides the changes in Configuration Locations and Network Environment on the managed device.

Event Classification:* ○ Critical ○ Major ○ Informational

Days to Keep:* day(s)

Notification Types

□ Send log message via E-mail

From:

To:

□ Send a SNMP Trap

□ Send message via UDP

*One or more of the selected events include the following setting. Changes are applicable only to the events that include them.

Sample Frequency:* day(s) 10 minute(s)

Fields marked with an asterisk are required.

For information about the agent event categories, see "Agent Event Categories" on page 21.

5 Expand the tree structure, then click *Agent Events* > *Remote Management* > *Session*.

6 Select the *File Transfer* check box. For this example we have used the *File Transfer* event. However, depending on which event you want to enable, you can select the appropriate check box.

7 Specify the following information for the *Event Settings*:

- **Event Classification:** Based on the importance of the event, select *Critical*, *Major,* or *Informational*.

   - **Days to Keep:** Indicate the number of days to keep the event before purging it.

     For information about purging audit events, see Section 6.1, “Scheduling Audit Purge,” on page 27.

   - **Notification Types:** Specify whether the event notifications should be sent via email, SNMP Trap, or UDP. Using the email option, you can send notifications to multiple email addresses. Each email address should be separated with a comma.

     You can also select multiple notification types. For more information, see “Using Message Logging.”

   - Specify the *Sample Frequency* rate at which data should be collected in order to generate audit events. This field is displayed only if a ZENworks Endpoint Security Management event or a ZENworks Adaptive Agent event is selected.

8. Click *OK* to add the event.

You can edit or delete an event by selecting the event in the Event Configuration page and clicking *Edit* or *Delete* from the menu bar. To select multiple events at a time, press *Ctrl* and click to select.

You can also search for events that have been enabled, by using the Search field in the *Events Configuration* page. For more information, see Section 6.2, “Searching for Events,” on page 28.

5.3 Refreshing the Device

An agent refresh is necessary in order to retrieve the audit event configuration settings. An audit event is generated only if the event is found to be enabled in the audit event configuration settings, and if the action is performed after the refresh. The audit event data then must be uploaded and processed by the server. You can either wait for the scheduled agent refresh to complete, or you can manually refresh the agent. To perform a manual refresh, in the notification area of the device, right-click the icon, then click *Refresh*. For more information on the agent events process, see

Considering the Remote Management *File Transfer* event for this workflow, after a remote management file transfer occurs, an audit event is generated. To perform a remote file transfer, see “Managing a File Transfer Session” in the *ZENworks 11 SP3 Remote Management Reference*.

5.4 Viewing a Generated Agent Event

After an audit event is generated, the details of the event can be accessed from the following locations:

- **Dashboard:** The Dashboard has the following tabs:
  - **Dashboard:** From this tab you can see a summary of the audit events that have occurred in the zone. You can see key indicators about top events and impacted objects, and can drill into the event log view in a filtered manner. By default, this dashboard shows you an overview of events in the last 4 hours. If you want to see more data, you can change the time period. For more information about the event details listed in the Dashboard, see Section 6.4, “Dashboard Details,” on page 31.
  - **Events (Audit Log):** This tab enables you to view all of the events that have occurred in the zone. The audit Change and Agent events are displayed. The information is displayed in a format similar to the Events Configuration page. A count is displayed against those categories for which an event has been generated. For example, if a *File Transfer* event has been generated, *1* is displayed against the *File Transfer* event in the tree structure. When you click the event, the details of the event are displayed in the right pane.

- **Devices Folder:** The *Audit* tab in the *Devices* folder enables you to view the events that are generated for a particular device (server or workstation).

To view the generated event details (Example: *File Transfer*):

1. Log in to ZENworks Control Center.
2. (Dashboard) To view the events in the *Events* tab of the Dashboard, in the left pane, click *Dashboard* > *Events.*

   or

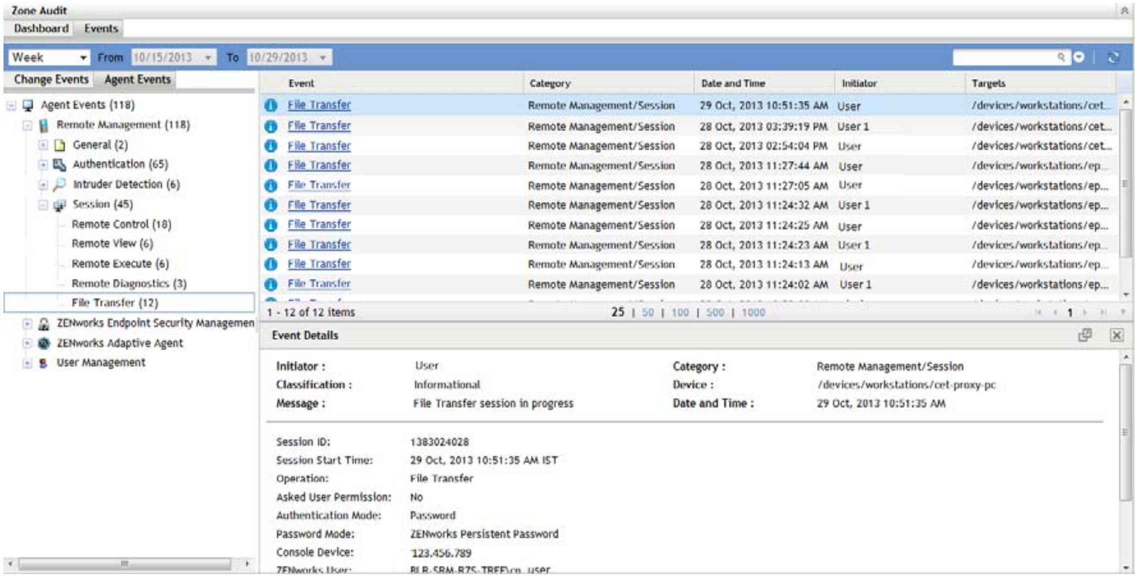
   (Devices Folder) To view the events in the Devices folder, in the left pane, click *Devices*. If the event has been performed on a server in the zone, click the server *Details*, or if the event has been performed on a managed device, click the workstation *Details*. Then click the *Audit* tab to view the Events screen.

   NOTE: Agent audit events are currently applicable only for Windows devices. Hence, if the audit event types are displayed for Linux and Mac devices, they should be ignored.

   ---
3. Click the *Agent Events* tab.
4. In the tree structure, click *Agent Events* and expand the *Remote Management* category.

   Depending on the number of audit agent events configured, the relevant count is displayed against the agent event category.
5. Click *Session* > *File Transfer*.

   The details of the generated event are displayed in the right pane.



Event	Category	Date and Time	Initiator	Targets
File Transfer	Remote Management/Session	29 Oct, 2013 10:51:35 AM	User	/devices/workstations/cet...
File Transfer	Remote Management/Session	28 Oct, 2013 03:39:19 PM	User 1	/devices/workstations/cet...
File Transfer	Remote Management/Session	28 Oct, 2013 02:54:04 PM	User	/devices/workstations/cet...
File Transfer	Remote Management/Session	28 Oct, 2013 11:27:44 AM	User	/devices/workstations/ep...
File Transfer	Remote Management/Session	28 Oct, 2013 11:27:05 AM	User	/devices/workstations/ep...
File Transfer	Remote Management/Session	28 Oct, 2013 11:24:32 AM	User 1	/devices/workstations/ep...
File Transfer	Remote Management/Session	28 Oct, 2013 11:24:25 AM	User	/devices/workstations/ep...
File Transfer	Remote Management/Session	28 Oct, 2013 11:24:23 AM	User 1	/devices/workstations/ep...
File Transfer	Remote Management/Session	28 Oct, 2013 11:24:13 AM	User	/devices/workstations/ep...
File Transfer	Remote Management/Session	28 Oct, 2013 11:24:02 AM	User 1	/devices/workstations/ep...

1 - 12 of 12 items 25 | 50 | 100 | 500 | 1000 1

Event Details

Initiator :	User	**Category :**	Remote Management/Session
Classification :	Informational	**Device :**	/devices/workstations/cet-proxy-pc
Message :	File Transfer session in progress	**Date and Time :**	29 Oct, 2013 10:51:35 AM

Session ID:	1383024028
Session Start Time:	29 Oct, 2013 10:51:35 AM IST
Operation:	File Transfer
Asked User Permission:	No
Authentication Mode:	Password
Password Mode:	ZENworks Persistent Password
Console Device:	123.456.789
ZENworks User:	BLR-SRM-R7S-TREE\cn_user

NOTE: To view the details of the event in a new window, click ⧉

5.5 Searching for Events

You can search for events after they are generated. For more information, see Section 6.2, “Searching for Events,” on page 28.

5.6 Generating Reports for Events

In addition to viewing information about generated audit events in ZENworks Control Center, you can also view information and generate reports for events using ZENworks Reporting. For more information, see Section 6.3, “Viewing and Generating Reports,” on page 30.

6 Common Tasks

The following sections provide information about tasks that are common to both change events and agent events:

- Section 6.1, “Scheduling Audit Purge,” on page 27
- Section 6.2, “Searching for Events,” on page 28
- Section 6.3, “Viewing and Generating Reports,” on page 30
- Section 6.4, “Dashboard Details,” on page 31

6.1 Scheduling Audit Purge

The data in the audit database is configured to be purged automatically after the event reaches its expiration date, based on the Days to Keep value set for that type of event. If you want to change the time when this purging operation occurs, how long it runs, or on which server it runs, you can use the Audit Purge Schedule. The Audit Purge Schedule enables you to configure the schedule to delete historical audit data from the database. All audit events that have expired (exceeded the Days to Keep configured value) will be purged. This setting is available only at the zone level. The default schedule will purge the data every Saturday at 1:00 a.m.

To change the schedule for purging audit events:

1. Log in to ZENworks Control Center.
2. Click *Configuration*.

   The Configuration tab is displayed.
3. In the *Management Zone Settings* section, click *Audit Management*.
4. Click *Audit Purge Schedule*.
5. In the *Schedule Type* field, select the *Recurring* schedule:
   - ***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 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.
   - **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 the 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.

- **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.
  - **Start Time:** Specifies the initial start time for the interval.

6. Select *Duration of the job in hours / run* to specify the total duration in number of hours, per run, for the purging process.
7. In the *Dedicated Server to run Audit Purge* field, browse and select a Primary Server, then click *OK*. Audit Purge takes place on the chosen Primary Server. If you do not select a server, then purging takes place on any server.
8. Click *OK* to save your settings.

6.2 Searching for Events

You can search for a specific event, or filter events based on category (*Critical*, *Major,* and *Informational*). You can also perform advanced searches and create, edit, and delete saved searches.

Using the Search feature, you can perform the following tasks:

- Section 6.2.1, “Search for Events,” on page 28
- Section 6.2.2, “Perform an Advanced Search,” on page 28

6.2.1 Search for Events

To search for events at the zone, device, or object level:

1. In ZENworks Control Center, select the *Events* tab in the *Dashboard*, or the *Audit* tab in the required object folder (example, *Bundles*, *Policies*, or *Users*) or *Device*s folder (servers or workstations).
2. In the *Events* page, select the event category from the *Change Events* or *Agent Events* tab.

   The search field is displayed.
3. Specify the name of the event in the search field (for example, *Bundle Assignment Management* or *File Transfer),* then press Enter.

   Events that match your search criteria are displayed.

Whenever you perform a search, the name of the selected search is displayed next to the Search field. To clear the search, click x next to the search name.

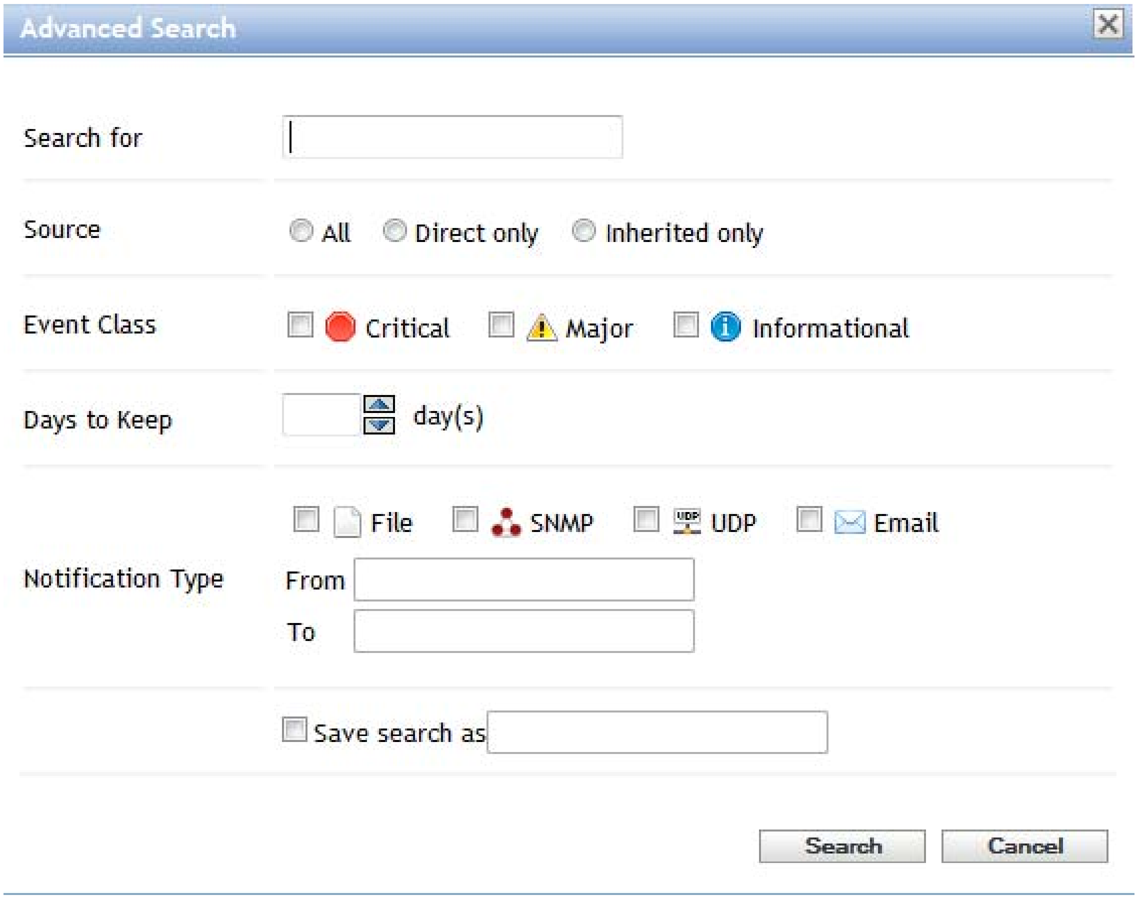
6.2.2 Perform an Advanced Search

You can use the Advanced Search feature to search for events at the Zone or Device level.

1. In the Event Configuration screen, click the down-arrow next to the Search field.

   A menu is displayed with various search-related options.

2 Click *Advanced Search* to display the Advanced Search screen.



3 Specify the following details:

- **Search for:** Specify the name of the audit event.
- **Source:** Select all events, those events that were set directly at the device level, or those that were set at the zone level and inherited by devices.
- **Event Class:** Select the classification type of the event.
- **Days to Keep:** Specify the number of days the event is stored in the database.
- **Notification Type:** Specify the notification type associated with the event.

4 To save the selected search criteria, select the Save search as check box, specify a search name, then click *Search*.

NOTE: If you have created saved searches, the search names will be displayed in the drop-down list. When you select a saved search name from the drop-down list, the relevant search results are displayed.

6.3 Viewing and Generating Reports

In addition to being able to view audit data in the ZENworks Control Center Audit log and Dashboard, you can also use ZENworks Reporting to generate reports against the events in the audit database.

By using the ZENworks Audit domain in ZENworks Reporting, you can create custom tabular, cross tab, and chart reports. You can further mix and match these reports into dynamic Dashboards that provide you with the required data view. ZENworks Reporting also enables you to view predefined reports.

6.3.1 Viewing a Predefined Audit Report

1. Use a web browser and navigate to the `http://<hostname>:<port-number>` or the `http://<IP address>:<port-number>` site and replace the IP address with the IP of the ZENworks Reporting Server installed in your zone.

   For the recommended browsers settings, refer to the *ZENworks Reporting 5 Installation Guide*.

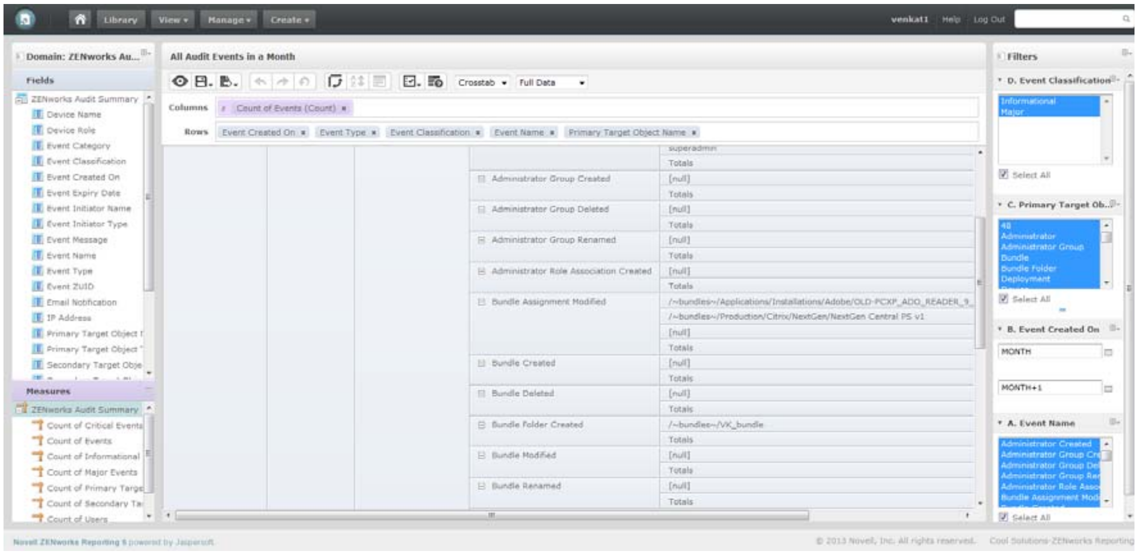
   - Mozilla Firefox 4.0 or higher
   - Microsoft Internet Explorer 7 (certified), 8 (certified), 9.0 (certified), 10.0 (v5.1)
   - Google Chrome 6.0 or higher

2. In the login screen, specify values for the *User ID* and *Password* fields.
3. In the Home screen, click *View* > *Repository*.
4. In the left pane, under root, expand the tree and navigate to *Organizations* > *Reports* > *ZENworks Audit* > *Predefined Reports*.

   The available predefined reports are displayed in the right pane.

5. Click *All Audit Reports in a Month*.

    This view displays the following objects as filters: *Events Count, Event Created On, Event Type, Event Name, Event Classification*, and *Primary Target Object Name* as filters.



All Audit Events in a Month

Columns: Count of Events (Count)

Rows: Event Created On, Event Type, Event Classification, Event Name, Primary Target Object Name

	superadmin
	Totals
Administrator Group Created	[null]
	Totals
Administrator Group Deleted	[null]
	Totals
Administrator Group Renamed	[null]
	Totals
Administrator Role Association Created	[null]
	Totals
Bundle Assignment Modified	/~bundles~/Applications/Installations/Adobe/OLD-PCXP_ADO_READER_9_
	/~bundles~/Production/Citrix/NextGen/NextGen Central PS v1
	[null]
	Totals
Bundle Created	[null]
	Totals
Bundle Deleted	[null]
	Totals
Bundle Folder Created	/~bundles~/VK_bundle
	Totals
Bundle Modified	[null]
	Totals
Bundle Renamed	[null]
	Totals

D. Event Classification: Informational, Major; ☑ Select All

C. Primary Target Ob...: 48, Administrator, Administrator Group, Bundle, Bundle Folder, Deployment; ☑ Select All

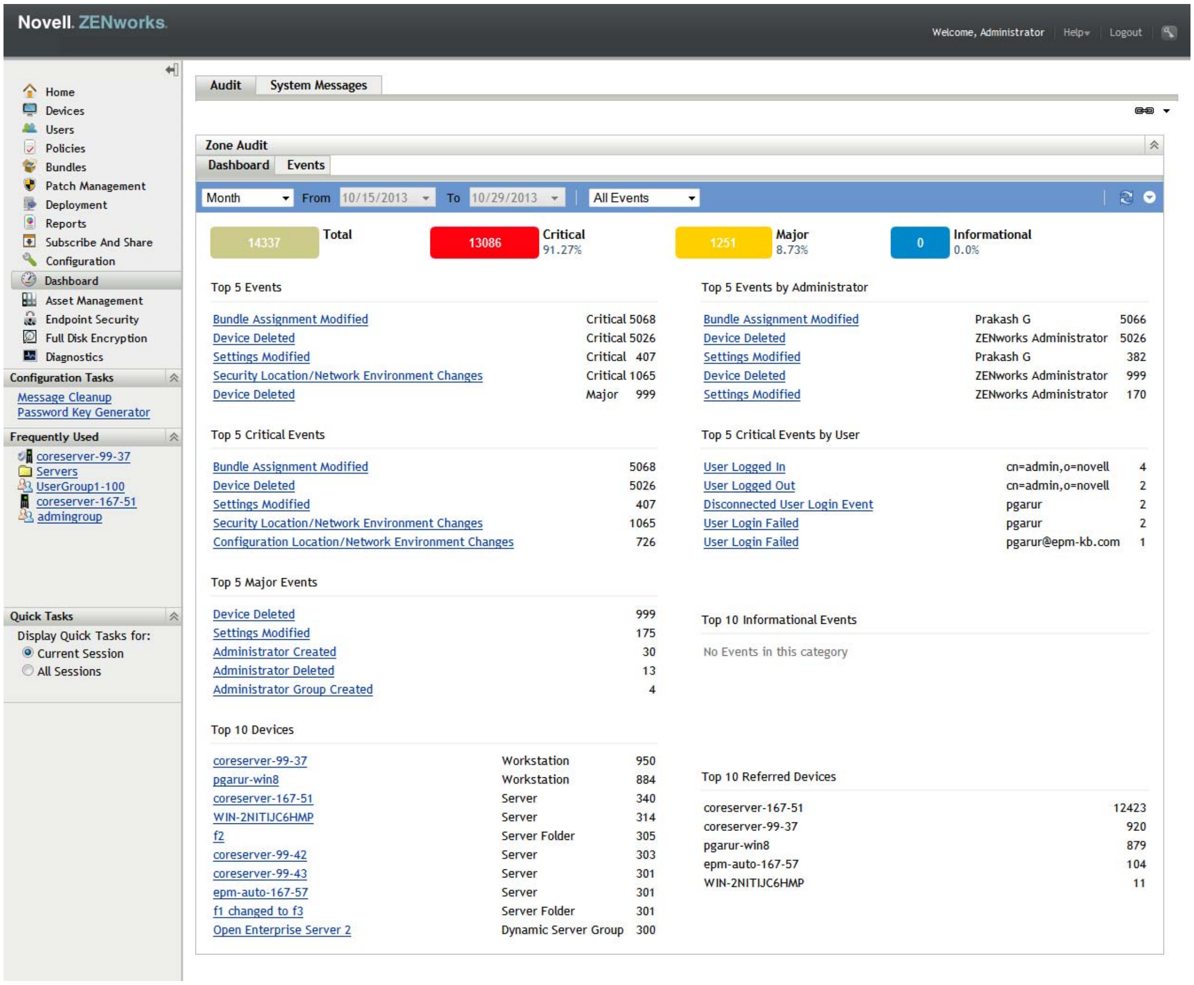
B. Event Created On: MONTH; MONTH+1

A. Event Name: Administrator Created, Administrator Group Cre, Administrator Group Del, Administrator Group Rer, Administrator Role Asso, Bundle Assignment Mod; ☑ Select All

NOTE: Depending on the kind of information you want to view, you can select the relevant predefined reports. For more information about reporting, see the *ZENworks Reporting 5 System Reference*.

6.4 Dashboard Details

Audit data can be viewed through the ZENworks Control Center Dashboard. To access this page, click the Dashboard link in the left pane of ZENworks Control Center. From this page you can see a zone-wide view of the audit events that have been logged into the system. You can see key indicators about top events and impacted objects, and drill into the Events (Audit Log) view in a filtered manner. By default, the Dashboard displays an overview of events in the last 4 hours. If you want to view more data, you can choose alternative schedules.



Month From 10/15/2013 To 10/29/2013 All Events

14337 Total | 13086 Critical 91.27% | 1251 Major 8.73% | 0 Informational 0.0%

Top 5 Events

Bundle Assignment Modified	Critical	5068
Device Deleted	Critical	5026
Settings Modified	Critical	407
Security Location/Network Environment Changes	Critical	1065
Device Deleted	Major	999

Top 5 Events by Administrator

Bundle Assignment Modified	Prakash G	5066
Device Deleted	ZENworks Administrator	5026
Settings Modified	Prakash G	382
Device Deleted	ZENworks Administrator	999
Settings Modified	ZENworks Administrator	170

Top 5 Critical Events

Bundle Assignment Modified	5068
Device Deleted	5026
Settings Modified	407
Security Location/Network Environment Changes	1065
Configuration Location/Network Environment Changes	726

Top 5 Critical Events by User

User Logged In	cn=admin,o=novell	4
User Logged Out	cn=admin,o=novell	2
Disconnected User Login Event	pgarur	2
User Login Failed	pgarur	2
User Login Failed	pgarur@epm-kb.com	1

Top 5 Major Events

Device Deleted	999
Settings Modified	175
Administrator Created	30
Administrator Deleted	13
Administrator Group Created	4

Top 10 Informational Events

No Events in this category

Top 10 Devices

coreserver-99-37	Workstation	950
pgarur-win8	Workstation	884
coreserver-167-51	Server	340
WIN-2NITIJC6HMP	Server	314
f2	Server Folder	305
coreserver-99-42	Server	303
coreserver-99-43	Server	301
epm-auto-167-57	Server	301
f1 changed to f3	Server Folder	301
Open Enterprise Server 2	Dynamic Server Group	300

Top 10 Referred Devices

coreserver-167-51	12423
coreserver-99-37	920
pgarur-win8	879
epm-auto-167-57	104
WIN-2NITIJC6HMP	11

When you log in to ZENworks Control Center and click Dashboard, the following information is displayed:

- **Top 5 Events:** The top 5 events generated by ZENworks Control Center administrators or managed devices, based on the event count. This list is not based on the classification type. Click the event name hyperlink to view the event details.
- **Top 5 Critical Events:** The top 5 events generated by ZENworks Control Center administrators or managed devices. This list is based on the maximum count for a particular event, with the classification type as *Critical*. Click the event name hyperlink to view the event details.
- **Top 5 Major Events:** The top 5 events generated by ZENworks Control Center administrators or managed devices. This list is based on the maximum count for a particular event, with the classification type as *Major*. Click the event name hyperlink to view the event details.

- **Top 5 Change Events by Administrator:** The top 5 events generated by a ZENworks administrator. This list is based on the maximum number of events generated by an administrator. Click the event name hyperlink to view the event details.
- **Top 5 Critical Events by User:** The top 5 events generated by users who have logged in to managed devices. This list is based on the maximum count for a particular event, generated by a managed device. Click the event name hyperlink to view the event details.
- **Top 10 Informational Events:** The top 10 events generated by ZENworks administrators, or managed devices. This list is based on the maximum count for a particular event, with the classification type as *Informational*. Click the event name hyperlink to view the event details.
- **Top 10 Devices:** The top 10 devices in the zone that are generating the maximum number of events. Click the device name hyperlink to view device details in the Audit Log panel.
- **Top 10 Referred Devices:** The top 10 devices in the zone on which the maximum events have occurred. The device might or might not be a target, but the actual target objects reside on this device. For example, a Primary Server on which a large number of bundles have been created can be a referred device. This is because although the target of change is the bundles, the events have occurred on the Primary Server.

A Troubleshooting

The following sections provide solutions to the problems you might encounter while using the Audit Management feature.

- "Agent Event Advanced Search containing special characters does not return results" on page 33
- "Some audit event details are not localized based on the locale" on page 33
- "Audit purging fails on an Oracle database" on page 33

Agent Event Advanced Search containing special characters does not return results

Source: ZENworks 11 SP3; Audit Management.

Explanation: Search containing special characters such as `"\"` does not return results.

Action: If the special characters search does not return results, you need to explicitly escape them in the search input. For example, if you want to search for a string such as `Workgroup\Win8`, you should specify `Workgroup\\Win8` in the search field.

Some audit event details are not localized based on the locale

Source: ZENworks 11 SP3; Audit Management.

Explanation: When an audit event is created in one locale, and the generated event details are viewed from another locale, some of the event details are not localized. For example, if you create a bundle by logging in to ZENworks Control Center (ZCC) using the *German* language, and then view details of the generated *Bundle Created* event by logging into ZCC using the *English* language, the audit bundle name is displayed in German, as it is based on the user input. However, the type of bundle, for example Windows bundle, which should appear in English, appears in German.

Action: None.

Audit purging fails on an Oracle database

Source: ZENworks 11 SP3; Audit Management.

Explanation: Audit purging fails when there are multiple audit schemas installed on the same Oracle database. The following error message is displayed: `[Loader.Audit Data Prune] [] [Audit Data Prune : Procedure call failed for <<Table Name>>. Error Code is : -1422] [] [] [] [ZENServer]`

Action: Re-create the `Z_AUDIT_PRUNING` procedure by running the script in the "Audit Pruning Procedure" file.