

ZENworks 11 SP4 - Auditing Endpoint Security Events

October 2016

Novell.

You can use the ZENworks Audit feature to capture Endpoint Security *change events* and *agent events* that occur in your zone. Change events are configuration changes made to the zone through ZENworks Control Center or the zman command line utilities. Agent events are activities that occur on managed devices.

- ◆ [Section 1, “Auditing Change Events,” on page 1](#)
- ◆ [Section 2, “Auditing Agent Events,” on page 2](#)
- ◆ [Section 3, “Legal Notices,” on page 3](#)

1 Auditing Change Events

You use change events to capture changes that ZENworks administrators make to Endpoint Security policies. You can capture any of the following events:

- ◆ Policy created
- ◆ Policy published
- ◆ Policy deleted
- ◆ Policy modified
- ◆ Policy moved
- ◆ Policy copied
- ◆ Policy renamed
- ◆ Policy shared or unshared
- ◆ Policy assignment modified
- ◆ Sandbox policy reverted to previous policy

Generated events provide information about the ZENworks administrator who performed the action, the affected policy, and the date the change occurred.

Enabling Change Events

You enable Endpoint Security change events at the Management Zone.

- 1 In ZENworks Control Center, click **Configuration** > **Management Zone Settings** > **Audit Management** > **Events Configuration** to display the Events Configuration page.
- 2 On the **Change Events** tab, click **Add** to display the Add Change Events dialog box.
- 3 In the **Change Events** tree, expand the **ZENworks Endpoint Security Management** section, then select the Endpoint Security policy change events you want to audit.
- 4 Configure the event settings, then click **OK** to add the events to the list of audited change events.

For more detailed information and instructions, see “[Enabling a Change Event](#)” in the [ZENworks 11 SP4 Audit Management Reference](#).

Viewing Generated Change Events

- 1 In ZENworks Control Center, click **Dashboard**.
- 2 In the Zone Audit panel, use the **Dashboard** and **Events** tabs to view the audited events:
 - ♦ **Dashboard:** Shows a summary of the audited events. You can see key indicators about top events and impacted objects, and can drill into the specific events. By default, the 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.
 - ♦ **Events:** Shows the change events being audited and the generated events. You can click a generated event to see its details. By default, the list shows the events generated in the last 4 hours. If you want to see more data, you can change the time period.

For more detailed information and instructions, see “[Viewing a Generated Change Event](#)” in the [ZENworks 11 SP4 Audit Management Reference](#).

2 Auditing Agent Events

You use agent events to capture Endpoint Security events that occur on managed devices. You can capture any of the following events:

- ♦ Number of files copied to removable storage devices
- ♦ Details of file activity for removable storage devices
- ♦ Changes to the effective security policies
- ♦ Changes to the assigned network environment and security location

Enabling Agent Events

You enable Endpoint Security agent events at the Management Zone.

- 1 In ZENworks Control Center, click **Configuration > Management Zone Settings > Audit Management > Events Configuration** to display the Events Configuration page.
- 2 Click the Agent Events tab, then click **Add** to display the Add Change Events dialog box.
- 3 In the **Agent Events** tree, expand the **ZENworks Endpoint Security Management** section, then select the agent events you want to audit.
- 4 Configure the event settings, then click **OK** to add the events to the list of audited agent events.

For more detailed information and instructions, see “[Enabling an Agent Event](#)” in the [ZENworks 11 SP4 Audit Management Reference](#).

Viewing Generated Agent Events

- 1 In ZENworks Control Center, click **Dashboard**.
- 2 In the Zone Audit panel, use the **Dashboard** and **Events** tabs to view the audited events:
 - ♦ **Dashboard:** Shows a summary of the audited events. You can see key indicators about top events and impacted objects, and can drill into the specific events. By default, the 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.
 - ♦ **Events:** Shows the agent events being audited and the generated events. You can click a generated event to see its details. By default, the list shows the events generated in the last 4 hours. If you want to see more data, you can change the time period.

For more detailed information and instructions, see “[Viewing a Generated Agent Event](#)” in the *ZENworks 11 SP4 Audit Management Reference*.

3 Legal Notices

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.novell.com/company/legal/>.

Copyright © 2016 Novell, Inc. All Rights Reserved.

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