

ZENworks 11 SP3

Test Scenarios for ZENworks Patch Management

This document contains test scenarios for ZENworks 11 SP3 Beta.

Purpose of these Test Scenarios

The purpose of this exercise is to help you become familiar with some of the new features included in the *Patch Management* component of ZENworks 11 SP3.

Assumptions

- You have followed the instructions for installing ZENworks 11 SP3 by using the *ZENworks 11 SP3 Installation Guide* (<http://www.novell.com/documentation/zenworks113/>).
- A ZENworks Server is installed and running, and at least one agent is connected to the ZCM Server.

Test Scenarios

1. [Defining a Patch Policy for a Windows System](#)
2. [Recalculating a Patch Policy](#)
3. [Editing Policy Requirements – by Architecture](#)
4. [Ensuring That a Name Can be Assigned to a Deployment](#)
5. [Pre-Enforcing an End Application Process Prior to Enforcing a Patch Policy](#)
6. [Ensuring That the Dashboard Can Be Configured](#)
7. [Deploying a Patch Using the Wake-on-LAN Function](#)
8. [Configuring a Download to Exclude Specific Vendors](#)
9. [Distributing a Patch to a Device by Selecting a Distribution Schedule](#)
10. [Deploying a Patch to Multiple Agents](#)
11. [Verifying Whether the User is Allowed to Snooze or Postpone an Installation](#)
12. [Setting the DAU at the Folder Level](#)

Test Scenario #1 Defining a Patch Policy for a Windows System

Objective

To enable you to define a Patch Policy for a Windows system.

Procedure

1. Log in to ZENworks Control Center.
2. Click *Patch Management* to open the *Patch Management* tab.
3. Open the *Patch Policy* tab.
4. Click *New > Patch Policy*. Select *Windows* as the platform, then click *Next*.
5. Specify the *Patch Policy Name* and *Administrator Notes*, then click *Next*.
6. Click *Add Filter*; select *Age* with options *<= 1 year*; then click *Apply*. A list of patches that are available for the Windows platform will appear for the last one year.
7. Proceed with the default options, then click *Next* and *Finish*.
8. Refresh the Client Agent, allowing time for patches to download.
9. Go to the Client Agent window and select *Bundles*. Verify that all patches from the Patch policy are deployed.

Note: A Patch policy is not the same as a policy.

Expected Results

- The available patches match the desired platform.
- The information in the Agent window is the same as the selections made.

Logs

If you are unable to successfully perform the scenario, send us the following log files:

- *zmd-messages.log*

On Windows:

c:\ProgramFiles\Novell\ZENworks\logs\LocalStore)

- *loader-messages.log*

On Windows:

c:\ProgramFiles\Novell\ZENworks\logs

Test Scenario #2: Recalculating a Patch Policy

Objective

To enable you to recalculate a Patch policy after a specific time.

Procedure

1. Log in to ZENworks Control Center.
2. Click *Patch Management* to open the *Patch Management* tab.
3. Open the *Patch Policy* tab.
4. Click *New > Patch Policy*. Select a *Platform*, then click *Next*.
5. Specify the *Patch Policy Name* and *Administrator Notes*, then click *Next*.
6. Click *Add Filter*, select the relevant filters, then click *Apply*.
7. Proceed with the default options, then click *Next*.
8. Specify the *Recalculate after* value as 0 to 90 days. Click *Finish*.
9. Change the server time to reflect the chosen parameter.
10. Verify that the patch list has been updated. For example, the oldest patch should have changed (Age).

Expected Results

The patch list is altered to reflect the recalculated filters.

Logs

If you are unable to successfully perform the scenario, send us the following file:

- *zmd-messages.log*
Windows: *c:\ProgramFiles\Novell\ZENworks\logs\LocalStore*;
Linux: */var/opt/novell/zenworks/logs/LocalStore*
- *loader-messages.log*
Windows: *c:\ProgramFiles\Novell\ZENworks\logs*;
Linux: */var/opt/novell/log/zenworks)*

Test Scenario #3: Editing Policy Requirements – by Architecture

Objective

To ensure that the patches released in the last 30 days are displayed in bold font.

Procedure

1. Log in to ZENworks Control Center. Click *Patch Management* to open the *Patch Management* tab.
2. Open the *Patch Policy* tab. Click the policy name to open the *Patch Policy* tab.
3. Open the *Requirements* tab, then click *Add Filter*. Select the *Architecture*, 32 or 64 from the drop-down, click *Apply*.
4. Open the *Summary* tab, then click *Rebuild* to update the patch list with the new policy setting.
5. Open the *Patch Policy* tab, then select the edited policy. From the *Action* menu, select *Assign to Device*. Provide the required information, then click *OK*. Click *Finish*.
6. Go to the Agent device and refresh.

Expected Results

The policy is enforced on the device. There are no error messages.

Logs

If you are unable to successfully perform the scenario, send us the following files:

- *zmd-messages.log*

Windows: *c:\ProgramFiles\Novell\ZENworks\logs\LocalStore*

Linux: */var/opt/novell/zenworks/logs/LocalStore*

- *loader-messages.log*

Windows: *c:\ProgramFiles\Novell\ZENworks\logs*.

Linux: */var/opt/novell/log/zenworks*

Test Scenario #4: Ensuring That a Name Can be Assigned to a Deployment

Objective

To ensure that a name can be assigned to a deployment.

Procedure

1. Install ZENworks Configuration Management on a Windows 2003 SP2 or a SLES 11 device.
2. Install the ZENworks Adaptive Agent on a Windows or Linux agent.
3. After the agents are installed, update the patch subscription services.
4. Log in to ZENworks Control Center.
5. To update the patch subscription services, click *Configuration > Patch Management > Subscription Service Information*, then select *Update Now*.
This process might take a few hours.
6. Run the DAU in Servers as well as in the Agents.
7. On the device, open a terminal window, type `zac ref`, then type `zac bl` a couple of times to verify that the device has finished running the DAU.
8. On the *Patch Management* page, you can view the patches that are populated.
9. Select a patch, then click *Update Cache* from the *Action* menu.
10. After the patch is cached, deploy the patch to the device by using the *Deployment Remediation* wizard.
11. Select any *Remediation Schedule Type*.
12. On the *Choose deployment name* page, specify the name of the assignment and finish the deployment.
13. On the device, type `zac ref` in the terminal window.
You can monitor the deployment progress by typing `zac bl`. Wait for about 10 minutes after the deployment finishes.
14. Check the name of the assignment.

Expected Results

The assignment is triggered with the assigned name in 10 minutes.

Logs

If you are unable to successfully perform the scenario, send us the following files:

- `zmd-messages.log`

Windows: `c:\ProgramFiles\Novell\ZENworks\logs\LocalStore`

Linux: `/var/opt/novell/zenworks/logs/LocalStore`

- *loader-messages.log*

Windows: *c:\ProgramFiles\Novell\ZENworks\logs.*

Linux: */var/opt/novell/log/zenworks*

Test Scenario #5: Pre-Enforcing an End Application Process Prior to Enforcing a Patch Policy

Objective

To enable you to terminate an application prior to a Patch Policy being enforced.

Procedure

1. Log in to ZENworks Control Center.
2. Click *Patch Management* to open the *Patch Management* tab.
3. Open the *Patch Policy* tab.
4. Click *New>Patch Policy*. Select the *Platform*, then click *Next*.
5. Specify the *Patch Policy Name* and the *Administrator Notes*, then click *Next*.
6. Click *Add Filter*; select the relevant filters, then click *Apply*.
7. Click *Add Filter*; select the *Age* with options *<= 1 year*, then click *Apply*.
A list of patches for the selected platform will appear for the last 1 year.
8. Proceed with the default options, then click *Next* and *Finish*.
9. After you have created or selected a policy, open the selection in the *Patch Policy* tab.
10. Open the *Actions* tab. On the *Pre-Enforcement* tab, select *End Process* from the *Add* menu.
11. Specify an application or process to end. For example, Notepad.
12. Open the specified application or process on the target device. Then click *Apply*.
13. Go to the Summary page, then click *Rebuild*.

Expected Results

The Notepad application is closed prior to the Patch Policy being enforced.

Logs

If you are unable to successfully perform the scenario, send us the following files:

- *zmd-messages.log*

Windows: *c:\ProgramFiles\Novell\ZENworks\logs\LocalStore*

Linux: */var/opt/novell/zenworks/logs/LocalStore*

- *loader-messages.log*

Windows: *c:\ProgramFiles\Novell\ZENworks\logs*.

Linux: */var/opt/novell/log/zenworks*

Test Scenario #6: Ensuring That the Dashboard Can Be Configured

Objective

To enable you to configure the Dashboard.

Procedure

1. In ZENworks Control Center, click *Configuration > Patch Management > Dashboard and Trending*.
2. In the *Dashboard and Trending* panel, select the *Dashboard Update Interval (Every Day at)* time and the *Days to store data in database* from the drop-down list.
3. In the *Criticalities to include* panel, select the criticality.
4. Click *Apply*, then click *OK*.
5. On the *Patch Management* page, click the *Dashboard* tab.
6. In the bottom right corner of the page, click *Update Dashboard Report*.
7. Verify that an updated dashboard report is generated.

Expected Results

- The Dashboard should update daily at the selected time and the dashboard data should be stored only for the number of the selected days.
- The Dashboard should display reports only for the selected criticalities.

Logs

If you are unable to successfully perform the scenario, send us the following files:

- *zmd-messages.log*

Windows: *c:\ProgramFiles\Novell\ZENworks\logs\LocalStore*

Linux: */var/opt/novell/zenworks/logs/LocalStore*

- *loader-messages.log*

Windows: *c:\ProgramFiles\Novell\ZENworks\logs.*

Linux: */var/opt/novell/log/zenworks*

Test Scenario #7: Deploying a Patch Using the Wake-on-LAN Feature

Objective

To deploy a Patch using the Wake-on LAN feature.

Procedure

1. Deploy a patch to a managed device that is shut down.
2. In the *Remediation Schedule* page, select the proper schedule settings, then verify the *Wake-on-LAN* option.
3. Complete the deployment wizard with the *Now* setting.
4. Go to the target device (that is shut down currently), verify whether the device has woken up.
5. After the device has restarted, verify whether the remediation is installed.

Expected Results

The device wakes up and the patch is installed.

Logs

If you are unable to successfully perform the scenario, send us the following files:

- *zmd-messages.log*

Windows: *c:\ProgramFiles\Novell\ZENworks\logs\LocalStore*

Linux: */var/opt/novell/zenworks/logs/LocalStore*

- *loader-messages.log*

Windows: *c:\ProgramFiles\Novell\ZENworks\logs.*

Linux: */var/opt/novell/log/zenworks*

Test Scenario #8: Configuring a Download to Exclude Specific Vendors

Objective

To ensure that patches from specific vendors can be disabled.

Procedure

1. Install the latest version of ZENworks Configuration Management. Patches marked *Critical* are automatically cached (This is known).
2. Go to the *Configuration>Subscription Download* page.
3. Under the *Select vendors to use in the system* section, disable the unwanted vendors, then click *Save*. For example, the user decides not to run Apple Safari in their environment, then hard drive space is not required to store the automatically cached package.

Expected Results

ZENworks only downloads patch releases by the vendors that you have selected, and omits the ones that are disabled.

Logs

If you are unable to successfully perform the scenario, send us the following files:

- *zmd-messages.log*

Windows: *c:\ProgramFiles\Novell\ZENworks\logs\LocalStore*

Linux: */var/opt/novell/zenworks/logs/LocalStore*

- *loader-messages.log*

Windows: *c:\ProgramFiles\Novell\ZENworks\logs.*

Linux: */var/opt/novell/log/zenworks*

Test Scenario #9: Distributing a Patch to a Device by Selecting a Distribution Schedule

Objective

To ensure that patches can be distributed to an agent by selecting a distribute schedule.

Procedure

1. Log in to ZENworks Control Center. Go to the *Patch Management* tab, select a patch, then click *Update Cache* from the *Action* menu.
2. After the patch is cached, deploy the cached patch to the device by using the *Deployment Remediation Wizard*.
3. Select any remediation schedule type.
4. In the *Remediation Options* page, select *Advanced* (individually set all possible deployment options), then proceed with default options.
5. In the *Distribution Schedule* page, select any distribution schedule.
6. Finish the deployment and trigger the assignment in the agent device.
7. To trigger the assignment on the device, type `zac ref` in the terminal window. You can monitor deployment progress by typing, `zac bl`. Wait for about 10 minutes after the deployment finishes.
8. Verify that the patch is distributed according to the selected distribution schedule.

Expected Results

The patch is distributed according to the distribution schedule that was selected in Step 8 of the Deployment wizard.

Logs

If you are unable to successfully perform the scenario, send us the following files:

- *zmd-messages.log*

Windows: `c:\ProgramFiles\Novell\ZENworks\logs\LocalStore`

Linux: `/var/opt/novell/zenworks/logs/LocalStore`

- *loader-messages.log*

Windows: `c:\ProgramFiles\Novell\ZENworks\logs.`

Linux: `/var/opt/novell/log/zenworks`

Test Scenario #10: Deploying a Patch to Multiple Agents

Objective

To deploy a patch on multiple agents and to check the results on the *Device Patches* page.

Procedure

1. Log in to ZENworks Control Center.
2. Create a deployment from the *Patches* screen by completing the Deployment wizard.
3. When prompted, send the patch to multiple agents. This is easily achieved when using MS security patches.
4. Select a universal patch and ensure that there are multiple devices with running agents.
5. Click the main *Patches* tab and search for the patch.
6. Open the *Device Patches* tab for the device to which the patch deployment is applicable, then verify the *Patched* status.
7. Open the device *Patches* tab for the device to which the patch deployment is not applicable, then verify the *Patched* status.

Expected Results

- In the *Patches* tab, the *Patched* count of the device increases by 1. The *Not Patched* count of device decreases by 1.
- In the *Device Patches* tab, after the successful deployment of the patch, the *Patched* column reads *Yes*.
- In the *Device Patches* tab, after the successful deployment of the patch, the *Patched* column reads *No*.

Logs

If you are unable to successfully perform the scenario, send us the following files:

- *zmd-messages.log*

Windows: *c:\ProgramFiles\Novell\ZENworks\logs\LocalStore*

Linux: */var/opt/novell/zenworks/logs/LocalStore*

- *loader-messages.log*

Windows: *c:\ProgramFiles\Novell\ZENworks\logs.*

Linux: */var/opt/novell/log/zenworks*

Test Scenario #11: Verifying Whether the User is Allowed to Snooze or Postpone an Installation

Objective

To confirm that the end user can choose to delay the installation of the patch remediation.

Procedure

1. Click the *Patches* tab for a device group.
2. Select a cached patch with reboot behavior, then click *Assign to Baseline*.
3. Click the *Configuration* tab.
4. Open the *Patch Management* tab.
5. Click the *Mandatory Baseline Settings* link.
6. Click the *Enable auto reboot of mandatory baseline* check box.
7. Select *No* for the *Suppress Reboot* option.
8. Select *Yes* for the *Allow User to Cancel* option.
9. Indicate the required number of seconds for the *Time to show dialog before reboot* option.
10. Indicate the required time to snooze.
11. Click *Apply*, then click *OK*.

Expected Results

Users should be allowed to postpone or snooze the installation for the number of days, hours or minutes indicated in the *Allow User to Snooze* field.

Logs

If you are unable to successfully perform the scenario, send us the following files:

- *zmd-messages.log*

Windows: *c:\ProgramFiles\Novell\ZENworks\logs\LocalStore*

Linux: */var/opt/novell/zenworks/logs/LocalStore*

- *loader-messages.log*

Windows: *c:\ProgramFiles\Novell\ZENworks\logs*.

Linux: */var/opt/novell/log/zenworks*

Test Scenario #12: Setting the DAU at the Folder Level

Objective

To ensure that the DAU can be set at the Folder level, rather than the Device level.

Precondition

Ensure that system setting for *Schedule Discover Applicable Update Bundles Distribution* under the *Configuration* tab is not set to the default value, *Distribute DAU on Launch*.

Procedure

1. Log in to ZENworks Control Center. Open the *Devices* page.
2. Click the *Details* link for the Servers folder.
3. Click *Patch Management* under the *Settings* tab
4. Set the *Schedule Discover Applicable Update Bundles Install* option to default.
5. Click *Schedule Discover Applicable Update Bundles Distribution*.
6. Click the *Override* settings.
7. Click *Distribute DAU on Launch*.
8. Click *Apply*.
9. Click *OK*.
10. Update the subscription and complete it. Verify the result.

Expected Results

In the Agent *ZENworks Property* window the *Device Assigned* bundles status is set as *Downloaded*, and once the DAU is distributed the status is changed to *Available*.

Logs

If you are unable to successfully perform the scenario, send us the following files:

- *zmd-messages.log*

Windows: *c:\ProgramFiles\Novell\ZENworks\logs\LocalStore*

Linux: */var/opt/novell/zenworks/logs/LocalStore*

- *loader-messages.log*

Windows: *c:\ProgramFiles\Novell\ZENworks\logs*.

Linux: */var/opt/novell/log/zenworks*