ZENworks 2017 Update 3 Readme

October 2018

MICRO FOCUS®

The information in this Readme pertains to the ZENworks 2017 Update 3 release.

1 Readme Updates

The following table contains information on the documentation content changes that were made in this Readme after the initial release of ZENworks 2017 Update 1:

Table 1   Readme Updates

Date	Readme Item Added or Updated
June, 2019	A new item has been included in the following section: Section 2, "Important," on page 1
	The following known issue has been added: Section 8.7, "Upgrade of a ZENworks 17.x appliance to a later version fails if the April 2019 Appliance Security Patches have been applied," on page 6

2 Important

Prior to installing the update, please read the following information:

- If you have downloaded ZENworks 2017 Update 3 but not deployed it in your zone as yet, ensure that you DO NOT deploy it. Please DELETE ZENworks 2017 Update 3 and only deploy ZENworks 2017 Update 3a to avoid the issue documented in TID 7023380.

- If you have already deployed or are in the process of deploying ZENworks 2017 Update 3, you need to contact customer support or refer to TID 7023380. After taking the required action, you can continue with the deployment of ZENworks 2017 Update 3 and ignore ZENworks 2017 Update 3a.

- If you have applied the April 2019 Appliance Security Patches, before upgrading to ZENworks 2017 Update 3a, you need to first apply the FTF that is available in bug 1134324.

3 What's New in ZENworks 2017 Update 3

For information on the new features included in this release, see the ZENworks What's New Reference.

4 Planning to Deploy ZENworks 2017 Update 3

Use the following guidelines to plan for the deployment of ZENworks 2017 Update 3 in your Management Zone:

- If you are using Disk Encryption and you want to update the Full Disk Encryption Agent from a version earlier than ZENworks 2017 Update 1, you MUST remove the Disk Encryption policy from those managed devices before you update them to ZENworks 2017 Update 3.

  If you are updating the Full Disk Encryption Agent from ZENworks 2017 Update 1 or 2017 Update 2 to ZENworks 2017 Update 3, leave the Disk Encryption policy in place, no change is required prior to the system update.

  For more information about updating Full Disk Encryption in ZENworks 2017 Update 3 from a version earlier than ZENworks 2017 Update 1, see the ZENworks 2017 Update 3 - Full Disk Encryption Update Reference.

- You must first upgrade the Primary Servers, then update the Satellite Servers, and finally the managed devices to ZENworks 2017 Update 3. Do not upgrade the managed devices and Satellite Servers (or add new 2017 Update 3 Agents in the zone) until all Primary Servers in the zone have been upgraded to ZENworks 2017 Update 3.

  NOTE: Agents might receive inconsistent data from the zone until all Primary Servers are upgraded. Therefore, this part of the process should take place in as short a time as possible - ideally, immediately after the first Primary Server is upgraded.

- You can directly deploy version 2017 Update 3 to the following devices:

Device Type	Operating System	Minimum ZENworks Version
Primary Servers	Windows and Linux	ZENworks 2017 and subsequent versions
Satellite Servers	Windows, Linux and Mac	ZENworks 11.x and subsequent versions
Managed Devices	Windows	ZENworks 11.x and subsequent versions
	Linux	ZENworks 11.x and subsequent versions
	Mac	ZENworks 11.2 and subsequent versions

- The system reboots once after you upgrade to ZENworks 2017 Update 3. However, a double reboot will be required in the following scenarios:
  - If you update from 11.x to ZENworks 2017 or a subsequent version (2017 Update1, Update 2 or Update 3) with Endpoint Security enabled, you will need a second reboot to load the ZESNETAccess driver.
  - If a managed device uses Windows 10 with Client Self Defense enabled and you are upgrading from 11.4.x to ZENworks 2017 or a subsequent version (2017 Update1, Update 2 or Update 3), you need to disable Client Self Defense in ZENworks Control Center, reboot the managed device, and then run the update, requiring a second reboot on the device.
  - If you have a Disk Encryption policy enforced on a managed device, and you want to update the Full Disk Encryption Agent from a version earlier than ZENworks 2017 Update 1 to ZENworks 2017 Update 3, you must first remove the policy and decrypt the device, which requires a device reboot. You then update the device to 2017 Update 3, requiring a second reboot.

IMPORTANT: Managed Devices running versions prior to 11.x must first be upgraded to 11.x. The system reboots after the upgrade to 11.x and then reboots again when the ZENworks 2017 Update 3 system update is deployed.

- Prior to installing the System Update, ensure that you have adequate free disk space in the following locations:

Location	Description	Disk Space
Windows: `%zenworks_home%\install\downloads` **Linux:** `opt/novell/zenworks/install/downloads`	To maintain agent packages.	5.7 GB
Windows: `%zenworks_home%\work\content-repo` **Linux:** `/var/opt/novell/zenworks/content-repo`	To import the zip file to the content system.	5.7 GB
Agent Cache	To download the applicable System Update contents that are required to update the ZENworks server.	1.5 GB
Location where the System Update file is copied. This is only applicable for the ZENworks Server that is used to import the System Update zip file	To store the downloaded System Update zip file.	5.7 GB

5 Downloading and Deploying ZENworks 2017 Update 3

For instructions on downloading and deploying ZENworks 2017 Update 3, see the *ZENworks System Updates Reference*.

If your Management Zone consists of Primary Servers with a version prior to ZENworks 2017, you can deploy ZENworks 2017 Update 3 to these Primary Servers only after all of them have been upgraded to ZENworks 2017. For instructions, see the *ZENworks Upgrade Guide*.

For administrative tasks, see the ZENworks 2017 Update 3 documentation site.

IMPORTANT: Do not update the Remote Management (RM) viewer until all the Join Proxy Satellite Servers are updated in the zone. To perform Remote Management through Join Proxy, you need to ensure that the RM viewer version and the Join Proxy version are the same.

Ensure that you read Section 4, "Planning to Deploy ZENworks 2017 Update 3," on page 2 before you download and deploy the ZENworks 2017 Update 3 update.

Do not deploy ZENworks 2017 Update 3 until all Primary Servers in the zone have been upgraded to ZENworks 2017

This update requires schema changes to be made to the database. During the initial patch installation, the services will run only on the Master or dedicated Primary Server. This is to ensure that other Primary Servers do not try to access the tables being changed in the database.

After the Master or dedicated Primary Server has been updated, the services will resume on the remaining servers and the update will be applied simultaneously.

NOTE: You do not need to manually stop or start the services on the servers during the update. The services will be stopped and started automatically.

When you postpone a system update and log out of the managed device, the system update is applied on the device.

For the list of supported Managed Device and Satellite Server versions in a Management Zone with ZENworks 2017 Update 3, see Supported Managed Devices and Satellite Server Versions.

6 Issues Resolved in ZENworks 2017 Update 3

Some of the issues identified in previous releases have been addressed in this release. For a list of the resolved issues, see TID 7023221 in the Support Knowledgebase.

7 Continuing Issues in ZENworks 2017 Update 3

Some of the issues that were discovered in versions prior to ZENworks 2017 Update 3 and have not yet been resolved. Review the following Readme documents for more information:

- ZENworks 2017 Readme
- ZENworks 2017 Update 1 Readme
- ZENworks 2017 Update 2 Readme

8 Known Issues

This section contains information about issues that might occur while you work with ZENworks 2017 Update 3:

8.1 Apply button is not re-enabled when you select or clear the Continue on Failure option

When you apply changes made to the actions of a bundle, and then select or clear the **Continue on Failure** option, the Apply button is not re-enabled.

Workaround: To re-enable the Apply button, based on the requirement, select or clear the **Continue on Failure** option, click the bundle action link and in the bundle action dialog, make any additional changes, if required and click OK.

8.2 Unable to drag objects and measures while creating a report

While using ZENworks Reporting Appliance 6.2.3 with Oracle 12c R1 or R2 database, when you drag any measure or dimension to create an Ad hoc view or report, the **An error occurred while creating connection. Try again.** error message is displayed.

Workaround: Navigate to `/opt/Novell/zenworks-reporting/js/apache-tomcat/lib`, delete the **ojdbc5.jar** file and then restart the reporting services.

8.3 The system update process does not stop the Novell Proxy DHCP Service

While deploying the system update, the Novell Proxy DHCP service might not stop automatically.

Workaround: Stop the Novell Proxy DHCP service manually:

1. Click **Start**, search for **Services**.
2. In the **Services** dialog box, right click **Novell Proxy DHCP Service**, and then click **Stop**.

8.4 Making a copy of a patch policy copies the Published version and not the Sandbox version

If you make a copy of a published patch policy that has a sandbox version, ZENworks copies the published version and not the sandbox version of the policy. In ZENworks 2017 Update 2 and earlier versions the sandbox version is copied. Enhancements made in ZENworks 2017 Update 3 reversed the behavior for the copy action.

Workaround: None

8.5 Agent fails to register to the Primary Server when installed as an add-on product

When an openSUSE Leap 15 or openSUSE Leap 42.3 agent is installed as an add-on product, using the YaST repositories, the agent fails to register to the Primary Server.

Workaround: None

8.6 A Windows device with Windows 10 updates might not boot

When you restore the image of a Windows device with Windows 10 updates, using the Legacy NTFS driver, the restored device might not boot the operating system.

Workaround: Perform any one of the following:

- Take and restore an image of the device using the Tuxera driver.
- Take and restore an image of the device in the .zmg format using WinPE.

8.7 Upgrade of a ZENworks 17.x appliance to a later version fails if the April 2019 Appliance Security Patches have been applied

If you have applied the April 2019 Appliance Security Patches and then you try to upgrade a ZENworks 17.x appliance to a later version, some of the symbolic links (symlinks) such as `/opt/novell/zenworks/lib32` and `/opt/novell/zenworks/lib64` are replaced by new folders and hence the update fails.

Workaround: Apply the FTF that is available in bug 1134324 and then run the update again.

9 Additional Documentation

This document includes information specific to the ZENworks 2017 Update 3 release. For all other ZENworks 2017 documentation, see the *ZENworks 2017 documentation website*.

10 Legal Notice

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/.