ZENworks 2017 Update 1 Readme

July 2017

The information in this Readme pertains to the ZENworks 2017 Update 1 release.

1 What’s New in ZENworks 2017 Update 1

For information on the new features included in this release, see What’s New in ZENworks 2017 Update 1.

2 Planning to Deploy ZENworks 2017 Update 1

Use the following guidelines to plan for the deployment of ZENworks 2017 Update 1 in your Management Zone:

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

  For more information about updating Full Disk Encryption in ZENworks 2017 Update 1, see the ZENworks 2017 Update 1 - 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 1. Do not upgrade the managed devices and Satellite Servers (or add new 2017 Update 1 Agents in the zone) until all Primary Servers in the zone have been upgraded to ZENworks 2017 Update 1.

  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.

- If the managed devices have been updated to ZENworks 11.x or later, you can directly update the managed devices in the zone to ZENworks 2017 Update 1.
- The system reboots once after you upgrade to ZENworks 2017 Update 1. However, a double reboot will be required in the following scenarios:
  - If you update from 11.x to ZENworks 2017 or 2017 Update 1 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 2017 Update 1, 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 to ZENworks 2017 Update 1, you must first remove the policy and decrypt the device, which requires a device reboot. You then update the device to 2017 Update 1, 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 1 system update is deployed.

Table 1 *ZENworks Cumulative Agent Update to ZENworks 2017 Update 1: Supported Paths*

Managed Device Type	Operating System	Supported Versions	Unsupported Versions
Primary Server	Windows/Linux	v2017 Update	Any version prior to v2017
Satellite Server	Windows/Linux/Mac	v11.0 and subsequent versions	Any version prior to v11.x
Managed Device	Windows	v11.0 and subsequent versions	Any version prior to v11.0
	Linux	v11.0 and subsequent versions	NA
	Mac	v11.2 and subsequent versions	NA

- 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 GB
Windows: `%zenworks_home%\work\content-repo` **Linux:** `/var/opt/novell/zenworks/content-repo`	To import the zip file to the content system.	5 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 GB

3 Downloading and Deploying ZENworks 2017 Update 1

For instructions on downloading and deploying ZENworks 2017 Update 1, see the *ZENworks 2017 Update 1 System Updates Reference*.

If your Management Zone consists of Primary Servers with a version prior to ZENworks 2017, you can deploy ZENworks 2017 Update 1 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 1 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 2, “Planning to Deploy ZENworks 2017 Update 1,” on page 1 before you download and deploy the ZENworks 2017 Update 1 update.

Do not deploy ZENworks 2017 Update 1 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 1, see Supported Managed Devices and Satellite Server Versions.

4 Issues Resolved in ZENworks 2017 Update 1

Some of the issues identified in previous releases have been addressed in this release. For a list of the resolved issues, see TID 7020155 in the Support Knowledgebase.

5 Continuing Issues in ZENworks 2017 Update 1

Some of the issues that were discovered in previous versions of ZENworks 2017 Update 1 have not yet been resolved. Review the following Readme documents for more information:

- ZENworks 2017 Readme

6 Known Issues

This section contains information about issues that might occur while you work with ZENworks 2017 Update 1:

6.1 ZENworks Configuration

6.1.1 On Windows 2012 R2 devices, the network adapter is not visible when the IPv4 and IPv6 values are changed using the zisedit command

After installing the agent on a Windows 2012 R2 device, when you boot the device using PXE or Boot CD, and run the zisedit command with the following settings, the network adapter is not visible in the network connections when you log into the device:

1. Set the DHCP and DHCP6 values to off.
2. Change the IPv4 and IPv6 values.

Workaround: Configure the IPv4 and IPv6 values separately.

6.1.2 On a SLES 11 device, Location and Network Environment detection might fail with the DHCP address

On a SLES 11 device, if a network is configured using NetworkManager, the Client IP address Network service might not match with the IPv6 DHCP address. Hence, location and network environment detection fails.

Workaround: Configure the network using the `ifup` method.

6.1.3 ZENworks Java applications might not work on Windows devices on which the IPv4 interface is not installed

Java 8 Applications require the IPv4 stack to be configured on a Windows device. Hence, ZENworks Java applications such as ZCC Helper might not work unless IPv4 is installed.

Workaround: Configure the IPv4 stack in addition to the IPv6 stack.

For more information, refer to the following links:

- http://www.oracle.com/technetwork/java/javase/8-known-issues-2157115.html
- http://bugs.java.com/bugdatabase/view_bug.do?bug_id=8040229

6.1.4 While performing a Change CA, validation of a chained certificate fails if the certificate chain is in the wrong order

While changing the external Certificate Authority, if the new certificate file includes the certificate chain in a wrong order, then certificate validation fails. For example, instead of Server > SubCA > RootCA, if the chain is in the following order: SubCA > Server > RootCA., the certificate will be considered as invalid.

Workaround: Re-create the server certificate chain (with certificates in the specified order) using your preferred method. One of the simplest ways of doing it as follows:

1. Save each certificate as a separate file in the base64 format.
2. Open each certificate in a text editor. The content will be similar to the content below:

   ```
   -----BEGIN CERTIFICATE-----
   <cert data>
   -----END CERTIFICATE-----
   ```

3. Create a new file and name it as `server.cer`.
4. Copy the text from each certificate file into the server.cer file so that the certificates are all in one file, in the following order:

   ```
   -----BEGIN CERTIFICATE-----
   <Server cert data>
   -----END CERTIFICATE-----
   -----BEGIN CERTIFICATE-----
   <SubCA cert data>
   -----END CERTIFICATE-----
   -----BEGIN CERTIFICATE-----
   <RootCA cert data>
   -----END CERTIFICATE-----
   ```

5. Save the `server.cer` file.
6. Use the `server.cer` file as the new certificate and complete the steps to change the external Certificate Authority (CA).

6.1.5 pgadmin3 does not start on a SLES device

When you open pgadmin3 on a SLES device, one of the following errors might be displayed:

- *pgadmin3: error while loading shared libraries: libiconv.so.2: cannot open shared object file: No such file or directory*
- *./pgadmin3: symbol lookup error: /usr/lib64/libgdk-x11-2.0.so.0: undefined symbol: pango_font_map_create_context*

Workaround: Execute the following command in the terminal before opening pgadmin3:

```
export LD_LIBRARY_PATH="/usr/local/lib64:/usr/local/lib:/lib64:/lib:/usr/lib64:/
usr/lib:/opt/novell/zenworks/share/pgsql/lib:/opt/novell/zenworks/share/pgsql/
pgAdmin3/lib:$LD_LIBRARY_PATH"
```

6.1.6 Install Network MSI and Create Directory bundle actions fail with the WNetAddConnection error when configured with DFS share

Bundles configured with the Install Network MSI or Create Directory action from DFS share, fail with the WNetAddConnection error.

Workaround: None.

While configuring the Install Network MSI action, use the UNC path instead of DFS share.

6.1.7 On iOS devices the prompt to enter the email account password might not be displayed

When an email account is remotely configured on an iOS device using a Mobile Email Policy, then the prompt to enter the email account password might not be displayed.

Workaround: Manually specify the password by navigating to the Settings menu on the device.

6.2 ZENworks Agent

6.2.1 When you restart the agent on an older managed device and the Primary Server host name resolves to an IPv6 address, then the managed device might not register to the zone

On a managed device, when cache is cleared and the device is restarted, the agent reads server URLs from the `initial-web-service` file. If the server URL contains a host name which resolves to an IPv6 address, then the SSL host name verification fails. Hence, the older agents might not be registered.

Workaround: Manually add the IPv4-based URL to the initial-web-service file and then refresh the older agent.

6.2.2 Agents on ZENworks 2017 or earlier versions are able to register to a ZENworks 2017 Update 1 server with an IPv6 address

Registering an older agent using an IPv6 address of ZENworks server may succeed, however, some agent features might not work as expected.

Workaround: Unregister the agent, and then register it using an IPv4 address of the ZENworks server. Avoid registering older agents using an IPv6 address.

6.3 ZENworks Application

6.3.1 ZAPP launches automatically after a reboot

If you create a ZECP policy to hide the ZENworks tray icon and then you assign the policy to a device, when you reboot the device, ZAPP is launched automatically.

Workaround: Delete the `ZAPP` registry key:

1. Open the Registry Editor.
2. Go to
   - For 32-bit: `HKLM\Software\Microsoft\Windows\CurrentVersion\Run`
   - For 64-bit: `HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run`
3. Delete the `ZAPP` registry key.

6.4 Remote Management

6.4.1 Open source VNC viewers are not supported when you remote control a Windows managed device using an IPV6 address

On a Windows device, the ZENworks Agent cannot connect with open source viewers such as RealVNC, TightVNC and UltraVNC using an IPv6 address.

Workaround: To manage Windows devices using IPv6 addresses, use IPv6 compatible open source VNC viewers. Open source VNC viewers can be used to communicate with managed devices using IPv4 addresses.

6.5 ZENworks Imaging

6.5.1 RHEL 7 device boots in the maintenance mode after restoring the image

When you take an image of an RHEL 7 device with SELinux enabled, the device boots in the maintenance mode after restoring the image.

Workaround: Before taking the image, disable SELINUX:

1. Go to the `/etc/selinux` folder.
2. In the `config` file, set the SELINUX value as `disabled`.
3. Restart the device.

6.5.2 Assigning the MDT Deployment bundle to re-install the operating system on a device that already has an operating system results in an infinite loop

When you assign the MDT Deployment bundle to re-install the operating system on a device that already has an operating system, it results in an infinite loop. On PXE boot, the device picks up the same MDT bundle every time. This issue occurs because the Microsoft Deployment Toolkit (MDT) wipes out the ZENworks Image Safe Data (ZISD) when preparing the disk to re-install the operating system on the device. Hence, the Imaging Server does not know the status of the imaging work assigned to the device and it is never cleared.

Workaround: Perform either of the following methods:

Method 1

1 Customize the corresponding MDT Deployment Share which the MDT WIM uploaded in the bundle contacts on booting. Use the `ISDTool.exe` to clear the MBR:

   1a Download the `32-bit ISDTool.exe` from the ZENworks Download page (`https://zenworks_server_IP_address:port/zenworks-setup`) under Imaging Tools. Place it in the MDT Deployment Share under the `/Tools/x86` folder.

   1b Download the 64-bit `ISDTool.exe` from the ZENworks Download page (`https://zenworks_server_IP_address:port/zenworks-setup`) under Imaging Tools. Place it in the MDT Deployment Share under the `/Tools/x64` folder.

   1c Open the `ZTIDiskpart.wsf` script file present in the MDT Deployment Share under the `Scripts` folder and insert the following lines just above the `Open an instance for diskpart.exe, and dynamically pipe the commands to the program` line:

```
Dim sampCmd
Dim aScriptDir
Dim aArchitecture
aScriptDir = oFSO.GetParentFolderName(WScript.ScriptFullName)
aArchitecture = oEnvironment.Item("Architecture")
sampCmd = aScriptDir & "\..\tools\" & aArchitecture & "\ISDTool.exe mdt
cleandisk " & iDiskIndex
oShell.Exec(sampCmd)
```

When the device boots the MDT WIM and contacts the above customized MDT Deployment Share, the script prevents MDT from wiping out the ZISD data,

Method 2

1 Clear the MBR using an Imaging Script Preboot bundle before applying the MDT Deployment bundle on the device:

   1a Create an Imaging Script Preboot bundle in ZENworks. Add the following command as the **Script Text**:

```
dd if=/dev/zero of=/dev/sdX count=1 bs=512
```

   Where `/dev/sdX` is the disk; X can be a value such as a, b or c.

   1b Apply the Imaging Script Preboot bundle on the device.

   1c Apply the required MDT Deployment bundle on the device.

IMPORTANT: Exercise extreme caution when using this option. The above `dd` command clears the MBR. After running this command, the operating system will not boot. Hence, the command should be run only before re-installing the operating system on the device.

6.6 A Windows device with Windows 10 updates might not boot

When you restore an image of a Windows device with Windows 10 Creator update 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 a device using Tuxera driver.
- Take and restore an image of a device in .zmg format using WinPE

6.7 ZENworks Appliance

- Section 6.7.1, “A blank page is displayed in the Internet Explorer 11 browser when you open the Terminal and File Explorer tile using an IPv6 address,” on page 9

6.7.1 A blank page is displayed in the Internet Explorer 11 browser when you open the Terminal and File Explorer tile using an IPv6 address

When you open the Terminal and File Explorer tile in ZENworks Appliance using an IPv6 address, a blank page is displayed in the Internet Explorer 11 browser.

Workaround: Open the ZENworks Appliance using literal IPv6 addresses in UNC path names.

For example, *2001:db8::ff00:42:8329* can be written as *2001:db8::ff00:42:8329.ipv6-literal.net*

7 Additional Documentation

This Readme lists the issues specific to ZENworks 2017 Update 1 release. For all other ZENworks 2017 documentation, see the *ZENworks 2017 documentation website*.

8 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/.