2019 - 02

Dell EMC OpenManage Release Notes Version 9.2.1

This document describes the new features, enhancements, and fixed issues in Server Administrator 9.2.1.

Topics:

Release Type and Definition

Server Administrator

This document contains updated information for the *Dell EMC OpenManage Server Administrator User's Guide* and any other technical documentation included with Server Administrator.

NOTE: System Management software, including the Server Administrator(Server Administrator), is available only on the *Dell EMC Systems Management Tools and Documentation* software.

The OpenManage Server Administrator documentation includes the User's Guide, Messages Reference Guide, CIM Reference Guide, Command Line Interface (CLI) Guide, SNMP Reference Guide, and Compatibility Guide.

You can access the documentation from **dell.com/openmanagemanuals**.

Version

9.2.1

Release Date

February 2018

Previous Version

9.2.0

Importance

RECOMMENDED: Dell recommends applying this update during your next scheduled update cycle. The update contains feature enhancements or changes that will help keep your system software current and compatible with other system modules (firmware, BIOS, drivers and software).

Platforms Affected

For a complete list of supported Dell PowerEdge systems and supported Operating systems, see the Dell EMC OpenManage Systems Software Support Matrix available in the required version of **OpenManage Software** at **dell.com/openmanagemanuals**.

What is Supported

Hardware Requirements

- Minimum of 2 GB RAM
- Minimum of 512 MB free hard drive space
- Administrator rights
- Monitor with a minimum screen resolution of 800 x 600. The recommended screen resolution is at least 1024 x 768

Software Requirements

- Supported operating system and web browser.
- TCP/IP connection on the managed system and the remote system to facilitate remote system management.
- Supported systems management protocol standard. For more information, see *Dell EMC Supported Systems Management Protocol Standards*.
- The Server Administrator Remote Access Controller service requires remote access controller (RAC) to be installed on the managed system. For more information on the software and hardware requirements, see the relevant *Integrated Dell Remote Access Controller User's Guide*.

  NOTE: The RAC software is installed as part of the Typical Setup installation option provided the managed system meets all of the RAC installation prerequisites.
- The OpenManage Server Administrator Storage Management Service requires Server Administrator to be installed on the managed system. For more information on the software and hardware requirements, see the *Dell EMC OpenManage Server Administrator Storage Management User's Guide*.
- Microsoft Software Installer (MSI) version 3.1 or later.

NOTE: Server Administrator software detects the MSI version on your system. If the version is earlier than 3.1, the prerequisite checker prompts you to upgrade to MSI version 3.1. After upgrading the MSI to version 3.1, you may have to reboot the system to install other software applications such as Microsoft SQL Server.

What's new in this release

The release highlights of Server Administrator and Storage Management are:

- Server Administrator supports the following features:
  - Support for Java Runtime Environment 10.0.1
  - Upgraded Tomcat version to 9.0.8
  - Minimum supported TLS version is TLSv1.1
  - ◦ Supports export and import of OMSA configuration
    - ◦ The OMSA enables the administrators to preserve and share OMSA system configuration of working environment.
    - ◦ The OMSA system working environment includes the web server settings, TLS certificates, user preferences and interface settings (SNMP alert settings, logging preferences).
  - Product use Feedback collection
    - ◦ OMSA provides reporting and configuration options through GUI, CLI interfaces for tracking the customer usage information.
- Supported operating systems:
  - Microsoft Window 2019
- Supported web browsers:
  - Internet Explorer - 10, 11
  - Google Chrome - 65, 66
  - Safari - 10.x
  - Mozilla Firefox - 59, 58
  - Microsoft Spartan / Edge8
- Supported network cards:
  - QLogic 10GE 4P QL41164HxRJ-DE Adapter
  - QL41262HMKR-DE 25 Gigabit Ethernet
  - QLogic FastLinQ 41262 Dual Port 25GbE SFP28 rNDC
  - QLogic 2x25GE QL41262HMCU CAN
  - Intel(R) Ethernet 25G 2P XXV710 Adapter
  - Intel(R) Ethernet 10G 2P X550-t Adapter
  - Intel(R) Gigabit 4P I350-t Adapter
  - Intel(R) 10GbE 4P X710-t Adapter
  - Intel(R) 4P X550 rNDC
  - ConnectX-5 Dual Port 100 GbE QSFP Network Adapter
  - ConnectX-4 Dual Port 100 GbE QSFP Network Adapter
  - ConnectX-5 Single Port VPI EDR QSFP28 Adapter
- New features added in Storage Management:
  - Hotplug removal of NVMe drives without Prepare to Remove.
  - Support for "Enhanced HBA mode" for PERC 10.2 H740P and H745P controllers.
  - Support for FD33XD-HBA Dual and FD33XS-HBA single controllers.
  - Removed "Rebuild Rate" property from Controller Property of BOSS-S1 controllers.
  - Support for Remaining Rated Write Endurance and SMART Alerts for BOSS-S1 controllers.
  - Support for Intel P4800X drives.

NOTE: For the list of supported operating systems and Dell servers, see the *Dell EMC OpenManage Software Support Matrix* in the required version of OpenManage Software at dell.com/openmanagemanuals.

NOTE: For more information about any features, see the *Dell EMC OpenManage Server Administrator online Help*.

Important Notes

Notes for Server Administrator

On 12th generation or later PowerEdge server with iDRAC7 1.30.30 and later versions, you can set the Platform Event Destination as IPv4, IPv6, or FQDN.

Notes for Instrumentation Service

- On 11th generation or later PowerEdge server, if conflicting BIOS settings exist while configuring BIOS setup options through Server Administrator, the update attempt may fail at system reboot and none of the BIOS setup options may be updated.
- For example, when you configure Embedded SATA Controller to RAID and Boot Mode to UEFI simultaneously (UEFI does not support RAID option), the conflict prevents the BIOS configuration updates (at system reboot).
- On certain systems, user-defined thresholds set under Server Administrator become the default thresholds after uninstalling Server Administrator.
- If you change the threshold value of a probe on certain systems, running Server Administrator, and then uninstall Server Administrator, the changed threshold value becomes the default threshold value.
- While modifying the warning threshold settings, the values are stored in the firmware as discrete integer values and scaled for display. If the modified value is not a discrete integer, it may change when saved.
- Fan redundancy can have the following states:
  - Fully Redundant — The sensors display this status if all the fans in the system are present and are in a non-failed state.
  - Redundancy Lost — The sensors display this status whenever any system fan fails or is removed from the chassis.
- If a system with memory redundancy enabled enters a **redundancy lost** state, it may not be clear which memory module caused it. If you cannot determine which DIMM to replace, see the **switch to spare memory detected** log entry in the ESM system log to find the memory module that failed.
- If you run Server Administrator when the system is in **OS Install Mode**, it may report the memory incorrectly. To avoid this issue, you must disable **OS Install Mode** before running the application.
- If you have to uninstall and reinstall the operating system SNMP service, then reinstall Server Administrator, so that the Server Administrator SNMP agents are registered with the operating system SNMP agent.
- Server Administrator Device Drivers for Linux: Server Administrator includes two device drivers for Linux: Systems - Management Base Driver (dcdbas) and BIOS Update Driver (dell_rbu).
- Server Administrator uses these drivers to perform the systems management functions. Depending on the system, the application loads one or both of these drivers. These drivers have been released as open source under the GNU General Public License v2.0. They are available in Linux kernels from kernel.org starting with kernel 2.6.14.
- CMC USB ports attached to a blade are not enumerated by Server Administrator.
- Except for AC power cord traps, SNMP traps for server instrumentation are not generated when the state of the device sensor changes from unknown to normal. While migrating the chassis of a PowerEdge M520, M620, or M820 server running Windows operating system from M1000e to VRTX chassis, reboot the server after the new drivers are detected and installed. If not, the DSM SA Data Manager service crashes on startup and OMSA fails. (BITS125071)

Notes for Storage Management Service

Detailed information on the Storage Management Service is available in the *Storage Management Service online help*. After installing and launching Server Administrator, you can access the Storage Management Service online help by selecting the Storage or lower-level tree object and clicking the **Help** button on the global navigation bar.

Notes for Remote Access Service

- The remote access service is available on supported systems only in this release. It enables remote access to a server that has lost its network connection or that has become unresponsive. In the current release of Server Administrator, the Remote Access Service uses Integrated Remote Access Controller (iDRAC).
- iDRAC also has its own CLI that is accessed through the **racadm** command. You can add **racadm** commands to a batch or script file to automate various user tasks. To limit the stress load on the managed system, and RAC, add **sleep** or **delay** commands of one or two seconds between the individual **racadm** commands.
- On systems prior to 11th generation PowerEdge server, Server Administrator slot page displays iDRAC information, but on 12th generation or later PowerEdge servers, the slot page does not display any iDRAC7 information.

Known Issues for Server Administrator

This section provides information on open issues and resolutions with this release of Server Administrator.

Issues of Server Administrator on All Microsoft Windows Operating Systems

- Perform all Server Administrator CLI commands from a 32-bit Windows command prompt. You can access the 32-bit command prompt by clicking **Start** > **Programs** > **Accessories** > **Command Prompt** or by clicking **Start** > **Run** and then typing **cmd.exe**. Attempts to run the CLI commands from the DOS command **command.com** may generate unpredictable results.
- The DSM Server Administrator Connection Service may hang on system startup if both Oracle and VERITAS Backup Exec are installed on the system. To manually start the DSM Server Administrator Connection Service on a system running Windows, click **Start** > **Programs** > **Administrative Tools** > **Service**, right-click **DSM Server Administrator Connections Services** and select **Start**.
- You may not have appropriate privileges on the Server Administrator GUI if you:
  - Belong to an Active Directory group that is part of another group.
  - Try to launch Server Administrator using the desktop icon when single sign- on is enabled.
- Broadcom architecture has a split driver implementation - evbdx.sys and bxnd60x.sys.
  - **evbdx.sys** is the Virtual Bus Driver (VBD); also called the Base Driver
  - **bxnd60x.sys** is the driver for the Broadcom NDIS device.

  Microsoft Device Manager reports both the drivers, but Server Administrator displays only the driver details specific to the VBD device.
- **BITS080169**: Documentation for Power Supply alerts mentions only AC power supply, but the alerts are valid for both AC and DC power supplies.
- **BITS054513**: On a system running Windows, while running CLI commands using telnet from a system running Linux, the telnet session may terminate if the amount of data being transferred is huge.

  Workaround: Redirect the CLI output to a text file and use the **type** command to view the output
- **DF551365**: Server Administrator does not display the IP Address for Network Adapters that are used for virtual machines

  Description: In a Microsoft Hyper-V environment, the Server Administrator Network page may indicate network adapters that are connected to a network and display Ethernet statistics but, the IP address is displayed as 'Unknown'. This is because Hyper-V virtualizes adapters that are bonded to its virtual switch. The Server Administrator only discovers physical network adapters and displays their IP addresses that are fully-controlled by the operating system and not by hypervisors.
- **BITS080696**: Windows **No Instance(s) Available** is reported for Dell_CMApplication class data To get the data for Dell_CM* wmi classes query, first query any one of the Dell_* classes.
- **JIT-58840**: On systems running Windows 10 operating system, the operating system is incorrectly displayed within OpenManage Server Administrator as Windows 2016 Server Operating System.
- **BITS129139**: On systems running Windows operating system, the command prompt closes if you run the following commands on any Dell PowerEdge systems:
  - **omconfig system platformevents event=systempowerfail action=powerreduction**

- **omconfig system platformevents event=systempowerwarn action=powerreduction**

  NOTE: The commands are supported only on 10th generation of PowerEdge servers.

- **DF94201** : When you double-click the Server Administrator icon on your desktop, a dialog box may appear, prompting you to enter credentials in Microsoft Internet Explorer for certain settings. Two possible workarounds are available for this issue: You can cancel the dialog box and enter the credentials to access Server Administrator, or enable SSO (Single Sign On) by changing the browser settings.

  To enable SSO on Internet Explorer:

  - Cancel the dialog box.
  - Go to "Tools" -> "Internet Options" -> "Security" ->Trusted sites -> "Custom Level.
  - Under "User Authentication Logon" option, change the settings to “Automatic logon with current user name and password".
  - Add the server URL to Trusted sites under "Tools" -> "Internet Options" -> "Security" ->”Trusted sites”->”Sites”.

Issues of Server Administrator on All Supported Operating Systems

- **BITS107804**: On PowerEdge R210 II and T110 II servers, clearing the **Shutdown OS First** check box and performing a reboot using the ‘Reboot’ option does not reboot the servers. After performing these steps if you refresh the Page, the options on the Remote Shutdown page are not displayed.
- On Dell PowerEdge T110 II systems, the following Server Administrator BIOS settings are not consistent with the F2 BIOS setup settings:
  - Watchdog timer: Server Administrator displays the option as disabled, but F2 BIOS allows to change the setting.
  - Embedded Video Controller: Server Administrator provides options to enable or disable, but in F2 BIOS the option is grayed out.
  - TPM Security: Server Administrator does not allow to change the settings, but F2 BIOS allows to change the settings.
  - System Profile State: Server Administrator does not allow to make changes, but F2 BIOS allows to make the changes.
  - Memory Testing: Server Administrator does not support this feature, but F2 BIOS supports this feature.
  - SRIOV option: Server Administrator does not display this information, but F2 BIOS displays this feature.
- Due to non-availability of resources, inventory collector may terminate unexpectedly and restart. If this occurs, the folder **C:\Temp \invcol** may be left as an artifact. The presence of this folder does not affect the functionality of the inventory collection. The folder can be deleted if required.
- After installing Server Administrator from the command prompt, typing an **omreport** or **mconfig** command from the same prompt can cause an error. Open a new command prompt window and type commands.
- If the command log page in the Server Administrator GUI displays an error message indicating that the XML is malformed, you must clear the command log from the CLI using the **omconfig system cmdlog action=clear** command
- After a **Reset to Defaults** operation of the Integrated Remote Access Controller, the first user configuration, operation fails if it is a single-user configuration item (such as enabling or disabling a user or changing user name). Always change a combination of two-user configuration items (such as enabling or disabling a user and changing user name) concurrently during your first configuration operation.
- While typing the command **omreport system version -outc <filename>**, ensure that you specify an absolute path name for the output file; else, the output file is empty. For example, **c:\out.txt**.
- Typing **omreport system esmlog/alertlog/cmdlog -fmt tbl** command on the CLI can result in XML parsing errors if the size of the log is large. Use the GUI or the **omreport system esmlog/alertlog/cmdlog** CLI command to view the contents of the log.
- For complex **omconfig** CLI commands that contain multiple set commands in one command line, the CLI may report a success status for the command even if a part of the command failed. To avoid this issue, run only one command per command line. The current settings can be confirmed by performing the corresponding **omreport** command.
- Some complex **omconfig** CLI commands that contain multiple set operations have been modified to avoid the above problem. While running a CLI command if the message, **Error! Illegal combination of parameters** is displayed, modify your command into several simpler commands. Each command should change only one setting.
- When running Server Administrator on a system with a traditional Chinese operating system, the application pages are displayed in simplified Chinese. To view the Server Administrator pages in English, go to your browser language preference page and change the language to English.
- Log files saved from Server Administrator are saved in zip format. It is recommended that you open this zip file using WinZip. Windows Server 2003 or Windows XP embedded **Compressed (zipped) Folder** utility is not recommended.
- After configuring BIOS settings on certain systems, a second reboot may be required for the Server Administrator to display the updated BIOS settings properly.

- If you import an invalid root certificate into Server Administrator, using **Preferences** > **General Settings** > **Web Server** > **X.509 Certificate**, and try to log on to the application after restarting the Web server, a blank page is displayed. To fix this issue, restore your original **keystore.db** file before importing a valid root certificate. To restore the **keystore.db** file, use both the basic operating system commands and the Server Administrator Command Line Instrumentation (CLI).

  Perform the following steps from your operating system command line:

  a Type: **omconfig system webserver action=stop**

  b Locate the **keystore.db.bak** file. The default path is **C:\program files\dell\SysMgt\apache-tomcat\conf**.

  c Copy **keystore.db.bak** to **keystore.db**keystore.db.

  d Type: **omconfig system webserver action=start**
- A temperature drop below a minimum failure threshold does not cause a system reset even if this alert action is set.
- Clicking the **Back** and **Refresh** buttons on the browser may not display the correct page regarding the Server Administrator component tree, tabs, tab menus, or help, as Server Administrator has been designed with limited functionality to reduce overhead. Full feature capabilities of the Web browser such as **Back**, **Refresh**, and **Open in New Window** may not be supported.
- Selecting the boot sequence under the BIOS **Setup** tab does not re-enable boot devices that have been disabled in the System Setup Program, earlier.
- The links on the Server Administrator home page may not work after repeated random clicking. To resolve this issue, refresh the browser by pressing **<F5>** or click the browser **Refresh** button.
- All unsecured HTTP requests to Server Administrator receive an invalid response. Server Administrator runs only one instance of the Web server, which is secure. Make all connections through **https://<ip address>: <port number>**. Any **http://<ip address>: <port number>** request for connection with the server receives an invalid response.
- If the web browser used with Server Administrator does not display a page or perform an action, make sure that the browser is in online mode. To go online, perform the following:
  - In Internet Explorer, on the menu bar, click **File** and clear the **Work Offline** option. When **Work Offline** is selected, a check mark is displayed to the left of the option on the **File** menu.
- If Internet Explorer prompts you to **Work Offline**, **Connect**, or **Try Again**, always select **Connect** or **Try Again**. Do not select **Work Offline**.
- In Internet Explorer, on the menu bar, click **File** and clear the **Work Offline** option. When **Work Offline** is selected, a check mark is displayed to the left of the option on the **File** menu.
- If Internet Explorer prompts you to **Work Offline**, **Connect**, or **Try Again**, always select **Connect** or **Try Again**. Do not select **Work Offline**.
- While setting dates in the **Asset Information** section of the Server Administrator home page, the current time is appended to the date. While setting dates with the CLI, the appended time is noon.
- On some systems, temperature probe values and settings are only supported for whole degrees, not tenths of a degree. On those systems, setting a fractional value for the minimum warning temperature threshold results in the set value being rounded off to the next whole number value. This behavior may cause the minimum warning threshold to have the same value as the minimum failure threshold.
- If you close the browser using the **Close** button on the browser or log off from the operating system, the Server Administrator session is not terminated. This session is listed in the Session Management page until the session time out occurs, or DSM SA connection service is restarted, or the operating system is rebooted.
- If you change the operating system Time Zone to a new time zone, Server Administrator session management does not display the time in the new time zone specified. Restart Server Administrator to display the accurate time for the time zone in the Session Management page.
- **DF78425**: The Server Administrator Auto Recovery feature may execute the configured action before the time interval when the system is under heavy stress.

  The Auto Recovery feature can be set to execute an action (For example, system reboot) to recover a hung system. Since the Auto Recovery timer is now an application-level timer instead of a kernel-level timer, heavy resource stress on the system may result in an inaccurate measurement of a short keep alive interval (less than 120 seconds), and the configured action may be triggered. The issue is more prevalent in systems that have only one CPU with hyper-threading unsupported/disabled or systems that are subjected to persistent stressful conditions such as, resource depletion and CPU running at 100% usage with significantly more threads than normal usage.

  The Auto Recovery feature is not enabled by default. If the Auto Recovery feature has been enabled, increase the System Reset Timer value to at least 120 seconds.

- Using the Internet Explorer browser, if you install Server Administrator on a system that includes an underscore in its host name, you must use the IP address of the target system in the browser URL to launch Server Administrator, as Host names with underscores are not supported. For example, (assuming Server Administrator is listening on port 1311): **https://192.168.2.3:1311**.

  For more information, see the following article on the: Microsoft website **http://support.microsoft.com/kb/312461**
- **DF152755**: The Server Administrator GUI does not respond when the alerts log has many events. If the Alert Log contains several entries and if you try to navigate to another page, the Server Administrator GUI may take about 30 seconds to display the content.
- **DF172125**: Power monitoring probes are displayed on certain systems that do not support power monitoring. On certain systems that do not support power monitoring, Server Administrator reports the two platform event filters related to a power monitoring as **System Power Probe Warning** and **System Power Probe Failure**. These two filters are not supported on these systems. That is, you can view and configure these filters, but no action is taken.
- **DF185770**: Primary User Telephone Number does not accept symbols. On Server Administrator, under **Asset Information** > **System Information** > **Primary User Telephone Number** configuration allows only alphanumeric characters.
- The selection of default option for the front panel LCD in Server Administrator displays the Model Name whereas the default is a Service Tag on the physical LCD.
- If Server Administrator does not respond or is locked to your selections on the component tree, perform the following steps:
  a Click **Preferences**. The Preferences page appears.
  b Click **Server Administrator**. The items on the front page may respond to your click.
- **DF277439**: Persistence of Configuration and Log File Changes in VMware ESXi On systems running the VMware ESXi operating system, the file system is ramdisk. Modifications made to the files within the file system are generally not persistent across reboots, with the exception of designated configuration and log files. These files are updated to the disk periodically and on system shutdown. If the system is reset without a graceful shutdown before the updated to the designated configuration are made and before log files are updated to the disk, the changes are lost.

  The following is an example of the effect of this behavior:

  – On certain systems, the first time that the thresholds for a probe are changed after Server Administrator is installed; the current threshold values for that probe are saved as the default threshold values by writing the values to a configuration file. When **Set to Default** is performed after the first change of the thresholds, Server Administrator sets the threshold values to the values that were saved in the configuration file as the default. If the system running the VMware ESXi operating system is reset without a graceful shutdown before the changes to the configuration file are updated to the disk, the user- defined thresholds become the default thresholds.
- **DF315853**: Some Server Administrator CLI commands, function properly only when run from the elevated console window. It is recommended that you use the elevated console for running the CLI.
- Due to some limitations, you cannot log on simultaneously to multiple browser instances/tabs using SSO login, as only one session remains active while the other sessions expire.
- **DF489034**: Intel TXT configuration fails due to Virtualization technology dependency.
- If the current Virtualization Technology attribute setting is **Disabled** (Virtualization Technology is part of the Processor Settings group on the BIOS setup page); the Intel TXT attribute configuration fails on the Server Administrator user interface (**System** > **Main System Chassis** > **BIOS** > **Setup** > **System Security**). To resolve this issue, configure Virtualization technology setting to **Enabled** and reconfigure the Intel TXT attribute, if it is configurable.
- **DF549057**: When an operating system is installed through USC, the BIOS attributes in Server Administrator are displayed as read-only. You can edit the BIOS attributes 18 hours after the operating system installation.

  Workaround: To enable editing of the Server Administrator BIOS attributes, launch Lifecycle Controller while booting.
- **BITS040169**: In case of Boot/HDD/UEFI sequence, if they are read-only, then toggle buttons (+ and -) and submit button are not visible. On the BIOS setup page, dependencies may exist between the various attributes for Bios settings. Setting an attribute value may change the state of the dependent attributes to non-editable or editable. For example, changing the Boot Mode to UEFI from the Boot Settings page does not allow you to configure the Boot or Hard-Disk Drive Sequence in the BIOS Boot Settings page. When the page is non-editable, the toggle buttons on the page allows toggling the order of the boot sequence. However, settings cannot be configured since **Apply** button will not available to submit the settings.
- **BITS050574**: On 11th generation and 12th generation of PowerEdge servers running the Linux OS, the omreport system summary command displays **RAC Command Interface** as 7.1.0. "RAC Command Interface" is a DRAC4 RPM and its version is 7.1. It is installed as a dependent package for iDRAC6 and iDRAC7 Command Interface packages.
- If a new certificate imported to Server Administrator is not active after restarting the Web server, restore the previous certificate. To restore the previous certificate, do the following:
  a Stop the Web server.

b Perform one of the following as applicable:

– On systems running Windows:

◦ Delete the file **keystore.db** at **<installed directory>\Dell\SysMgt\apache- tomcat\conf**

◦ Rename the file **keystore.db.bak** at **<installed directory>\Dell\SysMgt\apache- tomcat\conf** to **keystore.db**

– On systems running Linux:

◦ • Delete the **keystore.db** file at **/opt/dell/srvadmin/lib64/openmanage/apache- tomcat/conf**

• Rename the **keystore.db.bak** at **/opt/dell/srvadmin/lib64/openmanage/apache-tomcat/conf** to **keystore.db**

c Start the Web server.

- **BITS078118**: On 12th generation of PowerEdge servers with specific versions of iDRAC, you cannot set the platform event alert actions (reboot, shut down, and so on) through Server Administrator. Set the alert actions for the events through iDRAC GUI.
- **BITS144583**: On Mozilla Firefox 21 or later, the **Quit browser** option does not work after logging out from Server Administrator. To close the browser or tab, you must manually close the Firefox browser tab.
- **BITS177670**: On Chrome 38 or later, the **Quit browser** option does not work after logging out from Server Administrator. To close the browser or tab, you must manually close the Firefox browser tab.
- On PowerEdge T430, C4130, and R220 II, with PERC S130 configuration and no backplane, Storage Management displays a mock backplane which does not support the blink/unblink operation for disks available on this configuration.
- **BITS256932**: The default factory IP for an IDRAC is "192.168.0.120" or "192.168.0.*", which indicates that the iDRAC IP is not configured by the user. However, if you choose to configure the default factory IP (static or DHCP) as your iDRAC IP, then the "Not Configured" value for "iDRAC Network Settings" displayed on the OMSA "System Summary" page can be ignored. Note: On rack and tower systems, the default factory IP for iDRAC is "192.168.0.120". On modular systems, the default factory IP range for iDRAC is "192.168.0.*", where "*" can be any value from 0 to 255.
- **BITS265922**: The DSM SA Connection will fail to start if Java Runtime Engine 1.8.0 or newer is installed and specified as the "System JRE" in Preferences of the Server Administrator web GUI. OMSA 8.3 and older is currently not compatible with Java 1.8 or newer. To recover to the default Bundled JRE setting so that the web service starts again, enter the following command line: omconfig preferences webserver attribute=setjre jreversion=bundled
- **BITS260330/BITS260451**:Restart the data manager service, after Intel NIC driver update or NVIDIA graphics driver update is performed.
- **JIT-25314**: The alert log is not generated in Server Administrator, when the Power Supply Unit (PSU) is inserted in the server without connecting a power cable for that PSU. However, corresponding log is generated in ESM or Hardware logs.
- **JIT-22805**: Server Administrator does not recommend the upgrade to major versions of JRE. For more details, see the release notes of Server Administrator (packaged with Server Administrator application) or at dell.com/openmanagemanuals. All the Internet browsers required TLS1.1 or higher version to connect to Server Administrator web application. Please refer the vendor (Microsoft, Mozillla, Google) browser configurations for setting the TLS versions.
- **JIT-60297** - On RedHat Enterprise Linux 7.3, after performing ASR operation; restart the system once it recovers from ASR operation. Then navigate to Server Administrator Logs page in GUI. You could see an XML error. This could be due to xml log files being corrupted.

  To Recover: Perform clear logs operation so that new logs would be generated. Before performing this operation, if needed please take back up of old xml log files.
- **JIT-69735** - The Server Administrator web application blocks the client connections in the Internet browser settings with TLSv1.0 version and lesser.
- **JIT-60691**: In SCOM – Server Management Pack (MP) for monitoring Physical and Team network interfaces XML files are created due to the heavy usage of the Server Administrator CLI NIC command (omreport chassis nic -fmt xml).
- **JIT-36610/JIT-36599**: In OpenManage Server Administrator slots page, the Dell "HBA330 Adapter" PERC card will be enumerated as "12GB/s HBA internal" and Dell "HBA330 Mini" PERC card will be enumerated as "SAS3008 PCI-Express Fusion-MPT SAS-3
- **JIT-81211**: On 14th Generation of PowerEdge servers, Server Administrator displays the value of the enabled

  field for CPU 64 BIT capability as NO. User can ignore this.
- **JIT-81661**: On 14G PowerEdge servers, the embedded cache devices are incorrectly displayed as a Field Replaceable Unit (FRU). These embedded cache devices are not FRUs.
- **JIT-30251**: Alert log of Server Administrator logs few invalid informational alerts stating that, A device was added to the system to the location: PCIe SSD in Slot X in Bay Y, when user performs 'Prepare to Remove' operation on NVMe PCI SSD slot. These false alerts are displayed only for the first operation of Prepare to Remove after a fresh install or restart of data manager.

Issues for Remote Access

NOTE: The Remote Access Service is supported on 11th generation of PowerEdge servers only. The following subsections list the currently known issues regarding implementation and operation of your RAC and the Remote Access Service in Server Administrator.

Issues of Server Administrator on all Operating Systems

- The Server Administrator user interface and commands related to **local authentication enable** are not applicable for RAC firmware 3.20. The Active Directory authentication feature replaces the **local operating system authentication** feature in this version of firmware. Due to this change, the following commands return errors:
  - racadm localauthenable
  - omconfig rac authentication

  NOTE: The following packages will be deprecated from DellEMC Server Administrator current release (9.1.0):

  a Srvadmin-racadm4.

  b Srvadmin-racadm5.
- Due to fluctuations in the watchdog timer, the **Last Crash Screen** may not be captured when the Automatic System Recovery is set to a value of less than 30 seconds. To ensure the correct functioning of the **Last Crash Screen** feature, set the System Reset Timer to at least 30 seconds.
- **DF132894**: The cfgDNSServer1 and cfgDNSServer2 properties of group cfgLanNetworking may be set to identical values while swapping addresses. Some performance may be lost temporarily during the swapping. The cfgLanNetworking group is configured using the**racadm config** command.
- The remote access controller uses FTP protocol to perform some of the Server Administrator commands. If a firewall is installed in the system, it may cause these commands to fail.

  The following Server Administrator CLI commands use FTP protocol to communicate with the RAC:
  - omconfig rac uploadcert
  - omconfig rac generatecert

  The following racadm commands use FTP protocol to communicate with the RAC:
  - racadm sslcertupload
  - racadm sslcsrgen
  - racadm fwupdate
- If the RAC configuration is reset to factory defaults using the **racadm racresetcfg** command, the RAC configuration tab in Server Administrator does not reflect the reset configuration settings until the system reboots. Also, the RAC configuration page in Server Administrator cannot be used to make any configuration changes until the system reboots.
- The RAC does not support local RAC user IDs with special characters. When adding a local RAC user, use only alphanumeric characters for the user name.
- While the RAC is being reset, the Instrumentation Service cannot read sensor data for certain systems. As a result, the voltage, temperature, and other probes may not be visible on the Server Administrator home page until the RAC has completed resetting.
- The RAC may not send traps when your system is locked up. To enable traps to be sent when the system is locked, configure the watchdog timer using the Server Administrator GUI. On the GUI, click the "Properties" tab and ensure that **Auto Recovery** is selected. The default value of the**Action On Hung Operating System Detection** setting is **None**.**None** indicates that detection will not be performed.
- RAC firmware 2.0 and later does not support passwords with special characters (non- alphanumeric) only for RAC user IDs logging in using the Web-based interface (with Local RAC Authentication). You cannot log on to RAC, if you created RAC user IDs using previous versions of the firmware or using Server Administrator that is running version 2.0 firmware on the managed system.

  Use one of these methods to correct this issue:
  - Change your passwords before updating the firmware.

- Use the following CLI command to change the password: **omconfig rac users username=xx userpassword=yy** where **xx** is the original user ID and **yy** is the new password.
- Change the password through Server Administrator using the **User** tab. Make sure that the check box to change the password is checked. Enter a new password, and then enter it again to validate the change.
  - Use the racadm utility to change the password: **racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i <usr_index> <new_pwd>** where **<usr_index>** is the index of the user database entry to be modified and **<new_pwd>** is the new password.

- Depending on your network and proxy configurations and whether you are using Mozilla browser, you may need to enter the exact IP address of the RAC controller, you are trying to access in the **No Proxy for** field of your browser.

  Perform the following steps:

  a Open your Mozilla browser.

  b Click **Edit**.

  c Click **Preferences**.

  d Click **Advanced** in the left sidebar.

  e Click **Proxies** in the left sidebar.

  f Enter the RAC IP address in the **No Proxy for:** field.

  g Click **OK** and then close the browser.

- To view the RAC Web-based interface when using Mozilla 1.6, you must configure your cookie settings to **Enable all cookies**.
- To enable all cookies, go to the menu options and click **Edit** > **Preferences** > **Privacy & Security** > **Cookies**, and then select **Enable all cookies**. If you do not perform these steps, you cannot log on to the Web interface and a message appears indicating that your username and password are incorrect.
- **DF384061**: Self-signed certificate does not enable the compatibility listener in Windows 2008 R2 managed node. On a Windows 2008 R2 managed node, a valid CA signed certificate is required to create compatibility mode WinRM Listener. You cannot create a compatibility mode listener with a self-signed certificate.
- **DF380725**: On Internet Explorer or Firefox Web browsers, you cannot attach files to an e- mail if the filename contains non-ASCII letters. To attach files to an e-mail, rename files to contain ASCII characters.
- On 12th generation of PowerEdge servers, Server Administrator displays the Embedded Systems Management (ESM) or hardware logs. However, when the maximum limit for number of logs that can be recorded is reached, the existing oldest logs are overwritten. But for 11th generation of PowerEdge servers or prior, when the maximum limit is reached, the information logging is stopped.
- **BITS113585**: Server Administrator does not log CPU or CMOS Battery Probe Alerts and does not send SNMP traps.
- To resolve this issue, stop the USB arbitration service and run the Inventory Collector. To stop the USB arbitration service:

  a Run the **ps aux|grep usb** command to check if the USB arbitration service is running.

  b Run the **chkconfig usbarbitrator off** command to prevent the USB arbitration service from starting during boot.

  c After the USB arbitrator service is stopped, reboot the server to allow the Inventory collector to run.

- **DF520449**: On all versions of the ESX, the following USB connection error messages are generated. These messages can be ignored. The following is a typical message:

Table 1. USB connection error message

Vendor: iDRAC	**Model**: MAS022	**Rev**: 1.00
Type: Direct-Access	**ANSI SCSI revision**: 02	

Table 2. USB connection error message

Vendor: iDRAC	**Model**: SECUPD	**Rev**: 0329
Type: Direct-Access	**ANSI SCSI revision**: 02	

- **DF531509**: The setup and/or system password configuration from the Server Administrator GUI or CLI is successful, but the password is displayed as blank instead of asterisk (*) on the F2 BIOS page.
- **Workaround**: Perform the following and manage the remote system from the web server.

  a Configure TCP Chimney offload to disable state by running the following command: **netsh int tcp set global chimney=disabled**

  b Configure RSS (Receive Side Scaling) to disable state by running the following command: **netsh int tcp set global rss=disabled**

  c Configure NetDMA to disable state by running the following command: **netsh int tcp set global NetDMA=disabled**

- **BITS086423**: After an upgrade to the current version, Server Administrator does not retain the support link information on the Preferences page.
- **BITS040184**: User in IDRAC user authentication page showing operator privilege(IDRAC user privileges) is displayed as Custom in Server Administrator.
- With the following wsman rpm versions getting carried in SLES12 OS,OMSA DWS does not work. Update these rpms having same or later versions from SUSE

  openwsman-server-2.4.11-2.18.x86_64.rpm ,libwsman1-2.4.11-2.18.x86_64.rpm,

  libwsman_clientpp1-2.4.11-2.18.x86_64.rpm
- **JIT-95031**: On De-branded Servers , "Dell EMC" text is displayed on header of the login page, About page, command log and Email template along with the product name.
- **JIT-106131**: The server administrator's product use feedback logs does not get tracked because of the insufficient privileges of the user logged into the system.
- **JIT-106148**: While generating X.509 certificate through Server Administrator GUI or CLI interface, a special character is used for Locality parameter, and the same is imported. Therefore, the server administrator redirects to the login page.
- **JIT-111963**: The values displayed for Capabilities and Cache Information for 'processors' may contain invalid values if marked as Yes under 'Deprecated' field. These deprecated values should not be considered.

Dell EMC OpenManage Release Notes Version 9.2.1

The following section describes the issues and workaround in Server Administrator Storage Management.

Known Issues and Workarounds for Storage Management Service

- With Chinese or Japanese language browser settings, using the Storage Management Service Advanced Create Virtual Disk Wizard may occasionally result in text overflowing to the bottom of the side-by-side blue text boxes.
- Physical disk clear operation is not available on PERC 8, PERC 9, and PERC 10 family of Hardware controllers.
- Physical disk properties such as Manufacture day, Manufacture week, and Manufacture year are available for SAS drives only.
- Creating many sliced span virtual disks using the spun-down drives through the command line or GUI result may be delayed.
- **Workaround**: After creating one sliced span virtual disk, wait for some time to create the next sliced span virtual disk.
- For 14G servers, only two enclosures per controller is supported.
- A Security Key Identifier can contain numerals, lowercase alphabets, uppercase alphabets, nonalphanumeric characters (except space), or a combination of any of these.

  NOTE: If you have used the special characters "/" (forward slash) or " ' " (single quote) in the Security Key Identifier, they are displayed as "_" (underscore) on the Change Security Key page and Import Secured Foreign Configurations page. This is applicable only to the Security Key Identifier and not to the Passphrase.

- If Storage Management displays a path failure message for a Logical Connector after a reboot, use the **Clear Redundant Path View**, provided in the **Change Controller Properties** controller task, and restart the system.

  NOTE: Use this command only if you have intentionally removed the multipath connection while rebooting the system.

- Patrol Read is not supported on SSD media. The Patrol Read feature fails for any controller that has SSD media on a virtual disk.
- Hot plug of enclosures takes time to enumerate the enclosure and its components. During this time, there will be a delay in the response time of tasks, such as displaying the physical disks on the physical disk page and in the virtual disk selection page.
- All virtual disks from the SAS/iR controller display the name **IR Virtual Disk** on the **Preview** page. On successful import, another name is assigned to these virtual disks and the "IR Virtual Disk" name is not displayed on the "Preview" page.
- Storage Management does not permit connecting the first enclosure in single path and attaching the subsequent enclosures in multipath. All enclosures must be connected in multipath to enable the multipath view.
- An error message may not appear when **Import Foreign Configuration** task is not successful.
- **Description**: The **Import Foreign Configuration** task can only import virtual disks that have consistent data. A virtual disk with inconsistent data cannot be imported. When importing multiple virtual disks in a single operation, however, the **Import Foreign**

Configuration task may report successful completion even when inconsistent virtual disks are present and have not been imported successfully.

Solution: If the "Import Foreign Configuration" task is unable to import an inconsistent virtual disk, then the physical disks that belong to the virtual disk continue to display a "Foreign" state after the "Import Foreign Configuration" task completes. In this case, repeat the "Import Foreign Configuration" task until one of the following occurs:

- There are no longer any physical disks in **Foreign** state after the **Import Foreign Configuration** task completes.
- You receive an error stating that the **Import Foreign Configuration** task has not completed successfully. This error indicates that there are no longer any consistent virtual disks available to be imported. Therefore, all virtual disks that are not imported are inconsistent and you can either perform a **"Clear Foreign Configuration"** to remove the virtual disks or remove the physical disks from the controller.

- DF60696 : Storage Management responds slowly when using Internet Explorer 9.x or 10.x on a system with mixed SAS and SATA physical disks.

  Description: When using the "Create Virtual Disk" wizard from the Storage Management graphical user interface (GUI), you may notice decreased performance when using Internet Explorer 9.x or 10.x on a system with multiple physical disks. The MD1000/MD1400/MD1420 storage enclosures that are heavily populated with mixed SAS and SATA physical disks.

  Solution: Use a supported web browser other than Internet Explorer 9.x or 10.x or use the Storage Management command line interface (CLI) to create the virtual disk. See the Dell EMC OpenManage Server Administrator Release Notes for information on supported browsers. See the Storage Management online Help or the "Server Administrator Command Line Interface User's Guide" for information on using the Storage Management CLI.

- **DF152362**: Storage Management may not display controllers installed with the Service and Diagnostics utility.

- **Description**: Storage Management may not recognize devices that are installed after Storage Management is already running.

  Solution: If Storage Management does not recognize a newly-added device and this problem has not been corrected with a Global Rescan, then reboot the system.

- **DF120475**: Storage Management SNMP traps are not filtered by Server Administrator.

- **Description**: Server Administrator allows you to filter SNMP traps that you do not want to receive. To implement SNMP trap filtering, select the **System tree** > **Alert Management tab** > **SNMP Traps** subtab. The **SNMP Traps** subtab has options for enabling and disabling SNMP traps based on severity or the component that generates the trap. Even when the SNMP traps are disabled, Storage Management generates SNMP traps.

  Solution: SNMP trap filtering will be provided in a future release of Storage Management.

- When issuing certain **omconfig storage** CLI commands with **Power User** privileges, the **Error! User has insufficient privileges to run command: omconfig** message may be displayed. You must be logged on as an Administrator to perform these actions.

- Using the Storage Management Service **Advanced Create Virtual Disk Wizard** may occasionally result in a vertical scrollbar of less than normal width. If this occurs, resizing the Server Administrator window causes the vertical scrollbar to be redrawn correctly.

- Using the GUI, if a virtual disk is renamed to a name containing multiple blank and consecutive spaces, the name is truncated to a single space after **Apply** is clicked.

- **BITS118226**: The representation of NVMe devices residing on backplanes that attach to PCIe Extender cards is inaccurate on Storage Management. This is because Storage Management does not have a process to understand the mapping of the NVMe device, backplane, and the PCIe Extender card. This issue exists only on PowerEdge R920 servers and does not impact the operations on the NVMe device. Multiple backplanes on Server Administrator indicate the presence of multiple PCIe Extender cards on the system.

- **BITS124349**: Firmware version for SAS 9207_8e, SAS 9206_16e, and SAS 9300_8e, will not be displayed on the Storage Management GUI and CLI.

- **BITS123999**: SAS 9300_8e is not supported on systems running the VMware ESXi operating system.

- **BITS128355**: The slot occupancy report displays single backplane ID and backplane name in the Storage Management GUI and CLI. The physical disk slot occupancy report for PCIe Subsystem displays NVMe devices present in two different PCIe backplanes under the

same PCIe backplane on PowerEdge R920 servers. The NVMe devices connected to different PCIe backplanes are displayed correctly under **Storage** > **PCIe-SSD Subsystem** > **PCIe-SSD Extender** > **Enclosure**.

- **BITS146054**: The enclosure automatically sets the critical and default warning thresholds. The user cannot set or reset any warning threshold to any temperature probe through the Storage Management GUI or CLI.
- On a PowerEdge server with maximum configuration of 8 populated enclosures connected to the PERC hardware controller, the user can experience a delay in response. When Server Administrator storage commands such as Create Virtual Disk or Start check consistency are run, the delay in response can range from 10 — 30 minutes.
- **BITS161852**: The limitation is observed when two enclosures are connected to two ports of PERC H830 controller. The limitation is not observed when the enclosures are connected in a daisy-chain configuration. In the **Create Virtual Disk Advanced Wizard** screen, enclosures and physical disks are listed together. The user must select only the physical disks and not the enclosures when creating a virtual disk using the **Advanced Wizard** option.
- **BITS140465**: When the user tries to create another partial virtual disk of any RAID level, on an existing, but degraded disk group, Storage Management does not allow the user to perform this action. This limitation occurs because Storage Management does not support this functionality. However, this limitation is only observed on certain PERC 9 family of hardware controllers (PERC H330, H830, and H730).

  Workaround: The user can create a partial virtual disk during system restart using the CTRL+R configuration utility.
- **JIT-10452 (BITS236815)**: Occasionally, the virtual disk creation process on PERC 9 hardware controllers may fail on GUI and CLI. Workaround: Restart the server to resolve this issue.
- **JIT-8321 (BITS220411)**: Unable to create Partial Secure virtual disk using the GUI when all the available SEDs are selected. This operation will work if any other physical disk, which is not a part of any virtual disk, is connected.
- **JIT-11205 (BITS242664)**: When a physical disk, which is a part of multiple partial virtual disks, is reinserted into the system, the status of the partial virtual disks will be displayed on Storage Management after a short delay.
- **JIT-8442 (BITS221272)**: Few enclosure alerts such as Enclosure power on/off and Fan removal, does not appear if the enclosure is connected to the server using a SAS 12 Gbps HBA card. Restart Data Manager Service to update component status.
- **JIT-10933 (BITS240247)**: Storage Management does not display the Device name on a system where there more than 300 virtual disks.
- **JIT-72304**: Able to assign lesser capacity physical disk as a DHS to the virtual disk created with physical disk having higher capacity.
- **JIT-16919 (BITS270856)**: On Precision 7910 running a client operating system (for example, Windows 8.1 x64), the PERC 9.3 driver version is displayed as outdated and a yellow bang is shown on such hardware configurations. This issue does not cause any functionality limitation.
- **JIT-43557** : In Split Mode, Slot occupancy report displays inaccurate empty slots when there are no drives connected to the backplane. The report shows the message empty slots interchanged between controller. This issue occurs for the server with no drives attached to the backplane in split mode only. Slot occupancy report works fine as expected for servers with a minimum of one drive.
- **JIT-52091**: Cryptographic erase operation might take longer time to be visible in the dropdown list for the ISE Capable SATA SSDs after this operation is done.
- On a PowerEdge server with maximum configuration of 2 populated enclosures connected to the PERC hardware controller, the user can experience a delay in response.
- Unable to create Partial Secure virtual disk using the GUI when all the available SEDs are selected. This operation will work if any other physical disk, which is not a part of any virtual disk, is connected.
- **JIT-58147**: In the BOSS-S1 controller properties, slot ID is displayed as "Embedded".
- If the background IO is in progress, "Prepare to Remove" operation for the NVME devices might fail.
- From 14G onwards, no Channel/Connector information will be displayed under “PCIe SSD Subsystem”. Enclosure/Backplane will be directly connected to the “PCIe SSD Subsystem”. There is no change in the display of “NVMe Devices (Arraydisk) and Add-On Card (HHHL Card)”. NVMe Devices (Arraydisk) will be displayed under “Enclosure / Backplane” whereas Add-On Card (HHHL Card) will be displayed under “PCIe SSD Subsystem”.
- **JIT-60971** : In OMSA, the empty slots in slot-occupancy report is not displayed after "prepare to remove" operation is performed on the servers with one or more PCIe Backplane.

- **JIT-61216** : Unable to create virtual disks (Raid 0, 1, 5) using Advanced Wizard if NVME add in card is present

  Description: In PERC S140 advanced wizard, virtual disk creation fails if a combination of NVMe and HHHL addin cards(AIC) are present.

  This issue is observed if the PCI slot ID of the add-in card (AIC) matches with the NVMe drive slot number. However, if only NVMe drives are used, you can successfully create the virtual disks. This is because the GUI code is unable to differentiate the slot ID/number in Create Virtual Disks Advanced Wizard.

  NOTE: This issue does not cause any data loss. The RAID-5 on S140 with NVMe drives is not supported.

  Solution: To resolve this issue, you can create a virtual disk using the Create Virtual Disks Express Wizard and OM-CLI.

- **JIT-63561** : In Dell's 14th generation of PowerEdge servers, while doing the "Reconfiguration" operation, "Auto Configure RAID0" option is listed in OMSA under H730P controller's "Available tasks". It happens during RAID level migration from RAID1 to RAID0.
- **JIT-71918**: On 14th generation of PowerEdge servers when connected with two SAS 12Gbps controllers in Slot4 & Slot5 and each controllers are connected with separate MD1400 enclosure, both Enclosure EMMs are listed under "Connector 0" and no device is listed under "Connector 1 ". Slot-4 SAS 12Gbps controller is connected with two redundant EMMs which are listed in "Connector 0". Slot-5 12Gbps controller is also connected with two redundant EMMs, but both are listed under "Connector 0".
- **JIT-71919**: On 14th generation of PowerEdge servers when connected with two SAS 12Gbps controller in Slot4 & Slot5 and each controllers are connected with separate MD1400 enclosure, with two redundant cable i.e. EMM0 & EMM1, then with redundant EMM both enclosures are listed for EMM0 & EMM1, but physical disks are not displayed for EMM1. Slot-4 SAS 12Gbps controller is connected with two redundant EMMs – Here both EMMs are listed under "Connector 0", and for EMM0 physical Disk is listed and for EMM1 no physical disks are listed. Slot-5 SAS 12Gbps controller is connected with single EMM (ie.EMM1) – Here one EMM0 is listed under "Connector 0", and for EMM1 physical Disk are listed.
- **JIT-78857** : Successful Prepare to remove and reinsertion operation on a drive for 3-4 times, will result in all the drives getting removed and inserted back in ESXi 6.5 U1 operating system.
- **JIT-79925** : On 13th generation of PowerEdge servers, OMSS reports for PCIe Link Speed is negotiated and maximum link speed/width shows '0' for Slot 1 device.
- **JIT-76259**: EMMI alert description for Dedicated hot spare assigned physical disk should contain meaningful alert description instead of the statement, **This alert is provided for informational purposes**.
- **JIT-72304** : Able to assign lesser capacity physical disk as a DHS to the virtual disk created with physical disk having higher capacity.
- **JIT-80079**: If **Prepare to remove** operation is executed on a Non-RAID PCIe-SSD physical disk, the bus protocol for the virtual disk associated with that physical disk, changes to SATA from PCIe-SSD.
- **JIT-80085** : The alert descriptions, in the online help, for Set Available Spare Warning Threshold and Set Available Spare Critical Threshold show **The Available Spare Warning Threshold for PCIe SSDs is set to %1** and **The Available Spare Critical Threshold for PCIe SSDs is set to %1** respectively, instead of **The Available Spare Warning Threshold for PCIe SSDs is set to <value>** and **The Available Spare Critical Threshold for PCIe SSDs is set to <value>**.
- **JIT-94666**: For Non-RAID drives attached to SWRAID controller enumerates for virtual Disk layout as Non-RAID. Whereas on Storage Management GUI, when you click on virtual disk name the physical drives does not display as Non-RAID."
- **JIT-96484**: Auto Config RAID 0 task fails and displays improper error message, when there are no free drives to create RAID 0 virtual disks on the server. Exit the wizard of the error page as Server Administrator log out.

  Workaround: Once again login to OMSA GUI.
- **JIT-95176**: The Physical disks available in MX5016s connected to MX7000 chassis slot 8 does not support RAID-10 intelligent mirror virtual disk creation.
- **JIT-92467**: The dynamic mapping of an enclosure for the first time also displays the unmapped enclosure for a short period. Refresh the Server Administrator page to remove the unmapped enclosure entries.
- **JIT-93304**: Virtual disk created using compute backplane and MX5016s drives, is hot-plug removed and then inserted back into the chassis. When foreign config operations are executed immediately after the hot-plug operation, the Server Administrator GUI hangs for 2 minutes.

  This does not occur if the same foreign config operations are executed after sometime post MX5016s hot-plug.
- **JIT-97092**: Dynamic mapping of MX5016s on H745pMX controller displays the status as unknown. Upon, performing the service restart the status is reflected correctly.

- **JIT-97151**: Full view of Physical Disk Page in Server Administrator GUI, the negotiated speed for a 6Gbps drive capable speed is intermittently shown as 12Gbps.
- **JIT-94842**: Storage Management carries SHA1 signed library (storelibIR) in the current release.
- **JIT-91317**: The storage management displays an incorrect alert "The Patrol Read corrected a media error" instead of Patrol read completion alert "Media Patrol completed" on BOSS card.
- **JIT-97199**: In storage management, VDs created on MX5016s through PERC H745X take approximately 1 minute to confirm the creation to the user.
- **JIT-104975**: In storage management, FAN speed changes will not update dynamically.
  Workaround: Data manager service restart will update the latest FAN speed.
- **JIT-106970**:After change controller mode operation is performed, two alerts that are generated have the same alert ID and description.
- If the controller name is not displayed in the alert message, check the controller information for mapping the controller ID and controller name.
- **JIT-106295**: Critical and warning a lert is not displayed on Enhanced Event Message alert for Physical Device and Controller ID on Available Spare threshold.
- **JIT-103891**: Duplicate alerts for power supply removal are displayed while enclosure power supply cable is removed.
- **JIT-103962**: The Storage Management displays the removal and insertion alerts intermittently on EMM for HBA controllers during physical drive hot-plug-out and hot-plug-in.
- **JIT-104973**: On enhanced mode, an alert is displayed as A Device is inserted in the enclosure for both Power unit and FAN inserted into enclosure. The message does not state the specific device inserted.
- **JIT-106603**: On PowerEdge MX740c and MX840c, the sfcb core observes intermittently while I/O stress is taking place on VSAN which is created using MX5016s drives on systems running VMware Sphere ESXi 6.7 operating system.
- **JIT-97106**: You cannot create a partial RAID50 or a RAID60 virtual disk from IDRAC/HII. When the Foreign configuration drives are imported on the first RAID50 or RAID60 virtual disk with physical drive that is created on Storage Management.
- **JIT-103150**: On PowerEdge R940XA with dual backplane, the Storage tree does not display the Enclosure ID intermittently during insertion or removal of multiple drives.
  Workaround: Restart the Data-Manager service to resolve this discrepancy.
- **JIT-94890**: For fully populated chassis, the Storage Management system takes few minutes to load the storage components.
- **JIT-101739**: If an EMM is removed from MX5016s sled, EMM failure or removal alert is not observed on Server Administrator alerts.
- **JIT-108571**: Unable to display the dynamic hot-plug of enclosure with SAS 12 Gbps intermittently.
  Workaround: Restart the service, or reconnect the enclosure.
- **JIT-90125**: In Server Administrator while configuring the enclosure asset tag and name with maximum length , Server Administrator displays all the characters completely. But in iDRAC GUI, enclosure asset tag displays the last character as truncated.
- **JIT-109008**: Storage Management is enumerating more than one backplane that is not connected to SWRAID controller under SWRAID controller (S140) on PowerEdge R740xd2 system.
- **JIT-108897**: When maximum number of creations of virtual disk is reached in Storage Management, clearing the foreign configuration can be done only through system prompt.
- **JIT-109094, JIT-108567**: A delay of 10-15 minutes is observed initially for displaying Storage Management tree when degraded MX5016s or enclosure is present. The issue is observed only with HBA controllers like 12 GBPS HBA and HBA330 MMZ.
- **JIT-108844**: On Enhanced HBA mode, the controller displays for Manage Foreign Configuration operation both the online virtual disks and foreign virtual disks.
- **JIT-108887**: The alert log displays a message as XML not well-formed after a server restart and post controller mode change operation intermittently.
  Work-around: Clear Logs and restart the service.
- **JIT-105004**: The Physical attributes of SATA HDDs is not displayed when hotplugged into a system containing Dell FD33xD HBA or 12Gbps controllers.

- **JIT-109207**: Server Administrator displays incorrect capacity information of the drive when formatted with 4096 block size.
- **JIT-111297**: On Software RAID controller, Storage Management does not allow to expand the first Virtual Disk to maximum available drive space, if multiple the Virtual Disks are created on the same set of disks.

Installation Prerequisites

Storage Management does not display controllers and their features on systems that do not meet the driver and firmware requirements. At Storage Management runtime, you can determine whether the system meets the firmware requirement or not, by checking the application log files for notifications on outdated firmware. At runtime, On SCSI controllers, Storage Management displays the firmware version at runtime while on SAS controllers it displays the firmware and driver versions.

Installation Procedure

For complete installation instructions, see the *Dell EMC OpenManage Server Administrator version Installation Guide*.

This section provides information to enhance your experience with Server Administrator implementations and environments.

- Port 1311 is the default port for Server Administrator. It is a registered port number of Server Administrator. If another application is configured to run on port 1311 before Server Administrator is installed, the DSM SA Connection Service does not start after installation. Before you install Server Administrator, make sure that the port 1311 is not in use.
- Before starting Server Administrator, you must enable the client-side scripting in Internet Explorer.

  To do so, perform the following:

  a In Internet Explorer, navigate to the **Tools** menu.

  b Click **Internet Options**.

  c Click the **Security** tab.

  d Select the security zone to which the system running Server Administrator belongs.

  NOTE: This option should be set to Trusted sites.

  e Click the **Custom Level** button.

  f For Windows 2003, perform the following:

  1 In **Miscellaneous**, select the **Allow META REFRESH** radio button.

  2 In **Active Scripting**, select the **Enable** radio button.

  3 Under **Active scripting**, select the **Allow scripting of Microsoft web browser controls** radio button.

  g Click **OK** and restart your browser.
- To allow Single Sign-on for Server Administrator, perform the following steps:

  a In Internet Explorer, navigate to **Tools**.

  b Click **Internet Options**.

  c Click the **Security** tab.

  d Select **Trusted sites**.

  e Click the **Custom Level** button.

  f Under **User Authentication**, select the **Automatic Logon with current username and password**radio button. Click **OK** to exit the **Custom Level** window.

  g Select the **Advanced** tab and in **HTTP 1.1 settings**, make sure **Use HTTP 1.1** is checked.

  h Select **Trusted sites**. Click **Sites**. Add the server to the website.

  i Click **Close**.

  j Click **OK** and restart your browser.

- If you run a security scanner tool such as Nessus, against the Server Administrator Web server, security warnings may be displayed against port 1311, the port running the Server Administrator Web server. The warnings have been investigated by engineering and are determined to be "false positives" (invalid security warnings) that you can ignore. The following are the warnings:
  - The Web server on 1311 allows scripts to read the sensitive configuration and/or XML files.
  - The Web server on 1311 allows to delete "/" which implies that the web server will allow a remote user to delete the files in root on the server."
  - The web server on 1311 may be susceptible to a 'www Infinite Request' attack.
- It is possible to make the remote thttpd server execute arbitrary code by sending a request like: GET If-Modified-Since:AAA[...]AAAA

  Solution: If you are using thttpd, upgrade to version 2.0. Else, contact the vendor for a patch or change the web server. CVE on this one is CAN-2000-0359".
- Enabling Integrated Windows Authentication in Internet Explorer is not required to activate the Single Sign-On feature.
- The Server Administrator security settings are not applicable for Active Directory users. Active Directory users with read-only login can access Server Administrator, even if the access is blocked in the Server Administrator Preferences page.
- Dell SNMP MIB Files for Dell Systems:
- Dell SNMP MIB files for Dell systems allow you to obtain and verify information provided by supported software agents. The current MIB files supported by PowerEdge software agents are located at **\support\mib** on the *Systems Management Tools and Documentation* DVD.

  NOTE:
  A MIB-II-compliant, SNMP-supported network management station is required to compile and browse MIB files.

  OpenManage support for Encrypting File System (EFS)
- To improve security, Microsoft allows encrypting files using EFS. Note that SERVER ADMINISTRATOR will not function if its dependent files are encrypted.
- Server Administrator GUI and CLI Response Time
- On PowerEdge 10th generation of PowerEdge servers or later, the response time for some components of the Server Administrator GUI and CLI has increased to several seconds as Server Administrator does not cache some of the DRAC/iDRAC data. The data is retrieved from the DRAC/iDRAC when you request for it.

  Following are the Server Administrator GUI pages for which the response time may have increased:
  - Server Administrator home page on log in
  - **Remote Access** > **Users**
  - **Alert Management** > **Platform Events**
- Following are the Server Administrator CLI commands for which the response time may have increased:
  - omreport chassis remoteaccess config=user
  - omreport system platformevents
  - omreport system pedestinations

The amount of time varies depending on the hardware and operating system.

Firmware for PERC controllers

PERC H730P Adapter, PERC H730P Slim, PERC H730P Mini Blades, PERC H730P Mini, PERC H730 Adapter, PERC H730 Mini Blades, PERC H730 Mini, PERC H830 Adapter, PERC H330 Adapter, PERC H330 Mini, PERC H740P Adapter, PERC H740P Mini Monolithic, PERC H840 Adapter, PERC S140, PERC H330 Mini Blades, PERC H330 Embedded, HBA H330 Adapter, HBA H330 Mini, FD33XD-PERC Dual, FD33XS-PERC single and 12Gbps SAS HBA, HBA 330 MX, HBA 330 MMZ, PERC H745P MX, PERC H730P MX, FD33XD-HBA Dual, FD33XS-HBA single.

Table 3. Firmware for PERC controllers

Controller	Firmware/BIOS
PERC S130	4.1.0–0009
PERC S300	2.0.0-0166+00193000
PERC S140	5.1.0.0006
PERC H730P Adapter	25.4.0.0017
PERC H730P Mini Blades	25.4.0.0017
PERC H730P Mini	25.4.0.0017
PERC H730P Slim	25.4.0.0017
PERC H730 Adapter	25.4.0.0017
PERC H730 Mini 25.2.1.0011 Blades	25.4.0.0017
PERC H730 Mini	25.4.0.0017
PERC H830 Adapter	25.4.0.0017
PERC H330 Adapter	25.4.0.0017
PERC H330 Mini	25.4.0.0017
PERC H330 Mini Blades	25.4.0.0017
PERC H330 Embedded	25.4.0.0017
HBA 330 Adapter	09.17.20.07
HBA 330 Mini	09.17.20.07
FD33XD-PERC Dual	25.4.0.0017
FD33XS-PERC Single	25.4.0.0017
12Gbps SAS HBA	09.17.20.07

Table 4. Firmware for BOSS-S1 controller

Controller	Firmware/BIOS
BOSS-S1	2.3.13.1083

Microsoft Windows Drivers for PERC Controllers

Windows Drivers for PERC H310 Adapter,PERC H310 Mini Blades, PERC H310 Mini Monolithic, PERC H710 Adapter,PERC H710 Mini Blades, PERC H710 Mini Monolithic, PERC H710P Adapter,PERC H710P Mini Blades, PERC H710P Mini Monolithic, PERC H810 Adapter

Controllers, PERC H730P Adapter PERC H730P Mini Blades, PERC H730P Slim, PERC H730P Mini, PERC H730 Adapter, PERC H730 Mini Blades,PERC H730 Mini, PERC H830 Adapter, PERC H330 Adapter, PERC H330 Mini, PERC H330 Mini Blades, PERC H330 Embedded, HBA H330 Adapter, HBA H330 Mini, FD33XD-PERC Dual, FD33XS-PERC single and 12Gbps SAS HBA.

Table 5. Microsoft Windows drivers for PERC controllers

Controller	Windows Server 2019 Driver
PERC S300	2.0.0-0162
PERC S110	3.0.0.0134
PERC S130	4.2.0-0009
PERC H730P Adapter	6.600.55.00
PERC H730P Mini Blades	6.600.55.00
PERC H730P Mini Monolithic	6.600.55.00
PERC H730P Slim	6.600.55.00
PERC H730 Adapter	6.600.55.00
PERC H730 Mini Blades	6.600.55.00
PERC H730 Mini Monolithic	6.600.55.00
PERC H830 Adapter	6.600.55.00
PERC H330Adapter	6.600.55.00
PERC H330 Mini Monolithic	6.600.55.00
PERC H330 Mini Blades	6.600.55.00
PERC H330 Embedded	6.600.55.00
FD33XD- PERC Dual	6.600.55.00
FD33XS PERC Single	6.600.55.00
12Gbps SAS HBA	2.50.92.00
HBA 330 Adapter	2.50.92.00
HBA 330 Mini	2.50.92.00

Table 6. Windows Drivers for BOSS-S1 Controller

Controller	Windows Server 2019 Driver
BOSS-S1	1.2.0.1048

Installation and Configuration Notes

N/A