iDRAC9 Version 4.00.129.00

Release Notes

July 2020
Rev. A00

DELL EMC

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

Chapter 1: Release summary 6
Priority and recommendations 6

Chapter 2: Compatibility 7
License Requirements 7
Supported systems 7
Previous versions 7
Supported managed server operating systems and hypervisors 7
Supported web browsers 8
Supported software 8

Chapter 3: New and enhanced features 10
Features supported with Enterprise license 10
Features supported with all license levels 10
iDRAC and Lifecycle Controller firmware 10
Alerts and Monitoring 10
Security 10
Storage and Storage Controllers 10
GUI enhancements 11
API, CLI, and SCP 11

Chapter 4: Fixes 12
Hardware 12
iDRAC and LC firmware 12
Automation—API and CLI 12

Chapter 5: Deprecated features 13

Chapter 6: Important notes 14

Chapter 7: Known issues — To be fixed in future releases 17
Attributes for CNA cards not displayed through Redfish or RACADM interface 17
Rollback firmware Version is not displayed for NVDIMMs 18
Get method not displaying certificates after all certificates are deleted 18
iDRAC dashboard page in IE displays an expanded progress bar 18
Unable to create a recurring job after same recurring job was completed 18
Unable to create virtual disk through Redfish 18
SCP Import Job completes with error due to HddSeq error 19
iDRAC LC Log shows reset cause as 'watchdog' 19
Delayed response when iDRAC's network settings are reconfigured 19
Integrated/Embedded NIC displaying status as Unknown 19
No errors when the selected component and the selected device firmware do not match 20
SEL missed in the LCL during Racreset 20
PCIe SSD Backplane 2 is displayed as unknown 20

Firmware update operation not scheduled through WSMan.....20
Access to serial interface fails.....20
Delayed response when iDRAC's network settings are reconfigured.....21
iDRAC LC Log shows reset cause as watchdog.....21
Remote File Share (RFS) does not stay connected after downgrading iDRAC.....21
Boot Capture file does not have any content 21
LC log created after going to Virtual media page in iDRAC GUI.....21
Firmware update for a replaced PSU failing.....22
Device description and type not displayed.....22
Get method on UefiTargetBootSourceOverride attribute shows null value.....22
Sluggishness in Virtual Console.....22
Blank boot capture file generated.....22
Unable to export factory shipped inventory.....23
NIC or FC device slot listed in hardware inventory even when disabled in BIOS.....23
Get operation not displaying model or serial number for PCIe devices.....23
iDRAC DUP update fails on SLES when secure boot is enabled.....23
Boot mode error during OS deployment.....23
Repetitive PR7 messages related to PSU in LC logs after a system erase operation.....24
After a warm reboot, LC logs display Disk Inserted.....24
Header error while using Powershell for Redfish requests.....24
Port 5353 blocked by iDRAC internal firewall and appears as Open/Filtered.....24
Inlet temperature not reported for all PCIE slots.....24
Link Status displayed as Unknown.....25
RACADM inventory displaying incorrect Installation date for IDSDM.....25
BOSS-S1 sensor not listed in IPMI tool sensor list view.....25
Redfish GET method fails on the Storage Controller.....25

Chapter 8: Limitations.....26
Authentication.....26
Automation — API and CLI.....26
BIOS and UEFI.....27
Hardware.....27
iDRAC and LC firmware.....27
Monitoring and alerting.....27
Networking and IO.....28
OS deployment.....28
Security.....29
Storage and storage controllers.....29
SupportAssist and parts replacement.....29
Firmware and driver update.....29
Miscellaneous.....30

Chapter 9: Updating iDRAC firmware.....31
Downloading iDRAC firmware installation file.....31
Updating iDRAC firmware from host OS.....31
Updating iDRAC remotely using iDRAC web interface.....31

Chapter 10: Lifecycle Controller Remote Services — client tools.....33

Chapter 11: Resources and support.....34

Chapter 12: Contacting Dell EMC.....35

1

Release summary

The Integrated Dell Remote Access Controller (iDRAC) is designed to make server administrators more productive and improve the overall availability of Dell servers. This release adds few enhancements to PowerEdge XE2420.

Version

iDRAC9 4.00.129.00

Release date

July 2020

To download this version of iDRAC, see Downloading iDRAC firmware installation file on page 31.

NOTE: For details about the previous releases, if applicable, or to determine the most recent release for your platform, and for latest documentation version, see *KB article SLN308699* available at www.dell.com/support/article/sln308699.

Topics:

- Priority and recommendations

Priority and recommendations

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).

2

Compatibility

Topics:

- License Requirements
- Supported systems
- Previous versions
- Supported managed server operating systems and hypervisors
- Supported web browsers
- Supported software

License Requirements

iDRAC features are available based on the purchased license.

- iDRAC Express—Available by default on all blade servers, and rack or tower servers of 600 or higher series
- iDRAC Enterprise—Available on all servers as an upgrade
- iDRAC Secure Enterprise Key Manager(SEKM)—Only available on systems that are mentioned in the Supported Systems section

For more information about the features available for a license, see the iDRAC licenses section in the iDRAC 4.00.00.00 User's Guide available at dell.com/idracmanuals.

NOTE: To manage new and existing licenses, go to the Dell Digital Locker.

Supported systems

- PowerEdge XE2420

Previous versions

- 4.00.109.00

NOTE: Updating iDRAC firmware from a previous version such as 3.2x, 3.1x, 3.0x to the latest version is not supported. Update the firmware to version 3.30.30.30 first, and then update to version 4.00.00.00 or later.

Supported managed server operating systems and hypervisors

- Microsoft Windows
  - Server 2012 R2 Essentials
  - Server 2012 R2 Standard
  - Server 2012 R2 Datacenter
  - Server 2016 Essentials
  - Server 2016 Standard
  - Server 2016 Datacenter
  - Server 2019 Essentials
  - Server 2019 Datacenter
  - Server 2019 Standard
  - WinPE 5.0 64-bit
  - WinPE 10

- Linux
  - RHEL 8.0
  - RHEL 7.7
- SLES
  - SLES 15 SP1
- Ubuntu
  - Ubuntu 18.04.3
- VMware
  - ESXi 6.7 U3
  - ESXi 7.0

Supported web browsers

- Microsoft Internet Explorer 11
- Microsoft EDGE
- Safari 12.x
- Mozilla Firefox 64
- Mozilla Firefox 65
- Google Chrome 75
- Google Chrome 76

Supported software

Java

- Java - Oracle version

OpenSource tools

- OpenJDK 8u202
- Adopt Open JDK
- You may utilize the open source version of Open JDK ("Open JDK") subject to the terms and conditions of the Open JDK community at the link below.
- You use Open JDK at your own risk. Open JDK may not meet your requirements or expectations. It could include quality, technical or other mistakes, inaccuracies or typographical errors.
- Dell does not provide support or maintenance for Open JDK.
- Dell makes no express warranties, and disclaims all implied warranties, including merchantability, fitness for a particular purpose, title, and non-infringement as well as any warranty arising by statute, operation of law, course of dealing or performance or usage of trade regarding Open JDK.
- Dell has no liability to you for any damage that arise out of or relate to your use of Open JDK.

iDRAC tools

This version of iDRAC requires the following tools based on the operating system:

- Dell EMC iDRAC Tools for Microsoft Windows Server(R), v9.4.0
- Dell EMC iDRAC Tools for Linux, v9.4.0
- Dell EMC iDRAC Tools for VMware ESXi (R), v9.4.0

This version contains:

- Remote/Local RACADM on Windows or Linux or ESXi
- IPMI Tool on Windows or Linux

Download the DRAC tools from the **Drivers & downloads** page for your system at https://www.dell.com/support.

Before installing iDRAC tools from OM 9.4.0, you must uninstall any older versions of DRAC tools. For more information about uninstalling applications, see the documentation for your operating system.

3

New and enhanced features

- Improved iDRAC stability.

Topics:

- Features supported with Enterprise license
- Features supported with all license levels

Features supported with Enterprise license

- Multi Factor Authentication through email.
- Agent Free Crash Video Capture (Windows only).
- Connection View for LLDP transmit
- System Lockdown Mode - new icon in header available from any page
- Group Manager – 250 node support
- Enhanced support for Secure Enterprise Key Management (SEKM)
- Enable PERC to switch to SEKM security mode.

Features supported with all license levels

iDRAC and Lifecycle Controller firmware

- Added iDRAC support for PowerEdge XE2420
- Added thermal control and power management for DSS FE1 and EDSFF E.L SSD's in PowerEdge XE2420
- Added FRU support for DSS FE1

Alerts and Monitoring

- Alert on USB device insertion
- GPU inventory and monitoring
- Custom Sender Email Address for email alerts in SMTP configuration
- SMARTlogs in SupportAssist log collection for hard drives and PCIe SSD devices
- Display the output of SupportAssist Collector within the GUI
- Include Part Number of failed component in alert messages
- Capability for iDRAC to capture console redirection serial data for later retrieval
- iDRAC email alerting to work with cloud-based email servers

Security

- Up to five IP filtering ranges (using RACADM commands only)
- iDRAC user password maximum length increased to 40 characters.
- SSH Public Keys via Server Configuration Profile
- Customizable Security Banner to SSH login
- Force Change Password (FCP) feature for login

Storage and Storage Controllers

- Feature to enable PERC to switch to SEKM mode

GUI enhancements

- Job status section the dashboard
- Search box in the header
- Feature to collapse all the sub-headers

API, CLI, and SCP

- Operating system deployment by Server Configuration Profile (SCP)
- Enable and disable boot order control to SCP and RACADM
- Redfish APIs - See *iDRAC Redfish API Guide* available at www.dell.com/idracmanuals
- Option to change boot source state in SCP.
- Automation for command/attribute auto completion in RACADM
- Attribute IPVer for IP version in th list of I/O identity optimization attributes list

4

Fixes

Topics:

- Hardware
- iDRAC and LC firmware
- Automation—API and CLI

Hardware

- 150151: Fixed an issue that was causing high fan Pulse-width modulation(PWM) on PowerEdge R6525.
- 150394: Fixed an issue that was causing high fan revolutions per minute(RPM) on PowerEdge C6525 blades.
- 143092: Fixed an issue that caused a periodic input/output pause on PERC 9 controllers.

iDRAC and LC firmware

- 120813: Fixed an issue in IPMITool FRU list command, where Integrated PERC FRU was not getting displayed.
- 122565: Fixed an issue where the disk assignment was only reflecting after an iDRAC restart.
- 128920: Fixed an issue that was exceeding the on-screen timeout limit for Lifecycle Controller operations.
- 130475: Fixed an issue that was not allowing the firmware downgrade of storage controllers.
- 150842: Fixed an issue where some broadcast/ multicast packets caused iDRAC watchdog reboots.
- 148370: Fixed an issue that was leading to iDRAC Initialization failures on cold boot.
- 113901: Fixed an issue that was not detecting the storage devices in iDRAC.
- 120296: Fixed an issue that was allowing access to iDRAC Direct Port even after the port is turned off.
- 119161: Fixed an issue that was displaying different error messages in the SEL logs and LC logs.
- 118156: Fixed an issue that was displaying Persistent Memory after removing Apache Pass DIMM (AEP) after Resetting iDRAC and restarting the system simultaneously.
- 120534: Fixed an issue that was causing failure while setting Powercap values in Lockdown mode.
- 120820: Fixed an issue that was preventing iDRAC from detecting virtual disks in eHBA Mode during Warm Reboot job.
- 116586: Fixed an issue that was displaying unsupported RAID level while creating a virtual disk with controller in eHBA mode.
- 122290: Fixed an issue that was not reporting drive events when the drive sensors are disabled.
- 127197: Fixed an issue that was updating CPLD three times.
- 111379: Fixed an issue that was causing the vFlash initialization failure after iDRAC firmware was downgraded.

Automation—API and CLI

- 121111: Fixed an issue that was displaying incorrect time on the Legacy attribute System.Embedded.1#Diagnostics.1#OSAppCollectionTime.
- 119390: Fixed an issue that was causing an error while downloading DUP using Redfish interface.
- 122401: Fixed an issue that was causing failure while updating Redfish Simple Update Transfer Protocol.
- 119516: Fixed an issue that was displaying incorrect MaxReadingRange and MinReadingRange for Readingvolts attributes.

5

Deprecated features

The following table displays the features that are listed as Deprecated* or Removal**:

Features	iDRAC9	iDRAC9 x5
SM-CLP	Removal	Removal
VM CLI	Removal	Removal
VFlash	Deprecated	Removal
Backup and Restore	Deprecated	Removal
RBAP and Simple Identity profiles	Removal	Removal

Deprecated*-No longer being updated or new features added.

Removal**-Code has been removed, this feature is no longer functional.

6

Important notes

1. In LifeCycle Controller GUI, use mouse to browse files or folders. Keyboard navigation does not work while browsing files.
2. If the BIOS date and time are set incorrectly while resetting iDRAC to default settings, the iDRAC's IP address may be lost. Reset iDRAC or AC power cycling the server to recover iDRAC IP.
3. iDRAC GUI search output points to a GUI page where the search keywords are missing within the page. These are typical false positives like any other search engine that may be ignored.
4. While performing any method (GET/POST and so on) on an incorrect Dell specific URI, a proper extended error message specifying that "Resource URI is incorrect" is not provided in the response body.
5. PSU Part Replacement Firmware Update will not initiate if the secondary string of the new firmware is the same as the secondary string of replaced PSU's existing firmware. Firmware version string format is denoted as xx.yy.zz, where zz is the secondary string.
6. You may get an irrelevant response message while performing Poperating systemT method to Insertmedia with incorrect media for firmware upgradation or OS deployment.
7. While streaming telemetry reports for an older version of Rsyslog servers, the system may intermittently miss a few reported data. Upgrade the Rsyslog server to the latest version.
8. If a single DUP is used to update firmware for multiple devices, and if any one update fails then the firmware for the subsequent cards may display an incorrect version. Update the firmware for all the failed devices again.
9. SMART monitoring is disabled for a hard drive while it is set to Non-Raid mode.
10. In systems with network adapters without internal temperature sensors, for some adapters the NIC temperature sensors metric value is reported as 0.
11. After any iDRAC reset event, including the iDRAC firmware update, the LC Log event time is incorrectly reported for few events. This condition is momentary, and iDRAC time catches up to correct time.
12. Performing GET method on Steps only shows the next scheduled jobs and not the completed jobs.
13. If you install OMSA while iSM is already installed and connected, iSM may restart after the OMSA installation is complete.
14. After iDRAC is upgraded to version 4.00.00.00 for the first time, there may be a change in network settings option including IPv4 and IPv6. Reconfigure the network settings to resolve this.
15. After iDRAC is upgraded to version 4.00.00.00, you may stop receiving encrypted email alerts from iDRAC, if the external email server does not support encryption. iDRAC firmware version 4.00.00.00 introduces a user-selectable encryption option and the default protocol is StartTLS. To start receiving email messages again, disable the email encryption by using the following RACADM command:
    `racadm set idrac.RemoteHosts. ConnectionEncryption None`
16. Windows Server 2012, Windows Server 2008 R2, and Windows 7 do not support TLS 1.2 and TLS 1.1. Install the following update to enable TLS 1.2 and TLS 1.1 as a default secure protocols in WinHTTP in Windows: http://support.microsoft.com/kb/3140245/EN-US
17. The drivers that LC exposes are present in a read-only drive that is labeled OEMDRV and the drive is active for 18 hours. During this period:
    a. You cannot update any DUP.
    b. LC cannot involve CSIOR.

    However, if a server AC power cycle or iDRAC reboot is performed, the OEMDRV drive is automatically detached.
18. CPLD firmware update has no impact on Trusted Platform Module enablement.
19. Depending on the virtual storage device attached through iDRAC, that is, USB drive or CD/DVD .ISO file, LC displays Virtual Floppy or Virtual CD respectively.
20. If the network is not configured and you try to perform a network operation in LC, a warning message is displayed. When you go to the network settings page from this message, the left navigation panel on network settings page may not be displayed.
21. If a network operation fails for a valid address, try configuring the network settings again. If the issue persists, restart the system and retry the operation.
22. When you reset or update the iDRAC, you must reboot LC if it is launched already. If you do not reboot, LC may show unexpected behavior.
23. Fibre-channel NIC cards with dual or four ports are displayed as a single port card in LC. However, all ports are updated when a firmware update is performed.
24. The option to enable or disable the disk cache policy for SWRAID controllers are supported only on SWRAID controller driver version 4.1.0-0025 or later.
25. Rollback is not supported for CPLD and HBA controllers.
26. When CMCs are daisy chained, only the first CMC (CMC which is connected to Top of Rack switch) receives LLDP packets. Other CMCs do not receive LLDP packets. So, the iDRAC network port (dedicated mode) LLDP information is not available in the blades

whose corresponding CMC is not the first CMC in the daisy chain. The LLDP information is also not available for every CMC in the daisy chain that is not connected to TOR switch directly.

27. If any of the NVMe drives report a 'Failed' status (Red LED) due to any of NVMe controller SMART errors (critical warning bits set), it should be treated as a predictive failure (Blinking amber LED). These errors include SMART errors such as:
    a. Available spare threshold
    b. Reliability degraded
    c. Read-only mode
    d. Virtual memory backup failed, and so on.
28. This note is applicable only to PowerEdge C6420, DCS9650, DCS9670, and DCS9690 systems. If you update iDRAC to this version from version 3.02.x.x or earlier, you must perform a power cycle of the system before performing any power-related operations. The power cycle is required to tune the memory parameters without affecting the host. iDRAC tunes the memory parameters at the first power cycle after a firmware update. To allow the memory tuning to be completed:
    a. Update to this version of iDRAC.
    b. At the next possible maintenance cycle, or before any power operations are performed, power off the host.
    c. Wait for 2 minutes to allow iDRAC to reset and tune the memory parameters.
    d. Power on the host.
29. This note is applicable only to PowerEdge M640 and FC640. If you update iDRAC to this version, you must perform a virtual reseat of the system from CMC. Reseat is required to tune the memory parameters and to resolve issues that may lead to the watchdog timer causing iDRAC to be reset. To allow the memory tuning to be completed:
    a. Update to this version of iDRAC.
    b. At the next possible maintenance cycle, perform a virtual reseat.
30. After updating iDRAC Firmware to 3.30.30.30 from a previous version, the first inventory collection after system reboot may display both PR7 (New Device Detected) and PR8 (Device not detected) messages. This is an expected behavior that is caused by a change in the slot number display format.
31. Ensure that the SSH client is updated to the latest version. Following SSH configurations are no longer available on iDRAC:

    KEX algorithms:

    a. diffie-hellman-group14-sha1

    MAC:

    a. umac-64
    b. umac-64-etm@openssh.com
32. This note is applicable only to PowerEdge M640 and FC640. When performing BIOS Recovery operation, host may not turn on. To recover from this condition, do a virtual/physical reseat operation of the blade server.
33. After updating the iDRAC firmware, LC logs may display Message ID PR36 that "Version change detected for PCIe SSD firmware. Previous version:X.X.X, Current version:X.X.X." This is due to a change in the naming convention. Ignore the log entry.
34. After downgrading the iDRAC firmware to any previous versions, storage page and drives may display warnings. To resolve the issue, reset iDRAC using the 'racreset' command.
35. This note is applicable only to PowerEdge R540. While updating the BIOS firmware through local RACADM with local share, you may get an error "ERROR: RAC989: Unable to apply the BIOS_3P4XY_WN64_1.6.11.EXE firmware update." Use the direct DUP installation or installation through CIFS/NFS share to update the BIOS firmware.
36. If you get an error while performing SupportAssist collection through RACADM using HTTPS share, use the following commands to perform the collection:
    a. Racadm support assist collect.

    ```
    racadm supportassist collect -t Sysinfo
    ```

    b. Racadm SupportAssist exportlastcollection

    ```
    racadm supportassist exportlastcollection -l <https> -u <username> -p <password>
    ```
37. Features including Server Management Command Line Protocol (SMCLP) and Virtual Media Command Line Interface (VMCLI) will be deprecated in the later releases.
38. The LifeCycle Controller GUI features available on your system depends on the license installed. Some features that are mentioned in the GUI or documentation may be unavailable on your system.
39. For improved support on drives and operating system deployment, it is recommended to use the UEFI BIOS boot mode.
40. To create a virtual disk or deploy an operating system, ensure that you use the Dell supported SATA, SAS, or NVMe drives. For more information, see the documentation for BIOS, controller, and drive.
41. In the software inventory, the hash value for iDRAC firmware is displayed as NA instead of hash.
42. If SMBv2 share fails in Lifecycle GUI, ensure that:

- The **Digitally sign communications** option is disabled.
- Permissions to access the folder/file are granted.
- folder/file name does not have a space.
- Share contains fewer files and folders.

43. While iDRAC is initializing, all communications with iDRAC may fail. For any service requests, wait until the initialization process is complete.
44. Performing Redfish Patch method on Read-Only property for PowerControl resource returns a status code 200.
45. In iDRAC, if there is no link that is detected in the selected iDRAC port then the iDRAC IP is displayed as 0.0.0.0.
46. While performing a firmware update on a system where the operating system is installed with GNOME GUI enabled, system may get into Suspend mode. To avoid the system from going into suspend mode, ensure that you change the power settings in the operating system. To change the power settings:
    a. Go to Settings, and select Power.
    b. For the option, “When the Power Button is pressed” select Power Off.
47. Firmware update on drives and backplanes through Windows DUP will reflect in iDRAC after.

    A cold boot. In Lifecycle logs, version change may be displayed repeatedly if cold reboot.

    Is not done.
48. FRU objects or properties for Network adapters that are embedded on the motherboard are not available through any of the iDRAC interfaces.
49. Lifecycle Controller supports ISO images with ISO-9660 format only. Other formats including combination with ISO-9660 are not recommended.
50. UserDefined delay AC Recovery Power Delay is slow with lower limit of 60, but some conditions might cause BMC ready to be later than this and hence may not work. So, it is advised that the UserDefined delay be set to 80 s or higher. Any values less than this may cause the operation to fail.
51. The iDRAC feature “Topology LLDP,” is not supported on 1 GbE controllers and selects 10 GbE controllers (Intel X520, QLogic 578xx).
52. Mellanox network adapters that are used in PowerEdge MX740c and MX840c servers must be updated to version 14.23.10.20 or later, before updating the iDRAC firmware to version 4.00.00.00.
53. Install SEKM license before you update the iDRAC to SEKM supported version 4.00.00.00. If you install the SEKM license after updating the iDRAC to SEKM supported version, you have to reapply SEKM supported iDRAC firmware.
54. If you are configuring a Gemalto based KeySecure SEKM Server with iDRAC, and to get the redundancy feature functional, copy the certificates manually from primary Gemalto KeySecure cluster to secondary Gemalto SEKM KeySecure cluster. The redundance feature works after the iDRAC is set up for SSL certificate-based authentication.
55. Key sharing between multiple iDRACs is supported and can be configured on the SEKM server. Key sharing can be done if all the iDRACs are part of the same SEKM group and all keys are assigned to the same group with the right permissions.
56. When FCP is enabled, 'Default Password Warning' setting is disabled after the default user password is changed.
57. Firmware update from iDRAC versions earlier than version 3.30.30.30 is not supported (For example, updating iDRAC firmware from version 3.21.21.21 to version 4.00.00.00 is not supported). First update to version 3.30.30.30 or higher, and then initiate update to 4.00.00.00.
58. If system lockdown mode is enabled while a user is logged into LifeCycle Controller GUI, then lockdown mode will not be applicable on LifeCycle Controller.
59. Due to a DMTF tool limitation, the URIs for some OEM actions that are extensions to the DMTF schemas may not appear in the OpenAPI.YAML file.
60. The iDRAC Virtual Keyboard labeling is changed to upper case to align it with the physical keyboard layout.
61. Keyboard interactive authentication has been enabled on the iDRAC SSH Server to provide enhanced security. SSH clients now require both password authentication and keyboard interactive authentication to before logging in a user in to iDRAC.
62. If you see iSM0050 event in LC log, then ensure that you update the iDRAC Service Module (iSM) to version 3.4 or to a TLS-capable iSM. iSM without TLS capability is not supported on iDRAC firmware version 3.30.30.30 or later.

7

Known issues — To be fixed in future releases

Topics:

- Attributes for CNA cards not displayed through Redfish or RACADM interface
- Rollback firmware Version is not displayed for NVDIMMs
- Get method not displaying certificates after all certificates are deleted
- iDRAC dashboard page in IE displays an expanded progress bar
- Unable to create a recurring job after same recurring job was completed
- Unable to create virtual disk through Redfish
- SCP Import Job completes with error due to HddSeq error
- iDRAC LC Log shows reset cause as 'watchdog'
- Delayed response when iDRAC's network settings are reconfigured
- Integrated/Embedded NIC displaying status as Unknown
- No errors when the selected component and the selected device firmware do not match
- SEL missed in the LCL during Racreset.
- PCIe SSD Backplane 2 is displayed as unknown
- Firmware update operation not scheduled through WSMan
- Access to serial interface fails.
- Delayed response when iDRAC's network settings are reconfigured
- iDRAC LC Log shows reset cause as watchdog
- Remote File Share (RFS) does not stay connected after downgrading iDRAC
- Boot Capture file does not have any content
- LC log created after going to Virtual media page in iDRAC GUI
- Firmware update for a replaced PSU failing
- Device description and type not displayed
- Get method on UefiTargetBootSourceOverride attribute shows null value
- Sluggishness in Virtual Console
- Blank boot capture file generated
- Unable to export factory shipped inventory
- NIC or FC device slot listed in hardware inventory even when disabled in BIOS
- Get operation not displaying model or serial number for PCIe devices
- iDRAC DUP update fails on SLES when secure boot is enabled
- Boot mode error during OS deployment
- Repetitive PR7 messages related to PSU in LC logs after a system erase operation
- After a warm reboot, LC logs display Disk Inserted
- Header error while using Powershell for Redfish requests
- Port 5353 blocked by iDRAC internal firewall and appears as Open/Filtered
- Inlet temperature not reported for all PCIE slots
- Link Status displayed as Unknown
- RACADM inventory displaying incorrect Installation date for IDSDM
- BOSS-S1 sensor not listed in IPMI tool sensor list view
- Redfish GET method fails on the Storage Controller

Attributes for CNA cards not displayed through Redfish or RACADM interface

Description	If the partitions are disabled on FCoE capable CNA cards, few HII attributes values for WWN, VirtWWN, WWPN, VirtWWPN are displayed in the iDRAC GUI's Network page. However, the same data is not displayed when Get commands are performed in Redfish and RACADM interfaces.

Workaround	N/A
Systems affected	All systems supported by this release.
Tracking number	151560

Rollback firmware Version is not displayed for NVDIMMs

Description	After updating a NVDIMM component firmware with a new version, rollback option is not displayed.
Workaround	Restarting iDRAC to view the rollback firmware version.
Systems affected	All systems supported by this release.
Tracking number	153116

Get method not displaying certificates after all certificates are deleted

Description	After performing POST method ResetkeysType with DeleteAllleys option through Redfish interface, executing GET method is not listing the certificate URIs available for import.
Workaround	Use the RACADM interface.
Systems affected	All systems supported by this release.
Tracking number	152912

iDRAC dashboard page in IE displays an expanded progress bar

Description	While logging into iDRAC GUI on IE browser the progress bar may expand into a longer bar with more icons.
Workaround	Use another browser.
Systems affected	All systems supported by this release.
Tracking number	153331

Unable to create a recurring job after same recurring job was completed

Description	Creating a recurring job will fail if the same job was completed recently and its Task ID still exists.
Workaround	Wait for ten minutes for the Task ID to be deleted
Systems affected	All systems supported by this release.
Tracking number	147501

Unable to create virtual disk through Redfish

Description	On physical disks configured with software RAID, creating virtual disk is not supported in Redfish interface.
Workaround	Use any other iDRAC interface to create the VDs

Systems affected	All systems supported by this release.
Tracking number	153951

SCP Import Job completes with error due to HddSeq error

Description	In a system with BOSS card containing two M.2 SATA SSDs, if you export an SCP XML file and make some changes to the BIOS and NIC attributes before importing it, the import may fail with an error “HddSeq”.
Workaround	Configure the attribute using BIOS (F2) Page and set BIOS Boot-mode to UEFI mode before importing the file.
Systems affected	All systems supported by this release.
Tracking number	151725

iDRAC LC Log shows reset cause as ‘watchdog’

Description	Some of the log events in LC Log shows ‘The iDRAC firmware was rebooted with the following reason: Watchdog’. This happens when iDRAC recovers from an error that was captured error handler. This is part of iDRAC recovery mechanism.
Workaround	N/A
Systems affected	All systems supported by this release.
Tracking number	154238

Delayed response when iDRAC’s network settings are reconfigured

Description	When a Remote File Share is mounted on the iDRAC, changing network-related settings, or OS-BMC settings, on the iDRAC will take two minutes to apply. During this extended time, the iDRAC will not be reachable until after the reconfiguration is completed.
Workaround	Disconnect Remote File Share mounts before modifying network settings.
Systems affected	All systems supported by this release.
Tracking number	152168

Integrated/Embedded NIC displaying status as Unknown

Description	Systems with only Integrated/Embedded NIC may report the status as Unknown.
Workaround	Reboot the iDRAC or the host
Systems affected	All systems supported by this release.
Tracking number	151475

No errors when the selected component and the selected device firmware do not match

Description	While updating a component firmware using Component or Device update filter in OME-Modular, if the DUP device firmware selected is for another component, then the update goes through without any errors and device firmware for the relevant component is updated instead of the one selected.
Workaround	Use the firmware rollback option to downgrade the firmware to the previous version.
Systems affected	All MX platform systems supported by this release.
Tracking number	150783

SEL missed in the LCL during Racreset.

Description	During iDRAC reset, if SEL is getting logged, it might not be forwarded to LCL and its corresponding event is not forwarded to registered destination (SNMP, REDFISH, so on)
Workaround	If SEL is cleared, this issue will not be seen in the next Racreset.
Systems affected	All systems supported by this release.
Tracking number	154003

PCIe SSD Backplane 2 is displayed as unknown

Description	On the storage enclosure page, PCIe SSD Backplane 2 is displayed as unknown instead of showing the faulty physical drive. This issue is observed if there is any unsupported/unresponsive physical drive in the enclosure.
Workaround	Remove the unsupported/unresponsive physical drive from the enclosure and perform racadm racreset.
Systems affected	All root port attached NVMe configuration systems.
Tracking number	145300

Firmware update operation not scheduled through WSMan

Description	On Modular servers the firmware update operation on backplane cannot be scheduled through the WSMAN interface.
Workaround	Update firmware by using other interfaces such as GUI, LCUI, Redfish.
Systems affected	All modular systems supported by this release.
Tracking number	145300

Access to serial interface fails.

Description	The serial interface cannot be accessed with a user account that has Easy 2FA enabled. It is because the serial interface is an exempted interface which is not supported on Easy 2FA feature.
Workaround	Disable 2FA on user account, and retry the operation.
Systems affected	All systems supported by this release.
Tracking number	152106

Delayed response when iDRAC's network settings are reconfigured

Description	When a Remote File Share is mounted on the iDRAC, changing network-related settings, or OS-BMC settings, on the iDRAC will take two minutes to apply. During this extended time, the iDRAC will not be reachable until after the reconfiguration is completed.
Workaround	Disconnect Remote File Share mounts before modifying network settings.
Systems affected	All systems supported by this release.
Tracking number	152168

iDRAC LC Log shows reset cause as watchdog

Description	Some of the log events in LC Log shows 'The iDRAC firmware was rebooted with the following reason: Watchdog'. This happens when iDRAC recovers from an error that was captured error handler. This is part of iDRAC recovery mechanism.
Workaround	N/A
Systems affected	All systems supported by this release.
Tracking number	154238

Remote File Share (RFS) does not stay connected after downgrading iDRAC

Description	RFS does not stay connected after downgrading the iDRAC and user cannot reconnect and will not have access to the files mapped through RFS.
Workaround	Disable and re-enabling Virtual Media or restarting iDRAC
Systems affected	All modular systems supported by this release.
Tracking number	151995

Boot Capture file does not have any content

Description	Creating a job to change the BIOS configuration, and reboot host will generate an extra Boot Capture video file with no contents, in addition to a normal captured video. This empty file is due to the extra host power reset event while creating the boot video.
Workaround	Ignore the empty Boot Capture file.
Systems affected	All systems supported by this release.
Tracking number	152396

LC log created after going to Virtual media page in iDRAC GUI

Description	After navigating to the virtual media page, an LC log is created stating "The operation GetAttachStatus of the DCIM_OSDeploymentService was performed".
Workaround	No such operation is performed, ignore this log.
Systems affected	All systems supported by this release.

Tracking number	142442

Firmware update for a replaced PSU failing

Description	Unable to initiate the firmware update for a replaced PSU through Lifecycle Controller Option "Match firmware With Replaced Part", after the PSU was replaced with AC power off.
Workaround	Use the DUP method to update the PSU firmware or replace one PSU at a time to avoid system powering off.
Systems affected	All systems supported by this release.
Tracking number	149905

Device description and type not displayed

Description	In iDRAC GUI, device description and device type are not displayed in the Hardware Inventory page.
Workaround	Use any one of the following options to get the description and type: • Export the hardware inventory from iDRAC GUI • Hardware device FQDD • Device description is same as device title • Use the RACADM command racadm hwinventory
Systems affected	All systems supported by this release.
Tracking number	151796

Get method on UefiTargetBootSourceOverride attribute shows null value

Description	After performing Patch method on the attribute UefiTargetBootSourceOverride successfully, then the GET method on the attribute shows value as null.
Workaround	N/A
Systems affected	All systems supported by this release.
Tracking number	152088

Sluggishness in Virtual Console

Description	You may experience slight delay while accessing Virtual Console in Edge browser using HTML5 plug in.
Workaround	Use the Java plug in, or use other browser such as Firefox, Chrome, or Internet Explorer.
Systems affected	All systems supported by this release.
Tracking number	152306

Blank boot capture file generated

Description	While creating a job to update the BIOS configuration, if the host system is rebooted, then in addition to the normal captured video file an extra boot capture file gets created with no content.
Workaround	Ignore the blank Boot Capture file.
Systems affected	All systems supported by this release.
Tracking number	152396

Unable to export factory shipped inventory

Description	In Lifecycle GUI, Export Factory Shipped Hardware Inventory to a Network Share (CIFS/NFS/HTTP/HTTPS) fails with a critical error message.
Workaround	Export the inventory to a USB Drive.
Systems affected	All systems supported by this release.
Tracking number	152692

NIC or FC device slot listed in hardware inventory even when disabled in BIOS

Description	For some NIC or FC cards, even when the device slot is disabled in BIOS, the slot may still get listed in the hardware inventory.
Workaround	N/A
Systems affected	All systems supported by this release.
Tracking number	104535

Get operation not displaying model or serial number for PCIe devices

Description	If you perform a Get operation for a PCIe device using Redfish API, the response may not display the model and serial number of the device.
Workaround	N/A
Systems affected	All systems supported by this release.
Tracking number	111564

iDRAC DUP update fails on SLES when secure boot is enabled

Description	On the SLES OS version 15 while secure boot enabled, if you perform iDRAC DUP update, it fails with an error "This Update Package is not compatible with your system."
Workaround	For iDRAC DUP updates, use other interfaces such as iDRAC GUI, RACADM, or WSMAN.
Systems affected	All systems supported by this release.
Tracking number	113574

Boot mode error during OS deployment

Description	While deploying OS using LC UI, if the current boot mode is set to UEFI and you change the boot mode to BIOS and click Finish on the last LC UI page, an error is displayed stating that the boot mode could not be set. The system reboots after you click OK. However, on next boot to LC UI, the boot mode is changed to BIOS and the boot device selected during OS deployment is discarded.
Workaround	Before deploying OS using LC UI, change the boot mode to BIOS from BIOS setup (F2 at POST).
Systems affected	All systems supported by this release.
Tracking number	98665

Repetitive PR7 messages related to PSU in LC logs after a system erase operation

Description	When the system is powered on manually after performing a system erase on LC data, several messages are displayed in LC logs for PSU stating “PR7 New device detected: POWER SUPPLY (PSU.Slot.X)”.
Workaround	N/A
Systems affected	All systems supported by this release.
Tracking number	129440

After a warm reboot, LC logs display Disk Inserted

Description	After performing a server warm reboot, iDRAC may report Disk Inserted in LC logs for drives behind HBA. Please ignore the log entry.
Workaround	N/A
Systems affected	All systems supported by this release.
Tracking number	144819 and 141414

Header error while using Powershell for Redfish requests

Description	iDRAC REST API with Redfish displays an error stating unacceptable header specified in request for commands that run on PowerShell. Unlike other REST API tools such as Python, CURL and Postman, the PowerShell Invoke-WebRequest command does NOT automatically add a header to REST requests. The header must be explicitly included by the programmer.
Workaround	You need to explicitly include a header while using Powershell for any type of Redfish request.
Systems affected	All system supported by this release.
Tracking number	N/A

Port 5353 blocked by iDRAC internal firewall and appears as Open/Filtered

Description	When node-initiated discovery or Group Manager is enabled, iDRAC uses mDNS to communicate through port 5353. However, when both are disabled, port 5353 is blocked by iDRAC's internal firewall and appears as Open/Filtered port in the port scans.
Workaround	Group Manager and node initiated discovery need to be turned off in order to disable mDNS.
Systems affected	All system supported by this release.
Tracking number	NA

Inlet temperature not reported for all PCIE slots

Description	In PCIE airflow settings on iDRAC GUI, Inlet temperature is zero for all the PCIE slots.
Workaround	N/A
Systems affected	PowerEdge XE2420
Tracking number	168674

Link Status displayed as Unknown

Description	After NIC firmware is updated, the Link Status is displayed as Unknown on iDRAC GUI and an LC Log is created as "The data communication with the device NIC is lost". Ignore the log entry.
Workaround	Reboot the iDRAC.
Systems affected	PowerEdge XE2420
Tracking number	169345/168980

RACADM inventory displaying incorrect Installation date for IDSDM

Description	Installation date for IDSDM is displayed incorrectly in RACADM inventory.
Workaround	N/A
Systems affected	PowerEdge XE2420
Tracking number	169803

BOSS-S1 sensor not listed in IPMI tool sensor list view

Description	BOSS-S1 sensor is not appearing in IPMI tool sensor list view.
Workaround	N/A
Systems affected	PowerEdge XE2420
Tracking number	169145

Redfish GET method fails on the Storage Controller

Description	GET method fails on the Storage Controller instance.
Workaround	Use the other iDRAC interfaces to access Storage Controller information.
Systems affected	PowerEdge XE2420
Tracking number	169146

8

Limitations

Topics:

- Authentication
- Automation — API and CLI
- BIOS and UEFI
- Hardware
- iDRAC and LC firmware
- Monitoring and alerting
- Networking and IO
- OS deployment
- Security
- Storage and storage controllers
- SupportAssist and parts replacement
- Firmware and driver update
- Miscellaneous

Authentication

1. LC supports the following characters for username and password:
   - Alphabets (a-z, A-Z)
   - Numbers (0-9)
   - Special characters (-, _, .)
2. If there are no slots available to add a new user in iDRAC, the Group Manager Job for `Add New User` shows a failure with error `GMGR0047`. Use the web interface (**iDRAC Settings** > **Users**) to verify the number of iDRAC local users.
3. If the user does not exist on a specific iDRAC, Group Manager Jobs for `Change User Password` and `Delete User` show a failure with error `GMGR0047`. Use the web interface (**iDRAC Settings** > **Users**) to verify that the user exists.

Automation — API and CLI

1. Sometimes, when using WSMan, an Internal SSL Error is reported and the WSMan command fails. If this issue occurs, retry the command.
2. Using WSMan, the attribute *LCD.ChassisIdentifyDuration* cannot be set to **`-1 (indefinite blink)`**. To make the LED blink indefinitely, use the `IdentifyChassis` command with **`IdentifyState=1`**.
3. RACADM supports the underscore character (_) for `iDRAC.SerialRedirection.QuitKey` along with the existing symbols shown in the integrated help.
4. Using remote RACADM, if you use the `racadm hwinventory export` command to export the hardware inventory using an incorrect CIFS share, an incorrect message is displayed: `RAC930 : Unable to export the hwinventory`. If the issue persists, restart iDRAC and retry the operation after iDRAC has finished restarting.
5. If iDRAC is in lockdown mode and you run the command 'racadm rollback', followed by the command 'racadm resetcfg', an incorrect message is displayed: `ERROR: A firmware update is currently in progress. Unable to reset the RAC at this time`. Reboot iDRAC to display the correct error message.
6. While using a `Top` or `Skip` command, if you enter a value greater than the unsigned long type (4,294,967,295), you may get an incorrect error message.
7. You cannot use the FQDD of iDRAC (iDRAC.Embedded.1) when changing iDRAC mode from Shared LOM to Dedicated.

BIOS and UEFI

1. When setting the iDRAC Service Module (iSM) monitoring attributes from the web interface, if the BIOS watchdog timer is enabled, an error may be displayed but the attributes are set. To avoid the error, disable the BIOS watchdog timer or disable the iSM Auto System Recovery and then apply the attributes.

Hardware

1. In LC, not all the vendor FC cards are supported for VLAN configuration.
2. If an H730P adapter is installed in slot 9 (internal PERC slot) of PowerEdge T640, iDRAC displays it as H730P Integrated RAID Controller (Embedded).

iDRAC and LC firmware

1. Due to known limitations in OpenSource (SFCB), query filtering with long integers and lengthy strings may not work as expected.
2. LC can import and view an iDRAC license but cannot export or delete the iDRAC license. The iDRAC license can be deleted from iDRAC web interface.
3. The iSCSI offload attribute can be enabled only on two of the four available ports. If a card, which has this attribute that is enabled on two of its ports, is replaced with another card that has the attribute that is enabled on the other two ports, an error occurs. The firmware does not allow the attribute to be set because it is already set on the other two ports.
4. The "Discovered Servers" view of Group Manager may not show available iDRACs as available to onboard. Verify that the iDRACs are on the same link local network and not separated by a router. If they are still not visible, reset the Group Manager's controlling iDRAC.
   a. Open Group Manager on one of the member iDRACs.
   b. In the search box, type the controlling system's Service Tag.
   c. Double-click the iDRAC that matches the search results and go to iDRAC Settings -> Diagnostics.
   d. Select Reset iDRAC.

   When iDRAC fully restarts, Group Manager should see the new iDRAC.
5. If Emulex LightPulse LPe31002-M6-D and Emulex LightPulse LPe35002-M2 FC adapters are configured to boot from FC storage arrays using VAM method in iDRAC, then a maximum of two boot target arrays can be configured instead of eight.
6. During import server profile operation, if the image filename is "Backup.img", operation may fail. To avoid this failure, change the filename.

Monitoring and alerting

1. In certain cases, Group Manager Jobs view may not show a detailed error message for a member iDRAC job. For more information about the failure, review the job execution details in the Lifecycle Logs of the member iDRAC by using the web interface (**Maintenance** > **Lifecycle Log**) or by using the RACADM command `racadm lclog view`.
2. PCIe SSDs in NVMe RAID mode may not display the updated state due to predicted failure. To update RAID-related information, ensure that a CSIOR is performed.
3. If the LCD display is blank, press any one of the three LCD buttons to turn on the LCD before inserting a USB storage device.
4. If Flex Address is enabled on Chassis Management Controllers (CMC), iDRAC and LC do not display the same MAC addresses. To view the chassis-assigned MAC address, use the iDRAC web interface or the CMC web interface.
5. The inventory displayed in LC UI may not be the same as that of any iDRAC interfaces. To get the updated inventory, run the CSIOR, wait for 2 minutes, reboot the host, and then check the inventory in LC UI.
6. In certain cases, in Group Manager Jobs view, the completion percentage for a job may be displayed incorrectly (>100%) for a job in progress. This is a temporary condition and does not affect how Group Manager jobs are performed. When the job is completed, Group Manager Jobs view displays **Completed successfully** or **Completed with errors**.
7. While running host stress test, if the system ID/Health LED turns off from blue, then press the ID button for a second and press it again to turn on the LED.
8. When setting the iDRAC Service Module (iSM) monitoring attributes from the web interface, if the BIOS watchdog timer is enabled, an error may be displayed but the attributes are set. To avoid the error, disable the BIOS watchdog timer or disable the iSM Auto System Recovery and then apply the attributes.
9. iDRAC supports iSM version 3.4.1 and above.

Networking and IO

1. While performing any network operation, LC may go into an infinite loop if there are network glitches, leaks, or packet loss. Restart LC and retry the operation with the correct NFS share name details.
2. If NPAR is enabled, LC might show unexpected behavior when configuring network settings. Disable NPAR and execute the network setting configurations. To disable the NPAR option, go to **System Setup** > **Device Setting**.
3. When NPAR is enabled, the port numbers displayed on the LC **Network Settings** page (**Settings** > **Network Settings**) do not match the port numbers displayed on the **Device Settings** page (**System Setup** > **Advanced Hardware Configuration** > **Device Settings**).
4. When Virtualization Mode is set to NPAR for network adapters that support the partitioning feature, *PartitionState* attribute can only be used for checking the state of partitions created for base partition in WSMan enumeration. You can see the states of all the partitions by pressing F2 during POST and going to **Device Setting**.
5. The process of retrieving IPv6 address from the DHCP server with VLAN connection takes a few minutes. Wait for a few minutes and check the **Network Settings** page to view the assigned IPv6 address.
6. Network operations such as Update, Export, or Import may take more time than expected. The delay may occur because the source or destination share is not reachable or does not exist, or due to other network issues.
7. LC does not support SOCK4 proxy with credentials.
8. LC UI supports share names and file paths that are up to 256 characters long. However, the protocol you use may only allow shorter values for these fields.
9. Because of internal UEFI network stack protocol implementation, there may be a delay while opening the LC UI **Network Settings** page or while applying the network setting.
10. Before performing any network operations, verify that the network is configured with the network cable connected. In some scenarios, a warning message may not be displayed but the operation may fail. Following are some examples that may lead to failure:
    - Static IP is configured without the network cable being connected.
    - Network cable is disconnected.
    - After a Repurpose and Retire operation is performed.
    - Network is configured with the network cable connected but the network card is replaced later.
11. Any changes to the network settings in iDRAC take effect after 30 seconds. Any automation or user verification needs to wait for 30 seconds before verifying the new settings. iDRAC returns the old active value until the new values take effect. Any DHCP settings may take more time (>30 seconds) depending on the network environment.
12. When trying to save network details using the Network Configuration page of LC UI, the following error message may be displayed: `Unable to save the IPvX network settings`, where **x** is the version of IP (IPv4 or IPv6). The following could be one reason for this error:

    On the Network Settings page of Lifecycle Controller GUI, the IP Address Source for both IPv4 and IPv6 is either DHCP or Static and DHCP is selected by default. So, even if you want to use only one version of IP address, LC tries to validate both versions, and displays an error if the network details for the unintended version cannot be validated.

    If the error does not apply to the IP version you are using, click OK to close the error message. All the other settings that you configured are saved. You can either click Cancel or Back to navigate away from the Network Settings page.
13. If the Gateway IP is not configured in a network, the network settings and operations in LC UI may show some unexpected behavior.

OS deployment

1. Operating system installation fails when the OS media volume name (label) is blank. Recommendation is to add a valid volume name for OS media (USB drive, DVD and so on) before starting the OS installation.
2. While installing SUSE Linux Enterprise Server (SLES) operating system, a media verification warning message may be displayed. This has no impact on the installation, to proceed, click **Yes**.
3. Windows operating system deployment may intermittently fail with the following error message:

    ```
    A required CD/DVD drive device driver is missing. If you have a driver  floppy disk, CD,
    DVD, or USB drive, please insert it now.
    ```

    Reboot to LC and retry until the operating system is successfully deployed.
4. Deployment of Windows Server operating systems (OS) using LC may fail with one of the following messages:
    - Windows installation cannot continue because a required driver could not be installed
    - Product key required
    - Windows cannot find the software license terms

This issue occurs when the Windows setup copies the driver to the scratch space (X: drive) and the scratch space becomes full. To resolve this issue, do any of the following:

- Remove all the installed add-on devices before starting the OS installation. After the OS installation is complete, connect the add-on devices and manually install the remaining drivers using Dell Update Packages (DUPs).
- To avoid physically removing the hardware, disable the PCIe slots in the BIOS.
- Increase scratch space size beyond 32 MB using `DISM set-scratchspace` command when creating customized deployment. For more details, see Microsoft's documentation.

5. LC may display multiple drive names for some CDs or DVDs, such as the ones containing operating systems.
6. If the operating system (OS) selected for installation and the OS on the media used are different, LC displays a warning message. However, while installing Windows OS, the warning message is displayed only when the bit count (x86 or x64) of the OS does not match. For example, if Windows Server 2008 x64 is selected for installation and Windows Server 2008 x86 media is used, the warning is displayed.
7. In Windows10, HTML5 plug-in does not support Virtual media connection on the following versions of Edge browsers:
   a. Microsoft Edge 44.17763.1.0
   b. Microsoft EdgeHTML 18.17763

Security

1. Cryptographic Erase operation is not supported for hot-plugged NVMe disks. Reboot the server before starting the operation. If the operation continues to fail, ensure that CSIOR is enabled and that the NVMe disk is qualified by Dell EMC.

Storage and storage controllers

1. While renaming a virtual disk (VD), using a . (period) is not allowed in the VD name.
2. If your system has a PERC card configured in Enhanced HBA mode and you downgrade iDRAC to an older version, the SET commands for storage configuration may fail. To resolve the issue, ensure that a Collect System Inventory On Reboot (CSIOR) is performed after the downgrade. To perform a CSIOR, use the following methods:
   a. Completely turn off the system and then turn it on again.
   b. Ensure that CSIOR is enabled before turning off the system.
   c. Use the following RACADM command: racadm serveraction powercycle
3. Few legacy drives do not support the SMART ID #245 "Remaining Rated Write Endurance". In such cases, iDRAC interfaces may display the "Remaining Rated Write Endurance" attribute as unavailable.

SupportAssist and parts replacement

1. Part-replacement of BOSS-S1 controller is not detected by Lifecycle Controller. After replacing the controller, follow the instructions in the controller's documentation.

Firmware and driver update

1. After an iDRAC reset or firmware update operation, the *ServerPoweredOnTime*—a property in RACADM and WSMan—may not be populated until the host server is restarted.
2. Some of the supported components may not be displayed on the **Firmware Update** > **View Current Versions** page. To update this list, restart the system.
3. If the iDRAC firmware update is interrupted, you may have to wait up to 30 minutes before attempting another firmware update.
4. Firmware update is supported only for LAN on Motherboards (LoM), Network Daughter Cards (NDC), and network adapters from Broadcom, QLogic, and Intel, and some of the QLogic and Emulex fiber channel cards. For the list of supported fiber channel cards, see the *Lifecycle Controller User's Guide* available at www.dell.com/idracmanuals .
5. After the CPLD firmware is updated on modular systems, the firmware update date is displayed as 2000-01-01 on the View Current Versions page. The update date and time is displayed according to the time zone configured on the server.
6. On some modular systems, after a firmware update, the Lifecycle Log displays the time-stamp as 1999-12-31 instead of the date on which the firmware update was performed.
7. It is not recommended to perform CPLD update along with other updates. If a CPLD update is uploaded and updated along with other updates using iDRAC web interface, CPLD update completes successfully but the other updates do not take effect. To complete the iDRAC updates, reinitiate the updates.

Miscellaneous

1. You may be unable to scroll using the keyboard. Use the mouse to scroll.
2. Due to a limitation of Google Chrome browser, HTML5 virtual console intermittently displays the following error message:

```
Chrome ran out of memory while trying to display the webpage.
```

3. When accessing the iDRAC web interface for the first time using Google Chrome version 59.0, the mouse pointer may not be visible. To display the mouse pointer, refresh the page or use Google Chrome version 61.0 or later.
4. If you use the HTML5 plug-in on Chrome version 61.0 to access Virtual Console, you cannot connect to Virtual Media. To connect to Virtual Media using the HTML5 plug-in, use Chrome version 63 or later.
5. Launching Virtual Console with Java plug-in fails after the iDRAC firmware is updated. Delete the Java cache and then launch the virtual console.
6. A Serial-On-Lan (SOL) session that has been active for more than five days or multiple reboots may get terminated automatically. If the session terminates, you must reinitiate the session.
7. Due to an issue with Safari, if an ipv6 literal address is used to log into the Web GUI, Safari is not able to launch the HTML5 based vConsole. Alternative options are to use Java based vConsole, or HTML5 vConsole by using the corresponding DNS name or by using an alternate browser in Mac OS.
8. iDRAC login page does not allow password entry using Firefox browser in Ubuntu management OS.
9. iDRAC and LC features cannot access CIFS or Samba shares when only SMBv1 protocol is enabled. All iDRAC features work with SMBv2 protocol. For information on enabling SMBv2 protocol, see the documentation for your operating system.
10. In Lifecycle Controller GUI, using keyboard to browse folders and files is not supported. Use the mouse to navigate through files and folders.

9

Updating iDRAC firmware

Topics:

- Downloading iDRAC firmware installation file
- Updating iDRAC firmware from host OS
- Updating iDRAC remotely using iDRAC web interface

Downloading iDRAC firmware installation file

About this task

NOTE: For information about updating iDRAC firmware using various interfaces, see the *iDRAC User's Guide* available at www.dell.com/idracmanuals .

Steps

1. Go to https://www.dell.com/support.
2. In the **Enter a Service Tag, Serial Number...** field, type the Service Tag or the model number of your server, and press Enter or click the search icon.
3. On the product support page, click **Drivers & downloads**.
4. Select the appropriate operating system.
5. From the list, locate the iDRAC entry and click the download icon.

Updating iDRAC firmware from host OS

From the host operating system, execute the installation package that you downloaded and follow the instructions of the update wizard.

For more information about opening executable files on your system, see the operating system's documentation.

Updating iDRAC remotely using iDRAC web interface

About this task

You can remotely update the firmware from the management stations using the iDRAC web interface.

Steps

1. Extract the self-extracting installation package to the management station.
2. Access the iDRAC web interface using a supported web browser.
3. Log in as an administrator.
4. Click **Maintenance** > **System Update**.
   The **Manual Update** page is displayed.
5. Select **Local** to upload the firmware image from the local system.
6. Click **Browse**, select the .d9 file that you extracted or the Dell Update Package for Windows, and click **Upload**.
7. Wait for the upload to complete. After the upload is complete, the **Update Details** section displays the uploaded file and the status.
8. Select the firmware file and click **Install**.
   The message `RAC0603: Updating Job Queue` is displayed.
9. To view the status of the firmware update, click **Job Queue**.

Results

After the update is complete, iDRAC restarts automatically.

10

Lifecycle Controller Remote Services — client tools

OpenWSMAN CLI

OpenWSMAN CLI is an open source Linux WSMan client. You can use OpenWSMAN CLI to send WSMan commands to Lifecycle Controller.

OpenWSMAN CLI source code and installation details are available at sourceforge.net/projects/openwsman/files/wsmancli.

Sample OpenWSMAN CLI Command for an enumeration operation:

```
wsman enumerate http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_SystemView
-h (idrac ip address) -P 443 -u (idrac user) -p (idrac password) -v -j utf-8
-y basic -R -o -m 256 -N root/dcim -c cert_name.cer -V
```

NOTE: Lifecycle Controller uses a self-signed certificate for HTTPS (SSL) communication.

Self-signed certificates are not accepted by the OpenWSMAN CLI client and WSMan commands do not work without these options: -c, -v, and -V. See the OpenWSMAN CLI Readme for details about these options.

11

Resources and support

For more information about the features of this release, see the documentation for iDRAC 4.00.00.00.

Latest Release Notes

To access the latest Release Notes for this version of iDRAC:

1. Go to www.dell.com/idracmanuals.
2. Click the link for the generation and then click the firmware series of iDRAC.
3. Click **DOCUMENTATION**.
4. Click **MANUALS AND DOCUMENTS**.

Accessing documents using direct links

You can directly access the documents using the following links:

Table 1. Direct links for documents

URL	Product
www.dell.com/idracmanuals	iDRAC and Lifecycle Controller
www.dell.com/cmcmanuals	Chassis Management Controller (CMC)
www.dell.com/esmmanuals	Enterprise System Management
https://www.dell.com/serviceabilitytools	Serviceability Tools
www.dell.com/omconnectionsclient	Client System Management

Accessing documents using the product search

1. Go to https://www.dell.com/support.
2. In the **Enter a Service Tag, Serial Number...** search box, type the product name. For example, **`PowerEdge`** or **`iDRAC`**.

   A list of matching products is displayed.
3. Select your product and click the search icon or press enter.
4. Click **DOCUMENTATION**.
5. Click **MANUALS AND DOCUMENTS**.

Accessing documents using product selector

You can also access documents by selecting your product.

1. Go to https://www.dell.com/support.
2. Click **Browse all products**.
3. Click the desired product category, such as Servers, Software, Storage, and so on.
4. Click the desired product and then click the desired version if applicable.

   NOTE: For some products, you may need to navigate through the subcategories.
5. Click **DOCUMENTATION**.
6. Click **MANUALS AND DOCUMENTS**.

12

Contacting Dell EMC

Dell EMC provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell EMC for sales, technical support, or customer service issues, see www.dell.com/contactdell.

If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or the product catalog.