

iDRAC9 Version 4.40.29.00

Release Notes

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.

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.....	8
Supported web browsers.....	8
Supported software.....	8
Chapter 3: New and enhanced features.....	10
Hardware.....	10
Chapter 4: Fixes.....	11
Chapter 5: Deprecated features.....	12
Chapter 6: Important notes.....	13
Chapter 7: Known issues — To be fixed in future releases.....	17
Windows key not responding.....	18
LC logs reporting NIC link issues.....	18
Firmware update completed with errors.....	18
Firmware rollback failing for NIC cards	19
RAID operation failing	19
Chassis PSU firmware update fails.....	19
Sled not powering on with OME Modular in optimized mode.....	19
iDRAC unable to obtain the current time after reboot.....	19
Server stops responding during POST with Config Error.....	20
OME-M Deployment and Configuration Job Fails with Error LC063.....	20
Unable to generate CSR through Redfish.....	20
vFlash detaching after iDRAC firmware update.....	20
Unable to apply VAM properties.....	20
MAC identities displayed in RESERVED state.....	21
SEL events may not be correctly displayed in the earlier versions of iDRAC.....	21
LC logs display Version change for Disks.....	21
Telemetry data Disabled without confirmation.....	21
WWN details for the Mezz cards displayed randomly in the WWN/MAC GUI page.....	21
CPU information missing under Hardware Inventory.....	22
Storage Devices displayed in gray text.....	22
Backplane Rollback contents not populating in iDRAC.....	22
Test network connection fails.....	22
MetricReport output does not match the DMTF schema.....	22

Service Validator reporting errors for Redfish API services.....	23
Lifecycle Controller fails to resolve IPv6 DNS addresses.....	23
Performing GET with Top query parameter returns no error.....	23
Server Configuration Profile import job fails.....	23
Unable to add iDRAC Static IP.....	24
Creating virtual media image takes longer on safari browser.....	24
iDRAC displays warning message for different plug-in selection.....	24
Bootimg with ISO image fails from iDRAC Virtual Console.....	24
Virtual Console gets disconnected while trying to launch multiple Virtual Console sessions.....	24
iDRAC Virtual Console entering Connecting Viewer state.....	25
Virtual Keyboard not working.....	25
Read-only user Virtual Console session disconnects.....	25
Template deployment job fails.....	25
Deleting multiple jobs results RAC0519 LCL event.....	25
PR1 & PR10 Lifecycle logs displayed during Retire and Repurpose operation.....	26
CPU PPIN in Hardware inventory in iDRAC GUI shows as “Not Supported”.....	26
Virtual Media performance is degraded with QLogic 25G OCP.....	26
iDRAC time fails to synchronize when Server Configuration Profile is imported with SNTP settings.....	26
Virtual console display in iDRAC GUI is blurred.....	27
Firmware version change displayed multiple times in Lifecycle log for PCIe SSDs.....	27
Few Virtual Keyboard keys not working for other languages.....	27
Deleting VD creates pending operation with empty data.....	27
DellCertificateCollection URI response not according to DMTF standards.....	28
Disabling local server video attribute in iDRAC virtual console not supported on C6400 and C6525	28
Field required displayed in Internet Explorer browser.....	28
Firmware update using pud method failing.....	28
iDRAC DUP update fails in Linux operating systems when secure boot is enabled	28
Uploaded firmware link not available in the SoftwareImages property in Redfish.....	29
PCIe types and lanes information not getting populated using Redfish.....	29
iDRAC reboots while collecting SupportAssist logs.....	29
SupportAssist collection failing.....	29
SupportAssist collection job creation fails.....	29
Webserver restarts after remote presence port number is updated.....	30
Getting an error SWC0018 during OS installation	30
WSMan query with space between attributes fails.....	30
Attributes for CNA cards not displayed through Redfish or RACADM interface.....	30
Get method not displaying certificates after all certificates are deleted.....	31
Unable to create a recurring job after same recurring job was completed.....	31
iDRAC LC Log shows reset cause as ‘Internal Error’.....	31
Firmware update operation not scheduled through WSMAN.....	31
Access to serial interface fails.....	31
LC log created after going to Virtual media page in iDRAC GUI.....	32
NIC or FC device slot listed in hardware inventory even when disabled in BIOS.....	32
Get operation not displaying model or serial number for PCIe devices.....	32
Boot mode error during OS deployment.....	32
Repetitive PR7 messages related to PSU in LC logs after a system erase operation.....	33
After a warm reboot, LC logs display Disk Inserted.....	33
Chapter 8: Limitations.....	34
Authentication.....	34

Automation — API and CLI.....	34
BIOS and UEFI.....	34
Hardware.....	35
iDRAC and LC firmware.....	35
Monitoring and alerting.....	35
Networking and IO.....	36
OS deployment.....	36
Security.....	37
Storage and storage controllers.....	37
SupportAssist and parts replacement.....	37
Chapter 9: Firmware and driver update.....	38
Chapter 10: Miscellaneous.....	39
Chapter 11: Updating iDRAC firmware.....	40
Downloading iDRAC firmware installation file.....	40
Updating iDRAC firmware from host OS.....	40
Updating iDRAC remotely using iDRAC web interface.....	40
Chapter 12: Lifecycle Controller Remote Services — client tools.....	42
Chapter 13: Resources and support.....	43
Chapter 14: Contacting Dell EMC.....	45

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 support for the 3rd generation of Intel Xeon processors.

Version

iDRAC9 4.40.29.00

Release date

July 2021

 **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 <https://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).

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 Datacenter—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 User's Guide available at dell.com/idracmanuals.

 **NOTE:** To manage new and existing licenses, go to the [Dell Digital Locker](#).

Supported systems

- PowerEdge C6520
- PowerEdge R650
- PowerEdge R750
- PowerEdge R750xa
- PowerEdge MX750c
- OEMR R650
- OEMR R750
- OEMR R750xa

Previous versions

- 4.40.20.00
- 4.40.21.00
- 4.40.23.00

 **NOTE:** For systems with 3rd generation Intel Xeon scalable processors, iDRAC9 version 4.40.25.00 is the only previous version.

Supported managed server operating systems and hypervisors

- Microsoft Windows
 - 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 8.3
 - RHEL 7.9
- SLES
 - SLES 15 SP2
- Ubuntu
 - Ubuntu 20.04.1
- VMware
 - ESXi 6.7 U3
 - ESXi 7.0 U1

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 an open source version of AdoptOpenJDK or OpenJDK (“Adopt Open JDK”) subject to the terms and conditions of the Adopt Open JDK community at the link below.
- You use Adopt Open JDK at your own risk. Adopt 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 Adopt 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 Adopt Open JDK.

- Dell has no liability to you for any damage that arise out of or relate to your use of Adopt 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), v10.0.1
- Dell EMC iDRAC Tools for Linux, v10.0.1
- Dell EMC iDRAC Tools for VMware ESXi (R), v10.0.1

This version contains:

- Remote/Local RACADM on Windows or Linux or ESXi
- IPMI Tool on Windows or Linux
- Secured Component Verification (SCV)

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

Before installing iDRAC tools from OM 9.5.0, you must uninstall any older versions of DRAC tools. For more information about uninstalling applications, see the documentation for your operating system.

New and enhanced features

Topics:

- [Hardware](#)

Hardware

- Support for 3rd generation Intel Xeon scalable processors.

Fixes

N/A

Deprecated features

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

Features	iDRAC9	iDRAC9 for PowerEdge Rx5xx/ Cx5xx
SM-CLP	Removal	Removal
VM CLI	Removal	Removal
VFlash	Deprecated	Removal
Backup and Restore	Removal	Removal
 NOTE: Alternatively, use the Server Configuration Profiles (SCP) feature to import or export server configuration settings and firmware updates.		
RBAP and Simple Identity profiles	Removal	Removal
WSMan	Deprecated	Deprecated
DCIM_account profile	Removal	Removal
Telnet and TLS 1.0	Removal	Removal

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

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

Important notes

1. CPLD update may fail if DUP method is used while power cap policy is enabled.
2. While encrypting VDs through Lifecycle controller, ensure that the first VD in the list is selected. Selecting a VD that is already secured does not affect the existing encryption of the VD.
3. For partition enabled COMMs adapter, a PR6 Lifecycle Log message may be displayed as partition-1 even though the values are configured as other than first partition.
4. Before updating PSU firmware on PowerEdge C series systems, ensure that all the blades are powered off in the chassis first. If any of the blades are powered on, the PSU firmware update process may fail, and LC logs report the failure.
5. Before performing SecureErase on a vFlash, ensure that the partitions on the vFlash are detached.
6. When streaming alerts using Remote Syslog or Redfish event listener, not every message ID/message gets streamed. To confirm which message ID/messages can be streamed, see the [EEMI guide](#).
7. Ensure that you use digest authentication for HTTP/HTTPs share for all iDRAC and LC features, basic authentication is no longer supported and is blocked by iDRAC due to security risks.
8. Intel ColdStream NVMe devices do not support cryptographic erase. For more information, see Intel's documentation for the specific device.
9. Remote File Share (RFS) through HTTP is only supported without authentication.
10. If part replacement is performed on systems with two PSUs while upgrade option is enabled, then the firmware update for both the PSUs are repeated once.
11. While PERC inventory is in progress, Lifecycle controller logging may fail after a warm reboot by RTCM for HBA, BOSS, or NVME drives.
12. While accessing iDRAC GUI and Redfish through the same browser, if the webserver times out, then RedfishService may prompt you to enter the login credentials to create a session. Select Cancel to clear the Redfish login prompt and proceed to the iDRAC login page.
13. Creating RAID using the selected controller is not supported through Lifecycle Controller interface. Use iDRAC GUI to create the virtual disk, then relaunch Lifecycle Controller and retry the deployment operation.
14. A new storage GUI has been introduced with this release. The old storage GUI is still accessible but would be deprecated in a future iDRAC release.
15. For Telemetry reports through subscription, if there are more than two subscriptions, it is recommended to update the Metric Report Recurrence interval to above 60 seconds.
16. IPMItool interface does not report non-communicative PSU status for PowerEdge Rx4xx/Cx4xx servers.
17. In Redfish API, all BIOS certificate related operations are now supported using the new URI: /redfish/v1/Systems/{ComputerSystemId}/Boot/Certificates
18. Arrow keys on virtual keyboard of the iDRAC Virtual Console with eHTML5 plug-in do not respond inside BIOS boot manager after the system reboots. Close and reopen the eHTML5 Virtual console session.
19. Before deleting a VD that hosts the OS, ensure uninstalling the iSM. If VD is deleted without uninstalling iSM, LC log may display the following error: "ISM0007 The iDRAC Service Module Communication has ended with iDRAC".
20. If an Active Directory user is configured for SSO with RSA token authentication, then the RSA token is bypassed and user can log in directly. This is because RSA is not applicable for AD-SSO, Active Directory smart card, and local user smart card logins.
21. While performing any method (GET/POST and so on) on an incorrect resource URI, a proper extended error message specifying that "Resource URI is incorrect" is not provided in the response body.
22. When auto negotiation is disabled while iDRAC in Shared LOM mode, the speed and duplex values shown in the GUI and racadm output may not accurately show the actual speed and duplex on the link.
23. While performing a firmware update or rollback through LifeCycle controller GUI, the component information displayed in the table listing the available updates may be truncated if it exceeds the table column or row width.
24. If SOL session is active for a long duration or if the system is rebooted multiple times, the SOL session gets terminated automatically.
25. Critical event PDR1016 will not be generated when M.2 drives from the BOSS-S2 controller are removed since M.2 drives are directly attached to BOSS controller and not connected to the backplane.
26. While performing BIOS Recovery operation all iDRAC resets are blocked and if a iDRAC reset to default operation is performed, it causes iDRAC to be set to factory defaults and iDRAC will not reset. The condition is expected and a manual iDRAC reset is recommended.
27. After an iDRAC reboot, the iDRAC GUI may take some time to initialize causing some information to be unavailable or some options to be disabled.

28. AD/LDAP diagnostic results will display Not Run or Not Applicable for Ping Directory Server Tests. ICMP ping tests are no longer performed while running AD/LDAP diagnostics.
29. While generating Server Configuration Profile templates using the Clone or Replace option, ensure that the template is updated using a password that complies with the restrictions set on the target iDRAC, or use the 'Include Password Hash' option.
30. While clearing the Job queue using RACADM, WSMAN, or Redfish interface, it is recommended to use JID_CLEARALL instead of JID_CLEARALL_FORCE. Use JID_CLEARALL_FORCE only to recover iDRAC Lifecycle controller from either a failed state or job that is stuck in running. It is also recommended that after you use "JID_CLEARALL_FORCE", iDRAC reset is needed to ensure iDRAC is back in a good working state.
31. For Dell online catalog update, downloads.dell.com only supports https protocol.
32. After updating the iDRAC license to Data Center license, ensure that you reboot the iDRAC for Idle server detection feature related attributes to function.
33. In LifeCycle Controller GUI, use mouse to browse files or folders. Keyboard navigation does not work while browsing files.
34. 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.
35. 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.
36. 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.
37. 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.
38. You may get an irrelevant response message while performing operating system method to Insert media with incorrect media for firmware upgradation or OS deployment.
39. 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.
40. If a single DUP is used to update firmware for multiple devices, and if any update fails then the firmware for the subsequent cards may display an incorrect version. Update the firmware for all the failed devices again.
41. iDRAC RESTful API with Redfish displays an error stating unacceptable header specified in request for commands that are run on PowerShell. You need to explicitly include a header while using Powershell for any type of Redfish request.
42. When node initiated discovery or Group Manager is enabled, iDRAC uses mDNS to communicate through port 5353. Turn off Group Manager and node initiated discovery to disable mDNS.
43. SMART monitoring is disabled for a hard drive while it is set to Non-Raid mode.
44. In systems with network adapters without internal temperature sensors, for some adapters the NIC temperature sensors metric value is reported as 0.
45. 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.
46. Performing GET method on Steps only shows the next scheduled jobs and not the completed jobs.
47. If you install OMSA while iSM is already installed and connected, iSM may restart after the OMSA installation is complete.
48. After iDRAC is upgraded to version 4.00.00.00 or later, 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 or later 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`
49. 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>
50. 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.
51. CPLD firmware update has no impact on Trusted Platform Module enablement.
52. 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.
53. 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.
54. 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.
55. 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.

56. 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.
57. 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.
58. Rollback is not supported for CPLD and HBA controllers.
59. 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.
60. 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:
- Available spare threshold
 - Reliability degraded
 - Read-only mode
 - Virtual memory backup failed, and so on.
61. Ensure that the SSH client is updated to the latest version. Following SSH configurations are no longer available on iDRAC:
- KEX algorithms:
- diffie-hellman-group14-sha1
- MAC:
- umac-64
 - umac-64-etm@openssh.com
62. 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.
63. 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.
64. If you get an error while performing SupportAssist collection through RACADM using HTTPS share, use the following commands to perform the collection:
- Racadm SupportAssist collect.
- ```
racadm supportassist collect -t Sysinfo
```
- Racadm SupportAssist exportlastcollection
- ```
racadm supportassist exportlastcollection -l <https> -u <username> -p <password>
```
65. The Lifecycle Controller GUI features available on your system depends on the iDRAC license installed. The GUI help pages may display information about features that are not available with the license installed. For licensed feature list, see the Licensed Feature section in iDRAC User's guide available at Dell.com/iDRACmanuals.
66. For improved support on drives and operating system deployment, it is recommended to use the UEFI BIOS boot mode.
67. 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.
68. In the software inventory, the hash value for iDRAC firmware is displayed as NA instead of hash.
69. If SMBv2 share fails in Lifecycle GUI, ensure that:
- The **Digitally sign communications** option is disabled.
 - Permissions to access the folder or file is granted.
 - folder/file name does not have a space.
 - Share contains fewer files and folders.
70. While iDRAC is initializing, all communications with iDRAC may fail. For any service requests, wait until the initialization process is complete.
71. Performing Redfish Patch method on Read-Only property for PowerControl resource returns a status code 200.
72. 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.
73. 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:
- Go to Settings, and select Power.
 - For the option, "When the Power Button is pressed" select Power Off.
74. 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.

75. FRU objects or properties for Network adapters that are embedded on the motherboard are not available through any of the iDRAC interfaces.
76. Lifecycle Controller supports ISO images with ISO-9660 format only. Other formats including combination with ISO-9660 are not recommended.
77. 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.
78. The iDRAC feature "Topology LLDP" is not supported on 1 GbE controllers and on selected 10 GbE controllers (Intel X520, QLogic 578xx).
79. 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 redundancy feature works after the iDRAC is set up for SSL certificate-based authentication.
80. 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.
81. When FCP is enabled, 'Default Password Warning' setting is disabled after the default user password is changed.
82. 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.
83. Due to a DMTF tool limitation, the URLs for some OEM actions that are extensions to the DMTF schemas may not appear in the OpenAPI.YAML file.
84. The iDRAC Virtual Keyboard labeling is changed to upper case to align it with the physical keyboard layout.
85. For enhanced security, keyboard interactive authentication is enabled on the iDRAC SSH Server. SSH clients now require keyboard interactive authentication before logging in a user in to iDRAC.
86. 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.

Known issues — To be fixed in future releases

Topics:

- Windows key not responding
- LC logs reporting NIC link issues
- Firmware update completed with errors
- Firmware rollback failing for NIC cards
- RAID operation failing
- Chassis PSU firmware update fails
- Sled not powering on with OME Modular in optimized mode
- iDRAC unable to obtain the current time after reboot
- Server stops responding during POST with Config Error
- OME-M Deployment and Configuration Job Fails with Error LC063
- Unable to generate CSR through Redfish
- vFlash detaching after iDRAC firmware update
- Unable to apply VAM properties
- MAC identities displayed in RESERVED state
- SEL events may not be correctly displayed in the earlier versions of iDRAC
- LC logs display Version change for Disks
- Telemetry data Disabled without confirmation
- WWN details for the Mezz cards displayed randomly in the WWN/MAC GUI page
- CPU information missing under Hardware Inventory
- Storage Devices displayed in gray text
- Backplane Rollback contents not populating in iDRAC
- Test network connection fails
- MetricReport output does not match the DMTF schema
- Service Validator reporting errors for Redfish API services
- Lifecycle Controller fails to resolve IPv6 DNS addresses
- Performing GET with Top query parameter returns no error
- Server Configuration Profile import job fails
- Unable to add iDRAC Static IP
- Creating virtual media image takes longer on safari browser
- iDRAC displays warning message for different plug-in selection.
- Booting with ISO image fails from iDRAC Virtual Console
- Virtual Console gets disconnected while trying to launch multiple Virtual Console sessions
- iDRAC Virtual Console entering Connecting Viewer state
- Virtual Keyboard not working
- Read-only user Virtual Console session disconnects
- Template deployment job fails
- Deleting multiple jobs results RAC0519 LCL event
- PR1 & PR10 Lifecycle logs displayed during Retire and Repurpose operation
- CPU PPIN in Hardware inventory in iDRAC GUI shows as "Not Supported"
- Virtual Media performance is degraded with QLogic 25G OCP
- iDRAC time fails to synchronize when Server Configuration Profile is imported with SNTP settings
- Virtual console display in iDRAC GUI is blurred
- Firmware version change displayed multiple times in Lifecycle log for PCIe SSDs
- Few Virtual Keyboard keys not working for other languages
- Deleting VD creates pending operation with empty data

- [DellCertificateCollection](#) URI response not according to DMTF standards
- Disabling local server video attribute in iDRAC virtual console not supported on C6400 and C6525
- Field required displayed in Internet Explorer browser
- Firmware update using pud method failing
- iDRAC DUP update fails in Linux operating systems when secure boot is enabled
- Uploaded firmware link not available in the `SoftwareImages` property in Redfish
- PCIe types and lanes information not getting populated using Redfish
- iDRAC reboots while collecting SupportAssist logs
- SupportAssist collection failing
- SupportAssist collection job creation fails
- Webserver restarts after remote presence port number is updated
- Getting an error SWC0018 during OS installation
- WSMAN query with space between attributes fails
- Attributes for CNA cards not displayed through Redfish or RACADM interface
- Get method not displaying certificates after all certificates are deleted
- Unable to create a recurring job after same recurring job was completed
- iDRAC LC Log shows reset cause as 'Internal Error'
- Firmware update operation not scheduled through WSMAN
- Access to serial interface fails.
- LC log created after going to Virtual media page in iDRAC GUI
- 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
- 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

Windows key not responding

Description	Windows key and the shortcuts with Windows key may not respond in the KVM sessions.
Workaround	Use the Virtual Console session.
Systems affected	PowerEdge MX750c
Tracking number	202510

LC logs reporting NIC link issues

Description	LC logs may display NIC link down for embedded, integrated, or Mezz NIC cards after host OS reboot is performed.
Workaround	N/A
Systems affected	All systems supported by this release.
Tracking number	196912

Firmware update completed with errors

Description	Firmware update performed using Group Manager may display the status "Completed with errors" and "Failed" for each group member even though the update completed successfully.
Workaround	Validate the firmware version through any iDRAC interface.
Systems affected	All systems supported by this release.
Tracking number	195385

Firmware rollback failing for NIC cards

Description	Firmware rollback of a NIC card with multiple ports may fail through Redfish or RACADM interface if the instance ID entered is of any port other than the first port.
Workaround	Use the instance ID of the first port of the NIC card.
Systems affected	All systems supported by this release.
Tracking number	178855

RAID operation failing

Description	If a NVMe drive is removed and reinstalled while configuring RAID using software RAID and a system reboot is performed, iDRAC may fail to create the RAID.
Workaround	Install the drive into a different slot or reboot the system before reinstalling the drive.
Systems affected	All systems supported by this release.
Tracking number	178248

Chassis PSU firmware update fails

Description	Updating PSU firmware through Redfish interface may fail on a modular server as a reboot job is created to power on the sleds, while the update requires all the sleds to be powered off.
Workaround	Update the PSU firmware using iDRAC GUI or RACADM interface.
Systems affected	PowerEdge C6520
Tracking number	196104

Sled not powering on with OME Modular in optimized mode

Description	Boot power is denied to the sled while OME Modular calculates the savings in budget from all the sleds when switched to optimized mode. Logs about retry to power on after switching to optimized mode are also not logged.
Workaround	Power on the sled manually
Systems affected	PowerEdge MX750c
Tracking number	191037

iDRAC unable to obtain the current time after reboot

Description	While the system is in power off state, iDRAC fails to obtain the current time after it is reset. Older logs are displayed until iDRAC synchronizes with current time.
Workaround	N/a.
Systems affected	All PowerEdge Rxx5x/Rx5x/Cxx5x (15th Generation) systems supported by this release.
Tracking number	183347

Server stops responding during POST with Config Error

Description	Server may stop responding during POST after a Lifecycle Controller System Erase job with the message- The System Configuration Check operation resulted in the following issue: Config Error: CPU 1 and CPU ID.
Workaround	iDRAC reset.
Systems affected	PowerEdge R7525 with EPYC 7003-generation processors and x24 Expander or x4 Rear backplanes.
Tracking number	196985

OME-M Deployment and Configuration Job Fails with Error LC063

Description	OME-M deployment jobs fail when iDRAC NTP and Host NTP settings are out of sync.
Workaround	Ensure that the Host OS and iDRAC NTP settings are set accurately.
Systems affected	All PowerEdge MX series systems supported by this release.
Tracking number	195935

Unable to generate CSR through Redfish

Description	Generating CSR through Redfish action CertificateService.GenerateCSR fails while passing in dash for email string value.
Workaround	Use iDRAC GUI or RACADM to generate the CSR.
Systems affected	All systems supported by this release.
Tracking number	196084

vFlash detaching after iDRAC firmware update

Description	Updating iDRAC firmware to version 4.40.00.00 or later may cause the vFlash partitions to detach on first boot after the update.
Workaround	Reattach the detached vFlash partitions through any iDRAC interfaces after the first boot.
Systems affected	All systems supported by this release.
Tracking number	194849

Unable to apply VAM properties

Description	When VAM is enabled and iDRAC is configured in Shared LOM mode, VAM properties may not be applied at the first host bootup after the AC power cycle.
Workaround	Power cycle the host system.
Systems affected	All PowerEdge MX series systems supported by this release.
Tracking number	193142

MAC identities displayed in RESERVED state

Description	MAC identities displayed in RESERVED state for some of the partitions after Slot Deployment is performed using Attach and Apply Immediately operation.
Workaround	Redeploy OMEM.
Systems affected	All PowerEdge MX series systems supported by this release
Tracking number	194347

SEL events may not be correctly displayed in the earlier versions of iDRAC

Description	New SEL events were introduced in this version of iDRAC. If iDRAC is rolled back to an earlier version, then new events logged in this version of iDRAC may be displayed as an unknown event in the earlier version of iDRAC.
Workaround	N/a
Systems affected	All PowerEdge Rx5x5 or Cx5x5 series servers supported by this release.
Tracking number	186384

LC logs display Version change for Disks

Description	LC logs display PR36 messages, or Version change detected for disk after a BIOS upgrade to version 2.1.6 and host warm reboot on systems with NVME drives behind PERC controller.
Workaround	n/a
Systems affected	All systems supported by this release.
Tracking number	195302

Telemetry data Disabled without confirmation

Description	Disabling Telemetry data stream through iDRAC GUI, is applied immediately after Apply is selected instead of displaying a warning message for confirmation is not seen after selecting apply. The warning or confirmation message is only visible after the success window is closed and canceling the warning fails to cancel the task.
Workaround	Enable the Telemetry data stream using either iDRAC GUI or RACADM interface.
Systems affected	All systems supported by this release.
Tracking number	194248

WWN details for the Mezz cards displayed randomly in the WWN/MAC GUI page

Description	In certain configurations, if the NIC partitions are enabled, WWM/MAC page may display the MAC/WWN details for the Mezz cards that are installed in the system in random order. The display order may vary from the port or partition ordering.
Workaround	Go to the Network device page for specific device details that are associated with port and partitions.

Systems affected PowerEdge MX series

Tracking number 194452

CPU information missing under Hardware Inventory

Description iDRAC inventory fails to populate CPU information after a system reboot.

Workaround Reset iDRAC.

Systems affected All systems supported by this release.

Tracking number 189573/158951

Storage Devices displayed in gray text

Description After a reboot stress followed by BIOS update, storage devices may appear as not ready or in gray text.

Workaround Reset iDRAC.

Systems affected All PowerEdge Rx5xx/Cx5xx series supported by this release.

Tracking number 194537

Backplane Rollback contents not populating in iDRAC

Description After updating backplane firmware to a newer version and then updating it back to a previous version from host OS, the backplane information is not displayed while trying to apply the firmware Rollback.

Workaround

- Perform the following:
 - Reboot the iDRAC when an update is performed from host OS.
 - Use any iDRAC interfaces (RACADM/GUI/Redfish) for backplane update operation.

Systems affected All systems supported by this release.

Tracking number 184368

Test network connection fails

Description Testing the network connection may fail when IPv6 address is used for operations in LC GUI.

Workaround Ping and test the network IP through iDRAC GUI.

Systems affected All systems supported by this release.

Tracking number 180776

MetricReport output does not match the DMTF schema

Description LastDayMaxPowerTime, LastDayMinPowerTime, LastHourMaxPowerTime, LastHourMinPowerTime, LastMinuteMaxPowerTime, LastMinuteMinPowerTime, LastWeekMaxPowerTime, and LastWeekMinPowerTime may have an invalid MetricType in MetricDefinitions.

Workaround N/a. The MetricReport output is further modified to match DMTF schema, and will be fixed in subsequent releases.

Systems affected All systems supported by this release.

Tracking number 180398

Service Validator reporting errors for Redfish API services

Description To continue support firmware backward compatible, you may get errors for Redfish API services in the Service Validator. They do not have any functional impact on the system and may be ignored.

Workaround N/a

Systems affected All systems supported by this release.

Tracking number 183321

Lifecycle Controller fails to resolve IPv6 DNS addresses

Description Connection issues may occur if Lifecycle Controller network interface set to use IPv6 protocol, and FQDN is defined for share/repository address.

Workaround For local shares and repositories, enter the IPv6 address for the Share Name value as the issue is limited to DNS resolution. This will bypass requirement for DNS resolving.

Systems affected All systems supported by this release.

Tracking number 165692

Performing GET with Top query parameter returns no error

Description Top query on a Parity URI instance returns complete response instead of an error code.

Workaround N/a

Systems affected All systems supported by this release.

Tracking number 175801

Server Configuration Profile import job fails

Description Importing SCP fails with error "Not one of the Possible Values for Attribute" when VNC password is not set or set lower than eight characters in length.

Workaround Set eight character length VNC password.

Systems affected All systems supported by this release.

Tracking number 185635

Unable to add iDRAC Static IP

Description	After setting iDrac static IP using IPV4 group (IPv4.1.Address, IPv4.1.Gateway,IPv4.1.Netmask) using Redfish or RACADM interface, a new IP address may not apply and system may become inaccessible.
Workaround	Use the IPV4Static group (IPv4Static.1.Address, IPv4Static.1.Gateway,IPv4Static.1.Netmask) to set static IP address.
Systems affected	All systems supported by this release.
Tracking number	185458

Creating virtual media image takes longer on safari browser

Description	Creating a virtual media image takes longer when the target folder contains many files.
Workaround	N/a
Systems affected	All systems supported by this release.
Tracking number	185657

iDRAC displays warning message for different plug-in selection.

Description	iDRAC GUI displays a warning "Virtual console session of a different plug-in type is currently running. Please close existing session and try again".
Workaround	Close the existing session and change the plug-in to eHTML5.
Systems affected	All systems supported by this release.
Tracking number	184648

Booting with ISO image fails from iDRAC Virtual Console

Description	Booting with ISO image fails from iDRAC Virtual Console with eHTML5 plug-in type when iDRAC USB port is configured as All ports off or AllPortsOff (Dynamic).
Workaround	Configure iDRAC USB ports to "All ports on" or "Only back ports on" and boot into the ISO image that is attached to the Virtual console.
Systems affected	All systems supported by this release.
Tracking number	185537

Virtual Console gets disconnected while trying to launch multiple Virtual Console sessions

Description	iDRAC Virtual Console with eHTML5 plug-in may get disconnected if multiple Virtual Console sessions are launched on other systems.
--------------------	--

Workaround Close and reopen the eHTML5 Virtual console session.

Systems affected All systems supported by this release.

Tracking number 179927

iDRAC Virtual Console entering Connecting Viewer state

Description iDRAC Virtual Console with eHTML5 plug-in enters connecting viewer state when iDRAC is left idle for around 30 minutes.

Workaround Close and reopen the eHTML5 Virtual console session.

Systems affected All systems supported by this release.

Tracking number 180173

Virtual Keyboard not working

Description Virtual keyboard in Virtual Console with eHTML5 plug-in stops responding inside the BIOS boot manager menu after invoking the macro <Alt>+<Sysrq>+ from Linux OS.

Workaround Close and reopen the eHTML5 Virtual console session.

Systems affected All systems supported by this release.

Tracking number 185038

Read-only user Virtual Console session disconnects

Description Read-only Virtual Console session with eHTML5 plug-in disconnects while server is rebooting or due to a network disruption or when the primary session is in reconnecting state.

Workaround Close and reopen the eHTML5 Virtual console session.

Systems affected All systems supported by this release.

Tracking number 184596

Template deployment job fails

Description In a multi chassis management environment, the template deployment job fails while trying to set plug-in type as eHTML5.

Workaround N/a

Systems affected PowerEdge MX7000, PowerEdge MX740c, and PowerEdge MX840c.

Tracking number 184333

Deleting multiple jobs results RAC0519 LCL event

Description RAC0519 LCL could pops up when deleting multiple jobs like storage configuration jobs, update jobs, etc. in iDRAC job queue as deleting jobs may take longer time resulting in API timeout.

Workaround Refresh the page after some time to confirm all jobs are deleted.

Systems affected All systems supported by this release

Tracking number 181570

PR1 & PR10 Lifecycle logs displayed during Retire and Repurpose operation

Description PR1 & PR10 logs are displayed in Lifecycle logs for PSUs when Retire and Repurpose operation is executed. This doesn't impact server functionality.

Workaround N/a

Systems affected All systems supported by this release.

Tracking number 186119

CPU PPIN in Hardware inventory in iDRAC GUI shows as “Not Supported”

Description CPU PPIN in Hardware inventory in iDRAC GUI shows as "Not Supported" after iDRAC firmware update from previous version to 4.40.00.00.

Workaround Reboot the host so the CSIOR runs and populates supported CPU PPINs in Hardware inventory.

Systems affected All systems supported by this release.

Tracking number 185523

Virtual Media performance is degraded with QLogic 25G OCP

Description Virtual Media performance is degraded when iDRAC is configured on the QLogic 25G OCP for shared LOM.

Workaround Configure iDRAC on dedicated port or integrated port or embedded shared LOM.

Systems affected PowerEdge Rx5xx/ Cx5xx with QLogic 25G OCP.

Tracking number 183014

iDRAC time fails to synchronize when Server Configuration Profile is imported with SNTP settings

Description iDRAC time will not synchronize when Server Configuration Profile was exported with SNTP settings and then imported with SNTP settings.

Workaround Configure NTP settings and export the Server configuration Profile. Import the Server configuration profile with NTP and manually configure SNTP settings.

Systems affected All systems supported by this release

Tracking number 181069

Virtual console display in iDRAC GUI is blurred

Description	Virtual console display from iDRAC GUI is blurred for a fraction of second and gets corrected automatically when opened in Google chrome.
Workaround	Use any other browser.
Systems affected	All systems supported by this release.
Tracking number	182595

Firmware version change displayed multiple times in Lifecycle log for PCIe SSDs

Description	Firmware version change may be displayed multiple times in Lifecycle log for PCIe SSDs after performing the update through Lifecycle controller. The firmware is updated only once.
Workaround	N/a
Systems affected	PowerEdge R7525.
Tracking number	181254

Few Virtual Keyboard keys not working for other languages

Description	Some keys or key combination may not provide the correct output for languages other than english.
Workaround	Use the physical keyboard or Windows On-Screen Keyboard.
Systems affected	All systems supported by this release.
Tracking number	181505

Deleting VD creates pending operation with empty data

Description	When existing VD is deleted from iDRAC GUI using delete VD operation from the Virtual disk option and then added to pending operation, the pending operation displays no information. However, the delete VD pending operation is created successfully.
Workaround	To successfully delete the VD and add to pending operations, perform the following steps: 1. Select the Configuration option in iDRAC GUI 2. Select Storage Configuration, then select the Controller and click Apply now.
Systems affected	All systems supported by this release.
Tracking number	184393

DellCertificateCollection URI response not according to DMTF standards

Description	An array of members are missing in Dellcertificatecollection resource collection. Without the members this resource collection is not compliant to DMTF standards.
Workaround	N/a
Systems affected	All systems supported by this release
Tracking number	164791

Disabling local server video attribute in iDRAC virtual console not supported on C6400 and C6525

Description	Local video does not turn off and remains on regardless of the local video server setting in iDRAC virtual console on PowerEdge C6525 and PowerEdge C6400.
Workaround	N/a
Systems affected	PowerEdge C6525, PowerEdge C6400.
Tracking number	171650

Field required displayed in Internet Explorer browser

Description	If any invalid value(s) including alphabets or special characters are entered in a numeric field, Internet explorer browser displays "Field Required" instead of displaying an error "Invalid Value".
Workaround	Use other browsers such as Chrome/Firefox/Edge.
Systems affected	All systems supported by this release.
Tracking number	163829

Firmware update using pud method failing

Description	Updating firmware through RACADM fwupdate -p -u -d fails with remote RACADM.
Workaround	Use the RACADM update command to update the firmware.
Systems affected	All systems supported by this release.
Tracking number	166686

iDRAC DUP update fails in Linux operating systems when secure boot is enabled

Description	On all Linux Operating Distributions, while secure boot is 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

Uploaded firmware link not available in the SoftwareImages property in Redfish

Description	While performing GET method on BIOS or Manager Schema through Redfish, the SoftwareImages property may not display the uploaded firmware link.
Workaround	N/A
Systems affected	All systems supported by this release.
Tracking number	156737

PCIe types and lanes information not getting populated using Redfish

Description	When Get method is performed for PCIe slots schema, slots that do not have a PCIe card populated the PCIe types and lanes are displayed empty.
Workaround	N/A
Systems affected	All systems supported by this release.
Tracking number	157364

iDRAC reboots while collecting SupportAssist logs

Description	iDRAC may reboot with an “Internal Error” during SupportAssist logs collection when it experiences lower runtime resources.
Workaround	N/A
Systems affected	All systems supported by this release.
Tracking number	161623

SupportAssist collection failing

Description	Unable to generate SupportAssist collection while iDRAC is under stress and CPU utilization is above 90%.
Workaround	Generate SupportAssist collection with only system information option checked.
Systems affected	All systems supported by this release.
Tracking number	159527

SupportAssist collection job creation fails

Description	Unable to create a SupportAssist collection for the first time with the option “Do not ask me again” selected for saving the collection to the default share.
Workaround	Do not select the check box “Do not ask me again” and proceed.

Systems affected All system supported by this release.

Tracking number 155650

Webserver restarts after remote presence port number is updated

Description Changing the Remote Presence Port number through virtual console settings page may cause a system restart, further causing a session timeout for iDRAC GUI.

Workaround N/a

Systems affected All systems supported by this release.

Tracking number 144597

Getting an error SWC0018 during OS installation

Description Modifying BIOS Boot Mode while installing operating system thorough Lifecycle Controller GUI, an error "SWC0018" is displayed.

Workaround This message does not impact the installation, click OK to proceed.

Systems affected All systems supported by this release.

Tracking number 143561

WSMan query with space between attributes fails

Description Query parsing error is observed while parsing the SQL query with a space in some properties.

Workaround Scripts may be edited to remove the space between properties to be selected in the WSMAN Query parameter.

Systems affected All systems supported by this release.

Tracking number 153493

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

Get method not displaying certificates after all certificates are deleted

Description	After performing POST method ResetkeysType with DeleteAlleys 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

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

iDRAC LC Log shows reset cause as ‘Internal Error’

Description	Some of the log events in LC Log shows ‘The iDRAC firmware was rebooted with the following reason: Internal Error’. 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

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

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

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

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

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](#)

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. Creating RAID 10 configuration is not supported through Redfish interface. Use the other iDRAC interfaces to create a RAID 10 configuration.
2. Sometimes, when using WSMAN, an Internal SSL Error is reported and the WSMAN command fails. If this issue occurs, retry the command.
3. 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**.
4. RACADM supports the underscore character (_) for *iDRAC.SerialRedirection.QuitKey* along with the existing symbols shown in the integrated help.
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.

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).
3. Blinking operations are not supported on the Virtual disk created on BOSS-S2 cards.

iDRAC and LC firmware

1. In Firmware Rollback page, the component names may vary in iDRAC GUI and Lifecycle Controller GUI.
2. Due to known limitations in OpenSource (SFCB), query filtering with long integers and lengthy strings may not work as expected.
3. 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.
4. 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.
5. 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.

6. 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.
7. During import server profile operation, if the image filename is "Backup.img", operation may fail. To avoid this failure, change the filename.
8. In Lifecycle Controller GUI pages, part of some text may not render correctly. Use any other iDRAC interfaces to access the information.

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 lcllog 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.
10. Redfish or other iDRAC interfaces only display the FQDD of a faulty part, use the LCLogs for detailed information.

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. Part number for Predictive failure message "PDR16" for NVMe drive may appear as "Not Available" immediately after the cold reboot. Allow some time after the cold reboot for iDRAC to initialize the inventory.
2. While renaming a virtual disk (VD), using a . (period) is not allowed in the VD name.
3. 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`
4. 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.
5. If a M.2 SATA drive attached to BOSS-S2 controller is removed, performing a blink operation may not fail for the removed drive.

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 <https://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.

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 <https://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.

Lifecycle Controller Remote Services — client tools

Redfish API

For information about Redfish, see the DMTF website <https://www.dmtf.org/standards/redfish>. This website provides access to schema files, white papers, technical notes, and so on.

For iDRAC Redfish API guide, go to <https://developer.dell.com>

Resources and support

For more information about the features of this release, see the documentation for iDRAC 4.xx.

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
https://www.dell.com/idracmanuals	iDRAC and Lifecycle Controller
https://www.dell.com/cmcmanuals	Chassis Management Controller (CMC)
https://www.dell.com/esmanuals	Enterprise System Management
https://www.dell.com/serviceabilitytools	Serviceability Tools
https://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**.

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 <https://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.