iDRAC9 with Lifecycle Controller Version 3.00.00.00 Release Notes

DELLEMC

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

DELLEMC

Overview

The Integrated Dell Remote Access Controller (iDRAC) is designed to make server administrators more productive and improve the overall availability of Dell servers. iDRAC alerts administrators to server issues, helps them perform remote server management, and reduces the need for physical access to the server.

iDRAC with Lifecycle Controller (LC) technology is part of a larger data-center solution that ensures availability of business-critical applications and workloads. The technology enables administrators to deploy, monitor, manage, configure, update, troubleshoot, and remediate Dell servers from any location without using any agents. It accomplishes this regardless of the operating system or hypervisor presence or state.

Version

iDRAC9 with LC 3.00.00.00

Release Date

June 2017

Previous version

N/A

This release supports the 14th-generation servers and is not backward-compatible with any prior generations.

Importance

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

Platforms affected

- PowerEdge C6420
- PowerEdge R640
- PowerEdge R740
- PowerEdge R940
- PowerEdge R7920
- PowerEdge R740xd
- DSS 9600
- DSS 9620
- DSS 9630

What is supported

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.

For information on the features available for a license, see the Managing Licenses section in the iDRAC 3.00.00.00 User's Guide available at http://www.dell.com/idracmanuals

Supported managed server operating systems and hypervisors

Microsoft

- Server 2012 Foundation
- Server 2012 Essentials
- Server 2012 Standard
- Server 2012 Datacenter
- Server 2012 R2 Foundation
- Server 2012 R2 Essentials
- Server 2012 R2 Standard
- Server 2012 R2 Datacenter
- Server 2012 for Embedded Systems (Base and R2 with SP1)
- Server 2016 Essentials
- Server 2016 Standard
- Server 2016 Datacenter
- WinPE 5.0 64-bit
- WinPE 10

RedHat

- RHEL 6.9
- RHEL 7.3

SLES

- SLES 12 SP2

VMware

- vSphere 6.0 U3
- vSphere 2016

Citrix

- XenServer 7.1

iDRAC iSM support — Version 3.0.1

Microsoft Windows Server 2016	GUI and CLI
Microsoft Windows 2012	GUI and CLI
Microsoft Windows 2012 R2	GUI and CLI
Red Hat Enterprise Linux 6.9	GUI and CLI
Red Hat Enterprise Linux 7.3	GUI and CLI
SUSE Linux Enterprise Server 12 SP2	GUI and CLI
VMware ESXi 6.0 U3	GUI and CLI
VMware vSphere 2016	GUI and CLI
Citrix XenServer 7.1	GUI and CLI
CentOS 6.9**	GUI and CLI
CentOS 7.4**	GUI and CLI
Ubuntu 14.04.1 LTS	GUI and CLI
Ubuntu 16.04.1 LTS	GUI and CLI
Debian Wheezy 7.9 or later stable release	GUI and CLI
Debian Jessie 8.3 or later stable release	GUI and CLI

** iDRAC Service Module (iSM) can be installed on CentOS. Dell provides only limited support for CentOS. For more information or support on CentOS, contact the CentOS community.

Supported web browsers

- Microsoft Internet Explorer 11
- Microsoft EDGE
- Safari version 8.0.8
- Safari version 9.0.3
- Mozilla Firefox version 53
- Mozilla Firefox version 54
- Google Chrome version 58
- Google Chrome version 59

What's new

Authentication

- Default password is randomly generated and printed on the system information tag, unless the legacy password (calvin) was selected while ordering the system.

BIOS/UEFI

- Added BIOS configuration feature using iDRAC GUI.
- Added support for the UEFI 2.5 network and firmware management protocols.
- Added certificate management for secure UEFI boot.

Hardware (server/storage platform specific)

- iDRAC Direct USB on the front of the server is now a micro-B slot. For increased security, this port is hardwired to iDRAC.
- Quick Sync 2 replaces Quick Sync Near Field Communication (NFC) with Bluetooth Low Energy (BLE) and Wi-Fi. This interface provides higher throughput and supports iDRAC GUI and Virtual Console access.
- Internal 16 GB vFlash card (optional)
- Bezel with LCD panel (optional).
- Multi-vector cooling for better air-flow cooling of 3rd party PCIe cards.

iDRAC/LC firmware

- Improved adding and removing users from iDRAC.
- Added new System Lockdown feature to restrict use of Dell tools to make changes to BIOS, iDRAC, firmware, and so on.
- Added Group Manager. All iDRACs in the same subnet can be grouped together and managed by one master iDRAC of the group.
- Full HTML5 web interface for faster page loading and ease of use.
- Added **Power Control** and **Next Boot** options in HTML5 vConsole.
- Export and import Server Configuration Profiles (SCP) from the iDRAC GUI.
- Added support for HTTP/HTTPS file transfers.

Monitoring and alerting

- Streamlined alerts configuration

Networking and I/O

- By default, DHCP is enabled for iDRAC IP address. In previous generations, the default setting was static IP address.
- Added Connection View feature that provides information about the switch and port for iDRAC, LoMs, and Dell supported PCIe cards.

OS deployment

- iDRAC Service Module (iSM) is pre-installed on iDRAC.

Scripting (all CLI related items)

- Added support for Redfish 2016 R1 and R2, a RESTful Application Programming Interface (API), which is standardized by the Distributed Management Task Force (DMTF). It provides a scalable and secure systems management interface.
- Enhanced iDRAC RESTful API support for Server Configuration Profiles with access via local file streaming and via HTTP/S file transfer.
- Added support for WSMan streaming for Server Configuration Profiles.

Security

- By default, support for TLS 1.1 and higher is enabled. You can select TLS 1.0 and higher, TLS 1.1 and higher, or TLS 1.2 only. See Note 2 in the Important Notes section.
- Added security banner for GUI login page.

Storage and PERC

- Added support to perform disk erase (secure and non-secure disks) in the Retire and Re-purpose feature.
- Expanded storage functions through iDRAC. Perform tasks such as Online Capacity Expansion (OCE) and RAID Level Migration (RLM) without the use of agents, using GUI or CLI.
- Added support to create virtual disk for NVMe drives using PERC S140 - Windows RAID and Linux MD RAID.

SupportAssist and parts replacement

- SupportAssist can be set up through the iDRAC for 1x1 'phone home' service to Dell EMC Technical Assistance.
- SupportAssist Collector now includes iDRAC core dumps, hardware crash dumps, and ESXi logs.
- SupportAssist viewer — Export HTML5-formatted report for viewing on web browsers.
- Added option to collect iDRAC debug logs with the SupportAssist report export feature.

Updates

- Added Support for Firmware updates using SCP(System Configuration profile) XML Import.
- Added support for the DUP dependency to handle component dependencies.
- Added Server Configuration Profile support for firmware repository-based updates and JSON file format.

Fixes

N/A

This release supports the 14th generation servers and is not backward-compatible with any prior generations.

6

Important notes

1. 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

2. The drivers exposed by LC are present in a read-only drive labeled OEMDRV and the drive is active for 18 hours. During this period:

   - You cannot update any DUP.
   - LC cannot involve CSIOR.

   However, if an AC power cycle (cold boot) is performed, the OEMDRV drive is automatically deleted.

3. CPLD firmware update has no impact on Trusted Platform Module enablement.

4. 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.

5. If the network is not configured and you try to perform a network operation, a warning message is displayed. When you navigate to the network settings page from this message, the left navigation panel on network settings page may not be displayed.

6. If Test Network Connection fails for a valid address, try configuring the network settings again. If the issue persists, restart the system and retry the operation.

7. 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.

8. 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.

9. 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.

10. Rollback is not supported for CPLD.

Limitations

- 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.
- Sometimes, when using WSMan, an `Internal SSL Error` is reported and the WSMan command fails. If this happens, retry the command.
- Due to known limitations in OpenSource (SFCB), query filtering with long integers and lengthy strings may not work as expected.
- If the LCD display is blank, press any one of the 3 LCD buttons to turn on the LCD before inserting a USB storage device.
- 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.
- 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.
- Some of the supported components may not be displayed on the **Firmware Update → View Current Versions** page. To update this list, restart the system.
- 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.
- You may be unable to scroll using the keyboard. Use the mouse to scroll.
- 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**.
- 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**).
- When Virtualization Mode is set to NPAR for Network Adapter 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**.
- 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.
- Deployment of Windows Server operating systems (OS) using LC may fail with one of the following message:

  - Windows installation cannot continue because a required driver could not be installed.
  - Product key required.
  - Windows cannot find the software license terms.

  This happens 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.
- LC supports the following characters for username and password:

Alphabets	a-z, A-Z
Numbers	0-9
Special characters	- _ .

- If the iDRAC firmware update is interrupted, you may have to wait up to 30 minutes before attempting another firmware update.

- 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 LC 3.00.00.00 User's Guide available at **www.dell.com/idracmanuals**.

- 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.

- 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

- While viewing the current hardware inventory, some properties related to devices installed in PowerEdge VRTX system are not displayed.

- LC can import and view an iDRAC license but cannot export or delete the iDRAC license. The iDRAC license can be deleted from iDRAC GUI.

- The ISCSI offload attribute can be enabled only on two of the four available ports. If a card, which has this attribute enabled on two of its ports, is replaced with another card that has the attribute 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.

- In LC, not all the vendor FC cards are supported for VLAN configuration.

- LC displays two drive names for some CDs or DVDs, such as the ones containing operating systems.

- 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.

- 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 appears 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.

- LC does not support OS deployment on Dell Precision Workstation R7920.

- LC does not support SOCK4 proxy with credentials.

- LC GUI 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.

- Because of internal UEFI network stack protocol implementation, there may be a delay while opening the LC GUI **Network Settings** page or while applying the network setting.

- The inventory displayed in LC GUI 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 GUI.

- 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 Re-purpose and Retire operation is performed.

  - Network is configured with the network cable connected but the network card is replaced later.

- If you set a user with only SHA256 password, for example, through SCP, you cannot delete the user using the GUI. To delete such a user, edit the user explicitly setting a password and then try to delete the user.

- 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`.

- RACADM supports the underscore character (_) for **iDRAC.SerialRedirection.QuitKey** along with the existing symbols shown in the integrated help.

- 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 the iDRAC and then retry the operation after the iDRAC has finished restarting.`

- If iDRAC is in lock-down mode, and you run the `racadm rollback` command followed by the `racadm resetcfg` command, 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.

- 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`.

- 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 GUI (**Maintenance → Lifecycle Log**) or by using the RACADM command `racadm lclog view`.

- 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 GUI (**iDRAC Settings → Users**) to verify the number of iDRAC local users.

- 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 GUI (**iDRAC Settings → Users**) to verify that the user exists.

- 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 navigate to **iDRAC Settings → Diagnostics**.

    d. Select **Reset iDRAC**.

    When iDRAC fully restarts, Group Manager should see the new iDRAC.

- When setting the iDRAC Service Module (ISM) monitoring attributes from the GUI, 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.

- 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 till the new values take effect. Any DHCP settings may take more time (>30 seconds) depending on the network environment.

- If the system ID/Health LED turns from blue to off while running host stress test, press the ID button for one second and then press it again to turn on the LED.

Known Issues — To be fixed in future releases

1. **Description**

   Smash CLP support:

   - The SMCLP Delete SEL Record operation is not supported.
   - The SMCLP User Privilege Enable option is not supported.

   Resolution

   N/A

   Version/Systems affected:

   All systems supported by this release.

   Dell tracking: 55929; 55935

2. **Description**

   Using Group Manager, when you try to join an existing group of iDRACs and if the group has already reached the upper threshold of 100 members, the error GMGR0077 is displayed, but message details are not displayed. The message details are as mentioned in the Resolution below.

   Resolution

   ```
   GMGR0077: Unable to add the iDRAC to group because the maximum possible iDRACs are
   already added to the group. Remove the existing iDRAC(s) from the group. If available
   iDRACs are more than allowed number of iDRACs, upgrade to OpenManage Consoles.
   ```

   Version/Systems affected:

   All systems supported by this release.

   Dell tracking: 62262

3. **Description**

   On the firmware update page of LC GUI, some component names get truncated.

   Resolution

   To view the complete component names in LC GUI, navigate to **Firmware Update → View Current Versions**. You can also use iDRAC interfaces to see the component names.

   Version/Systems affected:

   All systems supported by this release.

   Dell tracking: 62050

4. **Description**

   An error is displayed if you change the Power Cap Policy from Disabled to Enabled, set the value, and try to save the changes.

   Resolution

   Change the **Power Cap Policy** from **Disabled** to **Enabled**, go back to the previous window, and click **Finish**. After the changes are saved, navigate to **iDRAC Settings → Power Configuration**, enter the power cap values, click **Back**, and then click **Finish** to save the changes.

   Version/Systems affected:

   All systems supported by this release.

   Dell tracking: 62413

5. **Description**

   If you enter uppercase letters (Ex: Test@abc.com, TEST@abc.com) in the email field of SMTP configuration screen in iDRAC GUI, 'Invalid Email Address' error is displayed.

Resolution

Use lowercase letters in the destination email address for SMTP configuration.

Version/Systems affected:

All systems supported by this release.

Dell tracking: 62633

6. **Description**

   While creating a vFlash partition from an image using iDRAC GUI, you may be able to attach files with invalid extension if the file type is selected as 'All Files' in the file browser. However, the emulation on the OS fails.

   Resolution

   When creating a vFlash partition from image in iDRAC GUI, default file type is set in the file browser based on the emulation type. Do not change the file type to 'All Files'. If changing the file type for any reason, always choose files with .iso extension for CD emulation type and files with .img extension for floppy drive/HDD.

   Version/Systems affected:

   All systems supported by this release.

   Dell tracking: 61962

7. **Description**

   When you launch the virtual console sessions from the iDRAC GUI using HTML5 plugin the session sharing window does not display the requester name. The following text is missing: `A connection request has been received from user: <username>`.

   Resolution

   You can still accept or reject the session sharing request.

   Version/Systems affected:

   All systems supported by this release.

   Dell tracking: 62812

8. **Description**

   Creating RAID-5 Virtual Disk using NVMe drives with the PERC S140 controller fails due to PERC S140 firmware limitations.

   Resolution

   N/A

   Version/Systems affected:

   All systems supported by this release.

   Dell tracking: N/A

9. **Description**

   Windows operating system (OS) installation initiated from LC with the PERC S140 storage controller cannot be completed without loading driver for PERC S140. This step is required because S140 drivers are not part of the OS driver pack.

   Resolution

   To install the driver, click **Load driver** on the windows installation page, select PERC S140 drivers path, and click **Next**. After the driver installation is complete, select the virtual disk and click **Next** to complete the OS installation.

   Version/Systems affected:

   All systems supported by this release.

   Dell tracking: N/A

10. **Description**

    When using SCP Export JSON with the 'Include Read Only' option, the resulting JSON file does not contain read-only attributes for RAID components.

    Resolution

    Use SCP Export with the default XML format instead of JSON to access these read-only RAID attributes.

    Version/Systems affected:

    All systems supported by this release.

Dell tracking: 62939

11. **Description**

When performing catalog updates simultaneously with OS driver pack and iDRAC DUPs, depending on the number of updates being performed, one of these updates may not get downloaded from repository due to size limit.

Resolution

Retry the catalog update operation after previous operation completes.

Version/Systems affected:

All systems supported by this release.

Dell tracking: N/A

12. **Description**

In iDRAC GUI, modifying the HotSpare value to disabled and reloading Power Management screen does not disable the Primary PSU options. You may be able to change the Primary PSU but the modified value do not get applied because HotSpare is disabled.

Resolution

To change the Primary PSU value, ensure that HotSpare is enabled.

Version/Systems affected:

All systems supported by this release.

Dell tracking: 63313

13. **Description**

When NVMe drives are set to RAID mode, storage configuration page error message is incomplete.

Resolution

The current message is generic for all SSDs. NVMe-specific message text will be updated in a future release. For more details, see the iDRAC integrated help.

Version/Systems affected:

All systems supported by this release.

Dell tracking: 63058

14. **Description**

An ambiguous message `Unable to log in for 1@@1404816348 from ...` is logged in Lifecycle logs (LCL).

Resolution

If the iDRAC is rebooted while a vConsole session is active, the vConsole attempts to reconnect with the server. If the vConsole has not been closed or timed out after the iDRAC reboots, the vConsole attempts to reconnect and is denied access because its temporary credentials are no longer valid. This causes the LCL to log the message `Unable to log in for X@@XXXXXXXX from <IP ADDRESS> using Virtual Console`.

Version/Systems affected:

All systems supported by this release.

Dell tracking: 61221

15. **Description**

Using iDRAC GUI interface, you may be unable to export the Lifecycle logs to a CIFS network share. The following error message is displayed: `RAC0509: The server is temporarily unavailable. Wait for a few minutes and refresh the page. If the problem persists, contact service provider.`

Resolution

From iDRAC GUI, export Lifecycle logs using local or NFS network share options. You can also use RACADM to export the Lifecycle logs.

Version/Systems affected:

All systems supported by this release.

Dell tracking: 60183

16. **Description**

In iDRAC GUI, closing the HTML5 virtual console session by exiting the browser does not terminate the mounted VMedia session. Because of this, you cannot connect to virtual media on your next virtual console session.

Resolution

To terminate the VMedia session, click **Disconnect Viewer**.

Version/Systems affected:

All systems supported by this release.

Dell tracking: 63411

17. **Description**

If no hard drive is inserted on systems with direct attached SSD, **PCIe Capable** is displayed as **No**.

Resolution

For backplane with direct attached PCIe SSD devices, PCIe capability is shown as **No** for empty slots. Both SSDs and HDDs can be inserted in universal slots. See your server configuration to get the details for PCIe capability.

Version/Systems affected:

All systems supported by this release.

Dell tracking: 63456

18. **Description**

In iDRAC GUI, inlet warning threshold for iDRAC temperature probes cannot be set to 0.

Resolution

Set the warning threshold [minimum/maximum] value to 0 (Zero) using RACADM.

Version/Systems affected:

All systems supported by this release.

Dell tracking: 63315

19. **Description**

Redundant path is shown as not being present even when one of the cable is reinserted from multi-path scenario.

Resolution

Restart iDRAC to display the correct status.

Version/Systems affected:

All systems supported by this release.

Dell tracking: 61154

20. **Description**

BGI, which is automatically started after RLM, is not logged in Lifecycle log.

Resolution

N/A

Version/Systems affected:

All systems supported by this release.

Dell tracking: 61427

21. **Description**

Using LC GUI, importing a Server Configuration Profile (SCP) file larger than 125 MB from a network share may fail.

Resolution

To import SCP file larger than 125 MB, use vFlash or import using iDRAC GUI

Version/Systems affected:

All systems supported by this release.

Dell tracking: 63688

22. **Description**

After AC power is applied on systems with mid-backplane installed and the host boots up for the first time, erroneous drive removal messages may be logged during subsequent power cycles of the host.

Resolution

N/A

Version/Systems affected:

All systems supported by this release.

Dell tracking: 63585

23. **Description**

You may be unable to set the value for LC attribute on creating a job using settings URI.

Resolution

For LC attributes, use Immediate PATCH operation on **/redfish/v1/Managers/LifecycleController.Embedded.1/Attributes** resource.

Version/Systems affected:

All systems supported by this release.

Dell tracking: 63921

24. **Description**

Firmware update from LC or iDRAC for multiple external enclosures connected to a 12G SAS HBA controller may fail when connected in a daisy-chain configuration.

Resolution

N/A

Version/Systems affected:

All systems supported by this release.

Dell tracking: 63680

25. **Description**

In iDRAC GUI, FC OS driver version is not displayed on the **Network Devices** section.

Resolution

To view the FC OS driver version, use other interfaces such as RACADM or WSMan.

Version/Systems affected:

All systems supported by this release.

Dell tracking: 64168

26. **Description**

Configuration result details may not be displayed in the OMM (OpenManage Mobile) application.

Resolution

Restart QuickSync connection.

Version/Systems affected:

All systems that support QuickSync 2.

Dell tracking: 64138

27. **Description**

If iDRAC to OS pass-through is disabled, SupportAssist registration may display error messages.

Resolution

Enable OS to iDRAC pass-through in iDRAC GUI. To enable the setting, go to **iDRAC Settings → Connectivity → OS to iDRAC Pass-through**.

Version/Systems affected:

All systems supported by this release.

Dell tracking: 64465

28. **Description**

The **Summary** view in Group Manager may show a server entry that has most server details missing, including the Service Tag. This may happen when `racadm racresetcfg -all` is invoked on a member iDRAC.

Resolution

To remove the entry from Group Manager's **Summary** view, reset 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 navigate to **iDRAC Settings → Diagnostics**.

d.   Select **Reset iDRAC**.

When iDRAC fully restarts, the entry no longer appears.

Version/Systems affected:

All systems supported by this release.

Dell tracking: 64213

29.   **Description**

While creating a virtual disk using NVMe physical disks, the LC RAID Configuration Wizard displays blank values for Read Policy, Write Policy, and Disk Cache Policy selections, but default settings are shown for the virtual disk in the **Summary** page.

Resolution

N/A. There are no user-selectable options for these settings.

Version/Systems affected:

All systems supported by this release.

Dell tracking: 59051

30.   **Description**

While setting AssetName and AssetTag for an external enclosure, the Lifecycle Logs as well as the job's ConfigResults do not contain the attribute or the value that was set.

Resolution

N/A

Version/Systems affected:

All systems supported by this release.

Dell tracking: 61929

31.   **Description**

If the host is powered off, the command to set AssetName and AssetTag for an external enclosure fails.

Resolution

To set AssetName or AssetTag, ensure that the host is powered on.

Version/Systems affected:

All systems supported by this release.

Dell tracking: 61932

32.   **Description**

After a SecureErase or PrepareToRemove job for a PCIe SSD in a universal slot, the iDRAC GUI Storage Overview page does not display any PCIe SSD in the Enclosure view for the universal backplane.

Resolution

Restart the iDRAC to display the PCIe SSDs in the Enclosure view.

Version/Systems affected:

All systems supported by this release.

Dell tracking: 64010

33.   **Description**

Using Lifecycle Controller, if you try to update firmware (except driver pack, ISM, OS collector, diagnostic DUPs) and the firmware partition is full, the following warning message is displayed:

```
Insufficient space to store the firmware images. Deleting all rollback firmware images.
Do you want to continue?
```

If you click **No**, the previous screen is displayed and if you click **Apply** again to update the firmware, the same warning message is displayed. If you click **Yes**, the update operation fails.

Resolution

To complete the firmware update operation:

- Click **Yes** when the warning message is displayed for the first time.
- If you clicked 'No' when the warning was displayed for the first time, go to the previous page (Step 2 of 3: Enter Access Details) and start the update again. When the warning message is displayed, click **Yes** to complete the update.

    If you do not want to delete the rollback firmware image, you can cancel the update.

    1. Click **No** on the warning message.
    2. On the Lifecycle Controller page (**Step 3 of 3: Select Updates**), click **Cancel**.

Version/Systems affected:

All systems supported by this release.

Dell tracking: 64280

34. **Description**

If a Backup and Export Server Profile operation is in progress and you set LC attributes using **DCIM_LCService.SetAttribute** method of WSMan interface, further **Set** operations on LC attributes from WSMan may fail.

Resolution

Clear the pending configuration for LC attributes using the Redfish interface.

Version/Systems affected:

All systems supported by this release.

Dell tracking: 62205

35. **Description**

Using iDRAC web interface, you may be unable to delete iDRAC users on first attempt. The following error message is displayed:

```
RAC0508: An unexpected error occurred. Wait for few minutes and retry the operation.
If the problem persists, contact service provider.
```

Resolution

Retry the operation to delete the user.

Version/Systems affected:

All systems supported by this release.

Dell tracking: 64404

Redfish

1. **Description**

iDRAC update performed by Redfish client may display `503 service unavailable error`. This is a time-out error while retrieving the data.

Resolution

Use the `racadm jobqueue view` command to view job status of iDRAC update. If iDRAC is rebooting after an update, wait till iDRAC boots back, and use `racadm jobqueue view` command to view the status.

Version/Systems affected:

All systems supported by this release.

Dell tracking: 63050

2. **Description**

For creating BIOS configuration job in Redfish interface, required privileges are **Login + SystemControl + Configure**, while other interfaces like RACADM and WSMan work with privileges **Login + SystemControl**. Redfish uses additional privilege **Configure** that is not required.

Resolution

N/A

Version/Systems affected:

All systems supported by this release.

Dell tracking: 63343

3. **Description**

OEM URI **/Redfish/v1/Managers/<ID>/Attributes**, can be used for configuring users. A user can only enabled after you provide a user name and password. If you attempt to enable a user, provide a user name, and provide a password in the same operation, Redfish service returns a `400 Bad request` error.

Resolution

Redfish client can use the Dependency section in Attribute Registry metadata to handle attribute dependency.

Version/Systems affected:

All systems supported by this release.

Dell tracking: 62179

4. **Description**

For creating job in Redfish interface, the parameters you need to provide are **TargetSettingsURI**, **StarTime**, and **EndTime**. **EndTime** has a special value **TIME_NA** that means time is not applicable for killing scheduled jobs.

Resolution

N/A

Version/Systems affected:

All systems supported by this release.

Dell tracking: 63526

5. **Description**

Performing Patch operations on attributes **Storage.1.AvailableSpareAlertThreshold, Storage. 1.RemainingRatedWriteEnduranceAlertThreshold**, and **GroupManager.1.Status** causes `Insufficient Privileges` issue.

Resolution

Use RACADM, WSMan, or GUI for configuring these attributes.

Version/Systems affected:

All systems supported by this release.

Dell tracking: 63399

6. **Description**

There is a difference in the way the job type is displayed between Redfish schema file and actual job output.

Resolution

JobType property in Job Instance needs to be read as String instead of ENUM value.

Version/Systems affected:

All systems supported by this release.

Dell tracking: 63699

9

Installation

Installation instructions

- From the Windows host operating system (managed node), run the Dell Update Package for Windows and follow the instructions on the update wizard.
- From the Linux host operating system (managed node), run the Dell Update Package for Linux from the shell prompt. Follow the instructions displayed on the console.
- From the management station, remotely update the firmware using the iDRAC web interface:

  a. Extract the firmware image self-extracting file to the management station.

  b. Open the iDRAC web interface using a supported web browser.

  c. Log in as an administrator.

  d. Go to **Maintenance** → **System Update**. The **Manual Update** page is displayed.

  e. Select **Local** to upload the firmware image file from the local system (Local is selected by default). Click **Browse**, select the .d9 firmware image file that you extracted (step 1), or the Dell Update Package (DUP) for Windows, and click **Upload**.

  f. Wait for the upload to complete. After the upload is completed, the **Update Details** section displays the uploaded file and the status.

  g. Select the firmware file and click **Install**. The message `RAC0603: Updating Job Queue` is displayed.

  h. Click **Job Queue**. The **Job Queue** page is displayed, where you can view the firmware update job status. After the update is completed, iDRAC restarts automatically.

For more information, see the iDRAC 3.00.00.00 User's Guide available at **dell.com/idracmanuals**.

Upgrade

N/A

Uninstallation

N/A

DELLEMC

Lifecycle Controller Remote Services — client tools

Use the OpenWSMAN CLI client tool to send WS-MAN commands to Lifecycle Controller.

OpenWSMAN CLI

OpenWSMAN CLI is an open source Linux WS-MAN client. OpenWSMAN CLI source code and installation details are available at **http://sourceforge.net/projects/openwsman/files/wsmancli**.

Sample OpenWSMAN CLI Command (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 WS-MAN commands do not work without these options: -c, -v, and -V. See the OpenWSMAN CLI Readme for details on these options.

Accessing documents from Dell Support site

Using direct links

You can directly access the documents using the following links:

URL	Product
dell.com/idracmanuals	iDRAC and Lifecycle Controller
dell.com/openmanagemanuals	Enterprise System Management
dell.com/serviceabilitytools	Serviceability Tools
dell.com/OMConnectionsClient	Client System Management
dell.com/OMConnectionsEnterpriseSystemsManagement	OpenManage Connections Enterprise Systems Management

Using the product selector

You can also access documents by selecting your product.

1. Go to **https://www.dell.com/manuals**.
2. In the **Choose from all products** section, click **View products**.
3. Click **Software and Security** and then click the required link.
4. To view the document, click the required product version.

Contacting Dell

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

Dell 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 for sales, technical support, or customer service issues, go to https://www.dell.com/contactdell.