iDRAC9 with Lifecycle Controller Version 3.21.23.22

Release Notes

Notes, cautions, and warnings

(i) **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

Release summary

This release improves the stability and security of iDRAC.

Version

iDRAC9 with LC 3.21.23.22

Release date

September 2018

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

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

Topics:

· Priority and recommendations

Priority and recommendations

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

Compatibility

Supported systems

- PowerEdge C4140
- PowerEdge C6420
- PowerEdge FC640
- PowerEdge M640
- PowerEdge R440
- PowerEdge R540
- PowerEdge R640
- PowerEdge R740
- PowerEdge R740xd
- PowerEdge R840
- PowerEdge R940
- PowerEdge R940xa
- PowerEdge R6415
- PowerEdge R7415
- PowerEdge R7425
- PowerEdge T440
- PowerEdge T640
- Dell Precision Rack R7920
- DCS 1610
- DCS 9650
- DCS 9660
- DCS 9670
- DCS 9690
- DSS 9620
- DSS 9600
- DSS 9630

Previous versions

- 3.00.00.00
- 3.01.00.00
- 3.02.00.01
- 3.05.109.05
- 3.11.11.11
- 3.15.15.15
- 3.15.17.15
- 3.15.18.15
- 3.15.19.15
- 3.15.129.15
- 3.16.16.16
- 3.17.17.17
- 3.17.18.17
- 3.17.20.17
- 3.18.18.18
- 3.21.21.21
- 3.21.21.22

- 3.21.100.21
- 3.21.103.21

Supported managed server operating systems and hypervisors

- Microsoft Windows

  - Server 2012 R2 Foundation
  - Server 2012 R2 Essentials
  - Server 2012 R2 Standard
  - Server 2012 R2 Datacenter
  - Server 2016 Essentials
  - Server 2016 Standard
  - Server 2016 Datacenter
  - WinPE 5.0 64-bit
  - WinPE 10
- Linux

  - RHEL 7.5
  - RHEL 6.9
- SLES

  - SLES 12 SP3
- Ubuntu

  - Ubuntu 16.04.04
- VMware

  - ESXi 6.5 U1
  - ESXi 6.5 U2
  - vSphere 6.7
- Citrix

  - XenServer 7.1 CU1

Supported web browsers

- Microsoft Internet Explorer 11
- Microsoft EDGE
- Safari 8.0.8
- Safari 9.0.3
- Mozilla Firefox 57
- Mozilla Firefox 58
- Google Chrome 62
- Google Chrome 63

Supported software

Java

- Java - Oracle version

DRAC tools

This version of iDRAC requires the DRAC tools from OpenManage 9.1.3 or later for the following:

- VMCLI on Windows or Linux
- Remote RACADM on Linux with IPv6

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

Before installing DRAC tools from OM 9.1.3, 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

Monitoring and alerting

- Enhanced SEL logs for NVDIMM erase errors.

Fixes

Authentication

- 109431: Fixed an issue that prevents Active Directory domain users from logging into iDRAC using QuickSync.

BIOS and UEFI

- 99979: Fixed an issue that may prevent the host from booting using PXE at the next boot cycle.

Hardware

- 109596: Fixed an issue that was sometimes causing PSU firmware update to fail on systems with AMD processors.
- 105885: Fixed an issue that was causing erratic fan speed when Intel X710 NIC/CNA adapters were installed.

iDRAC and LC firmware

- 106312: Fixed an issue that was sometimes causing Auto-config to fail.
- 105516: Fixed an issue that causing iDRAC update to fail when using local RACADM with local share.

Monitoring and alerting

- 108800, 106445: Fixed an issue on DSS 9630 that was preventing Link Status and other properties from being displayed on **Network Devices** page.
- 104875: Fixed an issue that was sometimes preventing iDRAC from displaying complete BOSS inventory.

Networking and IO

- 104465: Fixed an issue that was causing iDRAC to lose IP if iDRAC was reset multiple times.
- 93629: Fixed an issue that could prevent .local domain names from getting resolved using DNS.
- 108239: Fixed an issue that causing DNS sever settings to be deleted if VLAN ID was more than 3 digits.

Security

- 106303: Fixed WebERP vulnerability.
- 108974: Fixed CVE-2017-8890.

Important notes

1. This note is applicable only if you have not performed a power cycle earlier on the system for an iDRAC memory corruption fix. This note is applicable to PowerEdge C6420, DCS 9650, DCS 9660, DCS 9670, DCS 9690, DSS 9620, DSS 9600, and DSS 9630.

   If you update iDRAC to this version, you must perform a power cycle of the system before performing any power-related operations. The power cycle is required to tune the memory parameters without affecting the host. iDRAC tunes the memory parameters at the first power cycle after a firmware update. To allow the memory tuning to be completed:

   a. Update to this version of iDRAC.
   b. At the next possible maintenance cycle, or before any power operations are performed, power down the host.
   c. Wait for 2 minutes to allow iDRAC to reset and tune the memory parameters.
   d. Power on the host.

2. This note is applicable only to PowerEdge M640 and FC640.

   If you update iDRAC to this version, you must perform a virtual reseat of the system from CMC. The reseat is required to tune the memory parameters and to resolve issues that may lead to the watchdog timer causing iDRAC to be reset. To allow the memory tuning to be completed:

   a. Update to this version of iDRAC.
   b. At the next possible maintenance cycle, perform a virtual reseat.

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

4. Rollback is not supported for CPLD.

5. 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.

6. The drivers that LC exposes 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.

7. 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.

8. 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.

9. 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

10. 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: support.microsoft.com/kb/3140245/EN-US.

11. If the network is not configured and you try to perform a network operation in LC, 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.

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

13. 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.

14. 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.

Known issues — To be fixed in future releases

Unable to install RHEL 7.5 using HTML5 virtual console

Description	Installing RHEL 7.5 using an HTML5 virtual console may fail.
Workaround	Install RHEL 7.5 with Java or ActiveX virtual console.
Systems affected	All system supported by this release.
Tracking number	78656

WSMan job with ProcAts attribute fails

Description	Although the ProcAts attribute is not supported in BIOS, you may be able to create a configuration job using WSMan. However, the job fails and returns an error message. This attribute is not visible in any of the interfaces or WSMan enumeration.
Workaround	Do not use the ProcAts attribute because it is not supported in BIOS.
Systems affected	All system supported by this release.
Tracking number	78968

Incorrect slot names displayed in LC logs

Description	Incorrect slot names are displayed in LC logs when NVMe Disks are installed in the system.
Workaround	When an NVMe disk is replaced in a system that has multiple slots in a bay, PR7 message is displayed with Bay <number>, where the <number> is actually the slot number. For example, in the following message, Slot number is 3 and Bay number is 2:

```
[Date]   PR7   Dell NVMe PCIe SSD Configuration Data(Bay 3:Enclosure
Internal 0-2)
```

Systems affected	All system supported by this release.
Tracking number	79270

LC log message about CPU performance adjustment

Description	If the Chassis Manager firmware is older than version 1.45 and if you update iDRAC to this version, the following message is displayed in Lifecycle Log:

```
The performance of CPUx is automatically readjusted by Chassis Controller
because of unacceptable change in thermal and power conditions.
```

Workaround	This message can be ignored. Update the Chassis Manager firmware to version 1.45 or later to resolve the issue.
Systems affected	PowerEdge C6420

Tracking number   85136

ValueName regex does not match schema definition

Description   ValueName regex does not match the schema definition for some of the properties in the BIOS Attribute Registry and the Boot Sources Registry returned by Redfish API.

Workaround   Defer the regex check for the ValueName returned for BIOS Attribute Registry and the Boot Sources Registry against the schema.

Systems affected   All system supported by this release.

Tracking number   88651

iDRAC power allocation error prevents system boot

Description   Sometimes, if you reboot the system multiple times within a short duration, the following message is displayed and the boot process stops:

```
HALT:Did not get response for power allocation from iDRAC in time
```

Workaround   Restart iDRAC.

Systems affected   All system supported by this release.

Tracking number   91412

RACADM command does not fully clear a job configuration

Description   If a job is in Scheduled state and there is another job for the same component in Completed or Failed state, the `racadm JID_CLEARALL` command does not clear the configuration completely. In such a scenario, the device or component cannot be configured further.

Workaround   To clear the configuration completely, use the following command:

```
racadm jobqueue delete -i JID_CLEARALL_FORCE
```

Systems affected   All system supported by this release.

Tracking number   93652

Importing foreign virtual disk fails

Description   The import foreign virtual disk command fails in the following scenario:

1. Create a VD on a physical disk. A job is created and moved to Pending state.
2. Delete the pending job on the pending adapter.
3. Disconnect the physical disk without shutting down the system.
4. Reconnect and import the physical disk.

In this scenario, the pending adapter status mask is not reset.

Workaround   Before importing the disk, perform a clear-pending operation using any of the iDRAC interfaces.

| **Systems affected** | All system supported by this release. |
| **Tracking number** | 94823 |

Online Help text is cropped

Description	If the DPI of your screen in Windows is set to higher than 125%, some characters in the Online Help of iDRAC web interface get cropped.
Workaround	Use a DPI of 125% or lower.
Systems affected	All system supported by this release.
Tracking number	97805

Remote syslog alerts not received

Description	If the syslog server is configured with IPv6, remote syslog alerts are not received.
Workaround	Use IPv4 on the syslog server.
Systems affected	All system supported by this release.
Tracking number	98450

Error responses for HTTP status codes do not match Redfish standard

Description	The JSON error responses returned by Redfish API for HTTP status codes 501 and 401 do not follow Redfish extended error-response standard.
Workaround	Ignore any response-message parser errors.
Systems affected	All system supported by this release.
Tracking number	98614

Job completion percentage displayed incorrectly in Redfish

Description	In the Redfish interface, after a firmware update or rollback job is complete, the completion percentage displays as 254% instead of 100%.
Workaround	No action is required. A 'Completed' status indicates that the job is successful.
Systems affected	All system supported by this release.
Tracking number	98973

Easy Restore does not restore BIOS settings

Description	While replacing the system board, Easy Restore may not restore the BIOS settings unless there is a difference in the NIC configuration on the old and replacement system boards.
Workaround	N/A
Systems affected	All system supported by this release.
Tracking number	99973

Options not displayed in iDRAC web interface when accessed through CMC

Description	When you launch iDRAC from CMC using the Launch Remote Console option or by using the console URL https://[iDRAC IP]/console, the following options may not be displayed:

- **Configuration** > **System Settings** > **Hardware Settings**
- **Configuration** > **Storage Configuration**
- **Configuration** > **Server Configuration Profile** > **Import**

Workaround	When you launch iDRAC from CMC, click **Dashboard**, wait for the page to load, and then navigate to the desired pages.
Systems affected	All system supported by this release.
Tracking number	100013

Random characters displayed in LC log

Description	If an SSO login fails, the message in LC log displays random characters instead of indicating that an unknown SSO user attempted to log in.
Workaround	N/A
Systems affected	All system supported by this release.
Tracking number	100201

Undesired characters displayed while entering user name at the host OS prompt

Description	If you reboot the host and enter the user name followed by a backspace at the host OS prompt, undesired characters are displayed. The issue occurs only if a session with SSH and IPMI SOL is active.
Workaround	Press Enter to display the login prompt again and enter the correct characters. If you are at the password prompt, press ^C to exit the prompt.
Systems affected	All system supported by this release.
Tracking number	100327

Unable to download files from iDRAC using Safari

Description	If you access the iDRAC web interface using Safari, you may be unable to download some types of files. The files include SCP export, license, hardware inventory, video captures, Group Manager summary and jobs, Lifecycle logs, and so on.
Workaround	Use one of the other supported browsers.
Systems affected	All system supported by this release.
Tracking number	100814

Links to Enclosure and Chassis resources unavailable in Redfish

Description   In Redfish, the links to the Enclosure or Chassis are unavailable under the associated Storage and Drive resources within a storage subsystem. This issue affects systems that have a BOSS card, HHHL card, or direct-attached drives.

Workaround   Navigate to the Chassis resource collection to locate the storage subsystem and the drives associated with the Enclosure or Chassis.

Systems affected   All system supported by this release.

Tracking number   101035

Incorrect priority displayed for firmware on iDRAC web interface

Description   While updating any firmware from the iDRAC web interface, Recommended firmware versions are listed as **Critical** and Critical firmware versions are listed as **Recommended**.

Workaround   Firmware versions listed as **Critical** are Recommended versions. Firmware versions listed as **Recommended** are Critical versions.

Systems affected   All system supported by this release.

Tracking number   101676

Unable to set time zone to Canada/East-Saskatchew

Description   If you try to set the time zone to Canada/East-Saskatchew in iDRAC, an error is displayed stating that the data is incorrect.

Workaround   The Canada/East-Saskatchewan time zone is obsolete and is replaced by America/Regina. If you have a system with the time zone set to Canada/East-Saskatchew, reconfigure it to use America/Regina.

Systems affected   All system supported by this release.

Tracking number   101847

GET operation fails when using NetworkDeviceFunction URI

Description   For a Fibre channel card, when you perform a GET operation on the link in network ports provided under PhysicalPortAssignment and AssignablePhysicalPorts using the NetworkDeviceFunction URI, the command fails with the status `404 Not found`.

Workaround   To get the information, use other Redfish URIs such as NetworkInterfaces or NetworkAdapters.

Systems affected   All system supported by this release.

Tracking number   101982

Limitations

Authentication

1. LC supports the following characters for username and password:
   - Alphabets (a-z, A-Z)
   - Numbers (0-9)
   - Special characters (-, _, .)
2. If you set a user with only SHA256 password, for example, through SCP, you cannot delete the user using the web interface. To delete such a user, edit the user explicitly setting a password and then try to delete the user.
3. 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.
4. 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.

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. 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.
2. 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.
3. In LC, not all the vendor FC cards are supported for VLAN configuration.

iDRAC and LC firmware

1. Due to known limitations in OpenSource (SFCB), query filtering with long integers and lengthy strings may not work as expected.
2. LC can import and view an iDRAC license but cannot export or delete the iDRAC license. The iDRAC license can be deleted from iDRAC web interface.
3. The iSCSI offload attribute can be enabled only on two of the four available ports. If a card, which has this attribute 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.

Monitoring and alerting

1. The inventory displayed in LC UI may not be the same as that of any iDRAC interfaces. To get the updated inventory, run CSIOR, wait for 2 minutes, reboot the host, and then check the inventory in LC UI.
2. In certain cases, Group Manager Jobs view may not show a detailed error message for a member iDRAC job. For more information about the failure, review the job execution details in the Lifecycle Logs of the member iDRAC by using the web interface (**Maintenance** > **Lifecycle Log**) or by using the RACADM command `racadm lclog view`.
3. 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.
4. **Hardware Inventory** page lists only the primary backplane in cascaded backplane configurations. To view complete information, use the **Firmware Inventory** page.

Networking and IO

1. 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.
2. 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.
3. 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**.
4. 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**).
5. 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**.
6. 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.
7. 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.
8. LC does not support SOCK4 proxy with credentials.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.

OS deployment

1. 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.
2. 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.

3. LC displays two drive names for some CDs or DVDs, such as the ones containing operating systems.
4. 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.
5. LC does not support OS deployment on Dell Precision Workstation R7920.

Automation — API and CLI

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

Security

1. iDRAC 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.
2. By default, LC uses SMBv1 protocol and all LC features that use CIFS share fail if SMBv1 is disallowed on Windows/Samba mounts. To use CIFS shares, enable SMBv1 on the system where the share is located. This, however, may lower your system's security. To retain security and compatibility, it is recommended to upgrade your Samba server to version 4.0 or later, which supports SMBv2 protocol.
3. 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. If an H730P adapter is installed in slot 9 (internal PERC slot) of PowerEdge T640, iDRAC displays it as H730P Integrated RAID Controller (Embedded).
2. While renaming a virtual disk (VD), using a . (period) is not allowed in the VD name.

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 version 3.21.21.21 Lifecycle Controller User's Guide available at www.dell.com/idracmanuals.
5. After the CPLD firmware is updated on modular systems, the firmware update date is displayed as 2000-01-01 on the View Current Versions page. The update date and time is displayed according to the time zone configured on the server.
6. On some modular systems, after a firmware update, the Lifecycle Log displays the time-stamp as 1999-12-31 instead of the date on which the firmware update was performed.
7. It is not recommended to perform CPLD update along with other updates. If a CPLD update is uploaded and updated along with other updates using iDRAC web interface, CPLD update completes successfully but the other updates do not take effect. To complete the iDRAC updates, reinitiate the updates.
8. After downgrading iDRAC from this version to version 3.00.00.00, 3.11.11.11, or 3.15.15.15, the jobs created in the job queue are deleted. Recreate the jobs after the downgrade is complete.
9. On PowerEdge R6415, R7415, R7425, if you downgrade from this version of iDRAC to an earlier version, some certificate-related operations may not work correctly and certain hardware information may not be displayed correctly. To resolve the issue, reset iDRAC using the `racresetcfg` command.

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. When using Internet Explorer or Google Chrome to access the HTML5 virtual console from a Windows OS, the floating menu at the top of the window may not be displayed. Use Mozilla Firefox to view the menu.
6. Launching Virtual Console with Java plug-in fails after the iDRAC firmware is updated. Delete the Java cache and then launch the virtual console.
7. 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.

Updating iDRAC firmware

Downloading iDRAC firmware installation file

ⓘ **NOTE: For information about updating iDRAC firmware using various interfaces, see version 3.21.21.21 iDRAC User's Guide available at www.dell.com/idracmanuals.**

1. Go to 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

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

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**.

After the update is complete, iDRAC restarts automatically.

Lifecycle Controller Remote Services — client tools

OpenWSMAN CLI

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

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

Sample OpenWSMAN CLI Command for an enumeration operation:

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

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

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

Resources and support

For more information about the features of this release, see the documentation for iDRAC 3.21.21.21.

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 this version of iDRAC.
3. Click **Manuals & documents**.

Accessing documents using direct links

You can directly access the documents using the following links:

Table 1. Direct links for documents

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

Accessing documents using the product search

1. Go to www.dell.com/support.
2. In the **Enter a Service Tag, Serial Number...** search box, type the product name. For example, `PowerEdge` or `Integrated Dell Remote Access Controller`.

   A list of matching products is displayed.
3. Select your product and click the search icon or press enter.
4. Click **Manuals & documents**.

Accessing documents using product selector

You can also access documents by selecting your product.

1. Go to 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.
   (i) **NOTE: For some products, you may need to navigate through the subcategories.**
5. Click **Manuals & 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 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.