Dell Chassis Management Controller (CMC) Version 2.23 for Dell PowerEdge VRTX

Release Notes

Dell Chassis Management Controller

The Dell Chassis Management Controller (CMC) Version 2.22 for Dell PowerEdge VRTX is a System Management hardware and software solution for managing the Dell PowerEdge VRTX chassis.

Version

2.23

Release Date

April 2017

Previous Version

2.22

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.

Platform(s) Affected

Dell Chassis Management Controller (CMC) for Dell PowerEdge VRTX is supported on the following system:

Chassis:

- PowerEdge VRTX

Blades:

- Dell PowerEdge M630
- Dell PowerEdge M830
- Dell PowerEdge M620
- Dell PowerEdge M820
- Dell PowerEdge M520

IOMs:

- Dell PowerEdge VRTX Switch Module R1-2401
- Dell PowerEdge VRTX Switch Module R1-2210
- Dell PowerEdge VRTX 1Gb x8 pass-through module

License Requirements

The CMC supports software licensing to use advanced systems management features. For more information about the license requirements, see the Dell Chassis Management Controller for Dell VRTX User's Guide available at the support site.

What is Supported?

Supported Web Browsers for CMC for Dell PowerEdge VRTX

CMC version 2.23 is supported on the following web browsers:

- Microsoft Internet Explorer 9
- Microsoft Internet Explorer 10
- Microsoft Internet Explorer 11
- Microsoft EDGE
- Safari version 7.1
- Safari version 8.0
- Mozilla Firefox version 40
- Mozilla Firefox version 41
- Google Chrome version 49
- Google Chrome version 50

Supported Server Modules

- Supported platforms: PowerEdge M630, M520, M620, M820, and M830 servers.
- Mainboard firmware: 2.00 or later (2.20 or later for JBOD support)
- iDRAC7 Version: 1.66.56 or later
- iDRAC8 Version: 2.05.05 or later (M630 Servers)
- PowerEdge M520 BIOS Version: 2.1.3 or later
- PowerEdge M620 BIOS Version: 2.2.7 or later
- PowerEdge M820 BIOS Version: 2.0.24 or later
- PowerEdge M820 BIOS version: 0.3.35 or later
- PowerEdge M830 BIOS version: 1.1.5 or later

What is New?

- Federal Information Processing Standards (FIPS) certified. Certification Number: #2861. For details, see www.csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#2861

Release 2.22

- Updated the OpenSSL open source package to version 1.0.2j.

Release 2.21

N/A

Release 2.20

- Federal Information Processing Standards (FIPS) 140-2 cryptography capability.
- Disabling AC Power Recovery.
- Creating a Virtual Disk without initialization of the virtual disk.
- Pre-enablement of the following features for Self-Encrypting Drives (SEDs):
    - Creating, modifying, and deleting the security key (using key identifier and passphrase)
    - Secure erase
    - Encrypting virtual disks

    - Unlocking and importing secure foreign virtual disk configuration using RACADM and WSMan
- Querying shared storage health using SNMP.
- Enabling sPERC Redundancy and setting up Multiple Assignment Mode using WSMan.
- Performing racresetcfg from CMC GUI.
- Updating the OpenSSL open source package to version 1.0.2f.
- Updating the OpenSSH open source package to version 7.1p1.
- Updating glibc to version 2.23 to address new security vulnerabilities.
- TLS 1.2 and TLS 1.1 by default.
- User configuration option to enable TLS 1.0 using RACADM.
- SNMPv3 configuration only in RACADM.
- Querying the health status of the chassis components using WSMan.
- Initiating Quick Deploy of blade through RACADM.
- Configuring CMC using WSMan for the following features:
    - Host Name of Chassis
    - IP Configuration
    - DNS
    - DNS Registration
    - NTP
    - Change Default Password
- Sending alerts when the power state of an IOM changes and when a power ON of IOM fails.
- Populating CMC Device name correctly in the inventory.

Release 2.12

- Quick link to the Dell Tech Center page from the CMC web GUI.

Release 2.10

- Support for PowerEdge M830 Blade server for PowerEdge VRTX Chassis.
- Support for 1100W PSU.
- Pre-enablement support for Shared External Storage expansion (JBOD support).
- Firmware and driver refresh of COMMs cards on Dell's 13th generation PowerEdge servers.
- Support for Emulex Fibre Channel (FC) 8 HBA adapters.
- Capture and replicate chassis configurations through XML based on the Chassis configuration profile.
- Support for blinking server identification LED using Quick Link.
- Backup or restore through XML based on the chassis configuration profile.
- Create and deploy a library of Boot Identity Profiles (boot from iSCSI/SAN configurations) to enable a quick restore of workload to a spare server.

Fixes

- Fixed an issue causing CMC changeover when chassis overall health was updated.

Release 2.22

N/A

Release 2.21

N/A

Release 2.20

- Fixed an issue causing flash Media Status showing as "Version mismatch" during changeover or upgrade of the CMC.
- Fixed an issue that caused the **Server Profile** page to hang when a profile is applied to multiple servers.
- Fixed an issue limiting the speed of bNDC ports on some blades to 1 Gb after initial chassis turn on or blade insertion.

Release 2.12

- Fixed an issue causing failure of RAID10 Virtual Disc (VD) with 8, 12 or 16 drives in creating full VD when the span count 2 is selected.
- Fixed an issue with Server/Host operating system (OS) network flap, which occurs occasionally on Modular platforms for a short duration during CMC initialization.
- Fixed an issue with Server/Host OS network port off, which occurs after CMC is reset on full-height Modular platforms, when the second network daughter card is not installed.
- Fixed an issue causing the CMC Web GUI to become unresponsive while using Active Directory login with WinRM.
- Fixed an issue causing memory full condition when the internal log files are oversized.

Release 2.10

- Fixed an issue with the "getmacaddress -c all” command displaying partial IO Identity values for the Intel Dual Port Network Card 10 GBE.
- Fixed an issue with the “getmacaddress –m server-x –t iscsi” command displaying non-iSCSI MAC addresses after using the iSCSI filter.
- Fixed an issue with flash media features displaying invalid media for active controllers after restoring the chassis.
- Fixed an issue with the external storage expansion where chassis logs and alerts are not generated.

Release 2.04

- Fixed an issue where CMC sometimes does not notify or show storage changes until a chassis powercycle, CMC reset, or failover is performed.
- Fixed an issue where CMC User Interface is unresponsive while CMC is still accessible through other interfaces such as CLI (SSH, Serial, telnet) and WSMan.

Release 2.01

- Updated OpenSSL open source package to version 1.0.1j. For more information see the *OpenSSL Security Advisory* [15 Oct 2014] at <https://www.openssl.org/news/secadv_20141015.txt>.

Important Notes

- It is recommended not to downgrade CMC or Mainboard firmware below the supported versions mentioned in this release notes, since previous versions of CMC and Mainboard do not support SPERC disable option.
- When the second SPERC is in the disabled mode, if a CMC with firmware version 1.30 or 1.31 is inserted into the chassis, then update the CMC firmware to 1.35 and run the options to disable the PERC again.
- The shared hard disk drives (HDDs) and PCIe cards are managed by the CMC and are not visible to the operating system in the server modules, until the HDDs and PCIe cards are mapped by using the CMC web interface. For instructions about mapping PCIe cards and managing the storage subsystem, see the *Chassis Management Controller for PowerEdge VRTX User's Guide* available at the support site.
- All the server modules must be turned off before updating the firmware for chassis infrastructure and SPERC. CMC firmware can be updated while the servers are turned on.
- Some advanced features require CMC enterprise license. For more information about the CMC licenses, see the *Chassis Management Controller for PowerEdge VRTX Version User's Guide* available at the support site.
- Before updating the storage component using the web interface, make sure that the browser's Cookies are enabled.
- PERC storage rebuild may take more time when more number of I/O requests are processed, and could also make CMC and the TTY log to be out of sync for a short period of time.
- In fault-tolerant (Redundant) mode, the controller associated with virtual disks or physical disk drives is the active controller.
- When saving Server Profile under "**Server Overview > Setup > Profiles**", the list of characters that are not supported for the Profile Name include the characters hash(#), comma(,), and question mark(?).
- You may see an impact in the performance of the Graphical User Interface with this release of CMC. The performance impact varies by configuration, GUI page, and system load.
- Microsoft Windows Server 2012, Windows Server 2008 R2, Windows 7 do not support TLS 1.2 and TLS 1.1. Install update below to enable TLS 1.2 and TLS 1.1 as a default secure protocols in WinHTTP in Windows. For details, see the Microsoft knowledge base article 3140245 at **support.microsoft.com**.
- Supports LDAP authentication with OPEN-DS. OPEN-DS must have DH key larger than 768 bits.

Known Issues

Issue 1:

Description

XWKGY_Intel10G card shows Flex disabled address after racresetcfg of CMC in Network Device page and OS.

Resolution

Virtual reseat or Physical reseat of the server.

Versions/Systems Affected

All CMC versions including CMC 2.23 for Dell PowerEdge VRTX and PowerEdge servers with iDRAC7 or earlier.

Issue 2:

Description

After Shared PERC8 controller update, RAID related operations may take longer to report status.

Resolution

Wait for the operation status to report.

Versions/Systems Affected

CMC version 2.01 for Dell PowerEdge VRTX.

Issue 3:

Description

An error occurs while importing CMC configuration file using local racadm or remote racadm.

Resolution

This issue occurs when IPv6 is enabled or disabled from the configuration file. Enable or disable IPv6 using the command “racadm config -g cfgIPv6LanNetworking -o cfgIPv6Enable 0”.

Versions/Systems Affected

CMC 2.0 or later for Dell PowerEdge VRTX

Issue 4:

Description

At times when foreign drives are inserted, the Chassis Overview Health tab does not display the alert, “Foreign Configuration was detected on Physical Disk”.

Resolution

None. The alert is not displayed only at times. But, the functionality for foreign configuration is not affected.

Versions/Systems Affected

All CMC versions including CMC 2.23 for Dell PowerEdge VRTX.

Issue 5:

Description

When CMC firmware is downgraded to 1.36 from 2.00 or later while network share is configured, the **Server Components Update** page gets corrupted.

Resolution

Clear the network configuration before downgrading to 1.36

Versions/Systems Affected

CMC Version 1.36 or earlier for Dell PowerEdge VRTX

Issue 6:

Description

When pinned cache is present, the controller failover feature does not work.

Resolution

Address the pinned cache before controller failover is allowed.

Versions/Systems Affected

All CMC versions including CMC 2.23 for Dell PowerEdge VRTX.

Limitations

Issue 1:

Description

In the Microsoft Edge browser, the Boot Identity Profiles page in the CMC GUI is slow when 1500 or more MAC addresses are created from the MAC pool for the Boot Identity profile.

Resolution

Create less than 1500 MAC address in the Microsoft Edge browser. Use other supported browsers for more than 1500 MAC addresses.

Versions/Systems Affected

CMC Version 2.20 or later for Dell PowerEdge VRTX

Issue 2:

Description

Racresetcfg does not work when the six RSA-4096 or four RSA-2048, and two 2048 DSA SSH public keys are uploaded to the CMC.

Resolution

Do not upload six RSA-4096 or four RSA-2048, and two 2048 DSA SSH public keys to the CMC.

Versions/Systems Affected

CMC Version 2.00 or later for Dell PowerEdge VRTX

Installation

Prerequisites

Before setting up your CMC environment, download the latest version of CMC firmware for PowerEdge VRTX from the Dell Support Website at dell.com/support/. Also, make sure that you have the Dell Systems Management Tools and Documentation DVD that is included with your system.

Installation Procedure

1. In the CMC web interface, click **Chassis Overview**, and then click **Update**.
2. On the **Firmware Update** page, in the **CMC Firmware** section, select the required components under the **Update Targets** column for the CMC or CMCs (if a standby CMC is present) you want to update, and then click **Apply CMC Update**.
3. In the **Firmware Image** box, type the path to the firmware image file on the management station or shared network, or click **Browse** to browse through to the file location. The default name of the CMC firmware image file is vrtx_cmc.bin.
4. Click **Begin Firmware Update**, and then click **Yes**. The **Firmware Update Progress** section displays information about the firmware update status.

For more information, see the Chassis Management Controller for PowerEdge VRTX User's Guide available at the support site.

VRTX Update Procedure

Prerequisites

- iDRAC web interface for each server node must be accessible from management station.
- Local or remote access to OS management for each server node.
- VRTX chassis CMC web interface must be accessible from management station.
- All server and chassis components must be in a Healthy state with no outstanding issues or alerts. Any issues must be resolved prior to performing updates.

Server Node Updates

Visit support.dell.com and download the latest available Windows DUP versions of the following programmable components for the server node model (M520, M620, M630 or M820) used in the VRTX chassis to be updated:

- BIOS
- iDRAC7/8
- CPLD

Also, download the latest available Shared PERC8 driver for the operating system installed on the server node.

Note: If the OS is VMWare ESXi, the driver is part of the Dell ESXi image.

Updating the Server Nodes

1. Update the operating system-specific Shared PERC8 driver on all the server nodes. For Windows operating system, see the *Shared PERC8 User's Guide* available at **dell.com/support**. For VMware, the driver is part of the Dell-customized ESXi image. For more information, see installing async drivers at **kb.vmware.com**.
2. Update the iDRAC firmware using Windows DUP and the iDRAC web interface for each server node or on all server nodes at once through VRTX CMC web interface if Enterprise license is in place and

the Extended Storage feature is enabled. This update takes several minutes to complete. After the update, iDRAC web interface is inaccessible for approximately 3 minutes.

3. Update the CPLD on each server node using the Windows DUP and iDRAC web interface. Make sure to select “Install and Reboot” after uploading the DUP, which forces the server nodes to reboot and perform the CPLD update. After the CPLD update completes a complete server node power cycle occurs. This action results in the iDRAC web interface being inaccessible for approximately three minutes.
4. Update the BIOS on each server node using Windows DUP and the iDRAC web interface, or on all server nodes at once through the VRTX CMC web interface (**Server Overview -> Update** tab) if Enterprise license is in place. Make sure to select “Install and Reboot” after uploading the DUP, which forces the server nodes to reboot and execute the BIOS update.

VRTX Chassis Component Updates

Visit dell.com/support and download the latest available versions of the following programmable components for the VRTX chassis to be updated:

- CMC Firmware
- HDD Firmware (Windows DUP)
- Shared PERC8 Firmware (Windows DUP)
- VRTX Chassis Infrastructure Firmware
- VRTX Storage Backplane Expander Firmware (Windows DUP)

Note: To perform the following updates, refer to the “Updating VRTX Chassis Components” section.

Updating VRTX Chassis Components

1. Before updating any chassis components, the chassis must be powered on, all server nodes must be powered down, and remain powered down until all chassis component updates are complete.
2. Update the HDD firmware for each of the installed shared storage HDD, using the **Storage -> Update** tab in the CMC web interface.
3. Update the CMC firmware using the **Chassis Overview -> Update** tab in the CMC web interface. Make sure to update both CMC controllers in the same operation by selecting both the Active and Standby controller checkboxes. After the firmware upload completes, the CMC is rebooted to perform the update resulting in the CMC web interface being inaccessible for several minutes.
4. Update the VRTX chassis infrastructure firmware using the **Chassis Overview -> Update** tab in the CMC web interface. This update results in the chassis power cycling automatically and may result in a CMC controller reset as well. As e result, the CMC web interface becomes inaccessible for several minutes.
5. Update the VRTX storage backplane expander firmware using the **Storage -> Update** tab in the CMC web interface.
6. Verify that all installed Shared PERC8 controllers are enabled by checking the **Storage -> Controllers** tab in the CMC web interface. If the second Shared PERC8 controller is displayed as “Disabled PERC (Integrated 2)”, use the CMC command ‘racadm raid enableperc:RAID.ChassisIntegrated.2-1’ to enable the previously disabled controller prior to performing Step 7 below. The VRTX chassis power cycles after the Shared PERC8 enablement command is run.
7. Update the Shared PERC8 controller firmware on all installed controllers using the **Storage -> Update** tab in the CMC web interface. Make sure to update both controllers in the **High Availability Dual Shared PERC8** configuration in the same operation.
8. If a Shared PERC8 controller was required to be enabled for update in Step 6 above, you can disable the controller again if required. Use the CMC command ‘**racadm raid disableperc:Raid.ChassisIntegrated.2-1**’. This command results in a chassis power cycle.

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 see **dell.com/contactdell**.

Accessing Documents from Dell Support Site

For information about documentation support:

1. Go to **dell.com/support/manuals**.
2. In the **Tell us about your Dell system** section, under **No**, select **Choose from a list of all Dell products** and click **Continue**.
3. In the **Select your product type** section, click **Software and Security**.
4. In the **Choose your Dell Software** section, click the required link from the following:
   - Client System Management
   - Enterprise System Management
   - Remote Enterprise System Management
   - Serviceability Tools
5. To view the document, click the required product version.

You can also directly access the documents using the following links:

- For Chassis Management Controller documents - **dell.com/cmcmanuals**
- For iDRAC and Lifecycle Controller documents — **dell.com/idracmanuals**
- For Enterprise System Management documents — **dell.com/openmanagemanuals**
- For Serviceability Tools documents — **dell.com/serviceabilitytools**
- For Client System Management documents — **dell.com/OMConnectionsClient**
- For OpenManage Connections Enterprise systems management documents — **dell.com/OMConnectionsEnterpriseSystemsManagement**
- For OpenManage Connections Client systems management documents — **dell.com/OMConnectionsClient**

Information in this document is subject to change without notice.

© 2017 Dell Inc. All rights reserved.

This product is protected by U.S. and international copyright and intellectual property laws. Dell and the Dell logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Rev A00