Dell Chassis Management Controller Version 5.22

Release Notes

Dell Chassis Management Controller

The Dell Chassis Management Controller (CMC) is a hot-pluggable systems management hardware and software solution designed to provide the following functions for Dell PowerEdge M1000e chassis system:

- Remote management capabilities
- Power control
- Cooling control

Version

Dell Chassis Management Controller 5.22

Release Date

April 2017

Previous Version

Dell Chassis Management Controller Version 5.21

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).

Platform(s) Affected

CMC version 5.22 supports the following Dell PowerEdge(TM) systems in the Dell PowerEdge M1000e system enclosure:

- Dell PowerEdge M630
- Dell PowerEdge M830
- Dell PowerEdge M420
- Dell PowerEdge M520
- Dell PowerEdge M600
- Dell PowerEdge M605
- Dell PowerEdge M610
- Dell PowerEdge M610X
- Dell PowerEdge M620
- Dell PowerEdge M710
- Dell PowerEdge M710HD
- Dell PowerEdge M805
- Dell PowerEdge M820
- Dell PowerEdge M905
- Dell PowerEdge M910
- Dell PowerEdge M915
- Dell EqualLogic PS-M4110

What is Supported?

Supported Web Browsers

CMC version 5.22 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

What's 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 5.21

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

Release 5.20

- Federal Information Processing Standards (FIPS) 140-2 cryptography capability.
- Disabling AC Power Recovery.
- 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 5.13

- Added a RACADM command to enable or disable CMC failover due to network link loss.
- To check CMC changeover state for network failure : racadm cmcchangeover --state
- To enable this flag : racadm cmcchangeover -e 1
- To reset this flag : racadm cmcchangeover -e 0

Release 5.12

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

Release 5.10

- Firmware and driver refresh of COMMs cards on Dell's 13th generation of PowerEdge servers.
- Capture and replicate chassis configurations through XML based on the Chassis configuration profile.
- Support for blinking server identification LED from Quick Link on the Homepage.
- 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.
- Populate iDRAC DNS setting from the CMC Quick Deploy page.
- Display iDRAC DNS name as the slot name.
- Option to view iDRAC LCLog results directly in CMC after applying a Server Configuration Profile.
- Support for launching IOA GUI on Homepage, I/O Module overview page.
- Support to list IOA Flex modules on IOM properties page and in tooltip.

Release 5.01

- CMC Secure IOM mode is implemented in CMC 5.01. Secure IOM provides additional CMC security in support of MXL IOMs running in UC-APL secured environments.

Fixes

N/A

Release 5.21

N/A

Release 5.20

- Fixed an issue causing flash Media Status showing as "Version mismatch" during changeover or upgrade of the CMC.
- Fixed an issue causing 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.
- Fixed an issue causing the slots 1-4 not initializing iDRAC after initial turn on.

Release 5.12

- 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.
- Fixed an issue causing non-display of some of the KVM-related information on the CMC web GUI.

Release 5.11

- Fixed an issue causing the health of the IOMs in slot 5 and 6 displaying "Not OK" on the CMC Interface for chassis with an IOM installed in slot 6.

Release 5.10

- 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.

Release 5.02

- Fixed an issue causing CMC redundancy loss in CMC 5.0.
- Fixed an issue causing the CMC Web GUI to become unresponsive in CMC 5.0.

Release 5.01

- Upgraded OpenSSL to version 1.0.1j.
- Updated NTP to version ntp-ssl-4.2.6p3.
- Upgraded Apache to version 2.4.10.
- Fixed PS-M4110 failure to boot issue in CMC 5.0.
- When an IOM is connected through Data Center Bridging, then PS-M4110 must be configured through its own serial port and cannot be configured through CMC interfaces.
- Fixed the power budgeting issue that occurs when SPOR is disabled.

Release 5.00

- Upgraded an open source component of WS-MAN namely Small Footprint CIM Broker (SFCB) from 1.3.10 to 1.3.17, where CIM is Common Information Model.
- Fine-tuned memory monitoring daemons.

Important Notes

- While using Remote RACADM client with CMC 5.21 version, make sure that Remote RACADM client version 8.0.2 is installed.
- When Certificate Validation is Enabled, FQDN of the system must be provided. If IP address of the Domain Controller is specified when certificate validation is enabled, then the Active Directory login does not work.
- 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 5.22 and PowerEdge servers with iDRAC7 or earlier.

Issue 2:

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 version 5.11 or later

Issue 3:

Description

When CMC firmware is downgraded to 4.50 from 5.00 or later while network share is configured, the Server Components Update page gets corrupted.

Resolution

Clear the network configuration before downgrading to 4.50

Versions/Systems Affected

CMC version 4.50 or earlier

Limitations

Issue 1:

Description

While executing WSMan commands continuously, some commands may timeout occasionally, but get resolved quickly without CMC failover or reboot.

Resolution

None

Versions/Systems Affected

All CMC versions including CMC 5.22

Issue 2:

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 5.11 or later

Issue 3:

Description

When the M1000e chassis is power cycled, the Dell PowerEdge PS-M4110 may not turn on and the message "iDRAC Not Ready" is displayed.

Resolution

To turn on the server, reset CMC or virtually reseat the server.

Versions/Systems Affected

All CMC versions including CMC 5.22

Installation

Prerequisites

For information on pre-requisites, see the Dell PowerEdge M1000e Chassis Management Controller Firmware Version 5.20 User's Guide.

For information on Hardware and Software requirements, see the Dell PowerEdge M1000e Chassis Management Controller Firmware Version 5.20 User's Guide.

For information on Installation and Configuration, see the Dell PowerEdge M1000e Chassis Management Controller Firmware Version 5.20 User's Guide.

Installation Instructions

For information on installation, see the Dell PowerEdge M1000e Chassis Management Controller Firmware Version 5.20 User's Guide.

Upgrade

See the *Prerequisites* section for the correct version numbers.

Upgrading Dell PowerEdge M1000e I/O Aggregator

I/O Aggregator must first be updated to version 8.3.17.4 before updating to version 9.2.0.0 or greater.

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

To access the documents from Dell Support site:

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**

Rev A00