Chassis Management Controller Version 4.0

Readme

What’s New

These topics describe the new features.

1. Support for PowerEdge M620 and iDRAC7 servers.
2. Save and restore chassis configuration.
3. Improved SEL log.
4. Broadcom 57810-k Dual Port 10GB Blade Network Daughter Card.
5. Broadcom 57810-k Dual Port 10GB Blade Mezzanine Card.
6. Intel I350 Quad Port 1GB Blade Mezzanine Card.
7. Intel x520-k Dual Port 10GB Blade Network Daughter Card.
8. Intel x520-k Dual Port 10GB Blade Mezzanine Card.
9. Qlogic QMD8262-k Dual Port 10GB Blade Network Daughter Card.
10. Mellanox M4001Q QDR/DDR InfiniBand Switch.
11. Mellanox M4001F FDR InfiniBand Switch.
12. Mellanox ConnectX-3 QDR/DDR InfiniBand Blade Mezzanine Card.
13. Mellanox ConnectX-3 FDR InfiniBand Blade Mezzanine Card.
14. CMC MIB expansion to contain OIDs for Chassis Physical Location.
15. CMC MIB expansion to contain OIDs for Blade Server Service Tag and Slot name.
16. OpenManage Power Center enabled to manage server power.
17. One to many replication of BIOS server settings for iDRAC6 and iDRAC7 servers (Server Cloning).
18. Multi-Chassis Management feature enabled to synchronize properties of new member to those of the leader.
19. Availability of CPU and Memory information from GUI for servers, which support the Lifecycle Controller (LC).
20. Support for inventory of Servers and IOMs and report generation for an MCM (multi-chassis management) group.

Prerequisites

Supported System

CMC version 4.0 is supported on the following Dell PowerEdge(TM) systems in the Dell PowerEdge M1000e system enclosure:

- 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 M905
- Dell PowerEdge M910
- Dell PowerEdge M915

Recommended Module Firmware Versions

- iDRAC Firmware Version:

  - 3.30 for Dell PowerEdge M610, M610X, M710, M710HD, M910, M915

  - 1.60 for Dell PowerEdge M600, M605, M805, M905

- iDRAC7 Firmware Version:

  - 1.00 for Dell PowerEdge M620

- Dell Lifecycle Controller Version:

  - 1.5 for Dell PowerEdge M610, M610X, M710, M710HD, M910, M915

  - 2.0 for Dell PowerEdge M620

- BIOS Version:

  - 1.0.0 for Dell PowerEdge M620

  - 6.0.7 for Dell PowerEdge M610, M610X, M710

  - 5.0.0 for Dell PowerEdge M710HD

  - 2.4.4 for Dell PowerEdge M910

  - 2.6.0 for Dell PowerEdge M915

  - 2.4.0 for Dell PowerEdge M600

  - 5.4.1 for Dell PowerEdge M605

  - 2.3.3 for Dell PowerEdge M805, M905

Supported Web Browsers

CMC version 4.0 is supported on the following web browsers:

- Microsoft Internet Explorer 7: Windows XP 32-bit SP3, Windows Vista SP2 x32 and x64, Windows Server 2003 SP2 x32 and x64, Windows Server 2008 SP2 x32 and x64.
- Microsoft Internet Explorer 8: Windows XP 32-bit SP3, Windows Vista x32 and x64 SP2, Windows 7 x32 and x64, Windows Server 2003 x32 and x64 SP2, Windows Server 2008 x32 and x64, Windows Server 2008 R2 x64.
- Microsoft Internet Explorer 8 (x64): Windows Vista X64 SP2, Windows 7 x64, Windows Server 2003 x64 SP2, Windows Server 2008 x64, Windows Server 2008 R2 x64.
- Microsoft Internet Explorer 9: Windows Vista x32 and x64 SP2, Windows 7 x32 and x64, Windows Server 2008 R2 x64.
- Microsoft Internet Explorer 9 (x64): Windows Vista x64 SP2, Windows 7 x64, Windows Server 2008 R2 x64.

- Mozilla Firefox 6.0: Windows XP 32-bit SP3, Windows Vista x32 and x64 SP2, Windows 7 x32 and x64, Windows Server 2003 x32 and x64 SP2, Windows Server 2008 x32 and x64, Windows Server 2008 R2 x64.
- Mozilla Firefox 7.0: Windows XP 32-bit SP3, Windows Vista x32 and x64 SP2, Windows 7 x32 and x64, Windows Server 2003 x32 and x64 SP2, Windows Server 2008 x32 and x64, Windows Server 2008 R2 x64.

Upgrade

The Lifecycle Controller is a service available on each of the servers and is facilitated by iDRAC. The **Server Component Update** page enables you to manage the firmware of the components and devices on the servers using the Lifecycle Controller service. The Lifecycle Controller uses an optimization algorithm to update the firmware in the most efficient manner that reduces the number of reboots. Before using the Lifecycle Controller based update feature, update the server firmware versions.

Refer to the "Prerequisites" section for the proper version numbers. The modules should be updated in the following order:

- BIOS

- Lifecycle Controller

- iDRAC6

NOTE: Before you update the server component firmware modules listed above, you must update CMC firmware.

NOTE: To update firmware using Lifecycle Controller, iDRAC firmware must be of version 2.3 or greater.

If manually updating firmware using Dell Update Packages (DUPs), the firmware should be updated in the following order:

- BIOS

- Lifecycle Controller

- iDRAC6

NOTE: To update iDRAC firmware to 3.0 or greater from an iDRAC version less than 2.3, you must first update the iDRAC firmware to version 2.3 before updating to version 3.0 or greater.

Open Issues and Resolutions

- Versions 6.0 and 7.0 of Mozilla Firefox Web Browser do not support IPv6 addresses.
  You must use URLs that contain a registered hostname to access a CMC or an iDRAC Server that has an IPv6 address. A CMC or an iDRAC Server that also has an IPv4 address is supported.

- Non-English versions of the Online Help for power configuration pages incorrectly state that the required privilege for changing power configuration settings is "Chassis Control Administrator."
  The correct privilege is "Chassis Configuration Administrator."

- While using the command "racadm config -f" with:
  - CMC 3.21 or later versions of the firmware, make sure that the Remote RACADM client version 6.3.0 or later is installed.
  - CMC with an earlier version of 3.21 firmware, make sure that the Remote RACADM client version earlier than 6.3.0 is installed.
- The Remote RACADM testfeature command (racadm -r <IP Address> testfeature ...) does not support the -d (debug) option.

- For Single Sign-On and Smart Card login, the client system must be a part of the Active Directory domain and Kerberos Realm. On Windows 7, clients under the Local Security Policies must make sure to configure the security option "Network security: Configure encryption types allowed for Kerberos." This policy setting allows you to set the encryption types that Kerberos is allowed to use. The DES_CBC_MD5 encryption type must be selected. If this encryption type is not selected, the encryption type will not be allowed. This setting may affect compatibility with client computers or services and applications.
- When you add a member chassis to a chassis group using the Multi-Chassis Management feature, you cannot specify the group members with an IPv6 address.

Global Support

For information on technical support, visit **www.dell.com/contactus**.

For information on documentation support, visit **support.dell.com/manuals.** On the **Manuals** page, click **Software** ->**Systems Management.** Click on the specific product on the right -side to access the documents.

Information in this document is subject to change without notice.

2012 – 03 **Rev. A00**