##

DELL(TM) CHASSIS MANAGEMENT CONTROLLER Version 2.10

##
Version: 2.10
Release Date: 31 August 2009
This document contains updated information about the Dell Chassis
Management Controller (CMC).

For more information about the CMC, including installation and
configuration information, see the "Dell Chassis Management Controller
Firmware Version 2.10 User Guide" and the "Dell OpenManage(TM) Server
Administrator User's Guide." These documents are located on the Dell
Support website at "support.dell.com".

##
TABLE OF CONTENTS
##

This file contains the following sections:

##
CRITICALITY
##

2 - Recommended

##
MINIMUM REQUIREMENTS
##

The following subsections list the operating systems that are compatible
with the CMC version 2.10.

==
SUPPORTED SYSTEMS
==

CMC version 2.10 is supported on the following Dell PowerEdge(TM) systems
in the Dell PowerEdge M1000-e system enclosure:

* Dell PowerEdge M600
* Dell PowerEdge M605
* Dell PowerEdge M805
* Dell PowerEdge M905
* Dell PowerEdge M610
* Dell PowerEdge M710

==========
SUPPORTED WEB BROWSERS
==========

* Microsoft(R) Internet Explorer(R) 6.0 (32-bit) with SP1 for Windows Server(R) 2000 family

* Microsoft Internet Explorer 6.0 (32-bit) with SP2 for Windows(R) XP and Windows Server 2003 family

* Microsoft Internet Explorer 7.0 for Windows Vista(R), Windows XP, and Windows Server 2003 family

* Mozilla Firefox(R) 1.5 (32-bit) - limited functionality

* Mozilla Firefox 2.0-3.x (32-bit).

==========
FIRMWARE VERSIONS
==========

* CMC Firmware Version: 2.10

==========
RECOMMENDED MODULE FIRMWARE VERSIONS
==========
Additional recommended chassis module firmware if CMC version 2.10 is installed.

* iDRAC Firmware Version: 1.50 (or later) for Dell PowerEdge M600, Dell PowerEdge M605, Dell PowerEdge M805, Dell PowerEdge M905
2.10 (or later) for Dell PowerEdge M610, Dell PowerEdge M710

* BIOS Version: 2.1.4 for Dell PowerEdge M600
5.0.4 for Dell PowerEdge M605
2.0.2 for Dell PowerEdge M905, Dell PowerEdge M805
1.2.7 for Dell PowerEdge M610, Dell PowerEdge M710

* CPLD Version: 1.1.1 for Dell PowerEdge M600
1.1.0 for Dell PowerEdge M605
1.1.0 for Dell PowerEdge M905, Dell PowerEdge M805
1.0.2 for Dell PowerEdge M610, Dell PowerEdge M710

##########

RELEASE HIGHLIGHTS
##

Fixes and Enhancements in version 2.10
---
* IPv6 — CMC now supports the IPv6 protocol.
The IPv6 Ready Logo Committee's mission is to define the test
specifications for IPv6 conformance and interoperability testing,
provide access to self-test tools, and to deliver the IPv6 Ready Logo. The CMC
is Phase-2 IPv6 Ready Logo certified, and the Logo ID for the CMC is
02-C-000378 (Dell PowerEdge M1000e). For information on the IPv6 Ready Logo
Program, see www.ipv6ready.org.

* VLAN tagging — The CMC and the iDRACs now support the ability to
assign their network traffic to a virtual LAN (VLAN).

* Single sign-on for active directory accounts — Single sign-on allows
authenticated users using Microsoft® Active Directory® on their local systems
to automatically apply those credentials to the CMC Web user interface.

* Two-Factor Authentication using Smart Card — Provides added security
—a smart card plus a PIN to authenticate a user instead of only a password.

* Public Key Authentication (PKA) over SSH — Improves SSH scripting
automation by removing the need to embed or prompt for
user ID/password.

* Power management enhancements — Flexible redundancy modes: 1+1,
2+1, and 3+1 power supply redundancy. Additional fault-tolerant AC
redundant modes: 1+1, 2+2, and 3+3.

* Additional error reporting options — The iDRAC system events log (SEL) is displayed
on the Blade Status page eliminating the need to log into the iDRAC to
view the system events. Also, CMC events are now also posted to a remote syslog server.

* Remote Virtual Media File Share option — to map a file from a share drive
on the network to one or more blades through the CMC to deploy or
update an operating system.

* Ability to read and clear SEL entries for servers from the CMC command-line interface.

##
KNOWN ISSUES FOR BROWSERS
##

* In Internet Explorer version 6, the log data may not display. Instead
  the "Loading Chassis Event Log..." message may be displayed.
  To address this issue, go to Advanced Settings/Security and make sure
  the "Allow active content to run in files on My Computer" option is
  NOT checked.

* In Internet Explorer version 6, if the security setting is set to
  'Restricted', the CMC User Interface on the Alert Management pages for
  Email Alerts and SNMP Traps pops up a Security Information message

stating that the page contains both secure and non-secure items and will ask if you want to continue. Select "Yes". This is because Internet Explorer version 6 does not allow the use of hidden IFRAMES on secure (SSL) pages. (183022)

* In Firefox version 1.5, you must manually refresh pages. Automatic page updating is not fully supported in this version of the Firefox browser.

* In Internet Explorer version 6, after updating the active CMC you may need to close the browser used to login to the CMC before attempting to login again. (232942)

* When loading or sorting CMC log entries in a Firefox browser, you may get a pop up warning about an unresponsive script. To prevent these warnings, perform the following steps:

(a) In the Firefox address bar, enter "about:config".
(b) Scroll down and find the "dom.max_script_run_time" entry.
(c) Double-click that entry and change the value to at least 30. (248345)

* When using the CMC Web Interface, a popup dialog may appear with the message "Content from the website listed below is being blocked by the Internet Explorer Enhanced Security Configuration. https//".

You can perform one of two actions to prevent this popup dialog:

1. Uncheck the option on popup check box to "Continue to prompt when website content is blocked" and click Close.

-OR-

2. Enable scripting (Javascript) in the Internet zone.
   – From the browser menu, select: Tools->Internet Options->Security Tab
   – Select the "Internet" zone.
   – Click the "Custom Level…" button.
   – Scroll to "Scripting->Active scripting" section and click Enable.
   – Click the OK button.

Click the OK button. (297730)

##
KNOWN ISSUES FOR CMC Version 2.10
##

* CMC firmware 1.2 has enhanced the power allocation algorithms to allow modular servers to receive higher power allocations. If you downgrade the CMC to 1.10 or an earlier firmware version, servers with the new higher power allocations may be powered off because the earlier firmware cannot support the higher chassis power allocations. If this occurs, power the server back on. (230143)

* After a CMC reset, the CMC may require up to one minute after the login prompt is displayed before accepting the RACADM commands . Commands issued prior to that time may receive an error message. (273716)

* The RACADM command line tool uses TFTP to transfer image files for all firmware updates. Only the default port for TFTP (69) is supported. (157754)

* Clearing the CMC log may take up to one (1) minute to complete. (152860)

* If the CMC is on a private network without access to the Internet and you are using Internet Explorer 6 SP 2 or Internet Explorer 7, you may experience delays of up to 30 seconds when using remote RACADM commands. (161019)

* Some USB-to-serial adapters generate a large number of spurious interrupts when plugged in. If the adapter is connected to the CMC's serial port when this happens, the CMC may become overloaded while attempting to service these interrupts and may reboot. This problem is exacerbated when the serial cable is very long, causing voltage levels to drop and noise on the serial line to increase. To avoid this issue, Dell recommends first connecting the USB-to-serial adapter into the USB port, before connecting to the CMC. Dell also recommends disconnecting the adapter from the CMC before rebooting or performing other power management functions on a system that is attached to the CMC. (180373)

* If you setup Active Directory (AD) on the CMC using extended schema and the built-in Administrator privilege object, and then attempt to login to the CMC User Interface using this AD account, after a successful AD login, the user name and privilege level displayed on the right-hand side of the User Interface just beneath the log out link is displayed as a custom user rather than the privilege as created on the AD side (example: Administrator, power user). (183449)

* Using the RACADM command line utility, if you attempt to set the DNS CMC Name or DNS Domain Name without the proper rules, (Rules: A string of upto 63 (for CMC Name) / 254 (for DNS Domain Name) alphanumeric characters (a-z, A-Z, 0-9) and hyphens), the utility may display a non-specific error message (ERROR: Unable to perform requested operation). Enter a valid string for the above mentioned names.(173204)

* A 'racadm config' operation may fail, due to configuration property definition changes across firmware versions. For example, if the set of allowable values for a configuration property has been changed, and a snapshot of the prior values (from 'racadm getconfig') is used in a 'racadm config' operation on a newer version of firmware, the prior values may no longer be accepted, and thus cause the racadm config operation to fail.(229764)

  To resolve this issue, comment out the prior value in the captured file, and restart the 'racadm config' operation.

  The following lists the racadm property definitions that differ, depending on the CMC firmware version:

  group: cfgNetTuning, object: cfgNetTuningNicSpeed
  - CMC Firmware 1.0 and 1.10:

Allowed values: 10, 100, 1000 (default 1000)

- CMC version 1.20 and later:
  Allowed values: 10, 100 (default 100)

* While performing firmware updates on servers located in the chassis, make sure there is minimal to no activities on the server (for example, avoid running discovery on the servers through management applications such as IT Assistant or running IPMI commands). (276448)

* While performing multiple iDRAC firmware updates, the CMC performs CPU-intensive activities and may not respond or respond slower for the first couple of minutes. Please refrain from running additional commands during this period. (281719)

* Updating the firmware on an Infiniband IOM (IOMINF) causes the IOM to reset at the end of the update procedure. (270706)

* When configuring network settings on the iDRAC using the CMC RACADM commands, make sure the command executed is completed successfully, before running another network configuration command. To ensure that the settings are applied on the target iDRAC, check the current configuration using the appropriate RACADM command or use the Web GUI. (322063)

* When using the remote RACADM windows client, on a management station with Internet Explorer version 7.0 or above installed, to capture the existing RACADM configuration into a file, the command fails due to a timeout issue, without giving a success or failure message. Manually run the individual commands to capture cfgServerInfo(for all required indexes), cfgKvmInfo and cfgAlerting groups and add them to the configuration file.(303086)

* When browsing the Remote File Share page for the servers, some of the blade servers may indicate in the 'Connect Status' column they are already connected. The does not necessarily mean a Remote File Share is already in progress on the blade server. It is possible the blade server may have a 'Virtual Media' session in progress and in the connected state. In such situations and prior to proceeding with the Remote File Share operations (Connect/Disconnect/Deploy), please ensure the existing Virtual Media session on the blade server is not inadvertently overridden. If this is the intention, then it is possible to proceed with the Remote File Share operations and override the existing Virtual Media session on the blade server. Similarly, if an existing Remote File Share session was already in progress on the blade server, the 'Connect Status' column would indicate a connected state and it would be possible to override the existing Remote File Share session.(322091)

* When connecting to a switch with the connect command, an error message 'stty: /dev/ttyS1: unable to perform all requested operations: No such file or directory' may be displayed. This message does not prevent you from connecting you to the switch and may be ignored.(325197)

##
KNOWN ISSUES FOR USER INTERFACE ONLINE HELP
##

No known issues for this release.

##
KNOWN ISSUES FOR DOCUMENTATION
##

No known issues for this release.

##
FLEXADDRESS
##
Required Module Firmware to use the Chassis FlexAddress feature with CMC 2.10:

Component	Required version
Ethernet Mezzanine card - Broadcom M5708t/M5708is,M5708	Firmware 4.4.1, iSCSI boot firmware 2.7.11, PXE firmware 4.4.3
FC Mezzanine card - QLogic QME2472	BIOS 2.04 or later
FC Mezzanine card - Emulex LPe1105-M4	BIOS 3.03a3 and firmware 2.72A2
Blade Server BIOS	(PE M600) BIOS 2.1.4 or later (PE M605) BIOS 4.02 or later (PE M805) 1.1.2 or later (PE M905) 1.1.2 or later (PE M610) All BIOS versions (PE M710) All BIOS versions
iDRAC	Firmware 1.50 or later(PE M600, PE M605, PE M805, PE M905) or Firmware 2.10 or later(PE M610, PE M710)
CMC	Firmware 2.10

* FlexAddress: Prior to inserting the SD card into the CMC, verify the write
  protection latch is in the "unlock" position.
  The FlexAddress feature cannot be activated if the SD card is write-
  protected.
* FlexAddress: The system BIOS must be upgraded prior to installing
  FlexAddress. If not, a warning icon is displayed on the
  server health page. Once the system BIOS is updated, the modular
  server must be power cycled before the FlexAddress chassis-assigned
  MAC addresses are accepted by the modular server. The CMC
  displays that chassis-assigned MACs are configured but the server will
  use the server-assigned MAC configuration.
* FlexAddress: If you issue a CMCCHANGEOVER or RACRESET and then log
  into the CMC Web GUI, the FlexAddress Web page may take up
  to a minute to update the switch configurations.

* FlexAddress: If a chassis with a single CMC is downgraded with firmware earlier than version 1.10, the FlexAddress feature and configuration will be removed. Once the CMC firmware is upgraded to 1.10 or later, the FlexAddress feature must be reactivated and configured.
* FlexAddress: In a chassis with two CMCs, if you are replacing a CMC unit with one that has firmware earlier than version 1.10, perform the following procedure to ensure that the current FlexAddress feature and configuration is not removed.
  1. Ensure the active CMC firmware is always version 1.10 or later.
  2. Remove the standby CMC and insert the new CMC in its place.
  3. From the Active CMC, upgrade the standby CMC firmware to 1.10 or later.

  Note: If you do not update the standby CMC firmware to 1.10 or later and a failover occurs, the FlexAddress feature is not configured and you will need to reactivate the feature.
* FlexAddress: Wake-On-LAN (WOL) requires BIOS to initialize MAC values. When the FlexAddress feature is deployed for the first time on a given modular server, it requires at least one power-up and down sequence for FlexAddress to take effect. The reason for this is the FlexAddress on Ethernet devices is programmed by the BIOS. The BIOS needs to be functioning to program the address. This in turn requires the modular server to be powered up. Once the power-up and power-down sequence has been completed, FlexAddress is available for the Wake-On-LAN (WOL) function. You may perform power-up and power-down sequence on the modular server for fully deploying FlexAddress through the iDRAC or CMC interface.
* When changing from a server-assigned MAC to a chassis-assigned MAC on Linux operating systems, additional configuration steps may be required.
  - o SLES 9 and SLES 10: You may need to run YAST (Yet another Setup Tool) on your Linux system to configure the network devices and then restart the network services.
  - o Red Hat® Enterprise Linux® version 4 and version 5: You may need to run Kudzu, a utility to detect and configure new/changed hardware on the system. Kudzu displays the Hardware Discovery Menu and detects the MAC address change as hardware was removed and new hardware added.
* Prior to installing FlexAddress, you can determine the range of MAC addresses contained on the Flexaddress feature card by inserting the SD card into a USB “Memory Card Reader” and viewing the file "pwwn_mac.xml". The clear text XML file on the SD card contains an XML tag "mac_start" which is the first starting hex MAC address that is used for this unique MAC address range. The “mac_count” tag is the total number of MAC addresses that this SD card allocates. The total MAC range allocated can be determined by: "mac_start" + 0xCF (208 – 1) = mac_end.
  Example:(starting_mac)00188BFFDCFA + 0xCF =(ending_mac)00188BFFDDC9

  NOTE: Lock the SD card before inserting it in the USB “Memory Card Reader” to prevent accidental modification of any of the contents. You must unlock the SD card before inserting into the CMC.

##

August 2009