##

DELL(TM) CHASSIS MANAGEMENT CONTROLLER (CMC)

##

This document contains updated information about the Dell Chassis
Management Controller (CMC).

For more information about CMC, including installation and configuration information, see the "Dell Chassis Management Controller Firmware Version 2.00 User's Guide" and the "Dell OpenManage(TM) Server Administrator User's Guide." These documents are located on the Dell Support website at "support.dell.com" and with your Product Documentation CD.

##

TABLE OF CONTENTS

##

This file contains the following sections:

##

CRITICALITY

##

2 - Recommended

##

MINIMUM REQUIREMENTS

##

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

==

SUPPORTED SYSTEMS

==

CMC 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 6.0 (32-bit) with SP1 for Windows 2000
  Server family.

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

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

* Mozilla Firefox 1.5 (32-bit) - Limited Functionality.

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

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

* CMC Firmware Version:         2.00

==================================================
MODULE FIRMWARE VERSIONS RECOMMENDED
==================================================
Additional Chassis module Firmware recommended if CMC 2.00 is installed.

* iDRAC Firmware Version:        1.40 (or later) for PE M600, PE M605, PE M805, PE M905
                                 2.00 (or later) for PE M610, PE M710

* BIOS  Version:                 2.1.4 for PE M600
                                 4.02  for PE M605
                                 1.1.2 for PE M905, PE M805
                                 2.18  for PE M610, PE M710


##########################################################################
RELEASE HIGHLIGHTS
##########################################################################

Fixes and Enhancements in 2.00
---------------------------------------
* Support for PowerEdge M610 & M710 servers
* 1:Many iDRAC firmware update (from CMC)
* CMC to iDRAC Single Sign On (SSO)
```

* Improved iDRAC configuration/deployment:
  (a) QuickDeploy IP/root password for newly inserted servers.
  (b) Auto-increment and auto-populate static network settings for the iDRAC.
  (c) 1:many root password changes across existing & newly inserted servers.
* Improved DNS registration
* LCD deployment wizard improvements
* Navigation tree & tab improvements
* iDRAC GUI launch point from CMC Server Summary page
* iDRAC MAC address display on the CMC Server Summary page.
* IOM GUI launch point from CMC
* Improved troubleshooting from CMC
* Network time protocol (NTP) for CMC
* Improved power monitoring
* Improved power budgeting
* Improved temperature sensors Display
* CMC failover/reset via the GUI
* Server virtual reseat

##

KNOWN ISSUES FOR BROWSERS

##

* In Internet Explorer Version 6, the log data may not display, instead a message of "Loading Chassis Event Log..." is shown. To address this issue, go to Advanced Settings/Security and make sure the option, "Allow active content to run in files on My Computer" 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 will pop 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 the 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, take the following steps:

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

##
KNOWN ISSUES FOR CMC
##

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

* After a CMC reset, the CMC may require up to one (1) minute after the login prompt is displayed before RACADM commands will be accepted. Commands issued prior to that time may receive an error message.(273716)

* 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 can take a long time. Please allow up to one (1) minute for this operation 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 have been found to 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 can become overloaded when 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 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: start with an alphabetic character (a-z, A-Z) and follow by an alphanumeric (a-z, A-Z, 0-9) or a valid symbol (such as -)) then the utility will display a non-specific error message (ERROR: Unable to perform requested operation). Please enter a valid name 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 the servers located in the chassis, make sure there is minimal to no activities on the server (ex: avoid running discovery on the servers via management application such as IT Assistant or running IPMI commands). (276448)

* It is always recommended that once you have your configuration setup to then save the CMC configuration to a .cfg file using a specified file name. This can be accomplished by using the remote racadm (CLI) tool: racadm getconfig -f <filename>. If you ever have to restore the settings you can reimport them back using the same tool and running racadm config -f <filename> (279404)

* While performing firmware updates on chassis servers, make sure there are minimal or no server activities ;
  for example, avoid running server discovery using a management application such as IT Assistant or running IPMI commands. (276448)

* It is recommended that once you have your configuration completed, you save the CMC configuration to a .cfg file using a specified file name. To save the file, enter the following command using the remote RACADM (CLI) tool:

```
racadm getconfig -f <filename>.
```

  If you ever need to restore the configuration settings, you can re import them by entering the following command:

```
racadm config -f <filename> (279404)
```

* When performing firmware updates using the RACADM command line utility, make sure that you confirm the updates. Once you initiate the updates, you will not be able to cancel.(282471)

```
* While performing multiple iDRAC firmware updates, the CMC will be
  performing CPU-intense activities and may not respond, or respond
  slower, for the first couple of minutes. Refrain from running
  additional commands during this period. (281719)

* During an iDRAC Firmware update initiated from the CMC that contains
  a wrong  IP address, file name, or other typo, the result will be
  a valid failure. However, the log information will display the
  following:
  Failed to update iDRAC firmware on blade 5138: Transfer Failed.
  Error=0x2.
  The log entry has the chassis server and error code numbers
  interchanged. (279469)

* During an iDRAC Firmware update initiated from the CMC that contains
  a wrong file path that was unintentionally set, then error
  code 0x1407, for a file not found, may be displayed. (283351)

* Use the Web-based interface when setting the serial port timeout
  to a value greater than 1920 seconds. Use the RACADM command line utility
  to set timeout values that are either less than 1920 seconds, or to
  disable the timeout by setting a 0 value. (287918)

#######################################################################
KNOWN ISSUES FOR USER INTERFACE ONLINE HELP
#######################################################################

No known issues for this release.

#######################################################################
KNOWN ISSUES FOR DOCUMENTATION
#######################################################################

No known issues for this release.


#######################################################################
FLEXADDRESS (Provided in CMC 1.10 Release)
#######################################################################
Required Module Firmware to use Chassis FlexAddress feature:
----------------------------------------------------------------
 Component                          |  Minimum required version
----------------------------------------------------------------
 Ethernet Mezzanine card -              |  Firmware 4.4.1,
 Broadcom M5708t/M5708is,M5708          |  iSCSI boot firmware 2.7.11,
                                    |  PXE firmware 4.4.3
----------------------------------------------------------------
 FC Mezzanine card -                    |  BIOS 2.04 or later
 QLogic QME2472
----------------------------------------------------------------
 FC Mezzanine card -                    |  BIOS 3.03a3 and firmware 2.72A2
 Emulex LPe1105-M4                      |  or later
----------------------------------------------------------------
 Blade Server BIOS                      | (PE M600) BIOS 2.02 or later
```

```
                                  | (PE M605) BIOS 2.03 or later
                                  | (PE M805) All BIOS versions
                                  | (PE M905) All BIOS versions
                                  | (PE M610) BIOS 2.16 or later
                                  | (PE M710) BIOS 2.16 or later
---------------------------------------------------------------
 iDRAC                            | Firmware 1.11 or later
---------------------------------------------------------------
 CMC                              | Firmware 1.10 or later
---------------------------------------------------------------
```

* FlexAddress: Prior to inserting the SD card into the CMC, the user must 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 will be displayed on the server health page. Once the system BIOS is updated, the server blade must be power cycled before the FlexAddress chassis assigned MAC addresses will be accepted by the server blade. The CMC will display chassis assigned MACs are configured but the server will be using the server assigned MAC configuration.
* FlexAddress: If you issue a CMCCHANGEOVER or RACRESET and then log into the CMC Web GUI, the FlexAddress webpage could take up to a min to update the switch configurations.
* FlexAddress: If a chassis with a single CMC is downgraded with firmware prior to 1.10, the FlexAddress feature and configuration will be removed. Once the CMC firmware is upgraded to 1.10 or later, the FlexAddress feature will need to be reactivated and configured by the user.
* FlexAddress: In a chassis with a two CMC, if replacing a CMC unit with one that has firmware prior to 1.10, the following procedure must be used to ensure the current FlexAddress feature and configuration will NOT be 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 FlexAddress feature will not be configured and the user will need to reactive 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 blade, 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. In order for the BIOS to program the address it would need to be functioning, this in turn requires blade to be powered up. Once the power-up and power-down sequence has been completed, FlexAddress would be available for Wake-On-LAN (WOL) function. Users may perform power-up and power-down sequence on the blade for fully deploying FlexAddress via iDRAC or CMC interface.
* When changing from a Server-Assigned MAC to Chassis_Assigned MAC on Linux Based operating systems, additional configuration steps may be

required.
o SLES 9 and SLES 10: Users may need to run YAST (Yet another Setup
Tool) on their Linux system to configure their Network devices
and then restart the network services.
o RHEL 4 and RHEL 5:   Users will need to run Kudzu, a utility to
detect and configure new/changed hardware on the system. Kudzu
will present the user with The Hardware Discovery Menu, it will
detect the MAC address change as Hardware was removed and new
Hardware added.

* Prior to installing FlexAddress, the user can determine the range
of MAC addresses contained on their Flexaddress feature card by
inserting the SD card into an USB “Memory Card Reader” and viewing
the file "pwwn_mac.xml". The clear text XML file on the SD card
will contain an XML tag "mac_start" which is the first starting
hex MAC address that will be 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: You should lock the SD card prior to inserting in the USB
“Memory Card Reader” to prevent accidently modifying any of the
contents. You MUST UNLOCK the SD card before inserting into the CMC.

###

Information in this document is subject to change without notice.

Trademarks used in this text: "Dell", "Dell OpenManage", and
"PowerEdge" are trademarks of Dell Inc.; "Microsoft", "Windows",
"Windows Vista", "Windows Server", and "Active Directory" are
trademarks or registered trademarks of Microsoft Corporation.

Other trademarks and trade names may be used in this document to refer
to either the entities claiming the marks and names or their products.
Dell Inc. disclaims any proprietary interest in trademarks and trade
names other than its own.

March 2009