##

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 1.0 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
##

3 - Optional

##
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 and M605.

==========
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).

* Mozilla Firefox 2.0 (32-bit).

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

* CMC Firmware Version: 1.0

##########
RELEASE HIGHLIGHTS (FIRMWARE VERSION 1.0)
##########

The CMC provides the following management features:
---

* Dynamic Domain Name System (DNS) registration

* Remote system management and monitoring using a Web interface, iKVM, or Telnet/SSH connection.

* Support for Microsoft(R) Active Directory(R) authentication — Centralizes CMC user IDs and passwords in Active Directory using the Standard Schema or an Extended Schema.

* Monitoring — Provides access to system information and status of components

* Access to system event logs - Provides access to the hardware log and CMC log.

* Dell OpenManage(TM) software integration - Enables you to launch the CMC Web interface from Dell OpenManage Server Administrator or IT Assistant.

* CMC alert — Alerts you to potential managed node issues through an email message or SNMP trap.

* Remote power management - Provides remote power management functions, such as shutdown and reset on any chassis component, from a management console.

* Secure Sockets Layer (SSL) encryption — Provides secure remote system management through the Web interface.

* Password-level security management — Prevents unauthorized access to a remote system.

* Role-based authority — Provides assignable permissions for different systems management tasks.

* Launch point for the Integrated Dell Remote Access Controller (iDRAC) Web-based interface.

* Support for WS-Management.

The CMC provides the following security features:
---

* User authentication through Microsoft Active Directory (optional) or hardware-stored user IDs and passwords.

* Role-based authority, which enables an administrator to configure specific privileges for each user.

* User ID and password configuration through the Web-based interface or SMCLP CLI.

* SMCLP CLI and Web-based interface operation, which supports 128-bit SSL encryption and 40-bit SSL encryption (for countries where 128-bit is not acceptable).
NOTE: Telnet does not support SSL encryption.

* Configurable IP ports (where applicable).

* Login failure limits per IP address, with login blocking from the IP address when the limit is exceeded.

* Limited IP address range for clients connecting to the CMC.

* Secure Shell (SSH), which uses an encrypted layer for higher security.

* WS-Management requires client to provide the SSL CA certificate for secure connection. The certificate can be extracted from CMC via remote racadm tool with sslcertdownload or openssl tool with s_client -showcerts.

##
KNOWN ISSUES FOR BROWSERS
##

* In Internet Explorer Version 6, the log data may not display,
  leaving only the message, "Loading Chassis Event Log..." shown .
  To address this, 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. Please select "Yes". This is because
  the Internet Explorer Version 6 does not allow the use of hidden IFRAMES
  on secure (SSL) pages. (183022)

##
KNOWN ISSUES FOR CMC
##

* RACADM CLI based command line tool uses TFTP to transfer image files
  for all firmware updates. Only the default port for TFTP (69) is
  supported for transfers with version 1.0. (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)

* In the CMC User Interface, under Chassis -> Network/Security tab->
  Network subtab, If the network speed is set to 1GB to match your
  network environment then CMC will revert to Auto Negotiation internally
  to determine the network speed and Duplex Mode. It will not use the
  values set.(180871)

* Using the RACADM command line utility, setting the network speed to 1GB
  will cause the CMC to revert to Auto Negotiation internally to determine
  the network speed and Duplex Mode. (180873)
  For Example, this will be ignored and Auto Negotiation will be attempted.
       racadm setniccfg -k 1000 full

* 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)

* The "connect" to server command enables the user to access the server's

serial port through CMC's serial port. After this connection the user will be able to see the server's console redirection through CMC's serial port.

Following are the prerequisites for this feature:

1. The server should be Powered on.
2. Serial redirection has to be enabled in the servers BIOS Setup.
3. Not all keys will work so the user has to provide appropriate escape sequences for "CTRL+ALT+DEL" etc. The initial redirection screen displays the necessary escape sequences.(184385)

* 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 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 server slot name to a name greater than 15 characters (unsupported and documented in the CMC User's Guide) then you will get a generic error message. (ERROR: The specified object value is not valid) (181364)

* 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)

* If a firmware update operation is attempted via the CMC User Interface using an invalid image file of a very small size (few bytes) then there will be no error message indicating the failure of this operation. Please attempt to upload the valid image and restart the firmware update operation. (186170)

* If the standby CMC firmware was updated at a previous time and later made active, you will see an entry in the CMC log (raclog) that states the firmware update was successful but with the most recent time stamp. This is because the standby CMC cannot register its entries to the logs until it becomes active. (186858)

KNOWN ISSUES FOR USER INTERFACE ONLINE HELP

This section provides additional information about known issues with the CMC Firmware version 1.0 User Interfaces online help.

* The help for the Services Management page located in the Chassis->

Network/Security tab->Services sub-tab of the CMC user interface in localized languages does not list the Telnet Port legal values. (179080)

* The help for the Slot Names page located in the Chassis-> Servers -> Setup->Slot Names sub-tab of the CMC user interface in localized languages does not list the rules for the slot names, which are:
(a) The beginning of the string cannot be Switch-, Fan-, PS-, KVM, DRAC/MC-, Chassis and Housing-Left/Right/Center, which are case insensitive.
(b) ASCII characters between 32 and 126 are allowed, but excludes 34 (").
(c) Server-n, where n is 1 to 10, is not allowed except that Server-n is allowed for the n slot, which is case insensitive. Server-0n is different from Server-n, like Server-02 is different from Server-2. Therefore Server-2 is not allowed for any slot except the second one but Server-02 can be set in any slot. (178014)
(d) Maximum allowed characters for the Slot Name is 15. (181364)

* The help for the Server Status page located in the Chassis-> Servers -> Server 1-16 -> Properties tab->Status sub-tab of the CMC user interface in localized languages does not list the Slot Name, Present properties. It also has a reference to I/O module instead of servers under Health -> Informational section. (179718)

* The help for the Chassis Power Management page located in the Chassis-> Power Management tab->Control sub-tab of the CMC user interface in localized languages refers to Power Off System as equivalent to pressing the power button when the power is "ON". This is not accurate since this action performs a graceful shutdown of the chassis and if any of the modules do not shutdown within the time period, they will remain on. (181069)

* The help for the Identify page located in the Chassis-> Troubleshooting tab->Identify sub-tab of the CMC user interface in localized languages mentions the note:
To blink or unblink the servers, you must have Log in to iDRAC privilege on the iDRAC of these servers.

This is missing Server Administrator privilege on CMC and should be:

To blink or unblink the servers, you must have Server Administrator privilege on CMC or Log in to iDRAC privilege on the iDRAC of these servers. (175595)

* The help for the User Configuration page located in the Chassis-> Network/Security tab-> Users sub-tab-> click User ID number of the CMC user interface in localized languages does not have the Super User listed under the CMC User Privileges section. The super user privilege is currently reserved for future use. (180734)

* The help for the Power Budget Status page located in the Chassis-> Power Management tab-> Budget Status sub-tab of the CMC user interface in localized languages describes the Standby DC Power Capacity as:

Indicates the amount of power (in watts) available to be provided by Power

Supplies that are in standby mode. This power can be allocated to any hardware modules that are either added to the chassis or brought online.

This needs to be:

Indicates the amount of standby power (in watts) that is available in the event of a Power Supply fault or Power Supply removal from system. This field may show readings when the system has four or more power supplies and you have enabled Dynamic Power Supply Engagement.
NOTE: It is possible to see a PSU in standby mode but not contribute to the Standby DC Power Capacity value. In this case the watts from this PSU are contributing to Total DC Power Available for Allocation value. (182571)

* The help for the Server Power Throttling Enabled on the Power Management Budget/Redundancy configuration page located in the Chassis-> Power Management tab->Configuration sub-tab of the CMC user interface in all languages needs to explain that the power will be siphoned from lower priority servers in the order of increasing slot numbers.

Currently the help reads:
Enables (when checked) the CMC to siphon power from lower priority servers when power is needed for the entire chassis. In this case, the servers are allowed to continue operating at a degraded performance level rather than shut down.

This needs to be:
Enables (when checked) the CMC to siphon power from lower priority servers in the order of increasing slot number (slot 1 to 16) when power is needed for the entire chassis. In this case, the servers are allowed to continue operating at a degraded performance level rather than shut down. (186703)

* The help for Power Management Budget/Redundancy configuration page located in the Chassis-> Power Management tab->Configuration sub-tab of the CMC user interface in all languages refers to "System Max AC Power Limit (2768 - 7928)" field displayed on the User Interface as "Enclosure Max Power Limit" and "System AC Power Warning Threshold (2500 - 7130)" field on the User Interface as "Power Warning Threshold".

In addition the "System Max AC Power Limit (2768 - 7928)" needs to have the following detailed explanation:

System Max AC Power Limit is the max AC power that the system is allowed to draw from incoming AC power supply source. It can be configured by the user if and only if the value exceeds the AC Power equivalent (i.e. 15% higher than the DC allocated power value) of the currently allocated DC Power to Servers and Chassis Infrastructure. If an attempt is made by the user to configure the value such that it falls below the AC power equivalent of the currently allocated DC Power to Servers and Chassis Infrastructure the attempt would not be successful. In other words, users are NOT allowed to configure an AC power limit that is less than what is currently allocated to the servers and infrastructure as that would result in blades being automatically powered down. The DC power allocated to Servers and Chassis Infrastructure can be found in the User Interface on the Chassis -> Power Management-> Power Budget status page under Power Budgeting section or via CLI RACADM utility command (racadm

getpbinfo). User can, however, power OFF one or more server(s) to lower the current DC Power allocation and re-attempt setting a lower value for System Max AC Power Limit (if desired) or simply configure the limit prior to powering on the server blades.

NOTE: Please refer to the Datacenter Capacity Planner (DCCP) tool at www.dell.com/calc for capacity planning.(186670)

##
KNOWN ISSUES FOR DOCUMENTATION
##

This section provides additional information about known issues with the CMC Firmware version 1.0 User's Guide.

* On Page 273 of the user's guide, fwupdate racadm subcommand example states the following:
Example Input: racadm fwupdate -g -u -a 192.168.0.120 firmimg.cmc -m cmc-active

Output: Firmware update complete.

The output needs to be initially:
TFTP firmware update has been initiated. This update process may take several minutes to complete.

If this command is typed after the firmware has been completed then you will see the "Firmware update complete." as output. (181529)

* On Page 164 of the user's guide, Table 6-8 Default Role Group Privileges lists that the Role group 1, 2 and 3 has the default privilege level set to Administrator, Power User and Guest User. This needs to be none since all the role groups default to none.(182570)

* On Page 164 of the User's guide, In Table 6-8 the default privilege for Power User permissions list is incomplete. It should list the following permissions: (182570)
    - CMC Login User
    - Clear Logs Administrator
    - Chassis Control Administrator (Power Commands)
    - Server Administrator
    - Test Alert User
    - Fabric A Administrator
    - Fabric B Administrator
    - Fabric C Administrator

* On Page 138 of the User's guide, Updating the CMC Firmware section once the step 4 is attempted, the firmware will transfer and once the firmware update begins, the status will display "Firmware Update in Progress". Once the CMC update is complete, it resets the CMC. You will need to refresh the User Interface page to then relogin. (186490)

##

January 2008