Dell Chassis Management Controller Version 3.3 for PowerEdge VRTX

RACADM CLI Guide

July 2020
Rev. A00

DELL EMC

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

1

Introduction

This document provides information about the RACADM subcommands, supported RACADM interfaces, and property database groups and object definitions of CMC for PowerEdge VRTX.

Topics:

What's new in this release

- Added a new command, `sslcertdownload`, to download SSL certificates from CMC.

Supported RACADM Interfaces

The RACADM command-line utility provides a scriptable interface that allows you to remotely configure your Chassis Management Controller (CMC). The utility runs on the management station and the managed system. It is available on the *Dell OpenManage Systems Management and Documentation* DVD or at **support.dell.com**.

The RACADM utility supports the following interfaces:

- SSH or Telnet — Also referred as Firmware RACADM, is accessible by logging in to CMC using SSH or telnet. You do not have to specify the CMC IP, user name or password to run Firmware RACADM commands.
- Remote — Supports executing RACADM commands from a remote management station such as a laptop or desktop. You must install the DRAC Tools utility from the OpenManage software on the remote computer to run Remote RACADM commands. To execute Remote RACADM commands, you must formulate the command such as a an SSH/Telnet RACADM command except that you must also use the **–r –i** options or the **–r –u –p** options. For more information about these options, see the "RACADM Subcommand Details."

RACADM Syntax Usage

The following section describes the syntax usage for SSH/Telnet and Remote RACADM.

NOTE: The RACADM command-line interface in CMC does not ignore single or double quotation. When you enter an open quotation mark, ensure that you enter the close quotation mark too.

SSH or Telnet RACADM

```
racadm getconfig -g <groupname> [-o <objectname>]
[-i <indexnumber>]
```

```
racadm <subcommand>
```

Example

```
racadm getconfig -g idracinfo
```

```
racadm getsysinfo
```

Remote RACADM

```
racadm -r <CMC IP> -u <username> -p <password> getconfig -g <groupname> [-o
<objectname>] [-i <indexnumber>]
```

```
racadm -r <CMC IP> -u <username> -p <password> <subcommand>
```

Example

```
racadm -r <CMC IP> -u myuser -p mypass getconfig -g idracinfo
```

```
racadm -r <CMC IP> -u myuser -p mypass getsysinfo
```

RACADM Command Options

The following table lists the options for the RACADM command.

Table 1. Racadm command options

Option	Description
-r<*raclpAddr*> **-r** *raclpAddr* : <*port number*>	Specifies the remote IP address of the controller. Use:<*port number*> if the iDRAC port number is not the default port (443).
-u <*usrName*>	Specifies the username that is used to authenticate the command transaction. If the **-u** option is used, the **-p** option must be used, and the **-i** option (interactive) is not allowed. **NOTE: If you are using CIFS that is registered with a domain, and are accessing the CIFS using the IP with the CIFS local user credentials, it is mandatory to enter the hostname or host IP with the -u option. The format is - <hostname/username> or <host IP/username>**
-p <*password*>	Specifies the password that is used to authenticate the command transaction. If the **-p** option is used, the **-i** option is not allowed. **NOTE: CMC does not support extended ASCII characters, such as ß, å, é, ü, or other characters used primarily in non-English languages. Setting values with these characters causes unpredictable behavior.**
-S	Specifies that RACADM should check for invalid certificate errors. RACADM stops the execution of the command with an error message if it detects an invalid certificate.
-I <*indexnumber*>	Specifies the index number for the indexed group, if applicable.
-g <*groupname*>	Specifies the group name, if applicable.
-o *objectname*	Specifies the object name, if applicable.

The following table provides the supported RACADM interfaces.

Table 2. Racadm interfaces

Type	Local RACADM	SSH/Telnet RACADM	Remote RACADM
CMC	No	Yes	Yes

NOTE: Multiple instances of remote RACADM can be executed on a management station.

Supported RACADM Subcommands

The following table provides the list of RACADM subcommands and their corresponding interface support. For more information about the RACADM sub-commands including syntax and valid entries, see RACADM Subcommand Details.

Table 3. Racadm subcommands

Subcommand	CMC	
	Telnet/SSH/Serial	Remote RACADM
"?" and "?<subcommand>"	Yes	Yes
chassisaction	Yes	Yes
chassislog	No	No
closessn	Yes	Yes
clrsel	Yes	Yes
cmcchangeover	Yes	Yes
config	Yes	Yes
connect	Yes	Yes
deploy	Yes	Yes
eventfilters	Yes	Yes
fanoffset	Yes	Yes
feature	Yes	Yes
featurecard	Yes	Yes
fwupdate	Yes	Yes
get	Yes	Yes
getactiveerrors	No	Yes
getassettag	Yes	Yes
getchassisname	Yes	Yes
getconfig	Yes	Yes
getdcinfo	Yes	Yes
getflexaddr	Yes	Yes
getioinfo	Yes	Yes
getled	Yes	Yes
getmacaddress	Yes	Yes
getmodinfo	Yes	Yes
getniccfg	Yes	Yes
getpbinfo	Yes	Yes
getpciecfg	Yes	Yes
getpminfo	Yes	Yes
getraclog	Yes	Yes
getractime	Yes	Yes
getredundancymode	Yes	Yes

Table 3. Racadm subcommands (continued)

Subcommand	CMC	
getsel	Yes	Yes
getsensorinfo	Yes	Yes
getslotname	Yes	Yes
getssninfo	Yes	Yesz
getsvctag	Yes	Yes
getsysinfo	Yes	Yes
getversion	Yes	Yes
help and help <subcommand>	Yes	Yes
ifconfig	Yes	Yes
jobqueue	Yes	Yes
krbkeytabupload	No	Yes
license	Yes	Yes
netstat	Yes	Yes
ping	Yes	Yes
ping6	Yes	Yes
racdump	Yes	Yes
racreset	Yes	Yes
racresetpcie	Yes	Yes
racresetcfg	Yes	Yes
raid	Yes	Yes
remoteimage	Yes	Yes
serveraction	Yes	Yes
set	Yes	Yes
setassettag	Yes	Yes
setflexaddr	Yes	Yes
setled	Yes	Yes
setniccfg	Yes	Yes
setpciecfg	Yes	Yes
setractime	Yes	Yes
setslotname	Yes	Yes
setsysinfo	Yes	Yes
sshpkauth	Yes	Yes
sslcertview	Yes	Yes
sslcsrgen	Yes	Yes
sslresetcfg	Yes	Yes
testemail	Yes	Yes

Table 3. Racadm subcommands (continued)

Subcommand	CMC	
testfeature	Yes	Yes
testtrap	Yes	Yes
traceroute	Yes	Yes
traceroute6	Yes	Yes

Other documents you may need

To access the documents from the Dell Support site. Along with this Reference Guide, you can access the following guides available at **dell.com/support/manuals**.

- The *VRTX CMC Online Help* provides information about using the Web interface. To access the Online Help, click **Help** on the CMC web interface.
- The *Chassis Management Controller for PowerEdge VRTX User's Guide* provides information about using the VRTX–related Web interface features.
- The *Dell Chassis Management Controller (CMC) for Dell PowerEdge VRTX Version Release Notes* provides last-minute updates to the system or documentation or advanced technical reference material intended for experienced users or technicians.
- The *Integrated Dell Remote Access Controller User's Guide* provides information about installation, configuration, and maintenance of the iDRAC on managed systems.
- The *Dell OpenManage Server Administrator's User's Guide* provides information about installing and using Server Administrator.
- The *Dell Update Packages User's Guide* provides information about obtaining and using Dell Update Packages as part of your system update strategy.
- The *Dell Shared PowerEdge RAID Controller (PERC) 8 User's Guide* provides information about deploying the Shared PERC 8 card and managing the storage subsystem. This document is available online at dell.com/storagecontrollermanuals.
- Dell systems management application documentation provides information about installing and using the systems management software.

The following system documents provide more information about the system in which VRTX CMC is installed:

- The safety instructions that came with your system provide important safety and regulatory information. For additional regulatory information, see the Regulatory Compliance home page at **www.dell.com/regulatory_compliance**. Warranty information may be included within this document or as a separate document.
- The *Dell PowerEdge VRTX Getting Started Guide* shipped with your system provides an overview of system features, setting up your system, and technical specifications.
- The setup placemat shipped with your system provides information about the initial system setup and configuration.
- The server module's *Owner's Manual* provides information about the server module's features and describes how to troubleshoot the server module and install or replace the server module's components. This document is available online at dell.com/poweredgemanuals.
- The rack documentation included with your rack solution describes how to install your system into a rack, if required.
- For the full name of an abbreviation or acronym used in this document, see the Glossary at dell.com/support/manuals.
- Systems management software documentation describes the features, requirements, installation, and basic operation of the software.
- Documentation for any components you purchased separately provides information to configure and install these options.
- Any media that ships with your system that provides documentation and tools for configuring and managing your system, including those pertaining to the operating system, system management software, system updates, and system components that you purchased with your system. For more information on the system, scan the Quick Resource Locator (QRL) available on your system and the system setup placemat that shipped with your system. Download the QRL application from your mobile platform to enable the application on your mobile device.

Updates are sometimes included with the system to describe changes to the system, software, and/or documentation. Always read the updates first, because they often supersede information in other documents.

Accessing documents from the Dell EMC support site

You can access the required documents in one of the following ways:

- Using the following links:

- For Dell EMC Enterprise Systems Management, Dell EMC Remote Enterprise Systems Management, and Dell EMC Virtualization Solutions documents — https://www.dell.com/esmmanuals
- For Dell EMC OpenManage documents — https://www.dell.com/openmanagemanuals
- For iDRAC documents — https://www.dell.com/idracmanuals
- For Dell EMC OpenManage Connections Enterprise Systems Management documents — https://www.dell.com/OMConnectionsEnterpriseSystemsManagement
- For Dell EMC Serviceability Tools documents — https://www.dell.com/serviceabilitytools

- From the Dell EMC Support site:

1. Go to https://www.dell.com/support.
2. Click **Browse all products**.
3. From **All products** page, click **Software**, and then click the required link from the following:
   - **Analytics**
   - **Client Systems Management**
   - **Enterprise Applications**
   - **Enterprise Systems Management**
   - **Mainframe**
   - **Operating Systems**
   - **Public Sector Solutions**
   - **Serviceability Tools**
   - **Support**
   - **Utilities**
   - **Virtualization Solutions**
4. To view a document, click the required product and then click the required version.

- Using search engines:
  - Type the name and version of the document in the search box.

2

RACADM Subcommand Details

This section provides detailed descriptions about the RACADM subcommands, including the syntax and valid entries.

Topics:

- ifconfig
- jobqueue
- krbkeytabupload
- license
- netstat
- ping
- ping6
- racdump
- racreset
- racresetcfg
- racresetpcie
- raid
- remoteimage
- serveraction
- set
- setassettag
- setchassisname
- set controllers
- setflexaddr
- setled
- set enclosure
- setniccfg
- setpciecfg
- setractime
- setslotname
- setsysinfo
- SSH or Telnet RACADM
- sshpkauth
- sslcertdownload
- sslcertupload
- sslcertview
- sslcsrgen
- sslresetcfg
- sslsshresetcfg
- set tempprobes
- testcifsshare
- testemail
- testfeature
- testtrap
- traceroute
- traceroute6

Guidelines to Quote Strings Containing Special Characters When Using RACADM Commands

When using strings that contain special characters, use the following guidelines:

Strings containing the following special characters must be quoted using single quotation marks or double quotation marks:

- $ (dollar sign)
- " (double quotation marks)
- ' (single quotation marks)
- ` (back quotation marks)
- \ (backslash)
- ~ (tilde)
- ; (semicolon)
- | (vertical bar)

- ((left parentheses)
-) (right parentheses)
- & (ampersand)
- > (greater than)
- < (less than)
- # (pound)
- ASCII code 32 (space)

NOTE: The - (dash) character cannot be the first character of the string, regardless of whether the string is quoted.

There are different escaping rules for using single quotation mark and double quotation marks.

For double quoting:

The following characters must be escaped by prepending a backslash:

- $ (dollar sign)
- " (double quotation marks)
- ' (single quotation marks)
- ` (back quotation marks)
- \ (backslash)

For example, use the following for a string that contains the special characters, $, ",', `and \.

For single quotation marks:

- No character escaping is necessary.
- A single quotation mark cannot be used even with a backslash escaped.

NOTE: An empty string may be specified as either "" (using double quotation marks) or '' (using single quotation mark).

Racadm help and help with subcommand

Table 4. Racadm help commands

Description	Displays all the subcommands you can use with the RACADM command and a one-line description of each subcommand. ? followed by <*subcommand*> displays the syntax for the specified command. To use this subcommand, you must have the **CMC Login User** privilege. You can also use the **help** and **help <*subcommand*>** commands to obtain the same information.
Synopsis	`racadm ?` `racadm ? <subcommand>`
Input	NA
Output	NA

Example for RACADM ?

The following output example shows only part of the actual output for the `racadm ?` command. Descriptions shown in this example may vary slightly from the descriptions in your racadm session.

```
racadm ?
```

```
help            -- list racadm subcommand description
help <subcommand> -- display usage summary for a subcommand
?               -- list racadm subcommand description
? <subcommand>  -- display usage summary for a subcommand
arp             -- display the networking arp table
chassisaction   -- execute chassis or switch power-up/down/cycle or
```

```
KVM powercycle
clrraclog       -- clear the CMC log
clrsel          -- clear the System Event Log (SEL)
cmcchangeover   -- Changes the redundant state of the CMC from active
to standby and vice versa
config          -- modify CMC configuration properties
...
setniccfg       -- modify network configuration properties
setractime      -- set the time on the CMC
setslotname     -- sets the name of the slot in the chassis
setsysinfo      -- set the chassis name and chassis location
sslcertview     -- display a CA/server certificate in the CMC
sslcsrgen       -- generate a certificate CSR from the CMC
testemail       -- test CMC e-mail notifications
testfeature     -- test CMC feature x
testtrap        -- test CMC SNMP trap notifications
traceroute      -- determine the route of a packet
traceroute6     -- determine the route of a packet
```

Example for RACADM ? <*subcommand*>

```
racadm ? getsysinfo
```

```
getsysinfo -- display general CMC and system information
Usage:
racadm getsysinfo [-d] [-c] [-A] [-4] [-6]
------------------------------------------------------------
Valid Options:
-d : show CMC information
-c : show chassis information
-A : do not show headers or labels
-4 : show CMC IPv4 information
-6 : show CMC IPv6 information
```

help and help subcommand

Table 5. Help command

Description	Lists all the subcommands available for use with **RACADM** and provides a short description for each. You may also type a subcommand after `help`.
Synopsis	• `racadm help` • `racadm help <subcommand>`
Input	None
Output	• The **help** command displays a complete list of subcommands.
Example	`racadm help getsysinfo`

chassislog

Table 6. chassislog

Description	Allows you to view, export, or clear the chassis log history. To clear a chassis log, you must have the **Clear Logs Administrator** privilege. **NOTE: It is recommended that you use Firmware RACADM to run this subcommand.**

Table 6. chassislog (continued)

Synopsis	`racadm chassislog view [-i]`
	`racadm chassislog view [-c <category> [-s <severity>] [-b <subcategory>]`
	`[-q <sequence no.>] [-n <number of records>] [-r <start timestamp>]`
	`[-e <end timestamp>]`

Input	• -i — Displays the number of records present in the active log. You cannot use this option with any other option.
	• -c — The log type to filter the records. Provide multiple categories using a "," as the delimiter. The value is case-insensitive. Valid Category values:
	  ○ All
	  ○ System
	  ○ Storage
	  ○ Updates
	  ○ Audit
	  ○ Config
	• -q - The sequence number from which the records must be displayed.
	• -n - Specifies the n Number of records to be displayed.
	• -r - Displays events that have occurred after this time. The time format is yyyy-mm-dd HH:MM:SS. The time stamp must be provided within double quotes.
	• -e - Displays events that have occurred before this time. The time format is yyyy-mm-dd HH:MM:SS. The time stamp must be provided within double quotes.
	• -f *<filename>* - Specifies the file location and name where the chassis log is exported.
	• -a *<name>* - Specifies the FTP Server IP address or FQDN, user name, and password.
	• -d *<path>* - Specifies the path to the file on the FTP server.
	• -l *<location>* - Specifies the location of the network share or area on file system where chassis log is exported. Two types of network shares are supported:
	  — SMB mounted path: *//<ipaddress or domain name>/<share_name>/<path_to_image>*
	  — NFS mounted path: *<ipaddress>:/<path_to_image>*.
	• -u *<user>* — Specifies the user name for accessing the FTP Server, or Domain and User Name for accessing network share location.
	• -p *<password>* — Specifies the password for accessing the FTP Server or Share location.
	• -s — Filters records based on severity. Provide multiple severities using a comma (,) as the delimiter. The values are not case-sensitive. The valid severity values are:
	  ○ 1. Warning
	  ○ 2. Critical
	  ○ 3. Info
	• -b — The subcategory used to filter the records. Provide multiple subcategories using a comma (,) as the delimiter. The values are not case-sensitive. The valid subcategories are:
	  ○ CPUA: Proc Absent
	  ○ MEM: Memory
	  ○ UEFI: UEFI Event
	  ○ FC: Fiber Channel
	  ○ ENC: Storage Enclosure
	  ○ SYS: System Info
	  ○ LNK: Link Status
	  ○ BAT: Battery Event
	  ○ RSI: Remote Service
	  ○ OSE: OS Event
	  ○ VRM: Virtual Console
	  ○ PSU: Power Supply
	  ○ Log: Log event
	  ○ RDU: Redundancy

Table 6. chassislog (continued)

	○ FCD: Feature Card ○ CMC: Chassis Management Controller ○ CTL: Storage Controller ○ CPU: Processor ○ CBL: Cable ○ JCP: Job Control ○ VF: vFlash Media ○ IPA: DRAC IP Address ○ SUP: FW Update Job ○ RFM: FlexAddress SD ○ PSUA: PSU Absent ○ PCI: PCI Device ○ LIC: Licensing ○ RFL : IDSDM Media ○ NIC : NIC Config ○ VFL : vFlash Event ○ TMPS : Temperature Statistics ○ DIS : Auto-Discovery ○ STOR : Storage ○ SEL : Sys Event Log ○ OSD : OS Deployment ○ SRD : Software RAID ○ RFLA : IDSDM Absent ○ TST : Test Alert ○ FSD : Debug ○ RED : FW Download ○ PST : BIOS POST ○ BOOT : BOOT Control ○ SSD : PCIe SSD ○ IOV : IO Virtualization ○ PR : Part Exchange ○ SWU : Software Change ○ USR : User Tracking ○ PDR : Physical Disk ○ VDR : Virtual Disk ○ SWC : Software Config ○ DKM : Dell Key Mngr ○ NDR : NIC OS Driver ○ RAC : RAC Event ○ ASR : Auto Sys Reset ○ HWC : Hardware Config ○ RRDU : IDSDM Redundancy ○ AMP : Amperage ○ VLT : Voltage ○ DH : Cert Mgmt ○ TMP : Temperature ○ VME : Virtual Media ○ ITR : Intrusion ○ BAR : Backup/Restore ○ PWR : Power Usage ○ VFLA : vFlash Absent ○ BIOS : BIOS Management ○ LC : Lifecycle Contr ○ FAN : Fan Event

Table 6. chassislog (continued)

	○ SEC : Security Event **NOTE: To view or export the Chassis log, only the CMC Login User privilege is required.**

Example	• Display the number of records present in the Chassis Log:
	`racadm chassislog view -i`
	• Display the records under the storage category with severity set to warning:
	`racadm chassislog view -c storage -s warning`
	• Display the records under storage and system categories with severities set to warning or critical:
	`racadm chassislog view -c storage,system -s warning,critical`
	• Display the records having severities set to warning or critical, starting from sequence number 4:
	`racadm chassislog view -s warning,critical -q 4`
	• Display 5 records starting from sequence number 20:
	`racadm chassislog view -q 20 -n 5`
	• Display all records of events that have occurred between 2011-01-02 23:33:40 and 2011-01-03 00:32:15:
	`racadm chassislog view -r "2011-01-02 23:33:40" -e "2011-01-03 00:32:15"`
	• Display all the available records from the active Chassis log:
	`racadm chassislog view -n all`
	• Display the last 25 records from the Chassis log:
	`racadm chassislog view`

chassislog export

Table 7. chassislog export

Description	Exports the Chassis log to a remote share. To export the chassis log, you must have the **Clear Logs Administrator** privilege.

Synopsis	`racadm chassislog export -f<filename> -u<username> -p<password> -l<CIFS or NFS share>`
	`racadm -r<CMC IP> -u<CMC username> -p<CMC password> chassislog export -f<filename> -u<username> -p<password> -l<CIFS or NFS share>`
	• `racadm chassislog export -f <filename> -u <username> -p <password> -l <CIFS share>`
	• `racadm chassislog export -f <filename> -l <NFS share>`
	• `racadm -r <cmcip> -u <cmc username> -p <cmc password> chassislog export -f <filename> -u <username> - p <password> -l <CIFS share>`
	• `racadm -r <cmcip> -u <cmc username> -p <cmc password> chassislog export -f <filename> -l <NFS share>`

Input	• –f : Filename of the exported Chassis Log.

Table 7. chassislog export (continued)

	• –u : Username for the remote share to where the file must be exported. Username in a domain can be given as domain/username • –p : Password for the remote share to where the file must be exported. • –l : Network share location (see the "Example" section for NFS or CIFS share) to where the Chassis Log must be exported.

Example	• Export the Chassis Log to a remote CIFS share
	`racadm chassislog export -f Mylog.xml -u admin -p mypass -l // 192.168.0.5/share`
	- Export the Chassis Log to a remote NFS share
	`racadm chassislog export -f Mylog.xml -l 192.168.0.5:/home/ lclog_user`

chassislog clear

Table 8. chassislog clear

Description	Deletes the data in the chassis log. To clear the chassis log, you must have the **Clear Logs Administrator** privilege.
Synopsis	`racadm chassislog clear` `racadm -r <CMC IP> -u <CMC username> -p <CMC password> chassislog clear`

Example	• Clear the Chassis Log
	`racadm chassislog clear`
	• Clear the Chassis Log using remote racadm
	`racadm -r 192.168.0.11 -u root -p calvin chassislog clear`

chassisaction

Table 9. Chassisaction

Description	Runs a power action on the chassis or a switch. To use this subcommand, you must have the **Chassis Control Administrator** privilege. **NOTE: For remote racadm, check the power status of the module using the `getmodinfo` command.**
Synopsis	`racadm chassisaction [-m <module>] <action>`
Input	• -m <*module*> — Module on which you want to carry out the action. Values are: ○ chassis — this is the default value, if **-m** is not specified.

Table 9. Chassisaction (continued)

	○ **switch-n**, where n=1 · *<action>* — Action that you want to run on the specified module. Values are: ○ powerdown — (Chassis only) Turns off the chassis. ○ powerup — (Chassis only) Turns on the chassis. ○ powercycle — Power cycles the module. ○ nongraceshutdown — (Chassis only) Non-gracefully turns off the chassis. ○ reset — Performs a hard reset of the module. When *<module>* = switch, *<action>* must be powercycle or reset.
Output	None

Example	Perform a reset of switch-1:
	`racadm chassisaction -m switch-1 reset`
	`Module power operation successful.`

closessn

Table 10. Closessn

Description	Closes a communication session on the device. Use the `getssninfo` command to view a list of sessions that can be closed using this command. To use this subcommand, you must have the **Administrator** privilege.
Synopsis	· `racadm closessn -i <session id>` · `racadm closessn -a` · `racadm closessn -u <username>`
Input	· **-i***<session id>* — The session ID of the session to be ended, which can be retrieved using RACADM **getssninfo** subcommand. Session running this command cannot be ended. · **-a** — Closes all sessions. · **-u *<user name>*** — Close all sessions for a particular user name. ○ Remote RACADM: **-u** option or **-i** option
Output	None
Example	· `racadm closessn -i 1234` Closes the session 1234. · `racadm closessn -u root` Closes all the sessions for root user. · `racadm closessn -a` Closes all the sessions.

clrsel

Table 11. Clrsel

Description	Deletes all existing records from the System Event Log (SEL). To use this subcommand, you must have the **Clear Logs** privilege.
Synopsis	`racadm clrsel`

cmcchangeover

Table 12. Cmcchangeover

Description	Changes the state of the CMC from active to standby, or vice versa, in a redundant CMC configuration. This subcommand is useful for remote debugging or testing purposes. To use this subcommand, you must have the **Administrator** privilege. **NOTE: This command is valid only in redundant CMC environments. For more information, see the "Understanding the Redundant CMC Environment" section of the *Dell Chassis System User Guide*.**
Synopsis	`racadm cmcchangeover`
Input	None
Output	`CMC failover initiated successfully.`
Example	`racadm cmcchangeover`

config

Table 13. Config

Description	Allows you to set CMC configuration parameters individually or to batch them as part of a configuration file. If the data is different, that CMC object is written with the new value.

Synopsis	`racadm config [-c|-p] -f <filename>`
	`racadm config -g <groupName> -o <objectName> [-i <index>] <Value>`
	NOTE: The configuration file retrieved using remote racadm are not interoperable. For the config -f <file name> command, use the configuration file retrieved from the same interface.

Input	**NOTE: The -f and -p options are not supported for the serial/Telnet/SSH console.** · **-f** — The `-f` <*filename*> option causes config to read the contents of the file specified by <*filename*> and configure CMC.

Table 13. Config (continued)

	NOTE: When the `-f` option is specified and configuration of an attribute fails, then configuration of other attributes in that group is skipped. • **-p**— This option must be used with the **-f** option. It directs **config** to delete the password entries contained in the config file **-f** <*filename*> after the configuration is complete. To apply the password, you must remove the preceding Read-Only marker '#' in the config file before executing the config **-f** command. • **-g**— The **-g** <*groupName*>, or **group** option, must be used with the **-o** option. The <*groupName*> specifies the group containing the object that is to be set. • **-o** — The **-o** <*objectName*> <*Value*>, or **object** option, must be used with the **-g** option. This option specifies the object name that is written with the string <*value*>. • **-i** — The **-i** <*index*>, or **index** option, is valid only for indexed groups and can be used to specify a unique group. The <*index*> is a decimal integer from 1 through n, where n can vary from 1 to maximum number of indexes a particular group supports. If **-i** <*index*> is not specified, a value of 1 is assumed for groups, which are tables that have multiple entries. The index is specified by the index value, not a named value. • **-c** — The **-c,** or **check** option, is used with the **config** subcommand and allows the user to parse the **.cfg** file to locate syntax errors. If issues are found, the line number and a short description about the issue is displayed. This option is a check-only.
Output	This subcommand generates error output for any of the following reasons: • Invalid syntax, group name, object name, index, or other invalid database members. • RACADM CLI failures. This subcommand returns an indication of the number of configuration objects that were written out of the total objects in the **.cfg** file.
Examples	• `racadm config -g cfgLanNetworking -o cfgNicIpAddress 192.168.0.5.` Sets the **cfgNicIpAddress** configuration parameter (object) to the value 192.168.0.5. This IP address object is contained in the **cfgLanNetworking** group. • `racadm config -f myrac.cfg.` Configures or reconfigures CMC. The **myrac.cfg** file may be created from the **getconfig** command. This file may also be edited manually as long as the parsing rules are followed. **NOTE: The myrac.cfg file does not contain passwords. To include passwords in the file, you must enter them manually. If you want to remove password information from the myrac.cfg file during configuration, use the -p option.**

connect

Table 14. Details of connect

Description	Connects to the switch or server serial console.
Synopsis	• `racadm connect [-b] –m <module>` • `racadm connect [-b] <server-n>` • `racadm connect [-b] <switch-n>`
Input	**-b —** Connects to the switch or console using the binary mode. This is an optional argument; a server or a switch must be present. **NOTE: If you use the -b option, reset the CMC to terminate the connect operation.** • **server**-n, where *n*=1–4 • **switch**-n, where *n*=1 **NOTE: The values 2 and 4 for `n` are valid only for multi-node sleds.** • `switch-n`: where `n` = 1 to 2 or <a1 | a2>

Table 14. Details of connect (continued)

Example	• Connect to I/O Module 1 serial console
	`racadm connect -m switch-1`
	• Connect to server 1 serial console
	`racadm connect -m server-1`

deploy

Table 15. deploy

Description	Configures the static IP address, subnet mask, gateway, and password for the root user on iDRAC for the specified server. To use this subcommand, you must have the **Server Administrator** privilege. iDRAC allows you to set static IPV4 address irrespective of whether IPV4 is enabled or disabled. If IPv4 is disabled on iDRAC, the static or dynamic IP address is not applied to iDRAC nor does the IP address works. If the IPv4 is enabled and the static source is selected, the IP address is applied to iDRAC. **NOTE: You can also use setniccfg to configure static IP address, subnet mask, gateway, DHCP, speed, and duplex properties.**
Synopsis	• `racadm deploy -m <module> -u root -p <password> -s <ipaddress> <subnet> <gateway> -b <device> -o <no|yes>` • `racadm deploy -m <module> -u root -p <password> -s -6 <ipv6Address> <prefixlen> <gateway> -b <device> -o <no|yes>` where <*prefixlen*> is a number between 0 and 128. • `racadm deploy -m <module> -u root -p <password> -d [-6]` • `racadm deploy -a -u root -p <password>` • `racadm deploy –q –e 1` • `racadm deploy –q --qd`
Input	• **-b** <*device*>—Specifies the first boot device; must be used with `-o`. • Use with -m <*module*> to specify for an individual server, or with -a for all servers. Legal values: device=None, PXE, hard disk drive (HDD), CD-DVD, vFDD, vCD-DVD, iSCSI, SD, FDD, RFS • **-o** <*no|yes*>—Indicates if the server should boot from the device once; must be used with `-o`. Use with `-m` <*module*> to specify for an individual server, or with `-a` for all servers. • **-a** —Creates and enables an iDRAC root user if it does not exist, and is executed on all the existing servers in the chassis. • **-u root**—Indicates that the <*password*> is supplied for the root user on the server. root is a constant parameter, the only value that is valid with the `-u` option. • **-m** <*module*>—Specifies the server you want to configure. Legal value must be one of the following values: ○ server-<n> where n=1 to 4 ○ switch-<n> where n=1 • **-p** <*password*>—Specifies the password for the root user on the server. • **-s** <*ipaddress subnet gateway*>—Sets the IP address, subnet mask, and gateway for the specified server, separated by single spaces. ○ ipaddress—A string representing a valid IP address. For example, 192.168.0.20. ○ subnet—A string representing a valid subnet mask. For example, 255.255.255.0.

Table 15. deploy (continued)

	○ gateway—A string representing a valid gateway address. For example, 192.168.0.1. • **-d**—Enables DHCP for the specified server. The **-s** and **-d** options cannot be used together in the same command. • **-6**—Enables IPv6 auto configuration (when used with -d.) Sets static IPv6 addresses (when used with -s). • **-q**—Displays or modifies the quick deploy parameters. • **-n**<*numofblades*> — Specifies the number of reserved IP addresses for quick deploy. The valid values are 2 and 4. • **-e**—Uses the CMC DNS settings for quick deploy. The legal values are: ○ 1—Enable ○ 0—Disable • **--qd**—Updates the quick deploy parameters to the servers. This option works only with the –q option.
Output	None
Example	• `racadm deploy -m server-8 -s 192.168.0.20 255.255.255.0 192.168.0.1` The server was deployed successfully. The deploy command generates an error when used on the extension slot of a multi-slot server. • `racadm deploy -m server-9 192.168.0.11 255.255.255.0 192.168.0.1` ERROR: Server in slot 9 is an extension of the server in slot 1. • `racadm deploy -m server-7 -u root -p calvin -s -6 ::/64 :: 10`

Displayable Characters

Displayable characters include the following set:

```
abcdefghijklmnopqrstuvwxwz
ABCDEFGHIJKLMNOPQRSTUVWXYZ
0123456789~`!@#$%^&*()_+-={}[]|\:";'<>,.?/
```

eventfilters

Table 16. Details of eventfilters

Description	Gets, sets, and displays the list of event filter settings. To use this subcommand with the **get** option, you must have the **CMC Login User** privilege.

Synopsis	`racadm eventfilters <eventfilters command type>`
	`racadm eventfilters get -c <alert descriptor>`
	`racadm eventfilters set -c <alert descriptor>-n <notifications>`
	NOTE: The general format of an alert descriptor:
	`cmc.alert.category.[subcategory].[severity]`
	where, category is mandatory, but subcategory and severity are optional. A severity cannot precede a subcategory.

Table 16. Details of eventfilters (continued)

	Valid category values are: • System • Config • Updates • Storage • Audit Valid severity values are: • Critical • Warning • Informational Valid examples of alert descriptors are: • `cmc.alert.all` • `cmc.alert.audit` • `cmc.alert.audit.lic` • `cmc.alert.audit.warning` • `cmc.alert.audit.lic.critical`
Input	• **get** - Displays the list of event filter settings. • **set** - Configures the actions and notifications for a given event filter configuration. • **-c** - Alert descriptor of the specific event filter. • **-n** - The notification to be sent when the event occurs. Valid values are all, snmp, ipmi, lcd, email, or none. You can append multiple notifications separated by a comma. You cannot enter the values **all** or **none** with other notifications. **NOTE: If both event generation interval and notifications are configured and there is an error while configuring the notifications, the event generation interval is not set. The valid values are from 0–365. 0 disables the event generation.**

Example	• Display all available event filter configurations:
	`racadm eventfilters get -c cmc.alert.all`
	• Display eventfilter configurations for a specific category. For example, audit:
	`racadm eventfilters get -c cmc.alert.audit`
	• Display eventfilter configurations for a specific subcategory. For example, licensing under the audit category:
	`racadm eventfilters get -c cmc.alert.audit.lic`
	• Display eventfilter configurations for a specific severity. For example, warning under the audit category:
	`racadm eventfilters get -c cmc.alert.audit.warning`
	• Display eventfilter configurations for a specific severity and subcategory. For example, a severity of warning in the subcategory licensing under audit category:
	`racadm eventfilters get -c cmc.alert.audit.lic.warning`
	• Clear all available alert settings:
	`racadm eventfilters set -c cmc.alert.all -n none`

Table 16. Details of eventfilters (continued)

	• Configure using severity as a parameter. For example, all informational events in storage category are assigned poweroff as action, and email and snmp as notifications:
	`racadm eventfilters set -c cmc.alert.storage.info -n email,snmp`
	• Configure using subcategory as a parameter. For example, all configurations under the licensing subcategory in the audit category are assigned poweroff as action and all notifications are enabled:
	`racadm eventfilters set -c cmc.alert.audit.lic -n all`
	• Configure using subcategory and severity as parameters. For example, all Information events under the licensing subcategory in the audit category are assigned poweroff as action and all notifications are disabled:
	`racadm eventfilters set -c cmc.alert.audit.lic.info -n none`

fanoffset

Table 17. Details of fanoffset

Description	Configures the internal fans to run at a higher speed than the normal speed. To use this subcommand, you must have the **Chassis Configuration Administrator** privilege.
Synopsis	`racadm fanoffset [-s <off|low|medium|high>` Valid category values are: • off • low • medium • high
Input	**s** — Sets the fan speed.

Example	• Disable the fanoffset feature.
	`racadm fanoffset -s off`
	• Increases fan speed by 20% of fan's maximum speed. Minimum speed for fan is 35% of the maximum.
	`racadm fanoffset -s low`
	• Increases fan speed by 50% of fan's maximum speed. Minimum speed for fan is 65% of the maximum.
	`racadm fanoffset -s medium`
	• Sets fans to run at 100% of fan's maximum speed.
	`racadm fanoffset -s high`

fcp

Table 18. Details of fcp attribute

Description	Prompts you to change the password.

Table 18. Details of fcp attribute (continued)

Synopsis	`racadm fcp <enable/getstatus>`
Input	• `enable`: Enables the force password change feature • `getstatus`: Displays the status of force change password feature **NOTE: You must have the RAC_ADMIN privileges to run the fcp enable command.**
Legal Values	For the fcp get status, the values are: • `0` : FCP Feature has been disabled on CMC. • `1` : FCP Feature has been enabled on CMC.

Example	• To enable force change password feature:
	`racadm fcp enable`
	• To view the status of force change password feature:
	`racadm fcp getstatus`

feature

Table 19. Details of feature

Description	Displays all active chassis features. The information displayed includes feature name, date activated, and the serial number of the SD card used to activate the feature. Dell Feature Cards may contain more than one feature. **NOTE: To use this subcommand to deactivate FlexAddress or ExtendedStorage, you must have the Chassis Configuration Administrator privilege. A user with login privileges can view status only.** **NOTE: To deactivate FlexAddress features, the chassis must be turned off.**
Synopsis	• `racadm feature -s` • `racadm feature -d -c <featurename>` • `racadm feature -r -c ExtendedStorage`
Input	• `-s — Displays the status of active features.` • `-d — Deactivates the feature specified in -c option.` **NOTE: When the FlexAddress and FlexAddressPlus features are active, deactivating one of them results in deactivation of the other feature also. However, ExtendedStorage is not affected by the deactivation of FlexAddress or FlexAddresPlus.** • `-r — Repair damaged/unformatted ExtendedStorage media.` **NOTE: The –r switch requires that the ExtendedStorage feature be deactivated.** **CAUTION: Using the -r switch reformats the SD media in the active CMC card slot. Any existing ExtendedStorage data will be lost.** • `-c — <featurename> must be one of the following:` • `flexaddress (with -d)` • `flexaddressplus (with -d) ExtendedStorage (with -d or -r)`

featurecard

Table 20. Details of featurecard

Description	Verifies proper SD card installation and displays the SD card status. To use this subcommand, you must have the **Chassis Configuration Administrator** privilege.
Synopsis	`racadm featurecard -s`
Input	**-s** — Lists active SD card features and SD card status.

Output	An example of output is given here.
	`racadm featurecard -s`
	
	`Active CMC: The feature card inserted is valid, serial number = CN0H871T137401112222A00 The feature card contains the following feature(s):`
	`FlexAddress: bound`
	`FlexAddressPlus: bound`
	`ExtendedStorage: bound`
	
	`Standby CMC: The feature card contains the following feature(s):`
	`FlexAddress: not bound`
	`FlexAddressPlus: not bound`
	`ExtendedStorage: bound`

fwupdate

Table 21. Details of fwupdate

Description	Allows you to update the firmware on the active and standby CMC firmware, chassis infrastructure firmware, and storage component firmware (RAID controller, hard disk drive, and expander). You can: · Check the firmware update process status. · Update the firmware from a FTP or a TFTP server by providing an IP address and optional path. · Update the firmware from the local file system using remote RACADM. · The subcommand updates one or more devices of a single type at a time. To use this subcommand, you must have the **Chassis Configuration Administrator** privilege. **NOTE:** • **Running the subcommand to update the active CMC firmware resets the CMC, causing all network connections to get logged off. While updating all other modules, including the standby CMC, the active CMC continues to function normally without resetting.** • **The subcommand generates an error, when used on the extension slot of a multi-slot server.** • **The CMC firmware cannot be updated to any earlier version other than 2.0 for a chassis that is configured with 1600W PSU.** • **CMC firmware update or roll back is supported only for firmware versions 1.2, 1.25, 1.3, 1.31, 1.35, 1.36, 2.0, and later. For any version other than these, first update to any of these versions, and then update to the required version.** For 13th generation and later, CMC firmware includes a signature which is verified by CMC before update to ensure the authenticity of the uploaded firmware. The firmware update process is successful only if the firmware image is authenticated by CMC to be a valid image from the service provider and has not been altered. The firmware update process is stopped if CMC cannot verify the signature of the uploaded firmware image.

Table 21. Details of fwupdate (continued)

	Upload firmware image from TFTP server and start firmware update. **NOTE: Run the firmware update command through only one remote racadm session at a time.**
Synopsis	• Using Remote RACADM: `racadm -r fwupdate -p -u -d <firmware image>` **NOTE: iDRAC7 targets are not supported from CMC. Use the CMC GUI to update iDRAC7 targets from CMC.** When using FTP, if you provide the full path to the image file on the CLI, then the CMC uses that path to locate that file on the host. If you do not provide a full path, then the CMC searches the home directory of the specified user for the file if the host system is running Linux or another variant of UNIX. If the host system is running Windows, then a default folder, such as **C:\ftproot** is searched. **NOTE: While performing firmware update using the `racadm fwupdate` command, if the number of characters in the firmware image path is greater than 256 characters, Remote RACADM session logs off with the error message `ERROR: Specified path is too long`.** • `racadm fwupdate -g -u -a 192.168.0.100 -d firmimg.cmc -m cmc-active`
Input	**NOTE: Firmware update from local RACADM (using the -p, -u, or -d options) is not supported on Linux operating system.** • **-p** — The -p option is used to update the firmware file from the client. The **-u** option must be used with the **-p** option. • **-f** — The FTP is used to download the firmware. • **-g** — For CMC, the firmware is downloaded using the TFTP server. • **-u** — The firmware update operation is performed. • **-a** — Specifies the TFTP server IP address or FQDN used for the firmware image (used with -g). **NOTE: CMC accepts IPv4, IPv6, or fully qualified domain names (FQDN) for both FTP and TFTP servers.** • **-d** — Specifies the source path where the firmware image is stored. **NOTE: The default source path is local Default: Designated TFTP default directory on that host for the file if -g option is absent. If -g is used, it defaults to a directory configured on the TFTP server.** • **-o** — Turns off the servers to perform an update. • **-m** *<module>*— Specifies the module or device to be updated. *<module>* is one of the following values: **NOTE: You can also specify multiple modules: *–m <module 1> –m <module 2>*, and so on.** ○ cmc-active (default) ○ cmc-standby ○ iominf-n, where n = 1 **NOTE: You can specify the cmc-active and cmc-standby modules at the same time along with one or more server-n modules. This enables the devices to be updated together.** ○ main-board ○ perc-fqdd, where fqdd is FQDD of the PERC ○ expander-fqdd, where fqdd is FQDD of the Storage Expander ○ hdd-fqdd, where fqdd is FQDD of the HDD • **-s** — Displays the current status of the firmware update. **NOTE: Use -m to display the status of the module update. Omit -m to display the status of the active CMC update.** **NOTE: Use all to get the status of all the targets that must be updated.** • **-c** — Cancels the current firmware update of a module. **NOTE: The Enclosure, Expander, HDD, and PERC updates cannot be cancelled.**

Table 21. Details of fwupdate (continued)

Output	Displays a message indicating the operation that is being performed.

Example	**NOTE: The following commands specifically apply to an active-CMC update.**
	• Upload a firmware image from the client and start firmware update:
	`racadm fwupdate -p -u -d vrtx_cmc.bin`
	• Upload the firmware image from the TFTP server and start the firmware update:
	`racadm fwupdate -g -u -a 192.168.0.100 -d vrtx_cmc.bin -m cmc-active`
	`TFTP firmwareate has been initiated. This update process may take several minutes to complete.`
	• Upload the firmware image from the FTP server and start the firmware update.
	`racadm fwupdate -f 192.168.0.100 fred password123 -d vrtx_cmc.bin -m cmc-active`
	• Start IOM infrastructure firmware update.
	`racadm fwupdate -u -m iominf-1`
	• Update firmware on both the CMCs.
	`racadm fwupdate -g -u -a 192.168.0.100 -d vrtx_cmc.bin -m cmc-active -m cmc-standby`
	Signed CMC Firmware Image:
	• `racadm fwupdate -g -u -a <TFTP IP> -d <Firmware Path> -m cmc-active`
	Firmware update has been initiated. This update process may take several minutes to complete.
	• `racadm fwupdate -s -m cmc-active`
	Invalid firmware: The uploaded firmware image does not contain a verification signature

get

Table 22. Details of get

Description	Saves CMC configuration properties or CMC Event Filter configurations to a file. **NOTE:** • **If CMC is not in the network, you can only export the chassis configuration profile to the local management station.**

Table 22. Details of get (continued)

Synopsis	`racadm -r <cmc ip> -u <cmc username> -p <cmc password> get -f <filename>`
	
	`racadm -r <cmc ip> -u <cmc username> -p <cmc password> get -f <filename> -t xml`
	
	`racadm get -f <filename> -t xml -u <username> -p <password> -l <CIFS share>`
	
	`racadm get -f <filename> -t xml -l <NFS share>`
	
	`racadm get -f <filename> -t xml -u <username> -p <password> -l <CIFS share> -m server-<n>`
	
	`racadm get -f <filename> -t xml -l <NFS share> -m server-<n> [-d <Profile_description>]`
	
	`racadm get -f <filename> -t xml -l extended -m server-<n> [-d <Profile_Description>]`
	
	`racadm get -m server-<n> -s`
	
	`racadm get list serverprofiles -l extended`
	
	`racadm get list serverprofiles -m server-<n> --assign`
	
	`racadm get -f <profile_file_name> -u <network_share_username> -p <network_share_passwd> -l <CIFS Share> --export -t xml`
	
	`racadm get -f <profile_file_name> -l <NFS Share> --export -t xml`

Input	• `list`—lists stored or assigned profiles.
	  ○ `--assign`—specify if the profile requested is a server profile assigned to a blade.
	  ○ `--export`—copy profiles from Extended storage to network share.
	• `-f`—save CMC or server configuration or CMC event filter configurations to a file.
	• `-u`—username of the remote share where the file must be exported.
	• `-p`—password for the remote share where the file must be exported.
	• `-l`—network share location where the file must be exported. For more information about NFS or CIFS share, see the section, *Usage examples*.
	• `extended`—for saving server profile to extended storage.
	• `-t`—specify the file type to be exported. Valid value is “xml”. This option is case-sensitive.
	• `-m`—<module>, the possible values are:
	  ○ `server-<n>`—where n = 1 to 16
	  ○ `all`—for listing profiles assigned to all blades.
	  ○ `server-<nx>`—where n = 1 to 8; x = a to d (lower case)
	• `-s`—check the status of the last successfully initiated server profile operation.
	• `--clone`—export the cloned configuration file. Only the XML file format is supported. The configuration file can be exported to a local or remote share.
	• `--replace`—export the replaced configuration file. Only XML file format is supported. The configuration file can be exported to a local or remote share.
	• `--includeph`—include password hash attributes

Table 22. Details of get (continued)

Example	• Export event filter configurations to a file by using remote racadm
	`racadm -r 192.168.0.120 -u abc -p <password> get -f file.txt`
	• Export the CMC XML configuration to a local share using remote racadm
	`racadm -r 192.168.0.120 -u abc -p <password> get -f file.xml -t xml`
	• Export the CMC XML configuration to a CIFS share
	`racadm get -f file.xml -t xml -u myuser -p mypass -l //192.168.0.0/share`
	• Export the CMC XML configuration to an NFS share
	`racadm get -f file.xml -t xml -l 192.168.0.0:/myshare`
	• –Save the Server profile for server-1 to a CIFS share
	`racadm get -f file.xml -t xml -u myuser -p mypass -l //192.168.0.0/share -m server-1`
	• Save the Server profile for server-1 to extended storage
	`racadm get -f file.xml -l extended -m server-1 -t xml`
	• List the server profiles saved in extended storage
	`racadm get list serverprofiles -l extended`
	• Display profile assigned to server-1
	`racadm get list serverprofiles -m server-1 --assign`
	• Display profiles assigned to all blades
	`racadm get list serverprofiles -m all --assign`
	• Copy server profile `test_profile.xml` from extended storage to network share(CIFS)
	`racadm get -f profile_file_name.xml -u share_username -p share_passwd -l // 192.168.0.0/share --export -t xml`
	NOTE:
	Exporting CMC event filter configuration properties is supported only on remote interfaces.
	The options `--clone`, `--replace`, and `--includeph` are applicable only to chassis configuration file.
	The clone configuration file is default if `--clone` or `--replace` is not specified.

getactiveerrors

Table 23. Details of getactiveerrors

Description	Displays the active errors in a chassis. To run this subcommand, you must have the **CMC Login User** privilege.
Synopsis	`racadm getactiveerrors [-s <severity> ] [-m <module>]`
Input	valid values for <severity>: critical, warning, info valid values for <module>: server-n, where n = 1 to 4 switch-n, where n = 1

Table 23. Details of getactiveerrors (continued)

	cmc-n, where n = 1, 2 fan-n, where n = 1 to 6 ps-n, where n = 1 to 4 chassis kvm

Output	Display entire log:
	`racadm getactiveerrors`
	- Display specific module log:
	`racadm getactiveerrors -m server-1`
	- Display entire informational log:
	`racadm getactiveerrors -s info`

getassettag

Table 24. Details of getassettag

Description	Displays the asset tag for the chassis. To use this subcommand, you must have the **CMC Login User** privilege.
Synopsis	`racadm getassettag [-m <module>]`
Input	**-m** *<module>* — Specifies the module whose asset tag you want to view. `Legal value: chassis`
Example	· `racadm getassettag -m chassis` · `racadm getassettag` `chassis 78373839-33`

getchassisname

Table 25. Details of getchassisname

Description	Displays the name of the chassis. To use this subcommand, you must have the **CMC Login User** privilege.
Synopsis	`racadm getchassisname`
Example	`racadm getchassisname` `CMC-1`

getconfig

Table 26. Details of getconfig

Description	Retrieves CMC configuration parameters individually, or all CMC configuration groups may be retrieved and saved to a file.

Synopsis	`racadm getconfig -f <filename>`
	
	`racadm getconfig -g <groupName> [-i <index>]`
	
	`racadm getconfig -u <username>`
	
	`racadm getconfig -h`
	
	`racadm getconfig -g <groupName> -o <objectName> [-i index]`

Input	• **-f** — The **-f** *<filename>* option directs getconfig to write the entire iDRAC configuration to a configuration file. This file can be used for batch configuration operations using the **config** subcommand. • **-g** — The **-g** *<groupName>*, or group option, can be used to display the configuration for a single group. The **groupName** is the name for the group used in the **racadm.cfg** files. If the group is an indexed group, use the **-i** option. • **-h** — The **-h**, or **help** option, displays a list of all available configuration groups in alphabetical order. This option is useful when you do not have exact group names. • **-i** — The -i *<index>*, or **index** option, is valid only for indexed groups and can be used to specify a unique group. The *<index>*is a decimal integer from 1 through n, where n can vary from 1 to maximum number of indexes a particular group supports. If **-i** *<index>* is not specified, a value of 1 is assumed for groups, which are tables that have multiple entries. The index is specified by the index value, not a *named* value. • **-o** — The -o *<objectname>* or **object** option specifies the object name that is used in the query. This option is optional and can be used with the **-g** option. • **-u** — The -u *<username>*, or **user name** option, can be used to display the configuration for the specified user. The *<username>* option is the login name for the user. • **-v** — The **-v** option displays additional details with the display of the properties and is used with the **-g** option.
Output	This subcommand generates error output upon encountering either of the following: • Invalid syntax, group name, object name, index, or other invalid database members • RACADM CLI transport failures If errors are not encountered, this subcommand displays the contents of the specified configuration.
Example	• Displays all of the configuration properties (objects) that are contained in the group **cfgLanNetworking**. `racadm getconfig -g cfgLanNetworking`

Table 26. Details of getconfig (continued)

	• Saves all group configuration objects from iDRAC to **myrac.cfg**.
	`racadm getconfig -f myrac.cfg`
	• Displays a list of the available configuration groups on iDRAC in an alphabetical order.
	`racadm getconfig -h`
	• Displays the configuration properties for the user named **root**.
	`racadm getconfig -u root`
	• Displays the user group instance at index 2 with verbose information for the property values.
	`racadm getconfig -g cfgUserAdmin -i 2 -v`

Table 27. Groups-Key attributes

Groups	Key Attributes
cfgEmailAlert	cfgEmailAlertAddress
cfgLDAPRoleGroup	cfgLDAPRoleGroupDN
cfgServerInfo	cfgServerBmcMacAddress
cfgStandardSchema	cfgSSADRoleGroupName
cfgTraps	cfgTrapsAlertDestIPAddr
cfgUserAdmin	cfgUserAdminUserName

getdcinfo

Table 28. Details of getdcinfo

Description	Displays general I/O module and daughter card configuration information. Only the CMC controls daughtercards. To use this subcommand, you must have the **CMC Login User** privilege. **NOTE: Fabric verification for server DCs is performed only when the chassis is turned on. When the chassis is on stand-by power, iDRACs on the server modules remain turned off and thus are unable to report the server's DC fabric type. The DC fabric type may not be reported in the CMC user interface until iDRAC on the server is turned on.**
Synopsis	`racadm getdcinfo`
Input	**-n** — Displays the model names for the daughter cards in servers.

Table 29. Example

<IO#>	*<Type>*	*<State>*	*<Role>*
switch-1	Gigabit Ethernet	OK	Master

Table 29. Example

<Server#>	<Presence>	<DC1 Type>	<DC1 State>	<DC2 Type>	<DC2 State>
server-1	Present	PCIe	OK	PCIe	OK
server-2	Not Present	None	N/A	None	N/A
server-3	Present	PCIe	OK	None	N/A
server-4	Not Present	None	N/A	None	N/A

Table 30. getdcinfo

<Server#>	<Presence>	<DC1 Model Name>	<DC2 Model Name>
server-1	Present	None	None
server-2	Not Present	None	None
server-3	Not Present	None	None
server-4	Present	None	Broadcom M5708t

getflexaddr

Table 31. Details of getflexaddr

Description	Enabled or disabled status is displayed for the entire chassis and fabric ID decoder. Use the command with -i option to display the MACs/WWN on a per-slot-basis The decoder values in the **Type** column indicate the protocols of the network cards: · **0**— Unsupported · **1**— ISCSI · **2**— FCoE-FIP · **3**— iSCSI/FCoE-FIP To use this subcommand, you must have **CMC Login User** privilege. **NOTE: If FlexAddress is not activated on the chassis, the command displays server-assigned MAC/WWN addresses. If the slot is empty, the command leaves the server-assigned MAC/WWN addresses blank. If an external console controls the MAC/WWN addresses, the command displays an externally managed message.**

Table 31. Details of getflexaddr (continued)

Synopsis	`racadm getflexaddr [-i <slotNum>]`
Input	-i <*slotNum*> — Specifies the slot information to be displayed. <*slotNum*> must be from 1 to 4.

Table 32. Example

<Slot#>	*<Status>*	*<Server Presence>*
1	Enabled	Present
2	Enabled	Present
3	Enabled	Not Present
4	Enabled	Not Present

Table 32. Example

<Fabric>	*<Type>*	*<Status>*
A	Gigabit Ethernet	Enabled
B	None	Enabled
C	None	Enabled

Table 33. FlexAddress setting

<Name>	*<Type>*	*<Server-Assigned>*	*<Chassis-Assigned>*
slot4-idrac	Controller	18:A9:9B:FD:C7:57	F8:DB:88:3D:9F:A7(active)
slot4-A	10 GbE KR	00:90:FA:51:36:54	F8:DB:88:3D:9F:A8(active)
	10 GbE KR/3	00:90:FA:51:36:55	F8:DB:88:3D:9F:AA(active)
	FCoE-WWN	10:00:00:90:FA:51:36:55	20:01:F8:DB:88:3D:9F:AA(active)

Table 33. FlexAddress setting (continued)

	10 GbE KR/3	00:90:FA:51:36:56	F8:DB:88:3D:A2:78(active)

NOTE: 10 GbE KR/3— The value 3 indicates the protocol type.

getioinfo

Table 34. getioinfo

Description	Displays general information about the I/O modules on the chassis. To use this subcommand, you must have the **CMC Login User** privilege. **NOTE: The fabric type may be any supported I/O fabric type, such as Ethernet, Fiber Channel, and Infiniband.**

Synopsis	`racadm getioinfo`
	`racadm getioinfo [-m <module>]`
	`racadm getioinfo [-m  <module>][-s]`

Input	`-m` — Specifies the module or device. The <module> must be switch — <n>, where n = 1–2 `-s` — Displays the stack information.

Table 35. Example

<IO>	*<Power>*	*<Name>*	*<Role>*	*<Mode>*	*<Type>*	*<Presence>*	*<POST>*
switch-1	ON	R1-PT VRTX 1Gb Master	Pass-through	N/A	Gigabit Ethernet	Present	OK

getled

Table 36. Details of getled

Description	Displays the LED settings on a module: blinking, not blinking, or unknown (for empty slots). To use this subcommand, you must have the **Login User** privilege.
Synopsis	`racadm getled -m <module>`
Input	CMC only options: -m <*module*> — Specifies the module whose LED settings you want to view. <*module*> can be one of the following: • server-n where n=1–4 • switch-n where n=1

Table 36. Details of getled (continued)

	• chassis • cmc-active
Example	For CMC: • `racadm getled -m server-10` <*module*> <*LED state*> server-10 Blinking • `racadm getled -m chassis` <*module*> <*LED state*> server-10 Not blinking • `racadm getled -m server-1` <*module*> <*LED state*> server-1 ON • `racadm getled -m server-9` <*module*> <*LED state*> server-9 Extension(1)

getmacaddress

Table 37. Details of getmacaddress

Description	Displays the MAC/WWN addresses and fabric ID decoder for all modules or for a specified module. The decoder values indicate the protocols of the network cards: • **0**—Unsupported • **1**—ISCSI • **2**—FCoE-FIP • **3**—iSCSI/FCoE-FIP To use this subcommand, you must have the **CMC Login User** privilege.
Synopsis	• `racadm getmacaddress` • `racadm getmacaddress -m chassis` • `racadm getmacaddress -m switch-<n>` • `racadm getmacaddress [-m <module> [-x]] [-t iscsi]` • `racadm getmacaddress -a` • `racadm getmacaddress -c IO-Identity` • `racadm getmacaddress -c Flexaddress` • `racadm getmacaddress -c Factory` • `racadm getmacaddress -c all`
Input	• **-m** <*module*> — Specifies the module whose MAC address you want to view. <*module*> may be one of the following: `server-n`, where *n*=1–4 `switch-n`, where *n*=1 • **-t** —Displays the iSCSI MAC addresses for all servers or the specified server if used with -m option. • **-x** —Displays the extra MACs (Ethernet or iSCSI) for servers with additional LOM MACs and must be used with -m option.

Table 37. Details of getmacaddress (continued)

	• **-a**—Displays the Ethernet and iSCSI MAC/WWN addresses for all iDRAC/LOMs/mezzanine cards. When FlexAddress is enabled for a particular slot, then the chassis-assigned MAC/WWN address is displayed. • **-c** —Displays the ethernet, iSCSI, MAC/WWN, assignment type, and partition status of all LOMs or mezzanine cards. Valid values for the `-c` option are: ○ **IO-Identity**—Displays the user-defined MAC/WWN addresses. ○ **FlexAddress**—Displays the chassis-assigned WWN/MAC addresses. ○ **Factory**—Displays the MAC/WWN addresses for all LOMs or mezzanine cards. ○ **all**—Displays the console assigned MAC/WWN of all LOMs or mezzanine cards.

Example

- Displays the NDC or LOM MAC address.

```
racadm getmacaddress
```

- Display iSCSI MAC addresses for all servers.

```
racadm getmacaddress -t iscsi
```

- Display iSCSI MAC for server-1.

```
racadm getmacaddress -m server-1 -t iscsi
```

- Display extra iSCSI MACs for server-1 (if available).

```
racadm getmacaddress -m server-1 -t iscsi -x
```

- Displays the user-defined MAC and WWN address.
  - `racadm getmacaddress -c io-identity`
  - `racadm getmacaddress -c io-identity -m server -2`
- Displays the console assigned MAC/WWN of all LOMs or mezzanine cards.

```
racadm getmacaddress -c all
```

- Displays the chassis assigned WWN/MAC address.

```
racadm getmacaddress -c flexaddress
```

- Displays the MAC/WWN addresses for all LOMs or mezzanine cards.

```
racadm getmacaddress -c factory
```

Table 38. MAC address for chassis

<Name>	*<Presence>*	*<BMC MAC Address>*	*<NIC1 MAC Address>*	*<NIC2 MAC Address>*
CMC	Present	N/A	F0:4D:A2:77:71:72	N/A

Table 39. MAC address for switch-1

<Name>	*<Presence>*	*<BMC MAC Address>*	*<NIC1 MAC Address>*	*<NIC2 MAC Address>*

Table 39. MAC address for switch-1 (continued)

Switch-1	Present	Not Installed	00:00:00:00:00:00	Not Installed

Table 40. MAC for server-1

<Name>	*<Presence>*	*<BMC MAC Address>*	*<NIC1 MAC Address>*	*<NIC2 MAC Address>*
server-1	Present	00:11:43:FD:B7:2A	00:11:43:FD:B7:2A	00:11:43:FD:B7:2B
server-4	Extension(1)	N/A	00:11:43:FD:B7:2C	00:11:43:FD:B7:2D

Table 41. MACs for server-1

<Name>	*<Presence>*	*<BMC MAC Address>*	*<NIC1 MAC Address>*	*<NIC2 MAC Address>*
server-1	Present	00:11:43:FD:B7:2A	00:11:43:FD:B7:2A	00:11:43:FD:B7:2B
			00:11:43:FD:B7:2C	00:11:43:FD:B7:2D

Table 42. MAC address

<Name>	*<Presence>*	*<BMC MAC Address>*	*<NIC1 MAC Address>*	*<NIC2 MAC Address>*
CMC	Present	N/A	00:1E:4F:1F:3C:58	N/A
Server-1	Present	00:1E:4F:2A:AF:7B	00:1E:4F:2A:D3:97	00:1E:4F:2A:D3:99
Server-2	Present	00:22:19:D2:1E:84	N/A	N/A
Server-3	Not Present	N/A	N/A	N/A
Server-4	Present	00:18:8B:FF:45:2A	00:18:8B:FF:AA:02	00:18:8B:FF:AA:04
Switch-1	Present	N/A	00:00:00:00:00:00	N/A

Table 43. Ethernet and iSCSI MAC/WWN addresses

<Name>	*<Type>*	*<Presence>*	*<BMC MAC Address>*	*<NIC1 MAC Address>*	*<NIC2 MAC Address>*
CMC	N/A	Present	N/A	00:1E:4F:1F:3C:58	N/A
Server-1-A	Gigabit Ethernet	Present	00:1E:4F:2A:AF:7B	00:1E:4F:2A:D3:97	00:1E:4F:2A:D3:99
	iSCSI	Present		00:1E:4F:2A:D3:98	00:1E:4F:2A:D3:9A
Server-1-B	Gigabit Ethernet	Present		Not Installed	Not Installed
	iSCSI	Present		Not Installed	Not Installed
Server-1-C	Fibre Channel 4	Present		Not Installed	Not Installed
Server-2-A	Gigabit Ethernet	Present	00:22:19:D2:1E:84	N/A	N/A
	iSCSI	Present		N/A	N/A
Server-2-B	Gigabit Ethernet	Present		Not Installed	Not Installed
	iSCSI	Present		Not Installed	Not Installed
Server-2-C	Fibre Channel 4	Present		Not Installed	Not Installed
Server-3	N/A	Not Present	N/A	N/A	N/A
Server-4-A	Gigabit Ethernet	Present	00:18:8B:FF:45:2A	00:18:8B:FF:AA:02	00:18:8B:FF:AA:04
	iSCSI	Present		00:18:8B:FF:AA:03	00:18:8B:FF:AA:05
Server-4-B	Gigabit Ethernet	Not Present		Not Installed	Not Installed

Table 43. Ethernet and iSCSI MAC/WWN addresses (continued)

	iSCSI	Present		Not Installed	Not Installed
Server-4-C	Fibre Channel 4	Present		Not Installed	Not Installed
Switch-1	None	Present	N/A	00:00:00:00:00:00	N/A

Table 44. User-defined MAC and WWN address

<Name>	*<Type>*	*<Presence>*	*<Active WWN/ MAC>*	*<Partition Status>*	*<Assignment Type>*
server-1-A	IDRAC-Controller	Present	18:A9:9B:FD:C4:DF	N/A	Factory
	Gigabit Ethernet	Present	00:0A:00:0A:00:00	Unknown	IO-Identity
	Gigabit Ethernet	Present	00:0A:00:0A:00:01	Unknown	IO-Identity
	Gigabit Ethernet	Present	00:0A:00:0A:00:02	Unknown	IO-Identity
	Gigabit Ethernet	Present	00:0A:00:0A:00:03	Unknown	IO-Identity

Table 45. MAC/WWN addresses

<Name>	*<Type>*	*<Presence>*	*<Active WWN/ MAC>*	*<Partition Status>*	*<Assignment Type>*
Server-3-A	IDRAC-Controller	Present	5C:F9:DD:D6:1C:CE	N/A	Factory
	Gigabit Ethernet	Present	84:8F:69:FC:E8:F0	Unknown	Factory
	Gigabit Ethernet	Present	84:8F:69:FC:E8:F1	Unknown	Factory

Table 45. MAC/WWN addresses (continued)

Switch-1	10 GbE KR	Present	F8:B1:56:45:DD:BD	N/A	Factory

Table 46. Chassis-assigned WWN/MAC address

<Name>	<Type>	<Presence>	<Active WWN/MAC>	<Partition Status>	<Assignment Type>
Server-4-A	IDRAC-Controller	Present	F8:DB:88:3D:9F:A7	N/A	FlexAddress
	10 GbE KR	Present	F8:DB:88:3D:9F:A9	Disabled	FlexAddress
	10 GbE KR/3	Present	F8:DB:88:3D:A2:78	Unknown	FlexAddress
	10 GbE KR/3	Present	F8:DB:88:3D:A2:7B	Unknown	FlexAddress

NOTE: 10 GbE KR/3—The value 3 indicates the protocol type.

Table 47. Console assigned MAC/WWN

<Name>	<Type>	<Presence>	<Active WWN/MAC>	<Partition Status>	<Assignment Type>
CMC	N/A	Present	34:17:EB:E6:E0:24	N/A	Factory
Server-1-A	10 GbE KR	Not Installed	10:98:36:AC:70:EB	Not Installed	Not Installed
Server-2	Not Installed	Not Present	Not Installed	Not Installed	Not Installed
Server-3-A	Reserved	Present			
Switch-4	Not Installed	Not Present	Not Installed	Not Installed	Not Installed
Switch-1	Not Installed	Not Present	Not Installed	N/A	N/A

NOTE: If the I/O Modules in slots 1 and 2 are absent and the `getmacaddress -a` and `getmacaddress —c all` commands are run, the output is displayed as `Not Installed` in the following columns:

- **<Presence>**
- **<NIC1 MAC Address>**
- **<NIC2 MAC Address>**

getmodinfo

Table 48. getmodinfo

Description	Displays configuration and status information for all modules or a specified module (server, switch, CMC, fan unit, blower, power supply unit, chassis, DVD, main-board, IO cable, and FPC cable) in the chassis. To use this subcommand, you must have **CMC Login User** privilege. **NOTE: The service tag field is blank for modules that do not have service tags.**
Synopsis	`racadm getmodinfo [-m <module>] [-A]`
Input	• **-m** *<module>* — Specifies the module for which the configuration and status information is required. The default command (no options) displays information about all the major components in the chassis. *<module>* can be one of the following values: ○ `server-n`, where n = 1 to 4 ○ `switch-n`, where n = 1 ○ `CMC-n`, where n = 1 or 2 ○ `fan-n`, where n = 1 to 6 ○ `blower-n`, where n = 1 to 4 ○ `ps-n`, where n = 1 to 4 ○ `chassis` ○ `dvd` ○ `main-board` ○ `io-cable` ○ `fpc-cable` ○ `storage` • **-A —** Does not display the headers and labels in the output.

Example	• `racadm getmodinfo -m switch-1`
	`<module> <presence> <pwrState> <health> <svcTag> <nodeId>`
	`Switch-1 Present ON OK N/A N/A`
	• `racadm getmodinfo`
	NOTE: A power state of "Primary" denotes Active CMC.
	`<module> <presence> <pwrState> <health> <svcTag> <nodeId>`
	`Chassis Present ON Not OK 3BPV622 N/A`
	`Main-Board Present ON OK N/A N/A`
	`Storage Present ON OK 3BPV622`
	`Fan-1 Unknown N/A Not OK N/A N/A`
	`Fan-2 Present ON OK N/A N/A`
	`Fan-3 Present ON`

Table 48. getmodinfo (continued)

	OK N/A N/A Fan-4 Present ON OK N/A N/A Fan-5 Present ON OK N/A N/A Fan-6 Present ON OK N/A N/A Blower-1 Present ON OK N/A N/A Blower-2 Present ON OK N/A N/A Blower-3 Present ON OK N/A N/A Blower-4 Present ON OK N/A N/A PS-1 Present Online OK N/A N/A PS-2 Present Online OK N/A N/A PS-3 Not Present N/A N/A N/A N/A PS-4 Not Present N/A N/A N/A N/A CMC-1 Present Primary OK N/A N/A CMC-2 Present Standby OK N/A N/A Switch-1 Present ON OK N/A N/A Server-1 Not Present N/ A N/A N/A N/A Server-2 Not Present N/A N/A N/A N/A Server-3 Present OFF OK DJ22H82 DJ22H82 Server-4 Not Present N/A N/A N/A N/A DVD Present ON OK N/A N/A IO-Cable Present ON OK 3BPV622 N/A FPC-Cable Present ON OK 3BPV622 N/A

getniccfg

Table 49. getniccfg

Description	Displays the current NIC settings.
Synopsis	`racadm getniccfg`

Input	`racadm getniccfg`
	`racadm getniccfg -m <module>`
	where –m must be one of the following values:

Table 49. getniccfg (continued)

	• `chassis` : default state if -m is not specified • `server-n` : where n = 1 to 4 • `switch-n` : where n = 1

Example	`racadm getniccfg`
	`NIC Enabled = 1`
	`IPv4 Enabled = 1`
	`DHCP Enabled = 1`
	`Static IP Address = 192.168.0.120`
	`Static Subnet Mask = 255.255.255.0`
	`Static Gateway = 192.168.0.1`
	`Current IP Address = 10.94.225.212`
	`Current Subnet Mask = 255.255.255.128`
	`Current Gateway = 10.94.225.129`
	`IPv6 Enabled = 0`
	`Autoconfiguration Enabled = 1`
	`Static IPv6 Address = ::/64`
	`Static IPv6 Gateway = ::`
	`Link Local Address = ::`
	`Current IPv6 Address 1 = ::`
	`Current IPv6 Gateway = ::`
	`Speed = Autonegotiate`
	`Duplex = Autonegotiate`
	`VLAN Enable = 0`
	`VLAN ID = 1`
	`VLAN priority = 0`
	`racadm getniccfg -m server-3`
	`LOM Model Name = BRCM GbE 4P 5720 bNDC`
	`LOM Fabric Type = Gigabit Ethernet`
	`IPv4 Enabled = 1`
	`DHCP Enabled = 0`
	`IP Address = 0.0.0.0`
	`Subnet Mask = 0.0.0.0`
	`Gateway = 0.0.0.0`
	`IPv6 Enabled = 0`
	`Autoconfiguration Enabled = 1`
	`Link local Address =`
	`IPv6 Gateway = ::`
	`VLAN Enable = 0`
	`VLAN ID = 1`
	`VLAN priority = 0`
	`racadm getniccfg -m switch-1`
	`DHCP Enabled = 0`
	`IP Address = 0.0.0.0`
	`Subnet Mask = 0.0.0.0`
	`Gateway = 0.0.0.0`

getpbinfo

Table 50. Details of getpbinfo

Description	Displays power budget status information. To use this subcommand, you must have the **CMC Login User** privilege.
Synopsis	`racadm getpbinfo`

Example

```
racadm getpbinfo
```

```
[Power Budget Status]
System Input Power                              = 333 W
Peak System Power                               = 403 W
Peak System Power Timestamp                     = 15:38:01 06/14/2013
Minimum System Power                            = 269 W
Minimum System Power Timestamp                  = 19:12:27 09/22/2000
Overall Power Health                            = OK
Redundancy                                      = Yes
System Input Power Cap                          = 5000 W
Redundancy Policy                               = Power Supply Redundancy
Dynamic PSU Engagement Enabled                  = No
System Input Max Power Capacity                 = 2372 W
Input Redundancy Reserve                        = 1182 W
Input Power Allocated to Servers                = 327 W
Input Power Allocated to Chassis Infrastructure = 427 W
Total Input Power Available for Allocation      = 344 W
Standby Input Power Capacity                    = 0 W
Server Based Power Management Mode              = No
Max Power Conservation Mode                     = No
Server Performance Over Power Redundancy        = No
```

```
[Chassis Power Supply Status Table]
<Name>          <Presence>      <Power State>   <Input Current> <Input Volts>   <Output Rated
Power>
PS1             Present         Online          1.3 A           115.5 V         1050 W
PS2             Present         Online          1.6 A           116.0 V         1050 W
PS3             Not Present     Slot Empty      N/A             N/A             N/A
PS4             Not Present     Slot Empty      N/A             N/A             N/A
```

```
[Server Module Power Allocation Table]
<Slot#> <Server Name> <Power State>   <Allocation> <Priority>       <Blade Type>
1       SLOT-01         OFF             0 W            1           PowerEdge M620
2       SLOT-02         N/A             N/A            1           N/A
3       SLOT-03         ON              327 W          1           PowerEdge M620
4       SLOT-04         N/A             N/A            1           N/A
```

getpciecfg

Table 51. Details of getpciecfg

Description	Displays the FQDD of the PCIe slots and Virtual Adapters, and their mapping information and properties. **NOTE:** • **To use this subcommand, you must have the CMC Login User privilege.** • **Lengthy PCIe card names and server slot names are truncated when the assignments for all PCIe slots are displayed.**

Table 51. Details of getpciecfg (continued)

Synopsis	`racadm getpciecfg [-c <FQDD>][a]`
Input	• **-a** — Use this option to display the assignment of PCIe slots and Virtual Adapters. • **-c** — Use this option to select a specific PCIe adapter or Virtual Adapter. • **FQDD** — FQDD of the selected PCIe slot or Virtual Adapter. • **-r** — Use this option to view the ride-through configuration settings.
Example	• **Table 52. Details of shared external adapter in PCIe slots**

<PCIe Slot#>	<Name>	<Power State>	<Server Slot Name>	<Server Slot#>	<Server Presence>
PCIe slot-1	Broadcom Corporation NetXtreme II	OFF	Unmapped	N/A	N/A
PCIe slot-2	Ethernet Server Adapter I350-T2	OFF	Unmapped	N/A	N/A
PCIe slot-3	Broadcom Corporation NetXtreme BCM	OFF	Unmapped	N/A	N/A
PCIe slot-4	Not Present	N/A	N/A	N/A	N/A
PCIe slot-5	Shared PERC 8 External	ON	Shared	N/A	N/A
PCIe slot-6	Shared PERC 8 External	ON	Shared	N/A	N/A
PCIe slot-7	Not Present	N/A	N/A	N/A	N/A
PCIe slot-8	Not Present	N/A	N/A	N/A	N/A

Table 52. Details of shared external adapter in PCIe slots

<Virtual Adapter#>	<Storage Adapters Slots>	<Server Slot Name>	<Server Slot#>	<Server Presence>
1	5,6,9,10	SLOT-01	1	Present

Table 51. Details of getpciecfg (continued)

Table 52. Details of shared external adapter in PCIe slots (continued)

2	5,6,9,10	SLOT-02	2	Not Present
3	5,6,9,10	Unmapped	N/A	N/A
4	5,6,9,10	SLOT-04	4	Not Present

- Displays FQDDs of all the PCIe slots and PCIe Virtual Adapters:

```
racadm getpciecfg
```

```
<PCIe Slot#>     <FQDD>
PCIe slot 01     PCIE.ChassisSlot.1
PCIe slot 02     PCIE.ChassisSlot.2
PCIe slot 03     PCIE.ChassisSlot.3
PCIe slot 04     PCIE.ChassisSlot.4
PCIe slot 05     PCIE.ChassisSlot.5
PCIe slot 06     PCIE.ChassisSlot.6
PCIe slot 07     PCIE.ChassisSlot.7
PCIe slot 08     PCIE.ChassisSlot.8

<PCIe Slot#>     <Virtual Adapter#>      <FQDD>
PCIe slot 09     Virtual Adapter 01      RAID.ChassisIntegrated.1-1-1
PCIe slot 09     Virtual Adapter 02      RAID.ChassisIntegrated.1-1-2
PCIe slot 09     Virtual Adapter 03      RAID.ChassisIntegrated.1-1-3
PCIe slot 09     Virtual Adapter 04      RAID.ChassisIntegrated.1-1-4

PCIe slot 10     Virtual Adapter 01      RAID.ChassisIntegrated.2-1-1
PCIe slot 10     Virtual Adapter 02      RAID.ChassisIntegrated.2-1-2
PCIe slot 10     Virtual Adapter 03      RAID.ChassisIntegrated.2-1-3
PCIe slot 10     Virtual Adapter 04      RAID.ChassisIntegrated.2-1-4
```

- Displays the properties of a PCIe slot selected using FQDD:

```
racadm getpciecfg -c pcie.chassisslot.1
```

- Displays the properties of a Virtual Adapter selected using FQDD:

```
racadm getpciecfg -c RAID.ChassisIntegrated.2-1-4
```

- Displays the ride-through properties of the system

```
racadm getpciecfg -r
```

```
Ride-through mode is enabled
Ride-through timeout 1800 secs
```

getpminfo

Table 53. Details of getpminfo

Description	Displays power management status information. To use this subcommand, you must have **CMC Login User** privilege.

Table 53. Details of getpminfo (continued)

Synopsis	`racadm getpminfo`

Example	`racadm getpminfo`
	
	`[Real-Time Power Statistics]`
	`System Input Power = 600 W (188 BTU/hr)`
	`Peak System Power = 600 W (188 BTU/hr`
	`Peak System Power Start Time = 16:02:10 01/16/2008`
	`Peak System Power Timestamp = 06:32:55 01/26/2009`
	`Minimum System Power = 400 W (177 BTU/hr)`
	`Minimum System Power Start Time = 22:43:21 01/21/2008`
	`Minimum System Power Timestamp = 06:32:55 01/26/2009`
	`System Idle Power = 68 W (188 BTU/hr)`
	`System Potential Power = 68 W (188 BTU/hr)`
	`System Input Current Reading = 31.2 A`
	
	`[Real-Time Energy Statistics]`
	`System Energy Consumption = 6.4 kWh`
	`System Energy Consumption Start Time = 16:02:10 01/16/2008`
	`System Energy Consumption Timestamp = 16:02:10 01/16/2008`
	
	`[System Power Status]`
	`Chassis Power State = ON`
	`Overall Power Health = OK`
	`Redundancy = No`
	
	`[System Power Policy Configuration]`
	`System Input Power Cap = 7928 W (7928 BTU/hr | 10%)`
	`Surplus for Peak Performance = 7000 W (6130 BTU/hr)`
	`Redundancy Policy = None`
	`Dynamic PSU Engagement Enabled = No`
	
	`[Power Budgeting]`
	`System Input Max Power Capacity = 0 W`
	`Input Redundancy Reserve = 0 W`
	`Input Power Allocated to Servers = 0 W`
	`Input Power Allocated to Chassis Infrastructure = 51W`
	`Total Input Power Available for Allocation = 0 W`
	`Standby Input Power Capacity = 0 W`

getraclog

Table 54. Details of getraclog

Description	The `getraclog` command displays RAC log entries.
Synopsis	`racadm getraclog [-s <start>] [-c <count>]`
Input	**NOTE: If no options are provided, the entire log is displayed.** · **-c** — Specifies the number of records to display. · **-s** — Specifies the starting record used for the display. · **--more** — Displays one screen at a time and prompts the user to continue.

Output	The default output display shows the record number, message ID, category, agent ID, severity, time stamp, message arg, and message. The timestamp begins at midnight, January 1, and increases until the system restarts. After the system restarts, the system's timestamp is used.
	`SeqNumber = 4`
	`Message ID = CMC8550`
	`Category = Audit`
	`AgentID = CMC`
	`Severity = Information`
	`Timestamp = 1982-03-21 05:33:35`
	`Message Arg 1 = Healthy`
	`Message = Chassis health is Healthy`

Example	· Displays all the logs.
	`racadm getraclog`
	· Displays 3 records from record number 5:
	`racadm getraclog -s 5 -c 3`

getractime

Table 55. Details of getractime

Description	Displays the current iDRAC time.
Synopsis	· `racadm getractime [-d]` · `racadm getractime [-d][-z]` · `racadm getractime [-n]`
Input	· **-d** — Displays the time in the format, yyyymmddhhmmss.mmmmmms. · **-z** — Displays timezone. This option is specific to CMC only. · **-n** — Displays NTP peer information. This option is specific to CMC only. **NOTE: If no options are provided, the getractime subcommand displays the time in a common readable format.**
Output	The current iDRAC time is displayed.
Example	· `racadm getractime` Thu Dec 8 20:15:26 2005 · `racadm getractime -d` 20051208201542.000000

getredundancymode

Table 56. Details of getredundancymode

Description	Displays the redundancy status (Redundant or Non-Redundant) of the CMC. To use this subcommand, you must have **CMC Login User** privilege.
Synopsis	`racadm getredundancymode`
Example	`racadm getredundancymode` `Redundant`

getsel

Table 57. Details of getsel

Description	Displays all sensor event log entries in the DRAC.
Synopsis	• racadm getsel -i [-A] • racadm getsel [-s <*start*>] [-c <*count*>] [-A] [-o] [-E] [-R] [--more] If no arguments are specified, the entire log is displayed.
Input	• **-A** — Specifies output with no display headers or labels. • **-c** — Provides the number of records to be displayed. • **-o** — Displays each entry in the SEL in a single line. • **-s** — Specifies the starting record used for the display. • **-E** — Displays RAW SEL data with the other data for each entry. • **-R** — Displays only RAW SEL data for each entry. • **-i** — Displays the number of entries in the SEL. • **--more** — Displays one screen at a time and prompts the user to continue (similar to the UNIX **more** command.) **NOTE: The -A, -E, -o, and -R options are deprecated.**

Output	`Record: 12`
	`Date/Time: 11/20/2011 14:19:34`
	`Source: system`
	`Severity: Ok`
	`Description: C: boot completed.`

Example	`racadm getsel`

getsensorinfo

Table 58. Details of getsensorinfo

Description	Displays status of chassis sensors. **NOTE: To use this subcommand, you must have CMC Login User privilege.**
Synopsis	`racadm getsensorinfo` `racadm getsensorinfo -c`

Table 59. Examples

<Sensor Name>	<Status>	<Reading>	<LW>	<LC>	<UW>	UC
Fan-1	OK	0	840	600	N/A	N/A
Fan-2	OK	0	840	600	N/A	N/A
Fan-3	OK	4037	840	600	N/A	N/A
Fan-4	OK	4045	840	600	N/A	N/A
Fan-5	OK	4107	840	600	N/A	N/A
Fan-6	OK	0	840	600	N/A	N/A
Blower-1	N/A	0	3000	2250	N/A	N/A
Blower-2	N/A	0	3000	2250	N/A	N/A
Blower-3	N/A	0	3000	2250	N/A	N/A
Blower-4	N/A	2611	3000	2250	N/A	N/A

Table 60. Temperature sensor

<Sensor Name>	<Status>	<Reading>	<LW>	<LC>	<UW>	<UC>
Chassis Ambient	OK	22	3	-7	42	47

Table 60. Temperature sensor (continued)

Server-4	OK	20	3	-7	42	47

Table 61. Power, Cable, Intrusion, and FanSpeed sensor

<Num>	<sensorName>	<status>	<reading>	<LW>	<LC>	<UW>	<UC>	<PWM>
1	Fan-1	OK	3159 rpm	840	600	N/A	N/A	6
2	Fan-2	OK	3163 rpm	840	600	N/A	N/A	6
3	Fan-3	OK	3180 rpm	840	600	N/A	N/A	6
4	Fan-4	OK	3143 rpm	840	600	N/A	N/A	6
5	Fan-5	OK	3177 rpm	840	600	N/A	N/A	6
6	Fan-6	OK	3141 rpm	840	600	N/A	N/A	6
1	Blower-1	OK	1721 rpm	1108	923	N/A	N/A	20
2	Blower-2	OK	1733 rpm	1108	923	N/A	N/A	20
3	Blower-3	OK	1704 rpm	1108	923	N/A	N/A	20
4	Blower-4	OK	1702 rpm	1108	923	N/A	N/A	20

Table 62. Temp sensor

<Num>	<sensorName>	<status>	<reading>	<LW>	<LC>	<UW>	<UC>
1	Chassis Ambient	OK	27 C	3	–7	42	47
2	Server-1	OK	31 C	3	–7	42	47
3	Server-3	OK	29 C	3	–7	42	47

Table 63. Power sensor

<Num>	<sensorName>	<status>	<health>
1	PS-1	Slot Empty	N/A
2	PS-2	Online	OK
3	PS-3	Slot Empty	N/A
	PS-4	Slot Empty	N/A

Table 64. Cable sensor

<Num>	<seonsorName>	<status>
1	IO-Cable	OK
2	FPC-Cable	OK

Table 65. Door sensor

<Num>	<sensorName>	<status>
1	Chassis Intrusion	Closed

getslotname

Table 66. Details of getslotname

Description	Displays the name, host name (if available) and iDRAC DNS name of all the four slots, or of a specified slot (indicated by the slot number) in the chassis. Optionally, use this command to find if the slot name or host name, or iDRAC DNS name is displayed in the CMC Web interface, or with the getslotname [-i <*slotNum*> | -h] command. If the host name is not available, the static slot name is used. **NOTE: Lengthy slot names, host names, or iDRAC DNS names are truncated when the slot names are displayed.** To use this subcommand, you must have **CMC Login User** privilege.
Synopsis	• racadm getslotname • racadm getslotname [-i <*slotNum*> | -h] • racadm getslotname -h
Input	• None - Displays the slot name for all the four slots in the chassis. • -i <*slotNum*> - specifies the slot number. Values: 1 to 4 • -h - Specifies whether to display the slot name or the host name (if available). ○ 0 — Displays the slot name ○ 1 — Displays the host name instead of the slot name ○ 2 — Displays the iDRAC DNS name instead of the slot name

Example	• Display all slots names.
	`racadm getslotname`
	`<Slot #> <Slot Name>  <Host name>  <iDRAC DNS Name>`
	`1  SLOT-01`
	`2  WIN-UF2EVKG8PJ5  WIN-UF2EVKG8PJ5 idrac-2QDJH62`
	`3  SLOT-03`
	`4  SLOT-04`
	• Display the name of the third slot.
	`racadm getslotname -i 3`
	• Verify if the option '0' is set for displaying the slot name.
	• Verify if the option '1' is set for displaying the host name.
	• Verify if the option '2' is set for displaying the iDRAC DNS name.

getssninfo

Table 67. Details of getssninfo

Description	Displays a list of users that are connected to iDRAC. The following information is displayed: • Session ID • Username • IP address (if applicable) • Session type (for example, serial or Telnet) • Login date and time in MM/DD/YYYY HH:MM:SS format

Table 67. Details of getssninfo (continued)

	NOTE: Based on the Session ID (SSNID) or the user name (User), the iDRAC administrator can close the respective sessions or all the sessions using the, closessn subcommand. For more information, see closessn.
Synopsis	`racadm getssninfo [-A] [-u <username> | *]`
Input	• **-A** - eliminates the printing of data headers. • **-u** - The -u *<username>* user name option limits the printed output to only the detail session records for the given user name.

Table 68. Examples

SSNID	Type	User	IP Address	Login Date/Time
6	GUI	root	192.168.0.10	04/07/2010 12:00:34

```
racadm getssninfo -A
```

```
"root" "143.166.174.19" "Telnet" "NONE"
```

```
racadm getssninfo -A -u *
```

```
"root" "143.166.174.19" "Telnet" "NONE"
```

```
"bob" "143.166.174.19" "GUI" "NONE"
```

getsvctag

Table 69. Details of getsvctag

Description	Displays the service tag of the host system.
Synopsis	`racadm getsvctag`
Input	`getsvctag`

Output	`<Module>  <ServiceTag>`
	`Chassis  PLPC033`
	`Switch-1  N/A`
	`Server-1  7654321`
	`Server-2  N/A`
	`Server-3  Extension(1)`
	`Server-4  PLSMS04`

Example	`racadm getsvctag`

getsysinfo

Table 70. Details of getsysinfo

Description	Displays information related to CMC and chassis.

Table 70. Details of getsysinfo (continued)

	NOTE: The Hostname and OS Name fields in the getsysinfo output display accurate information only if Dell OpenManage Server Administrator is installed on the managed system. Else, these fields may be blank or inaccurate. An exception to this are VMware operating system names, which are displayed even if Server Administrator is not installed on the managed system.
Synopsis	`racadm getsysinfo [-d] [-c] [-A] [-4] [-6]`
Input	• **-d** - Displays CMC information. • **-c** - Displays chassis information. • **-A** - Does not display headers and labels. • **-4** - Displays IPv4 information. • **-6** - Displays IPv6 information.

Output	`CMC Information:`
	`CMC Date/Time = Sat Mar 27 1982 11:36`
	`Primary CMC Location = CMC-1`
	`Primary CMC Version = 1.00`
	`Standby CMC Version = N/A`
	`Last Firmware Update = Sun Mar 21 1982 05:53`
	`Hardware Version = X12`
	
	`CMC Network Information:`
	`NIC Enabled = 1`
	`MAC Address = 78:45:C4:F7:8B:29`
	`Register DNS CMC Name = 1`
	`DNS CMC Name = cmc-servicetag`
	`Current DNS Domain = swtest.com`
	`VLAN ID = 1`
	`VLAN Priority = 0`
	`VLAN Enabled = 0`
	
	`CMC IPv4 Information:`
	`IPv4 Enabled = 1`
	`Current IP Address = 192.168.0.1`
	`Current IP Gateway = 192.168.0.1`
	`Current IP Netmask = 255.255.255.128`
	`DHCP Enabled = 1`
	`Current DNS Server 1 = 192.168.0.1`
	`Current DNS Server 2 = 0.0.0.0`
	`DNS Servers from DHCP = 1`
	
	`CMC IPv6 Information:`
	`IPv6 Enabled = 0`
	`Autoconfiguration Enabled = 1`
	`Link Local Address = ::`
	`Current IPv6 Address 1 = ::`
	`Current IPv6 Gateway = ::`
	`Current IPv6 DNS Server 1 = ::`
	`Current IPv6 DNS Server 2 = ::`
	`DNS Servers from DHCPv6 = 1`
	
	`Chassis Information:`
	`System Model = PowerEdge VRTX`
	`System AssetTag = 00000`
	`Service Tag =`
	`Express Service Code =`
	`Chassis Name = CMC-`
	`Chassis Location = [UNDEFINED]`
	`Chassis Midplane Version = 1.0`
	`Power Status = ON`
	`System ID = 1487`

Table 70. Details of getsysinfo (continued)

Examples	`racadm getsysinfo -d`
	`racadm getsysinfo -c`
	`racadm getsysinfo -A`
	`racadm getsysinfo -4`
	`racadm getsysinfo -6`

gettracelog

Table 71. Details of gettracelog

Description	Lists all the trace log entries in CMC.
Synopsis	• `racadm gettracelog -i [-A]` • `racadm gettracelog [-s <start>] [-c <count>] [--more] [-A] [-o]`
Input	• **-i** - Displays the number of entries in iDRAC trace log. • **--more** - Displays one screen at a time and prompts the user to continue (similar to the UNIX more command). • **-o** - Displays each entry in a single line. • **-c** - Specifies the number of records to display. • **-s** - Specifies the starting record to display. • **-A** - Does not display headers or labels. **NOTE: The -A and -o options are deprecated.**
Output	The default output display shows the record number, timestamp, source, and description. The timestamp begins at midnight, January 1 and increases until the system boots. After the system boots, the system's timestamp is used.

Example	`Record: 1`
	`Date/Time: Dec 8 08:21:30`
	`Source: ssnmgrd[175]`
	`Description: root from 143.166.157.103: session timeout sid 0be0aef4`

getversion

Table 72. getversion

Description	Displays the current firmware version of various modules in the chassis, iDRAC version on the attached servers, and whether the target device can be updated. **NOTE: To use this subcommand, you must have CMC Login User privilege.**

Table 72. getversion (continued)

Synopsis	· racadm getversion · racadm getversion [-b | -c] [-m <*module*>] · racadm getversion -l [-m <*module*>] [-f <*filter*>]
Input	**NOTE: The -b, -c and -l options are not available for CMC modules.** **NOTE: The -l option requires that the Lifecycle Controller service is enabled on the servers. For version information, see the RACADM Readme available at dell.com/support/manuals.** · **(none)** — Displays the version information for all targets or devices.

```
<Server>    <iDRAC Version>        <Blade Type>           <Gen>
<Updatable>
server-3                    2.20.20.20 (41)        PowerEdge M630
(VRTX)                  iDRAC8                    Y
```

```
<Switch>    <Model Name>                      <HW Version>      <FW
Version>
switch-1               R1-PT VRTX 1Gb Pass-through
A00                     1.0.0.8
```

```
<CMC>    <CMC Version>              <Updatable>
cmc-1               3.00.000.201609223282                                Y
cmc-2
3.00.000.201609223282                                        Y
```

```
<Chassis Infrastructure>    <FW Version>               <FQDD>
Main Board                      2.21.A00.201510302495
System.Chassis.1#Infrastructure.1
```

```
<Storage Controller>    <FW Version>               <FQDD>
Shared PERC8
23.13.06.0011                RAID.ChassisIntegrated.1-1
```

```
<Storage Enclosure>    <FW Version>               <FQDD>
VRTX2.5x25 0:0                      1.02
Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1
```

```
<Physical Disk>         <FW Version>           <FQDD>
Physical Disk 0:0:0             AS09
Disk.Bay.0:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1
Physical Disk 0:0:1             AS09
Disk.Bay.1:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1
Physical Disk 0:0:10            AS09
Disk.Bay.10:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1
Physical Disk 0:0:11            AS09
Disk.Bay.11:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1
Physical Disk 0:0:12            AS09
Disk.Bay.12:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1
Physical Disk 0:0:13            AS09
Disk.Bay.13:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1
Physical Disk 0:0:14            AS09
Disk.Bay.14:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1
Physical Disk 0:0:18            AS09
Disk.Bay.18:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1
Physical Disk 0:0:19            AS09
Disk.Bay.19:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1
Physical Disk 0:0:2             AS09
Disk.Bay.2:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1
Physical Disk 0:0:3             AS09
Disk.Bay.3:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1
Physical Disk 0:0:4             AS09
```

Table 72. getversion (continued)

	``` Disk.Bay.4:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1 Physical Disk 0:0:5 AS09 Disk.Bay.5:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1 Physical Disk 0:0:6 AS09 Disk.Bay.6:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1 Physical Disk 0:0:7 AS09 Disk.Bay.7:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1 Physical Disk 0:0:8 AS09 Disk.Bay.8:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1 Physical Disk 0:0:9 AS09 Disk.Bay.9:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1 ``` • **-b** - Displays the server's current BIOS version (default is iDRAC version). • **-c** - Displays the server's current CPLD version. • **-l** - Displays the firmware versions Lifecycle Controller components. • **-f** *<filter>* - Filters the components. Must be used with **-1** and be one of the following values: ○ bios: BIOS ○ idrac: iDRAC ○ usc: Unified Server Configurator (Lifecycle Controller) ○ diag: 32-bit Diagnostics ○ drivers: OS Driver Package ○ nic-x: Network Interface card. See -l output for possible values of x. ○ raid-x: RIAD Controller. See -l output for possible values of x. • **-m** *<module>* - Specifies the module or device for which you must retrieve the version information. *<module>* is one of the following: ○ `server-n`, where n = 1 to 4. For example, cmc-2. ○ `switch-n`, where n = 1 ○ `CMC-n`, where n = 1 or 2 ○ `mainboard` ○ `perc` ○ `expander` ○ `hdd` ○ `perc-fqdd`, where fqdd is FQDD of the PERC. ○ `expander-fqdd`, where fqdd is FQDD of the Storage Expander. ○ `hdd-fqdd`, where fqdd is FQDD of the HDD. **NOTE: The Linux shell script does not support the characters—$ (dollar),` (back quote), \ (forward slash), & (ampersand), ((open bracket),) (Close bracket), = (equal), | (Pipe), ; (semi colon)," (Double quote), ' (single quote), < (less than), and > (greater than).**
Example	• Retrieve the version for a server 4 ``` racadm getversion -m server-4 ``` • Retrieve the Lifecycle Controller component versions for servers 1 and 3: ``` racadm getversion -l -m server-1 -m server-3 ``` • Retrieve the Lifecycle Controller BIOS versions for servers 1 and 3: ``` racadm getversion -l -m server-1 -m server-3 -f bios ``` • Retrieve the version for all modules: ``` racadm getversion ``` • Retrieve the iDRAC version in all the servers that are attached to the chassis: ``` racadm getversion -f idrac ```

ifconfig

Table 73. Details of ifconfig

Description	Displays the contents of the network interface table. To use this subcommand, you must have the **Execute Diagnostic Commands or Configure iDRAC** privilege.
Synopsis	`racadm ifconfig`

Example	`$ racadm ifconfig`
	`eth0 Link encap:Ethernet HWaddr 00:1D:09:FF:DA:23`
	`inet addr:10.35.155.136 Bcast:192.168.0.1 Mask:255.255.255.0`
	`UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1`
	`RX packets:2550665 errors:0 dropped:0 overruns:0 frame:0`
	`TX packets:0 errors:0 dropped:0 overruns:0 carrier:0`
	`collisions:0 txqueuelen:1000`
	`RX bytes:272532097 (259.9 MiB) TX bytes:0 (0.0 B)`

jobqueue

Table 74. Details of jobqueue

Description	Displays the jobs in that are currently being run, delete the jobs, and create a job. **NOTE: To view the jobs, you must have CMC Login User privilege.** **NOTE: To delete the jobs, you must have Chassis Configuration Administrator privilege.**

Synopsis	`racadm jobqueue view`
	`racadm jobqueue delete`
	`racadm jobqueue create`

Input	• **—i** — Specifies the JobID that is displayed or deleted.

Table 74. Details of jobqueue (continued)

	• **– –all** — The JobIDs that are not applied are deleted. • **<fqdd>** — Specifies an FQDD for which a job has to be created. • **reboot type** — Specifies a reboot type. Valid options are **none: No Reboot Job** which is the default. • **start time** — Specifies a start time for job to be scheduled in yyyymmddhhmmss format. If you specify TIME_NOW, the job is immediately run. • **Expiration time** — Specifies the expiry time for the job to complete in yyyymmddhhmmss format. If you specify TIME_NA, the wait-time is not applicable for the job.

Example	• Display all the jobs:
	`----------JOB QUEUE----------`
	`[Job ID=RID_853106266329]`
	`Job Name=Reboot4`
	`Status=New`
	`Start Time=[NOW]`
	`Expiration Time=[NOW]`
	`----------`
	`[Job ID=RID_852218430518]`
	`Job Name=Reboot4`
	`Status=New`
	`Start Time=[NOW]`
	`Expiration Time=[NOW]`
	`----------`
	`[Job ID=RID_852215634901]`
	`Job Name=Reboot4`
	`Status=New`
	`Start Time=[NOW]`
	`Expiration Time=[NOW]`
	`----------`
	`[Job ID=JID_852215394003]`
	`Job Name=ConfigRAID:GUI:RAID.ChassisIntegrated.1-1`
	`Status=New`
	`Start Time=[NOW]`
	`Expiration Time=[NOW]`
	`----------`
	• Delete the specified job:
	`racadm jobqueue delete -i RID_860202993201`
	• Job being created to turn on the RAID controller installed in the chassis.
	`racadm jobqueue create RAID.ChassisIntegrated.1-1 -r pwrup -s TIME_NOW -e 20120501100000`
	• racadm jobqueue delete -i <JobID>

krbkeytabupload

Table 75. Details of krbkeytabupload

Description	Uploads a Kerberos keytab file. To use this subcommand, you must have the **Configure iDRAC** permission.
Synopsis	`racadm krbkeytabupload [-f <filename>]` `<filename> is the name of the file including the path.`

Table 75. Details of krbkeytabupload (continued)

Input	**-f** — Specifies the file name of the keytab to be uploaded. If the file is not specified, the keytab file in the current directory is selected.
Output	Returns 0 when successful, and a non–zero number, when unsuccessful.
Example	`racadm krbkeytabupload -f c:\keytab \krbkeytab.tab`

license

Table 76. Details of license

Description	Manages the CMC licenses.
Synopsis	`racadm license <license command type>`. The command type can be: · View the license using the following options: ○ `racadm license view` ○ `racadm license view [-c <component>]` · `racadm license import [-u <username>] [-p <password>] [-f <license file name>] [-l <NFS or CIFS share>] [-c <FQDD>]` · Export the license using the following options: ○ `racadm license export [-u <username>] [-p <password>] [-f <license file name>] [-l <NFS/CIFS share>] [–t <transaction ID>]` ○ `racadm license export [-u <username>] [-p <password>] [-f <license file name>] [-l <NFS/CIFS share>] [–e <entitlement ID>]` ○ `racadm license export [-u <username>] [-p <password>] [-f <license file name>] [-l <NFS/CIFS share>] [–c <FQDD>]` ○ `racadm license export [-u <username>] [-p <password>] [-f <license file name>] [-l <NFS/CIFS share>] [–c <FQDD>] [–e <entitlement ID>] [–t <transaction ID>]` · Delete the license using the following options: ○ `racadm license delete [-t <transaction ID>]` ○ `racadm license delete [-e <entitlement ID>]` ○ `racadm license delete [-c <component]` · Replace the license: `racadm license replace [-u <username>] [-p <password>] [-f <license file name>] [-l <NFS/CIFS share>] [–t <transaction ID>]`
Input	**NOTE: License operations the <licensefile> name should be fewer than 56 Characters.** **NOTE: During Remote file share, SSH/telnet supports the Import and Export options.** **NOTE: Only a user with administrator-level privileges can use the import, export, delete, and replace commands. An Administrator privilege is not necessary to use the view command.** · **view** — View license information. · **import** — Installs a new license. · **export** — Exports a license file. · **delete** — Deletes a license from the system.

Table 76. Details of license (continued)

<table>
<tr><td></td><td>

replace — Replaces an older license with a given license file.

Use the following options along with the commands:

-c — Specifies the FQDD of the component or device, on which the license is present.
-l — Network share location to import or export the license file.
-f — File name of the license file.
NOTE: During export, the license file is named <servicetag>_<entitlement ID>.xml.
-u— User name of the remote share.
-p — Password for the remote share.
-e — Specifies the entitlement ID of the license file.
-t — Specifies the transaction ID of the license file.

</td></tr>
<tr><td>Examples</td><td>

View licenses:

View all the license information in the chassis.
<pre>racadm license view</pre>
<pre>CMC.Integrated.1
        Status   = OK
        Device   = CMC.Integrated.1
        Device Description   = Chassis Management Controller for
PowerEdge VRTX
        Unique Identifier   =
                License #1
                        Status   = OK
                        Transaction ID   = 8
                        License Description = CMC Enterprise
Evaluation License

                        License Type   = EVALUATION
                        Entitlement ID   =
A2Wir6lJ1MoP8iBAtqsEKDv8
                        Expiration   = 1982-04-07T21:00:00</pre>

Display licenses available on a specific device. For example, for RAID slot 4:
<pre>racadm license view -c RAID.slot.4</pre>

Import a license:

Import a license from a CIFS share to a device (for example, Integrated CMC):
<pre>racadm license import -u admin -p passwd -f License.xml -l //
192.168.2.140/licshare -c cmc.integrated.1</pre>

Import a license from an NFS share to a device (for example, Integrated CMC):
<pre>racadm license import -f License.xml -l 192.168.2.14:/share -c
cmc.integrated.1</pre>

Import a license from the local file system using Remote RACADM:
<pre>racadm -u admin -p passwd -r 192.168.0.120 license import -f
C:\Mylicdir\License.xml -c cmc.integrated.1</pre>

Export a license file:

Export license to an NFS share using transaction ID (for example, transaction 27).
<pre>racadm license export -f License.xml -l 192.168.2.140:/licshare -
t 27</pre>

</td></tr>
</table>

Table 76. Details of license (continued)

	○ Export the license to a CIFS share specifying the entitlement ID (for example, abcdxyz):
	`racadm license export -u admin -p passwd -f License.xml -l // 192.168.2.140/licshare -e abcdxyz`
	○ Export license to a CIFS share specifying the FQDD. While using the -c option and exporting licenses from a device, more than one license file must be exported. Therefore, if a file name is provided, an index is appended to the end of the file name such as LicenseFile**0**.xml, LicenseFile**1**.xml, and so on. In this case, the device is an embedded CMC:
	`racadm license export -u root -p calvin -f LicenseFile.xml -l // 192.168.2.140/licshare -c cmc.integrated.1`
	· Delete a license:
	○ Delete licenses on a particular device. For example. Integrated CMC:
	`racadm license delete -c cmc.integrated.1`
	○ Delete license using an entitlement ID. For example, xYZabcdefg
	`racadm license delete -e xYZabcdefg`
	○ Delete license using a transaction ID. For example, 2.
	`racadm license delete -t 2`
	· Replace a license.
	○ Replace the license on a device with a license file that is on an NFS share, and using a transaction ID. For example, transaction 27.
	`racadm license replace -f License.xml -l 192.168.2.140:/licshare -t 27`
	○ Replace license on a device with a license file that is on a CIFS share and using a transaction ID. For example, transaction 27.
	`racadm license replace -u admin -p passwd -f License.xml -l // 192.168.2.140/licshare -t 27`
	○ Replace license on a device with a license file on the local file system.
	`racadm license replace -f License.xml -t 27`

netstat

Table 77. Details of netstat

Description	Displays the routing table and the current connections. To use this subcommand, you must have the **Execute Diagnostic Commands** privilege.
Synopsis	`racadm netstat`
Input	`racadm netstat`

Output

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0                     100.101.22.1    0.0.0.0                         UG
0         0          0 eth0
```

```
100.101.22.0    0.0.0.0                 255.255.255.0   U       0          0          0
eth0
```

ping

Table 78. Details of ping

Description	Verifies that the destination IP4address is reachable from iDRAC with the current routing-table contents. A destination IP4address is required. An ICMP echo packet is sent to the destination IP address based on the current routing-table contents. To use this subcommand for CMC, you must have the Administrator privilege for CMC, and for iDRAC you must have the Execute Diagnostic Commands privilege.
Synopsis	`racadm ping <ip4address>`

ping6

Table 79. Details of ping6

Description	Verifies that the destination IPv6 address is reachable from an iDRAC or CMC, or with the current routing-table contents. A destination IPv6 address is required. An ICMP echo packet is sent to the destination IPv6 address on the basis of current routing-table contents. To use this subcommand for CMC, you must have the Administrator privilege.
Synopsis	`racadm ping6 <ipv6address>`

Example	`racadm iping6 198.162.0.2`
	`IPING6 198.162.0.2 (192.168.0.1): 56 data bytes`
	`64 bytes from 198.162.0.2: icmp_seq=0 ttl=121 time=2.9 ms`
	
	`--- 198.162.0.2 ping statistics ---`
	`1 packets transmitted, 1 packets received, 0 percent packet loss`
	`round-trip min/avg/max = 2.9/2.9/2.9 ms`

racdump

Table 80. Details of racdump

Description	This subcommand displays the comprehensive chassis status and configuration state information, and historic event logs. Used for post-deployment configuration verification and during debugging sessions. To use this subcommand for CMC, you must have the **Administrator** privilege.
Synopsis	`racadm racdump`
Input	`Racdump` includes the following subsystems and aggregates the following RACADM commands: • General System/RAC information - `getsysinfo` • Session information - `getssinfo` • Sensor information - `getsensorinfo` • Switches information (IO Module) - `getioinfo` • Mezzanine card information (Daughter card) - `getdcinfo` • All modules information - `getmodinfo` • Power budget information - `getpbinfo` • KVM information - `getkvminfo` • NIC information (CMC module) - `getniccfg` • Redundancy information - `getredundancymode` • Trace log information - `gettracelog` • RAC event log - `getraclog` • System event log - `getsel`
Output	The following information is displayed when the `racdump`subcommand is processed: • General system/RAC information • Coredump • Session information • Process information • Firmware build information

Example

```
racadm racdump
```

```
================================================================================
 General System/RAC Information
================================================================================

CMC Information:
CMC Date/Time           = Wed, 28 Nov 2007 11:55:49 PM
CMC Version             = X08
Last Firmware Update    = Wed Nov 21 21:37:56 2007
Hardware Version        = 2
Current IP Address      = 192.168.155.10
Current IP Gateway      = 192.168.155.1
Current IP Netmask      = 255.255.255.128
DHCP Enabled            = 1
MAC Address             = 00:55:AB:39:10:0F
Current DNS Server 1    = 0.0.0.0
Current DNS Server 2    = 0.0.0.0
DNS Servers from DHCP   = 0
```

```
Register DNS CMC Name    = 0
DNS CMC Name             = cmc-servicetag
Current DNS Domain       =


Chassis Information:
System Model             = PowerEdge VRTX
System AssetTag          = 00000
Service Tag              =
Chassis Name             = Dell Rack System
Chassis Location         = [UNDEFINED]
Power Status             = ON

================================================================================
 Session Information
================================================================================

Type    User     IP Address      Login Date/Time
SSH     root     192.168.155.10     11/28/2007 23:40:53
KVM     root     169.254.31.30   11/28/2007 18:44:51
```

```
================================================================================
 Sensor Information
================================================================================

<senType> <Num> <sensorName> <status> <reading> <units> <lc>
<uc>
FanSpeed    1    Fan-1          OK      14495    rpm     7250 14500
FanSpeed    2    Fan-2          OK      14505    rpm     7250 14500
FanSpeed    3    Fan-3          OK       4839    rpm     2344 14500
FanSpeed    4    Fan-4          OK      14527    rpm     7250 14500
FanSpeed    5    Fan-5          OK      14505    rpm     7250 14500
FanSpeed    6    Fan-6          OK       4835    rpm     2344 14500
FanSpeed    7    Fan-7          OK      14521    rpm     7250 14500
FanSpeed    8    Fan-8       Not OK         1    rpm     7250 14500
FanSpeed    9    Fan-9          OK       4826    rpm     2344 14500

<senType> <Num> <sensorName> <status> <reading> <units> <lc>
<uc>
Temp        1   Ambient_Temp    OK       21     celcius  N/A  40

<senType> <Num>  <sensorName>  <status>   <AC-OK status>
PWR         1       PS-1        Online          OK
PWR         2       PS-2        Online          OK
PWR         3       PS-3        Online          OK
PWR         4       PS-4       Slot Empty       N/A
PWR         5       PS-5        Failed          OK
PWR         6       PS-6        Slot Empty      N/A
```

racreset

Table 81. Details of racreset

Description	Performs a CMC or a RAC reset operation. **NOTE: To use this subcommand, you must have the Chassis Administrator privilege.** **NOTE: When you run a racreset subcommand, iDRAC may require up to two minutes to return to a usable state.** **NOTE: You must restart your system after performing a hard reset of iDRAC.**
Synopsis	`racadm racreset [-m <module>]`
Input	**(module)** — `sled-n`, where n=1–4.

Table 81. Details of racreset (continued)

	NOTE: You can specify multiple modules: -m <module 1> –m <module 2>.

Example	• Reset CMC:
	`racadm racreset`
	• Reset server 1.
	`racadm racreset -m server-1`
	• Reset servers 1 and 3.
	`racadm racreset -m server-1 -m server-3`

racresetcfg

Table 82. Details of racresetcfg

Description	Resets CMC configuration to factory default settings. **NOTE: To use this, you must have the Chassis Administrator privilege.**
Synopsis	`racadm racresetcfg [-m <module>] [-c <feature>]`
Input	• -m : <module> — Must be one of the following values: ○ chassis — default state, if -m is not specified. ○ server-n, where n=1–4 ○ switch-n, where n=1 • -c : <feature> — Must be one of the following values: ○ ad — Reset Active Directory properties to the default value. The default setting is “disabled”. ○ pcap — Reset Power Cap properties to the default value. ○ flex — Reset FlexAddress properties to the default value. The default setting is “enabled”. ○ dpse — Reset Dynamic Power Supply Engagement to the default value. The default setting is “disabled”. **NOTE: The –c option is valid with only <module=chassis>.**

Example	• Perform reset of configuration data to defaults for server-1 module
	`racadm racresetcfg -m server-1`
	• Perform reset of power cap feature.
	`racadm racresetcfg -c pcap`
	• Perform reset of configuration data to default for switch-1 module
	`racadm racresetcfg -m switch-1`

racresetpcie

Table 83. Details of racresetpcie

Description	Resets the PCIe blade mapping in the chassis to factory defaults. **NOTE:**

Table 83. Details of racresetpcie (continued)

	• **To use this subcommand for CMC, you must have the Chassis Administrator privilege.** • **This command cannot run successfully, if any blade server is powered on.**
Synopsis	`racadm racresetpcie`

raid

Table 84. Details of raid

Description	Allows you to execute commands to control RAID arrays.
Synopsis	`racadm raid`

Example

- Monitor Health of Storage root node.

```
racadm raid get status
```

```
Storage Root Node Status : Ok
```

This command retrieves the controllers keys (FQDDs).

- Monitor and Inventory all Controllers connected to the server.

```
racadm raid get controllers
```

```
racadm raid get controllers -o
```

This command is an optimized version and displays the full controller objects along with their keys.

```
racadm raid get controllers -o -p <property names separated by comma>
```

This command displays the filtered property values for all returned controller objects.

- Monitor and Inventory all batteries connected to the controller

```
racadm raid get batteries --refkey <controller FQDDs
separated by comma>
```

This command displays all battery keys connected to the controllers referred to as refkeys.

```
racadm raid get batteries --refkey <controller FQDDs
separated by comma > -o
```

This command is an optimized version and displays all battery objects for the controller FQDD.

```
racadm raid get batteries --refkey <controller FQDDs
separated by comma > -o -p <property names separated by comma>
```

This command is an optimized and filtered version.

```
racadm raid get batteries --refkey <controller FQDDs
separated by comma > -o -p <property names separated by comma>
```

- Monitor and Inventory all virtual disks connected to the controller

```
racadm raid get vdisks --refkey <controller FQDDs
separated by comma>
```

This command displays all vdisk keys connected to the controllers being mentioned as refkeys.

```
racadm raid get vdisks --refkey <controller FQDDs
separated by comma > -o
```

This command is an optimized version and displays all vdisk objects for the controller FQDD.

```
racadm raid get vdisks
```

```
racadm raid get vdisks --refkey RAID.ChassisSlot.5-1 -o -p status
```

```
racadm Disk.Virtual.5:RAID.ChassisSlot.5-1
Status                          = Ok
```

```
racadm Disk.Virtual.0:RAID.ChassisSlot.5-1
Status                          = Ok
```

```
racadm Disk.Virtual.1:RAID.ChassisSlot.5-1
Status                          = Ok
```

```
racadm Disk.Virtual.2:RAID.ChassisSlot.5-1
Status                          = Ok
```

- Monitor and Inventory all storage enclosures connected to the controller

```
racadm raid get enclosures --refkey <controller FQDDs
separated by comma>
```

This command displays all enclosure keys connected to the controller being mentioned as refkeys.

```
racadm raid get enclosures --refkey <controller FQDDs
separated by comma > -o optimized version.
```

This command displays all enclosure objects for the controller's FQDD.

```
racadm raid get enclosures --refkey <controller FQDDs
separated by comma > -o -p <property names separated by comma>
```

This command is an optimized and filtered version.

- Monitor and Inventory all Physical Disks connected to the enclosure /Controllers

```
racadm raid get pdisks --refkey <enclosure/Controllers
FQDDs separated by comma>
```

This command displays all physical disk keys connected to the enclosures being mentioned as refkeys.

```
racadm raid get pdisks --refkey <enclosure/Controllers
FQDDs separated by comma > -o
```

This command displays the wear gauge property of the Solid State Drives (SSDs).

```
racadm raid get pdisks -o -p RemainingRatedWriteEndurance
```

This command is an optimized version and displays all disk objects for the enclosure FQDD.

```
racadm raid get pdisks --refkey <enclosure/Controllers
FQDDs separated by comma > -o -p <property names separated by comma>
optimized and filtered version.
```

- Monitor and Inventory all Fans connected to the enclosure

```
racadm raid get fans --refkey <enclosure/Controllers FQDDs separated
by comma>
```

This command displays all fan keys connected to the enclosures referred as refkeys.

```
racadm raid get fans --refkey <enclosure/Controllers FQDDs separated
by comma > -o optimized version.
```

This command displays all fan objects for the enclosure FQDD.

```
racadm raid get fans --refkey <enclosure/Controllers FQDDs separated
by comma > -o -p <property names separated by comma> optimized and
filtered version.
```

- Monitor and Inventory all EMMs connected to the enclosure

```
racadm raid get emms --refkey <enclosure/Controllers FQDDs separated
by comma>
```

This command returns all EMM keys connected to the enclosures being mentioned as refkeys.

```
racadm raid get emms --refkey <enclosure/Controllers FQDDs separated
by comma > -o
```

This command is an optimized version and displays all EMM objects for the enclosure FQDD.

```
racadm raid get emms --refkey <enclosure/Controllers FQDDs separated
by comma > -o -p <property names separated by comma>
```

This command is an optimized and filtered version.

- Monitor and Inventory all Temperature Probes connected to the enclosure

```
racadm raid get tempprobes --refkey <enclosure/Controllers FQDDs
separated by comma>
```

This command displays all temperature probe keys connected to the enclosures being mentioned as refkeys.

```
racadm raid get tempprobes --refkey <enclosure/Controllers FQDDs
separated by comma > -o
```

This command is an optimized version and displays all temperature probe objects for the enclosure FQDD.

```
racadm raid get tempprobes --refkey <enclosure FQDDs
separated by comma > -o -p <property names separated by comma>
optimized and filtered version
```

- Monitor and Inventory all Power Supply Units connected to the enclosure

```
racadm raid get psus --refkey <enclosure/Controllers FQDDs separated
by comma>
```

This command displays all power supply units connected to the enclosures being mentioned as refkeys.

```
racadm raid get psus --refkey <enclosure/Controllers FQDDs separated
by comma > -o
```

This command is an optimized version and displays all power supply units objects for the enclosure FQDD.

```
racadm raid get psus --refkey <enclosure/Controllers FQDD's separated
by comma > -o -p <property names separated by comma>
```

This command is an optimized and filtered version.

blink

Table 85. Details of blink

Description	Starts blinking or identifies operation on the specified device.

Table 85. Details of blink (continued)

	NOTE: The physical disks associated with the adapter blink or unblink.

Synopsis	`racadm raid blink:<PD FQDD>`
	`racadm raid blink:<VD FQDD>`
	`racadm raid blink {-pdkey:<comma separated PD FQDDs|-vdkey:<comma separated VD FQDDs}`
	`racadm raid blink:Enclosure.External.0-0:RAID.ChassisSlot.5-1`

Input	• –pdkey: A comma-separated list of physical disk drive FQDDs to use in the operation. • –vdkey: A comma-separated list of virtual drive FQDDs to use in the operation.

Example	`racadm raid blink:Disk.Bay.0:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1`
	`racadm raid blink:Disk.Virtual.0:RAID.ChassisIntegrated.1-1`
	`racadm raid blink -pdkey:Disk.Bay.0:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1,Disk.Bay.0:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1`
	`racadm raid blink -vdkey:Disk.Virtual.0:RAID.ChassisIntegrated.1-1,Disk.Virtual.0:RAID.ChassisIntegrated.1-1`
	`racadm raid blink:Enclosure.External.0-0:RAID.ChassisSlot.5-1`

createvd

Table 86. Details of createvd

Description	Creates a virtual disk based on the specification that you enter with this command. **NOTE: You can create multiple virtual disks using the script at an instance. But, ensure that there is an interval of about 30 seconds to facilitate completion of the first slice virtual disk creation before running the second slice virtual disk command.**

Synopsis	`racadm raid createvd:<Controller FQDD> -rl {r0|r1|r5|r6|r10|r50|r60} [-wp {wt|wb|fwb}] [-rp {nra|ra|ara}]`
	`[-ss {1k|2k|4k|8k|16k|32k|64k|128k|256k|512k|1M|2M|4M|8M|16M}] -pdkey:<comma separated PD FQDD>`
	`[-dcp {enabled|disabled|default}] [-name <VD name>] [-size <VD size>{b|k|m|g|t}] [-cc]`
	`[-sc {span count}] {-current|-pending} [-vdinit {yes|no}] [-secure {yes|no}]`

Input	• -rl: Set the RAID Level. • r0: RAID 0 – Striping. • r1: RAID 1 – Mirroring. • r5: RAID 5 – Striping with Parity. • r6: RAID 6 – Striping with Extra Parity. • r10: RAID 10 – Spanned Striping with Mirroring. • r50: RAID 50 – Spanned Striping with Parity. • r60: RAID 60 – Spanned Striping with Extra Parity. • -wp {wt | wb | fwb}: Set the write policy to Write Through, Write Back, or Forced Write Back. • -rp {nra|ra|ara}: Set the read policy to No Read Ahead, Read Ahead, or Adaptive Read Ahead. • -ss: Specify the stripe size to use. • -sc: Number of spans in the virtual disk. This value must be entered while creating spanned RAID levels such as 10, 50, and 60. • -pdkey: <PD FQDD list>: The PDs to use in the VD. • -dcp: Set the Disk Cache Policy in the VD. • enabled: Enabled – Allow the disk to use its cache.

Table 86. Details of createvd (continued)

	• disabled: Disabled – Disallow the disk from using its cache.
	• default: Default – Use the default cache policy. SAS Drives - Use Disabled by Default. SATA Drives - Use Enabled by Default.
	• –name: <VD name>: The name to give the VD.
	• –size: <VD size>: The size of the VD.
	  ○ b: Specify the size in bytes.
	  ○ k: Specify the size in kilobytes
	  ○ m: Specify the size in megabytes.
	  ○ g: Specify the size in gigabytes.
	  ○ t: Specify the size in terabytes.
	• -cc: Create a CacheCade or Enhanced Cache VD.
	• -vdinit: Create a virtual disk with or without initialization. The available values are:
	  ○ yes
	  ○ no
	  If `-vdinit` is not specified, the default value is "yes".
	• -secure: Create a virtual disk using Self-Encrypting Drives (SEDs). The available values are:
	  ○ yes
	  ○ no
	  If `-secure` is not specified, the default value is "no".

Example	`racadm raid createvd:RAID.ChassisIntegrated.1-1 -rl r0 -pdkey:Disk.Bay.0:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1` **NOTE: Make sure to provide the current active controller FQDD in the `createvd` command.**

deletevd

Table 87. Details of deletevd

Description	Deletes the specified virtual drive.
Synopsis	`racadm raid deletevd:<VD FQDD> {-current|-pending}`
Input	• –current <optional>: Performs the configuration right now. **NOTE: If this requires the system to reboot, it will reboot.** • –pending: Save the configuration change for a later application. You can use a combination of the –pending and –current flags on multiple commands to reduce the possible number of system reboots.
Example	`racadm raid deletevd:Disk.Virtual.0:RAID.ChassisIntegrated.1-1`

discardcache

Table 88. Details of discardcache

Description	Discards any pinned or persistent cache present on the RAID controller.
Synopsis	`racadm raid discardcache:<Controller FQDD> {-current | -pending}`

Table 88. Details of discardcache (continued)

Input	• –current <optional>: Performs the configuration right now. **NOTE: If this requires the system to reboot, the system is rebooted.** • –pending: Save the configuration change for a later application. You can use a combination of the –pending and –current flags on multiple commands to reduce the possible number of system reboots.
Example	`racadm raid discardcache:RAID.ChassisIntegrated.1-1`

exportlog

Table 89. Details of exportlog

Description	Export a log from the device.
Synopsis	`racadm raid exportlog:<FQDD> -l<CIFS or NFS share> -u<username> -p <password> [-f <filename>]`
Input	• –l<CIFS or NFS share>: The network share to write the log to. • –u<username: The network username for the share. • –p <password>: The network password for the share • –f <filename>: The file name to write the log to.
Example	`racadm raid exportlog:RAID.ChassisIntegrated.1-1 -l <CIFS or NFS share> -u<username> -p <password> [-f <filename>]`

forceonline

Table 90. Details of forceonline

Description	Forces the RAID Controller to make the specified drive online. This operation may result in obsolete or corrupted data, and should only be attempted in cases where a rebuild operation has failed or is not applicable.
Synopsis	`racadm raid forceonline:<PD FQDD> {current|pending}`
Input	• –current <optional>: Performs the configuration right now. • **NOTE: If this requires the system to reboot, then the system is rebooted.** • –pending: Save the configuration change for a later application. You can use a combination of the –pending and –current flags on multiple commands to reduce the possible number of system reboots.
Example	`racadm raid forceonline:Disk.Bay.0:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1`

get controllers

Table 91. Details of get controllers

Description	The command lists all RAID controllers detected in the system and their properties.

Table 91. Details of get controllers (continued)

	NOTE: To use this subcommand, you must have the CMC Login User privilege.
Synopsis	`raid get controllers -o`
Input	· **-o** — The **-o** is used to display the fault-tolerant status of a RAID controller.

Example	Sample output of a CMC in which either fault-tolerant mode is not available or is not enabled.
	`RAID.ChassisIntegrated.1-1`
	`Status = Ok`
	`RollupStatus = Ok`
	`Name = Shared PERC8 (Embedded)`
	`FirmwareVersion = 23.8.3-0027`
	`DriverVersion = 06.802.11.00`
	`RebuildRate = 30 %`
	`BgiRate = 35 %`
	`CheckConsistencyRate = 40 %`
	`ReconstructRate = 30 %`
	`PatrolReadRate = 30 %`
	`PatrolReadMode = Manual`
	`PatrolReadState = Stopped`
	`CheckConsistencyMode = Stop On Error`
	`LoadBalanceSetting = Disabled`
	`CopybackMode = OFF`
	`PreservedCache = Not Present`
	`CacheMemorySize = 1024 MB`
	`PersistHotspare = Disabled`
	`SpindownUnconfiguredDrives = Disabled`
	`SpindownHotspare = Disabled`
	`Timeintervalforspindown = 30 (Minutes)`
	`SecurityStatus = Unknown`
	`EncryptionMode = None`
	`SasAddress = 0x590B11C02620E600`
	`PciDeviceId = 0x2f`
	`PciSubdeviceId = 0x1f3e`
	`PciVendorId = 0x1000`
	`PciSubvendorId = 0x1028`
	`PciBus = 0x0`
	`PciDevice = 0x0`
	`PciFunction = 0x0`
	`BusWidth = Unknown`
	`SlotLength = Short`
	`SlotType = Unknown`
	`CapableSpeeds = 6.0 Gb/s, 3.0 Gb/s`
	`LearnMode = Not supported`
	`HighAvailabilityMode = None`
	`PeerController = N/A`
	Sample output of a CMC in which you have firmware support for the fault-tolerant mode and the hardware, and fault-tolerant mode is active.
	`RAID.ChassisIntegrated.1-1`
	`Status = Ok`
	`RollupStatus = Ok`
	`Name = Shared PERC8 (Embedded)`
	`FirmwareVersion = 23.8.3-0027`
	`DriverVersion = 06.802.11.00`
	`RebuildRate = 30 %`
	`BgiRate = 35 %`
	`CheckConsistencyRate = 40 %`
	`ReconstructRate = 30 %`
	`PatrolReadRate = 30 %`
	`PatrolReadMode = Manual`
	`PatrolReadState = Stopped`
	`CheckConsistencyMode = Stop On Error`

Table 91. Details of get controllers (continued)

```
LoadBalanceSetting           = Disabled
CopybackMode                 = OFF
PreservedCache               = Not Present
CacheMemorySize              = 1024 MB
PersistHotspare              = Disabled
SpindownUnconfiguredDrives   = Disabled
SpindownHotspare             = Disabled
Timeintervalforspindown      = 30 (Minutes)
SecurityStatus               = Unknown
EncryptionMode               = None
SasAddress                   = 0x590B11C02620E600
PciDeviceId                  = 0x2f
PciSubdeviceId               = 0x1f3e
PciVendorId                  = 0x1000
PciSubvendorId               = 0x1028
PciBus                       = 0x0
PciDevice                    = 0x0
PciFunction                  = 0x0
BusWidth                     = Unknown
SlotLength                   = Short
SlotType                     = Unknown
CapableSpeeds                = 6.0 Gb/s, 3.0 Gb/s
LearnMode                    = Not supported
HighAvailabilityMode          = Fault Tolerant(Active/Passive)
PeerController                =
RAID.ChassisIntegrated.2-1


RAID.ChassisIntegrated.2-1
Status                       = Ok
RollupStatus                 = Ok
Name                         = Shared PERC8 (Embedded)
FirmwareVersion              = 23.8.3-0027
DriverVersion                = 06.802.11.00
RebuildRate                  = 30 %
BgiRate                      = 35 %
CheckConsistencyRate         = 40 %
ReconstructRate              = 30 %
PatrolReadRate               = 30 %
PatrolReadMode               = Manual
PatrolReadState              = Stopped
CheckConsistencyMode         = Stop On Error
LoadBalanceSetting           = Disabled
CopybackMode                 = OFF
PreservedCache               = Not Present
CacheMemorySize              = 1024 MB
PersistHotspare              = Disabled
SpindownUnconfiguredDrives   = Disabled
SpindownHotspare             = Disabled
Timeintervalforspindown      = 30 (Minutes)
SecurityStatus               = Unknown
EncryptionMode               = None
SasAddress                   = 0x590B11C02620E600
PciDeviceId                  = 0x2f
PciSubdeviceId               = 0x1f3e
PciVendorId                  = 0x1000
PciSubvendorId               = 0x1028
PciBus                       = 0x0
PciDevice                    = 0x0
PciFunction                  = 0x0
BusWidth                     = Unknown
SlotLength                   = Short
SlotType                     = Unknown
CapableSpeeds                = 6.0 Gb/s, 3.0 Gb/s
LearnMode                    = Not supported
HighAvailabilityMode         = Fault Tolerant(Active/Passive)
PeerController                =
RAID.ChassisIntegrated.1-1
```

get enclosure

Table 92. Details of get enclosure

Description	Displays the status and attributes of the enclosure. **NOTE: To use this subcommand, you must have the CMC Login User privilege.**
Synopsis	`racadm raid get enclosures -o -p Status` `racadm raid get enclosures -o`
Input	· **-o** — The **-o** is used to display the fault-tolerant status of a enclosure. · **-p** — The network password of the share.

Example	`racadm raid get enclosures -o -p Status`
	
	`Enclosure.Internal.0-0:RAID.ChassisIntegrated.2-1`
	`Status = Ok`
	`Enclosure.External.0-1:RAID.ChassisSlot.5-1`
	`Status = Ok`
	`Enclosure.External.0-0:RAID.ChassisSlot.5-1`
	`Status = Failed`
	
	`racadm raid get enclosures -o`
	
	`Enclosure.Internal.0-0:RAID.ChassisIntegrated.2-1`
	` Status = Ok`
	`  RollupStatus = Ok`
	`  Name = VRTX2.5x25 0:0`
	`  BayId = 0`
	`  FirmwareVersion = 2.00`
	`  AssetTag = elan3`
	`  AssetName = VRTX200  ternal backplane`
	`  SasAddress = Not applicable`
	`  SlotCount = 25`
	`Enclosure.External.0-1:RAID.ChassisSlot.5-1`
	`  Status = Ok`
	`  RollupStatus = Ok`
	`  Name = MD1220 0:1`
	`  EnclosurePosition = 1`
	`  ConnectedPort = 0`
	`  FirmwareVersion = 1.05`
	`  ServiceTag = 6Q2XMQ1`
	`  AssetTag = slot 5 1`
	`  AssetName = MD1220`
	`  RedundantPath = Present`
	`  SasAddress = Not applicable`
	`  SlotCount = 24`
	`Enclosure.External.0-0:RAID.ChassisSlot.5-1`
	`  Status = Failed`
	`  RollupStatus = Failed`
	`  Name = MD1220 0:0`
	`  EnclosurePosition = 0`
	`  ConnectedPort = 0`
	`  FirmwareVersion = 1.05`
	`  ServiceTag = BWQPWP1`
	`  AssetTag = slot 5 0`
	`  AssetName = MD1220`
	`  RedundantPath = Present`
	`  SasAddress = Not applicable`
	`  SlotCount = 24`

get emms

Table 93. Details of get emms

Description	Displays the status and attributes of the Enclosure Management Module (EMM). **NOTE: To use this subcommand, you must have the CMC Login User privilege.**
Synopsis	`racadm raid get emms -o -p Status` `racadm raid get emms -o`
Input	· **-o** — The **-o** is used to display the fault-tolerant status of a enclosure. · **-p** — The network password of the share.

Example	`racadm raid get emms -o -p Status`
	
	`Expander.Slot.0:Enclosure.Internal.0-0:RAID.ChassisIntegrated.2-1`
	`  Status = Ok`
	`Expander.Slot.1:Enclosure.Internal.0-0:RAID.ChassisIntegrated.2-1`
	`  Status = Ok`
	`EMM.Slot.0:Enclosure.External.0-1:RAID.ChassisSlot.5-1`
	`  Status = Ok`
	`EMM.Slot.1:Enclosure.External.0-1:RAID.ChassisSlot.5-1`
	`  Status = Ok`
	`EMM.Slot.0:Enclosure.External.0-0:RAID.ChassisSlot.5-1`
	`  Status = Failed`
	`EMM.Slot.1:Enclosure.External.0-0:RAID.ChassisSlot.5-1`
	`  Status = Unknown`
	
	`racadm raid get emms -o`
	
	`Expander.Slot.0:Enclosure.Internal.0-0:RAID.ChassisIntegrated.2-1`
	`  Status = Ok`
	`  State = Ready`
	`  Name = Expander 0`
	`  PartNumber = 0TJ2VKA00`
	`  FirmwareVersion = 2.00`
	`Expander.Slot.1:Enclosure.Internal.0-0:RAID.ChassisIntegrated.2-1`
	`  Status = Ok`
	`  State = Ready`
	`  Name = Expander 1`
	`  PartNumber = 0TJ2VKA00`
	`  FirmwareVersion = 2.00`
	`EMM.Slot.0:Enclosure.External.0-1:RAID.ChassisSlot.5-1`
	`  Status = Ok`
	`  State = Ready`
	`  Name = EMM 0`
	`  PartNumber = 0W307KA00`
	`  FirmwareVersion = 1.05`
	`EMM.Slot.1:Enclosure.External.0-1:RAID.ChassisSlot.5-1`
	`  Status = Ok`
	`  State = Ready`
	`  Name = EMM 1`
	`  PartNumber = 0W307KA00`
	`  FirmwareVersion = 1.05`
	`EMM.Slot.0:Enclosure.External.0-0:RAID.ChassisSlot.5-1`
	`  Status = Failed`
	`  State = Failed`
	`  Name = EMM 0`
	`  PartNumber = 0W307KA00`
	`  FirmwareVersion = 1.05`
	`EMM.Slot.1:Enclosure.External.0-0:RAID.ChassisSlot.5-1`
	`  Status = Unknown`
	`  State = Unknown`
	`  Name = EMM 1`

Table 93. Details of get emms (continued)

	PartNumber = 0W307KA00 FirmwareVersion = 1.05

get fans

Table 94. Details of get fans

Description	Displays the status and attributes of the fans in the storage enclosure that are connected to chassis. **NOTE: To use this subcommand, you must have the CMC Login User privilege.**
Synopsis	`racadm raid get fans -o -p Status` `racadm raid get fans -o`
Input	· **-o** — The **-o** is used to display the fault-tolerant status of a enclosure.

Example	`racadm raid get fans -o -p Status`
	
	`Fan.Slot.0:Enclosure.External.0-1:RAID.ChassisSlot.5-1`
	`FanOperationalStatus = Ok`
	`Fan.Slot.1:Enclosure.External.0-1:RAID.ChassisSlot.5-1`
	`FanOperationalStatus = Ok`
	`Fan.Slot.2:Enclosure.External.0-1:RAID.ChassisSlot.5-1`
	`FanOperationalStatus = Ok`
	`Fan.Slot.3:Enclosure.External.0-1:RAID.ChassisSlot.5-1`
	`FanOperationalStatus = Ok`
	`Fan.Slot.0:Enclosure.External.0-0:RAID.ChassisSlot.5-1`
	`FanOperationalStatus = Ok`
	`Fan.Slot.1:Enclosure.External.0-0:RAID.ChassisSlot.5-1`
	`FanOperationalStatus = Ok`
	`Fan.Slot.2:Enclosure.External.0-0:RAID.ChassisSlot.5-1`
	`FanOperationalStatus = Ok`
	`Fan.Slot.3:Enclosure.External.0-0:RAID.ChassisSlot.5-1`
	`FanOperationalStatus = Ok`
	
	`racadm raid get fans -o`
	
	`Fan.Slot.0:Enclosure.External.0-1:RAID.ChassisSlot.5-1`
	`FanOperationalStatus = Ok`
	`State = Ready`
	`Name = Fan 0`
	`Speed = 4620 RPMS`
	`Fan.Slot.1:Enclosure.External.0-1:RAID.ChassisSlot.5-1`
	`FanOperationalStatus = Ok`
	`State = Ready`
	`Name = Fan 1`
	`Speed = 4620 RPMS`
	`Fan.Slot.2:Enclosure.External.0-1:RAID.ChassisSlot.5-1`
	`FanOperationalStatus = Ok`
	`State = Ready`
	`Name = Fan 2`
	`Speed = 4490 RPMS`
	`Fan.Slot.3:Enclosure.External.0-1:RAID.ChassisSlot.5-1`
	`FanOperationalStatus = Ok`
	`State = Ready`
	`Name = Fan 3`
	`Speed = 4560 RPMS`
	`Fan.Slot.0:Enclosure.External.0-0:RAID.ChassisSlot.5-1`
	`FanOperationalStatus = Ok`
	`State = Ready`
	`Name = Fan 0`

Table 94. Details of get fans (continued)

	`Speed = 4670 RPMS`
	`Fan.Slot.1:Enclosure.External.0-0:RAID.ChassisSlot.5-1`
	`FanOperationalStatus = Ok`
	`State = Ready`
	`Name = Fan 1`
	`Speed = 4670 RPMS`
	`Fan.Slot.2:Enclosure.External.0-0:RAID.ChassisSlot.5-1`
	`FanOperationalStatus = Ok`
	`State = Ready`
	`Name = Fan 2`
	`Speed = 4670 RPMS`
	`Fan.Slot.3:Enclosure.External.0-0:RAID.ChassisSlot.5-1`
	`FanOperationalStatus = Ok`
	`State = Ready`
	`Name = Fan 3`
	`Speed = 4700 RPMS`

get psus

Table 95. Details of get psus

Description	Displays the status and attributes of the Power Supply Unit (PSU) in the storage enclosure that are connected to chassis **NOTE: To use this subcommand, you must have the CMC Login User privilege.**
Synopsis	`racadm raid get psus -o -p Status` `racadm raid get psus -o`
Input	· **-o** — The **-o** is used to display the fault-tolerant status of a enclosure.

Example	`racadm raid get psus -o -p Status`
	
	`PSU.Slot.0:Enclosure.External.0-1:RAID.ChassisSlot.5-1`
	`Status = Ok`
	`PSU.Slot.1:Enclosure.External.0-1:RAID.ChassisSlot.5-1`
	`Status = Ok`
	`PSU.Slot.0:Enclosure.External.0-0:RAID.ChassisSlot.5-1`
	`Status = Ok`
	`PSU.Slot.1:Enclosure.External.0-0:RAID.ChassisSlot.5-1`
	`Status = Ok`
	
	`racadm raid get psus -o`
	
	`PSU.Slot.0:Enclosure.External.0-1:RAID.ChassisSlot.5-1`
	`Status = Ok`
	`State = Ready`
	`Name = PSU 0`
	`PartNumber = 0NFCG1A01`
	`PSU.Slot.1:Enclosure.External.0-1:RAID.ChassisSlot.5-1`
	`Status = Ok`
	`State = Ready`
	`Name = PSU 1`
	`PartNumber = 0NFCG1A01`
	`PSU.Slot.0:Enclosure.External.0-0:RAID.ChassisSlot.5-1`
	`Status = Ok`
	`State = Ready`
	`Name = PSU 0`
	`PartNumber = 0D1YWRA00`
	`PSU.Slot.1:Enclosure.External.0-0:RAID.ChassisSlot.5-1`

Table 95. Details of get psus (continued)

	Status = Ok State = Ready Name = PSU 1 PartNumber = 0GV5NHA00

get tempprobes

Table 96. Details of get tempprobes

Description	Displays the status and attributes of the temperature sensors in the storage enclosure that are connected to chassis **NOTE: To use this subcommand, you must have the CMC Login User privilege.**
Synopsis	`racadm raid get tempprobes -o -p Status` `racadm raid get tempprobes -o`
Input	· **-o** — The **-o** is used to display the fault-tolerant status of a enclosure.

Example	`racadm raid get tempprobes -o -p Status`
	
	`TempSensor.Embedded.2:Enclosure.External.0-1:RAID.ChassisSlot.5-1`
	`Status = Ok`
	`TempSensor.Embedded.3:Enclosure.External.0-1:RAID.ChassisSlot.5-1`
	`Status = Ok`
	`TempSensor.Embedded.0:Enclosure.External.0-0:RAID.ChassisSlot.5-1`
	`Status = Ok`
	`TempSensor.Embedded.1:Enclosure.External.0-0:RAID.ChassisSlot.5-1`
	`Status = Ok`
	`TempSensor.Embedded.2:Enclosure.External.0-0:RAID.ChassisSlot.5-1`
	`Status = Ok`
	`TempSensor.Embedded.3:Enclosure.External.0-0:RAID.ChassisSlot.5-1`
	`Status = Ok`
	
	`racadm raid get tempprobes -o`
	
	`TempSensor.Embedded.2:Enclosure.External.0-1:RAID.ChassisSlot.5-1`
	`Status = Ok`
	`State = Ready`
	`Name = Temp Sensor 2`
	`ReadingDegreeCelcius = 29 C`
	`MinimumWarningThreshold = 8 C`
	`MaximumWarningThreshold = 45 C`
	`MinimumFailureThreshold = 3 C`
	`MaximumFailureThreshold = 55 C`
	`TempSensor.Embedded.3:Enclosure.External.0-1:RAID.ChassisSlot.5-1`
	`Status = Ok`
	`State = Ready`
	`Name = Temp Sensor 3`
	`ReadingDegreeCelcius = 25 C`
	`MinimumWarningThreshold = 10 C`
	`MaximumWarningThreshold = 46 C`
	`MinimumFailureThreshold = 3 C`
	`MaximumFailureThreshold = 55 C`
	`TempSensor.Embedded.0:Enclosure.External.0-0:RAID.ChassisSlot.5-1`
	`Status = Ok`
	`State = Ready`
	`Name = Temp Sensor 0`
	`ReadingDegreeCelcius = 32 C`
	`MinimumWarningThreshold = -2 C`

Table 96. Details of get tempprobes (continued)

	MaximumWarningThreshold = 65 C MinimumFailureThreshold = -2 C MaximumFailureThreshold = 65 C TempSensor.Embedded.1:Enclosure.External.0-0:RAID.ChassisSlot.5-1 Status = Ok State = Ready Name = Temp Sensor 1 ReadingDegreeCelcius = 31 C MinimumWarningThreshold = -2 C MaximumWarningThreshold = 65 C MinimumFailureThreshold = -2 C MaximumFailureThreshold = 65 C TempSensor.Embedded.2:Enclosure.External.0-0:RAID.ChassisSlot.5-1 Status = Ok State = Ready Name = Temp Sensor 2 ReadingDegreeCelcius = 27 C MinimumWarningThreshold = 12 C MaximumWarningThreshold = 50 C MinimumFailureThreshold = 3 C MaximumFailureThreshold = 55 C TempSensor.Embedded.3:Enclosure.External.0-0:RAID.ChassisSlot.5-1 Status = Ok State = Ready Name = Temp Sensor 3 ReadingDegreeCelcius = 26 C MinimumWarningThreshold = 13 C MaximumWarningThreshold = 46 C MinimumFailureThreshold = 3 C MaximumFailureThreshold = 55 C

hotspare

Table 97. Details of hotspare

Description	Assign or unassign global and dedicated hotspares.
Synopsis	`racadm raid hotspare:<PD FQDD> -assign {yes | no} {type {ghs | dhs}} {-vdkey:<VD FQDD>} {-current | -pending}`
Input	• –current <optional>: Performs the configuration right now. **NOTE: If this requires the system to reboot it will reboot then.** • –pending: Save the configuration change for a later application. You can use a combination of the –pending and –current flags on multiple commands to reduce the possible number of system reboots. • –assign {yes | no}: Assign or Unassign the physical disk drive as a hotspare. • –type { ghs | dhs} : Assign as a global or dedicated hotspare. • –vdkey: <VD FQDD>: Required for dedicated hotspare. Assign the dedicated hotspare to the specified VD.

Example	`racadm raid hotspare:Disk.Bay.0:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1 -assign no`
	`racadm raid hotspare:Disk.Bay.0:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1 -assign yes -type ghs`
	`racadm raid hotspare:Disk.Bay.0:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1 -assign yes -type dhs -vdkey:Disk.Virtual.0:RAID.ChassisIntegrated.1-1`

cancelinit

Table 98. Details of cancelinit

Description	Stops an initialization operation on the specified virtual drive.
Synopsis	`racadm raid cancelinit:<VD FQDD> {-current | -pending}`
Input	• –current <optional>: Immediately performs the configuration operation. **NOTE: If this requires the system to restart, the system will be restarted.** • –pending: Save the configuration change for a later application. You can use a combination of the –pending and –current flags on multiple commands to reduce the possible number of system rerestartts.
Example	`racadm raid cancelinit:Disk.Virtual.0:RAID.ChassisIntegrated.1-1`

cancelrebuild

Table 99. Details of cancelrebuild

Description	Stops a rebuild on a specified physical disk drive.
Synopsis	`racadm raid cancelrebuild:<PD FQDD> {-current | -pending}`
Input	• –current <optional>: Performs the configuration right now. **NOTE: If this requires the system to restart, the system is restarted.** • –pending: Save the configuration change for a later application. You can use a combination of the –pending and –current flags on multiple commands to reduce the possible number of system rerestarts.
Example	`racadm raid cancelrebuild:Disk.Bay.0:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1`

assignva

Table 100. Details of assignva

Description	Assigns a virtual disk to one or more virtual adapters. **NOTE: You can assign virtual disk to multiple virtual adapters when you select the mode of assignment as multiple.** **NOTE: You can assign a virtual disk to multiple virtual adapters from CMC CLI even when the Assignment Mode is set to Single Assignment in the CMC web interface.**
Synopsis	`racadm raid assignva:<VA FQDD> -vdkey:<VD FQDD> -accesspolicy {na | rw} -assignpolicy {single | multiple}{-current | -pending}`
Input	• –current <optional>: Performs the configuration right now. **NOTE: If this requires the system to reboot, the system reboots then.** • –pending: Save the configuration change for a later application. You can use a combination of the –pending and –current flags on multiple commands to reduce the possible number of system restarts. • –assignpolicy {single|multiple}: Uses the specified assign policy to determine if the virtual disk can be assigned to multiple virtual adapters.

Table 100. Details of assignva (continued)

	NOTE: Enable cluster services on the servers when assigning virtual disk to multiple virtual adapters. Use of this mode without Cluster Services may lead to corrupted or lost data. • –accesspolicy {na | rw}: Set the access policy to **No Access** or **Read/Write**. • –vdkey:<VD FQDD>: The virtual drive to change the access to.
Example	`racadm raid assignva:RAID.ChassisIntegrated.1-1-1 -vdkey:Disk.Virtual.0:RAID.ChassisIntegrated.1-1 -accesspolicy { na | rw }` `racadm raid assignva:RAID.ChassisIntegrated.1-1-2 -vdkey:Disk.Virtual.0:RAID.ChassisIntegrated.1-1 -accesspolicy rw -assignpolicy multiple`

unblink

Table 101. Details of unblink

Description	Stops blinking or identifies an operation on the specified device.

Synopsis	`racadm raid unblink:<PD FQDD>`
	`racadm raid unblink:<VD FQDD>`
	`racadm raid unblink {-pdkey:<comma separated PD FQDDs|-vdkey:<comma separated VD FQDDs}`
	`racadm raid unblink:Enclosure.External.0-0:RAID.ChassisSlot.5-1`

Input	• –pdkey: A comma-seperated list of physical disk drive FQDDs to use in the operation. • –vdkey: A comma-seperated list of virtual drive FQDDs to use in the operation.

Example	`racadm raid unblink:Disk.Bay.0:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1`
	`racadm raid unblink:Disk.Virtual.0:RAID.ChassisIntegrated.1-1`
	`racadm raid unblink -pdkey:Disk.Bay.0:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1,Disk.Bay.0:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1`
	`racadm raid unblink -vdkey:Disk.Virtual.0:RAID.ChassisIntegrated.1-1,Disk.Virtual.0:RAID.ChassisIntegrated.1-1`
	`racadm raid unblink:Enclosure.External.0-0:RAID.ChassisSlot.5-1`

init

Table 102. Details of init

Description	Starts an initialization operation on the specified virtual drive.
Synopsis	`racadm raid init:<VD FQDD> -speed {fast | full} {-current | -pending}`
Input	• –current <optional>: Performs the configuration right now. **NOTE: If this requires the system to reboot it will reboot then.** • –pending: Save the configuration change for a later application. You can use a combination of the –pending and –current flags on multiple commands to reduce the possible number of system reboots. • –speed{fast | full}: Perform a fast or full (slow) initialization on the virtual drive.

Table 102. Details of init (continued)

Example	`racadm raid init:Disk.Virtual.0:RAID.ChassisIntegrated.1-1 -speed fast` `racadm raid init:Disk.Virtual.0:RAID.ChassisIntegrated.1-1 -speed full`

raid

Table 103. Details of raid

Description	Monitors, retrieves inventory, and configures the storage components connected to the chassis. **NOTE: To use this subcommand, you must have the Chassis Administrator privilege.**

Synopsis	`racadm raid get status`
	`racadm raid get <Object type>`
	`racadm raid get <Object type> -o`
	`racadm raid get <Object type> -o -p <property names separated by comma>`
	`racadm raid get <Object type>:<FQDD's of Object type separated by comma>`
	`racadm raid set <Set Operation>:<FQDD of Object type>`
	`racadm raid set <Set Operation> -pdkey:<FQDD of PD>`
	`racadm raid set <Set Operation> -vdkey:<FQDD of VD>`

Input	**NOTE:** • **Maximum property names that can be specified in –p option is 10.** • **Maximum FQDDs that can be specified is 3.** · **(Object type)** — controllers, vdisks, pdisks. · **Set Operation** ○ resetconfig ○ exportlog ○ forceonline ○ deletevd ○ blink ○ unblink ○ clearconfig ○ importconfig ○ ccheck ○ cancelcheck ○ patrolread ○ hotspare ○ init ○ assignva ○ createvd · **–o** — Displays all the properties of the selected Key or Object. · **–p** — Displays the property names with filter. · **FQDD** — Displays all the properties of the FQDD's Key.

Table 103. Details of raid (continued)

Example	· racadm raid get controllers · racadm raid get controllers -o · racadm raid get controllers -o -p name,status · racadm raid get vdisks -o -p layout,status · racadm raid get controllers:RAID.ChassisIntegrated.1-1 · racadm raid get controllers:RAID.ChassisIntegrated.1-1 -p status · racadm raid resetconfig:RAID.ChassisIntegrated.1-1 · racadm raid exportlog:RAID.ChassisIntegrated.1-1 -l <CIFS or NFS share> -u <user name> -p <password> [-f <filename>] · racadm raid forceonline:Disk.Bay.0:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1 · racadm raid deletevd:Disk.Virtual.0:RAID.ChassisIntegrated.1-1 · racadm raid blink:Disk.Virtual.0:RAID.ChassisIntegrated.1-1 · racadm raid clearconfig:RAID.ChassisIntegrated.1-1 · racadm raid importconfig:RAID.ChassisIntegrated.1-1 · racadm raid ccheck:Disk.Virtual.0:RAID.ChassisIntegrated.1-1 · racadm raid cancelcheck:Disk.Virtual.0:RAID.ChassisIntegrated.1-1 {-pdkey:<comma separated PD FQDDs> | {-vdkey:<comma separated VD FQDDs>} · racadm raid ccheckall:RAID.ChassisIntegrated.1-1 · racadm raid cancelcheckall:RAID.ChassisIntegrated.1-1 · racadm raid unblink {-pdkey:<comma separated PD FQDDs> | -vdkey:<comma separated VD FQDDs>} · racadm raid patrolread:RAID.ChassisIntegrated.1-1 [-mode {auto | manual | disabled}] [-state {start | stop}] racadm raid hotspare:Disk.Bay.0:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1 -assign {yes | no} -type { ghs | dhs} -vdkey:<FQDD of VD> · racadm raid init:Disk.Virtual.0:RAID.ChassisIntegrated.1-1 -speed { fast | full } racadm raid cancelinit:Disk.Virtual.0:RAID.ChassisIntegrated.1-1 racadm raid assignva:<VA FQDD> -vdkey:<FQDD of VD> -accesspolicy { na | rw } · racadm raid cancelinit:Disk.Virtual.0:RAID.ChassisIntegrated.1-1 · racadm raid assignva:<VA FQDD> -vdkey:<FQDD of VD> -accesspolicy { na | rw } -assignpolicy {single|multiple} · racadm raid createvd:RAID.ChassisIntegrated.1-1 -rl {r0|r1|r5|r6|r10|r50|r60} [-wp {wt|wb|fwb}] [-rp {nra|ra|ara}] [-ss {1k|2k|4k|8k|16k|32k|64k|128k|256k|512k|1M|2M|4M|8M|16M}] -pdkey:<comma separated PD FQDD> [-dcp {enabled|disabled|default}] [-name <VD name>] [-size <VD size>{b|k|m|g|t}] [-cc] [-sc {span count}] {-current|-pending} [-vdinit {yes|no}] [-secure {yes|no}] · [-dcp {enabled|disabled|default}] [-name <VD name>] [-size <VD size> {b|k|m|g|t}] [-cc] · racadm raid discardcache:RAID.ChassisIntegrated.1-1 · racadm raid changepolicy:Disk.Virtual.0:RAID.ChassisIntegrated.1-1 -wp {wt|wb} -rp {nra|ra|ara} -dcp {enabled|disabled|default} racadm raid rename:Disk.Virtual.0:RAID.ChassisIntegrated.1-1 -name <VD name> · racadm raid rename:Disk.Virtual.0:RAID.ChassisIntegrated.1-1 -name <VD name> · racadm raid ctrlprop:RAID.ChassisIntegrated.1-1 [-rebuild <value>>] [-bgi <value>] [-reconstruct <value>] [-checkconsistency <value>] [-ccmode {abortonerror | normal}] [-copybackmode {off | on | onwithsmart}] [-lb {auto | disabled}] [-prunconfigured {yes | no}] · racadm raid rebuild:Disk.Bay.0:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1

Table 103. Details of raid (continued)

	• racadm raid cancelrebuild:Disk.Bay.0:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1 • racadm raid disableperc:RAID.ChassisIntegrated.2-1 • racadm raid enableperc:RAID.ChassisIntegrated.2-1 • racadm raid createsecuritykey:RAID.ChassisIntegrated.1-1 -key <Key id> -passwd <passphrase> • racadm raid modifysecuritykey:RAID.ChassisIntegrated.1-1 -key <Key id> -oldpasswd <oldpassphrase> -newpasswd <newpassphrase> • racadm raid deletesecuritykey:RAID.ChassisIntegrated.1-1 • racadm raid encryptvd:Disk.Virtual.0:RAID.ChassisIntegrated.1-1 • racadm raid cryptographicerase:Disk.Bay.0:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1 • racadm raid unlock:RAID.ChassisIntegrated.1-1 -key <Key id> -passwd <passphrase>

rebuild

Table 104. Details of rebuild

Description	Starts a rebuild on a specified virtual drive.
Synopsis	`racadm raid rebuild:<PQ FQDD> {-current | -pending}`
Input	• –current <optional>: Performs the configuration. **NOTE: If this requires the system to restart, the system is restarted.** • –pending: Save the configuration change for a later use. You can use a combination of the –pending and –current flags on multiple commands to reduce the possible number of system restarts.
Example	`racadm raid rebuild:Disk.Bay.0:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1`

resetconfig

Table 105. Details of resetconfig

Description	Removes the current RAID Configuration (Virtual Drives and Hotspares) from the RAID controller. This operation is not data-destructive, but is difficult to reverse.
Synopsis	`racadm raid resetconfig:<Controller FQDD> {-current|pending}`
Input	• –current <optional>: Performs the configuration right now. **NOTE: If this requires the system to reboot, then the system will reboot.** • –pending: Save the configuration change for a later application. You can use a combination of the –pending and –current flags on multiple commands to reduce the possible number of system reboots.
Example	• `racadm raid resetconfig:RAID.ChassisIntegrated.1-1`

enableperc

Table 106. Details of enableperc

Description	Indicates the RAID configuration of hardware RAID connected to the server. This subcommand enables the power to a RAID card. **NOTE:** • **Using this subcommand will power cycle the chassis and set the fault-tolerant system configuration to fault-tolerant mode.** • **If any PERC adapter settings are changed or firmware is updated, a message is displayed and the fault-tolerant status is degraded. Make sure that the firmware and the settings of the SHARED PERC match to set the fault-tolerant system configuration to fault-tolerant mode.**
Synopsis	`racadm raid enableperc:<AdapterFQDD>`
Example	`racadm raid enableperc:RAID.ChassisIntegrated.2-1`

disableperc

Table 107. Details of disableperc

Description	Indicates the RAID configuration of hardware RAID connected to the system. This subcommand disables the power to a RAID card. **NOTE:** • **Using this subcommand power cycles the chassis and sets the fault-tolerant system configuration to Single PERC mode.**
Synopsis	`racadm raid disableperc:<ControllerFQDD>`
Example	`racadm raid disableperc:RAID.ChassisIntegrated.2-1`

createsecuritykey

Table 108. Details of createsecuritykey

Description	Assigns a security key to the controller.
Synopsis	`racadm raid createsecuritykey:<ControllerFQDD> -key <Key id> -passwd <passphrase>`
Input	`-key <Key id>` — key id. The key identifier can be a minimum of one character and maximum of 32 characters. It must not have spaces. `-passwd <passphrase>` — passphrase. The passphrase can be a minimum of eight characters and a maximum of 32 characters. The passphrase must have one character from each of the following: · uppercase · lowercase · number · non-alphanumeric character except space

Table 108. Details of createsecuritykey (continued)

Example	`racadm raid createsecuritykey:RAID.ChassisIntegrated.1-1 -key Key@123_ -passwd Pass@123_`

modifysecuritykey

Table 109. Details of modifysecuritykey

Description	Modifies the security key and password of the controller.
Synopsis	`racadm raid modifysecuritykey:<ControllerFQDD> -key <Key id> -oldpasswd <oldpassphrase> -newpasswd <newpassphrase>`
Input	• `-key <Key id>` — New key identifier for the controller • `-oldpasswd <passphrase>` — old passphrase • `-newpasswd <passphrase>` — new passphrase
Example	`racadm raid modifysecuritykey:RAID.ChassisIntegrated.1-1 -key New@123_ -oldpasswd Pass@123_ -newpasswd NEWpass@123_`

deletesecuritykey

Table 110. Details of deletesecuritykey

Description	Deletes the security key of the controller.
Synopsis	`racadm raid deletesecuritykey:<ControllerFQDD>`
Example	`racadm raid deletesecuritykey:RAID.ChassisIntegrated.1-1`

encryptvd

Table 111. Details of encryptvd

Description	Encrypts the virtual disk, if the virtual disk is created with Self-Encrypting Drives (SEDs) and is not encrypted. **NOTE: Virtual disk must be created with SEDs. You cannot create a mix of non-secure and secure disks on same disk groups.**
Synopsis	`racadm raid encryptvd:<VD FQDD>`
Example	`racadm raid encryptvd:Disk.Virtual.0:RAID.ChassisIntegrated.1-1`

cryptographicerase

Table 112. Details of cryptographicerase

Description	Erases the contents of a physical disk, which is part of a secure virtual disk that has been deleted.

Table 112. Details of cryptographicerase (continued)

Synopsis	`racadm raid cryptographicerase:<SED FQDD>`
Example	`racadm raid cryptographicerase:Disk.Bay.0:Enclosure.Internal.0-0:RAID.ChassisIntegrated.1-1`

unlock

Table 113. Details of unlock

Description	Unlocks the SEDs migrated from a controller with different security key. The security status of such drives is displayed as "Locked".
Synopsis	`racadm raid unlock:RAID.ChassisIntegrated.1-1 -key <Key id>  -passwd <passphrase>`
Input	• `-key` — Key ID used to secure on old controller. • `-passwd` — Passphrase used to secure on old controller. **NOTE: You can get the key ID using the following command:** **`raid get pdisks -o -p foreignkeyidentifier`**
Example	`racadm raid unlock:RAID.ChassisIntegrated.1-1 -key KeyID@123_ -passwd Pass@123_`

remoteimage

Table 114. Details of remoteimage

Description	Connects, disconnects, or deploys a media file on a remote server. To use this subcommand, you must have the **Administrator** privilege.
Synopsis	`racadm remoteimage <options>`
Input	• **-c** - Connect the image. • **-d** - Disconnect the image. • **-u** - Username to access the network share. • **-p** - Password to access the network share. • **-l** - Image location on the network share; use double quotation marks with a location. • **-s** - Display current status; –a is assumed, if not specified.
Example	• `racadm remoteimage -c -u "user" -p "pass" -l //shrloc/foo.iso` Remote Image is now Configured • `racadm remoteimage -d - disconnect` Disable Remote File Started. Please check status using -s option to know Remote File Share is ENABLED or DISABLED. • `racadm remoteimage -s - status`

Table 114. Details of remoteimage (continued)

	Remote File Share is Enabled UserName Password ShareName //192.168.0.1/xxxx/dtk_3.3_73_Linux.iso

serveraction

Table 115. Details of serveraction

Description	Enables you to perform power management operations on the host system. To use this subcommand, you must have the **Execute Server Control Commands** permission.
Synopsis	`racadm serveraction <action>`
Input	• -m <*module*> - server-n, where *n*=1–4 • -a - Performs action on all servers. Not allowed with the powerstatus action. • -f - Force the action. Required for the reseat action. • <*action*>- Specifies the action. The options for the <*action*> string are: — graceshutdown — Performs a graceful shutdown of the server. If the operating system on the server cannot be cleanly shutdown, this operation will not be performed. — hardreset — Performs a reset (reboot) operation on the managed system. — powercycle — Issues a power-cycle operation on the managed system. This action is similar to pressing the power button on the system's front panel to turn off, and then turn on the system. — powerdown — Turns off the managed system. — powerup — Turns on the managed system. — powerstatus — Displays the current power status of the server (ON or OFF). — reseat — Performs a virtual reseat of the server. This operation simulates reseating the server by resetting the iDRAC on a server. **NOTE: The action powerstatus is not allowed with an -a option.**
Output	Displays an error message if the requested operation fails, or a success message if the operation is completed.

Example	• Turn off server 3 from the CMC
	`racadm serveraction -m server-3 powerdown`
	Server power operation successful
	• Turn off server 3 from iDRAC
	`racadm serveraction powerdown`
	Server power operation successful
	• Turn off server 3 from CMC when Power is already Off on that server
	`racadm serveraction -m server-3 powerdown`
	Server is already powered OFF.

Table 115. Details of serveraction (continued)

	• Turn off the server from iDRAC when Power is already off on that server.
	`racadm serveraction powerdown`
	Server is already powered OFF
	• Get Power Status of server 2 on CMC
	`racadm serveraction -m server-2 powerstatus`
	ON
	• Get Power Status on iDRAC
	`racadm serveraction powerstatus`
	Server Power Status: ON
	• Reseat server 2 on CMC
	`$ racadm serveraction -m server-2 reseat -f`
	Server power operation successful
	• Explanation of Support
	iDRAC needs to support graceful shutdown
	The support of address individual blades is expected on the CMC

set

Table 116. Details of set

Description	Import saved CMC or server configuration or CMC Event Filter configuration from a file. **NOTE: If CMC is not in the network, you cannot import the chassis configuration profile from a remote network share with proxy using the set command. But, you can import the chassis configuration profile from the local management station.**

Table 116. Details of set (continued)

Synopsis	`racadm -r <CMC IP> -u <CMC username> -p <CMC password> set -f <filename>`
	
	`racadm -r <CMC IP> -u <CMC username> -p <CMC password> set -f <filename> -t xml`
	
	`racadm set -f <filename> -t xml -u <username> -p <password> -l <CIFS share>`
	
	`racadm set -f <filename> -t xml -l <NFS share>`
	
	`racadm set -f <filename> -t xml -u <username> -p <password> -l <CIFS share> -m server-<n>`
	
	`racadm set -f <filename> -t xml -l <NFS share> -m server-<n>`
	
	`racadm set -f <filename> -t xml -l extended -m server-<n>`
	
	`racadm set delete serverprofiles -f <filename> -l extended -t xml`
	
	`racadm set delete serverprofiles -m server-<n> --assign`
	
	`racadm set -f <filename> -t xml -l <CIFS share> -u <username> -p <password> -m server-<n> --assign`
	
	`racadm set -f <filename> -t xml -l <NFS share> -m server-<n> --assign`
	
	`racadm set -f <filename> -t xml -l extended -m server-<n> --assign`
	
	`racadm set -f <profile_file_name> -u <network_share_username> -p <network_share_passwd> -l <CIFS Share> --import -t xml`
	
	`racadm set -f <profile_file_name> -l <NFS Share> --import -t xml`
	
	`racadm set -m server-<n> -s`

Input	• `delete`—remove stored or assigned profiles.
	• `--import`—copy profiles from network share to extended storage.
	• `--assign`—specify profile that is requested is a server profile assigned to a blade.
	• `-f`—import CMC configuration or CMC event filter from a file.
	• `-u`—username of the remote share from where the file must be imported.
	• `-p`—password for the remote share from where the file must be imported.
	• `-l`—network share location from where the file must be imported.
	• `-t`—specify the file type to be imported. The valid value is “xml”. This option is case-sensitive.
	• `-m`—`<module>`—the possible values are:
	  ○ `server-<n>`—where n = 1 to 16
	  ○ `all`—for listing profiles assigned to all blades.
	  ○ `server-<nx>`—where n = 1 to 8; x = a to d (lower-case)
	• `-s`—check the status of the last successfully initiated server profile operation.

Table 116. Details of set (continued)

Example	• Configure event filter configurations from a configuration file using remote racadm
	`racadm -r 192.168.0.120 -u <username> -p <password> set -f file.txt`
	• Configure a CMC from an XML configuration file on a local share using remote racadm
	`racadm -r 192.168.0.120 -u <username> -p <password> set -f myfile.xml -t xml`
	• Configure a CMC from an XML configuration file on a remote CIFS share
	`racadm set -f myfile.xml -t xml -u myuser -p mypass -l // 192.168.0.0/myshare`
	• Configure a CMC from an XML configuration file on a remote NFS share
	`racadm set -f myfile.xml -t xml -l 192.168.0.0:/myshare`
	• Apply server profile located on a remote NFS share to server-1
	`racadm set -f myfile.xml -t xml -l 192.168.0.0:/myshare -m server-1`
	• Apply server profile from extended storage to server-1
	`racadm set -f myfile.xml -t xml -l extended -m server-1`
	• Delete server profile `Test_Profile` from extended storage
	`racadm set delete serverprofiles -f Test_Profile.xml -l extended -t xml`
	• Assign server profile from `server_profile.xml` stored in extended storage to server-3
	`racadm set -m server-3 -l extended -f server_profile.xml -t xml --assign`
	• Assign server profile from `server_profile.xml` stored in network share (CIFS)to server-3
	`racadm set -m server-3 -l //192.168.0.0/cifsshare -u username -p password -f server_profile.xml -t xml --assign`
	• Delete server profile assigned to server-3
	`racadm set delete serverprofiles -m server-3 --assign`
	• Delete server profiles that are assigned to all blades
	`racadm set delete serverprofiles -m all --assign`
	• Copy server profile `test_profile.xml` from network share(NFS) to extended storage
	`racadm set -f test_profile.xml -l 192.168.0.0:/nfsshare --import -t xml`
	NOTE:
	Importing CMC event filter configuration properties is supported only on remote interfaces.
	The options `-u`, `-p`, `-l`, and `-t` are applicable only to chassis or server configuration file.
	The maximum number of profiles saved in the extended storage is 100 (number of profiles assigned from network share).

setassettag

Table 117. Details of setassettag

Description	Sets the N-byte ASCII asset tag for the chassis. To use this subcommand, you must have the **Administrator** privilege. **NOTE: The special characters \ (backslash), & (ampersand), ` (backward quotation mark), and " (double quotation mark) are not supported for this subcommand.**
Synopsis	`racadm setassettag -m chassis <asset tag>`
Input	**-m** *<module>* — Specifies the module whose asset tag you want to set. Legal value: chassis You can obtain the same output if you do not include this option, because there is only one legal value. *<assettag>* is a maximum of 64 non-extended ASCII characters.
Example	· `racadm setassettag -m chassis 783839-33` · `racadm setassettag 783839-33` `The asset tag was changed successfully.`

setchassisname

Table 118. Details of setchassisname

Description	Sets the name of the chassis in the LCD. To use this subcommand, you must have the **Administrator** privilege. **NOTE: The special characters \ (backslash), & (ampersand), ` (back quote), > (greater than), < (less than), and " (double quote) are not supported for this subcommand.**
Synopsis	`racadm setchassisname <name>` **NOTE: Chassisname is a maximum of 64 non-extended ASCII characters.**
Example	`racadm setchassisname dellchassis-1` `The chassis name was set successfully.`

set controllers

Table 119. Details of set controllers

Description	Sets the RAID controllers detected in the system and fault-tolerant mode is configured on external controllers (Shared PERC 8 External).

Table 119. Details of set controllers (continued)

Synopsis	To enable fault-tolerant mode:
	`Racadm raid set controllers:<FQDD of controller> -p HighAvailabilityMode ha`
	To disable fault-tolerant mode:
	`Racadm raid set controllers:<FQDD of controller> -p HighavailabilityMode none`

Input	

Example	`Racadm raid set controllers:<FQDD of controller> -p HighAvailabilityMode ha`
	`racadm raid set controllers:RAID.ChassisSlot.5-1 -p HighAvailabilityMode ha`
	`Racadm raid set controllers:<FQDD of controller> -p HighavailabilityMode none`
	`racadm raid set controllers:RAID.ChassisSlot.5-1 -p HighAvailabilityMode none`

setflexaddr

Table 120. Details of setflexaddr

Description	Enables or disables FlexAddress on a particular slot or fabric. To use this subcommand, you must have the **Chassis Configuration Administrator** privilege. If the fabric type is determined to be Infiniband, the operation is canceled and the command returns an error. If the FlexAddress feature is not activated, the command returns an error. **NOTE: The server must be turned off to change the slot state. All servers must be turned off to change the fabric state. The MAC/WWN addresses must be managed locally (not by an external console) to use this command.**

Synopsis	`racadm setflexaddr [-i <slot#> <state>]`
	`[-f <fabricName> <state>]`
	<*slot#*> = 1 to 4
	<*fabricName*> = A
	<*state*> = 0 or 1
	where **0** is disable and **1** is enable.

Input	• -i <*slot#*> <*state*> — Enables or disables FlexAddress for the specified slot. • -f <*fabricName*> <*state*> — Enables or disables FlexAddress for the specified fabric.
Example	• `racadm setflexaddr -i 1 0` `Slot 1 FlexAddress state set successfully`

Table 120. Details of setflexaddr (continued)

	• `racadm setflexaddr -f A 1` `Fabric A FlexAddress state set successfully` • `racadm setflexaddr -f idrac 1`

setled

Table 121. Details of setled

Description	Sets the state (blinking or not blinking) of the LED on the specified module. To blink or unblink the chassis, I/O modules or the CMC, you must have the **Debug Administrator** privilege on CMC. To enable the servers to blink or unblink, you must have the **Server Administrator** or **Debug Administrator** privilege on CMC.
Synopsis	`racadm setled -m <module> -l <ledState>`
Input	• -m <*module*> - Specifies the module whose LED you want to configure. <*module*> can be one of the following: — server-n, where *n*=1–4 — switch-n, where n=1 — cmc-active — chassis • -l <*ledstate*> - Specifies whether the LED should blink. <*ledstate*> can be one of the following: – 0 — no blinking – 1 — blinking
Example	• `racadm setled -m server-1 -l 1` LED state was set successfully. **NOTE: The `setled` command generates an error when used on the extension slot of a multi-slot server.** • `racadm setled -m server-9 -l 1` ERROR: Server in slot 9 is an extension of the server in slot 1.

set enclosure

Table 122. Details of set enclosure

Description	Sets the asset tag and asset name of the enclosures. **NOTE: Set enclosure is used for the storage expansion feature when available with shared external PERCs.** **NOTE: You cannot modify the asset names for internal enclosures.**

Table 122. Details of set enclosure (continued)

Synopsis	`racadm raid set enclosures: Enclosure.External.0-0:RAID.ChassisSlot.5-1 -p AssetTag <value>` `racadm raid set enclosures: Enclosure.External.0-0:RAID.ChassisSlot.5-1 -p AssetName <value>`
Input	**-p** — Specifies the property of the enclosure to be modified.

setniccfg

Table 123. Details of setniccfg

Description	Sets the iDRAC IP address. It displays an error message if the requested operation could not be performed, or a success message, if the operation is completed successfully. To use this subcommand, you must have the **Configure iDRAC** privilege. **NOTE: The terms NIC and Ethernet management port may be used interchangeably.**
Synopsis	• `racadm setniccfg -d` • `racadm setniccfg -d6` • `racadm setniccfg -s <IPv4Address> <netmask> <IPv4 gateway>` • `racadm setniccfg -s6 <IPv6 Address> <IPv6 Prefix Length> <IPv6 Gateway>` • `racadm setniccfg -o`
Input	• -d — Enables DHCP for the NIC (default is "DHCP disabled".) • -d6 — Enables AutoConfig for the NIC. It is enabled by default. • -s — Enables static IP settings. The IPv4 address, netmask, and gateway can be specified. Otherwise, the existing static settings are used. *<IPv4Address>*, *<netmask>*, and *<gateway>* must be typed as dot-separated strings. racadm setniccfg -s 192.168.0.120 255.255.255.0 192.168.0.1 • -s6 — Enables static IPv6 settings. The IPv6 address, Prefix Length, and the IPv6 gateway can be specified. • -o — Enable or disable NIC.
Example	• `racadm setniccfg -s 192.168.0.120 255.255.255.0 192.168.0.1` • `racadm setniccfg -d` • `racadm setniccfg -d6`

setpciecfg

Table 124. Details of setpciecfg

Description	You can configure PCIe slots and Virtual Adapters, and also set the ride-through properties. **NOTE: To use this subcommand, you must have Chassis Administrator privilege.** **NOTE: The slot assignment feature is licensed.**

Table 124. Details of setpciecfg (continued)

Synopsis	`racadm setpciecfg assign [-c <FQDD>] [-i <server slot>]`
	`racadm setpciecfg unassign [-c <FQDD>]`
	`racadm setpciecfg ridethru -e`
	`racadm setpciecfg ridethru -d`
	`racadm setpciecfg ridethru -t <time out value>`

Input	• **-c** — Use this option to specify a PCIe adapter or Virtual Adapter. • **-i** — Use this option to specify the server or module slot number. • **FQDD** — FQDD of the specified PCIe slot or Virtual Adapter. • **-e** — Use this option to enable the ride-through mode. • **-d** — Use this option to disable the ride-through mode. • **-t** — Use this option to set the time-out property of a ride-through mode in seconds (0, 60–1800; 0=infinite).

Example	• Assign a PCIe slot to a server:
	`racadm setpciecfg assign -c PCIE.ChassisSlot.5 -i 2`
	• Assign the Virtual Adapter to a server:
	`racadm setpciecfg assign -c RAID.ChassisIntegrated.1-1-2  -i 3`
	• Unassign a PCIe slot:
	`racadm setpciecfg unassign -c PCIE.ChassisSlot.3`
	• Unassign a Virtual Adapter:
	`racadm setpciecfg unassign -c RAID.ChassisIntegrated.1-1-3`
	• Enable ride-through mode
	`racadm setpciecfg ridethru -e`
	`IOV000: Successfully completed the operation.`
	• Disable ride-through mode
	`racadm setpciecfg ridethru -d`
	`IOV000: Successfully completed the operation.`
	• Set the ride-through time out value in seconds (0, 60–1800; 0 = infinite)
	`racadm setpciecfg ridethru -t 300`
	`IOV000: Successfully completed the operation.`

setractime

Table 125. Details of setractime

Description	Sets the date and time on the CMC. To use this subcommand, you must have the **Administrator** privilege.
Synopsis	• racadm setractime -d *<yyyymmddhhmmss.mmmmmmsoff>* • racadm setractime -l YYYYMMDDhhmmss

Table 125. Details of setractime (continued)

	• racadm setractime -z {?|timezone|timezone-prefix*}
Input	• -d — Sets the time to value in the string: — yyyy is the year — mm is the month — dd is the day — hh is the hour — mm is the minutes — ss is the seconds — mmmmmm is the number of microseconds — s is a + (plus) sign or a - (minus) sign, which indicates the sign of the offset. — off is the offset in minutes **NOTE: 'Off' is the offset in minutes from GMT and must be in 15-minute increments. The timezone is represented as an offset from GMT, and the clock does not automatically adjust to daylight savings time (for the '-d' option).** • -z <*zone*> - Sets the time zone by name or index, or lists possible time zones. For example, PST8PDT (Western United States), 294 (Seoul), 344 (Sydney). <*zone*> may be: — <?> lists the major timezone names/prefixes. — <*timezone*> is the case-sensitive name of your timezone or the index listed by '-z timezone-prefix*'. — <*timezone-prefix**> is a prefix of one or more timezones, followed by '*'. **NOTE: The timezone or daylight savings time is fully supported for '-l' and '-z' options. Omit the '-l' option to set the timezone only (eg. '-z US/Central').** • -l — Sets the local date and time in the string yyymmddhhmmss where: — yyyy is the year — mm is the month — dd is the day — hh is the hour — mm is the minute — ss is the second — Setting the time using the -l and -z options is recommended. This command format allows the CMC to fully support local time zones, including the ability to automatically adjust the CMC time to the local Daylight Savings Time.

Example	The setractime subcommand supports dates ranging from 1/1/1970 00:00:00 through 12/31/2030 23:59:59. To set the local time to October 24, 2007 at 3:02:30 PM:
	`racadm setractime -l 20071024150230`
	`The time was set successfully.`

setslotname

Table 126. Details of setslotname

Description	Sets the name of the server slot and enables the feature to display the slot name, host name or iDRAC DNS name of all the four server slots, or of a specified slot (indicated by the server slot number) in the chassis. Optionally, use this command to set whether the server slot name or host name is displayed in the CMC Web interface or with the **getslotname -i <*slot Num*>** command. If the host name is not available, the static server slot name is used. To use this subcommand, you must have the **Administrator** privilege. **NOTE:** • **The OMSA server agent must be present and running on the server to use the Display Hostname feature. If the agent is not running, the setting is ignored. For more information, see the *Dell OpenManage Server Administrator User's Guide* at support.dell.com/manuals.** • **The special characters \ (backslash), & (ampersand), ` (backward quotation mark), " (double quotation mark), ; (semicolon), ' (single quote), < (open angular bracket), and > (close angular bracket) are not supported for this subcommand.**
Synopsis	`racadm setslotname [-i<Slot_Number><Slot_Name_To_Be_Set> | -h 0|1|2]` `racadm setslotname -h <enabled>`
Input	• *<Slot_Number>* — Specify the slot number in the chassis. Valid values: 1 to 4. • *<Slot_Name_To_Be_Set>* — The new name to be assigned to the slot. • *<enabled>* — Sets whether the server's host name is used for display purposes. Valid values: 0, 1 or 2.

Example	• Set the name of slot 3 as server3:
	`racadm setslotname -i 3 server3`
	• Enable system to display host names (1= Hostname):
	`racadm setslotname -h 1`

setsysinfo

Table 127. Details of setsysinfo

Description	Sets the name or location of the chassis. To use this subcommand, you must have the **Administrator** privilege. **NOTE: The special characters \ (backslash), & (ampersand), ` (back quote), > (greater than), < (less than), and " (double quote) are not supported for this subcommand.**
Synopsis	`racadm setsysinfo [-c chassisname| chassislocation] <string>`

Table 127. Details of setsysinfo (continued)

Input	• *<string>* — Indicates a maximum of 64 non-extended ASCII chassis name or location. • **-c** — Sets the chassis name or location.

Example	`racadm setsysinfo -c chassisname "Dell Rack System"`
	
	`The chassis name was set successfully.`

SSH or Telnet RACADM

```
racadm getconfig -g <groupname> [-o <objectname>]
[-i <indexnumber>]
```

```
racadm <subcommand>
```

Example

```
racadm getconfig -g idracinfo
```

```
racadm getsysinfo
```

sshpkauth

Table 128. Details of sshpkauth

Description	Enables you to upload and manage up to six (6) different SSH public keys. You can upload a key file or key text, view keys, or delete keys.
	
	`racadm sshpkauth -i svcacct -k <key index> -p <privilege> -t <PK key text>`
	
	`racadm sshpkauth -i svcacct -k <key index> -p <privilege> -f <PK key file>`
	
	`racadm sshpkauth -v -i svcacct -k <key index>`
	
	`racadm sshpkauth -d -i svcacct -k <key index>`
	
	NOTE:
	
	For DSA keys greater than 2048, use the following racadm command. CMC accepts RSA keys up to key strength 4096, but the recommended key strength is 1024.
	
	`racadm -r 192.168.8.14 -u root -p calvin sshpkauth -i svcacct -k 1 -p 0xfff -f dsa_2048.pub`

Synopsis	`racadm sshpkauth`
Input	• **-i** Index for the user. *<svcacct>* is the Index for CMC. • **-k** index from 1-6 (or all for -v / -d options) to assign the PK key being uploaded. • **-p** privilege level to give to user for this PK key.

Table 128. Details of sshpkauth (continued)

	• **-t** Key text for the PK key. • **-r** Specifies the controller's remote IP address. • **-u** Specifies the user name. • **-f** file containing key text to upload. **NOTE: This option is supported only on the remote interface(s).** • **-v** - View privilege and key text. • **-d** - Delete key and privilege for the index provided.

Examples :

- View all keys

```
racadm sshpkauth -i svcacct -k all -v
```

- Delete all keys

```
racadm sshpkauth -i svcacct -k all -d
```

- Upload key at index 2 using text option

```
racadm sshpkauth -i svcacct -k 2 -p 0xfff -t "key text"
```

- Upload key at index 1 using file upload option.

```
racadm sshpkauth -i svcacct -k 1 -p 0xfff -f idrsa.pub
```

sslcertdownload

Table 129. Details of sslcertdownload

Description	Downloads a custom SSL server or CA certificate for Directory Service from CMC. This subcommand is supported only on remote interfaces.
Synopsis	`racadm sslcertdownload -f <filename> -t <type>`

Input	• -f— Specifies the target filename on local filesystem to download to
	• -t—<type>—Specifies the type of the certificate. The available options are:
	  ○ 1— Server
	  ○ 2—Active Directory or LDAP

Example	• Download server certificate
	`racadm -r 1.2.3.4 -u root -p calvin sslcertdownload -t 1 -f cert.txt`
	• Download Active Directory certificate
	`racadm -r 1.2.3.4 -u root -p calvin sslcertdownload -t 2 -f ad_cert.txt`

sslcertupload

Table 130. Details of sslcertupload

Description	Uploads a custom SSL server or CA certificate for Directory Service from the client to iDRAC. To use this subcommand, you must have the **CMC Configuration** permission.
Synopsis	`racadm sslcertupload -t <type> [-f <filename>]`
Input	· -t — Specifies the type of certificate to upload, either the CA certificate for Directory Service or the server certificate. — 1 = server certificate. — 2 = CA certificate for Directory Service — 5 = Kerberos keytab — 6 = Server certificate and key · -f — Specifies the file name of the certificate to be uploaded. · -k — Specifies the optional source filename for private key when uploading type 6.
Output	The sslcertupload command returns 0 when successful, and returns a nonzero number when unsuccessful.
Example	`racadm sslcertupload -t 1 -f c:\cert \cert.txt`

sslcertview

Table 131. Details of sslcertview

Description	Displays the SSL server or CA certificate that exists on iDRAC.
Synopsis	`racadm sslcertview -t <type> [-A]`
Input	· -t — Specifies the type of certificate to view, either the CA certificate or server certificate. —1 = server certificate —2 = CA certificate for Directory Service. · **-A** — Prevents printing of headers or labels.

Table 132. Output

`Serial Number`	`00`
Subject Information:	
`Country Code (CC)`	`US`

Table 132. Output (continued)

State (S)	Texas
Locality (L)	Round Rock
Organization (O)	Dell Inc.
Organizational Unit (OU)	Remote Access Group
Common Name (CN)	iDRAC Default certificate
Issuer Information:	
Country Code (CC)	US
State (S)	Texas
Locality (L)	Round Rock
Organization (O)	Dell Inc.
Organizational Unit (OU)	Remote Access Group
Common Name (CN)	iDRAC Default certificate
Common Name (CN)	iDRAC Default certificate
Valid From	Jul 8 16:21:56 2005 GMT
Valid To	Jul 7 16:21:56 2010 GMT

```
racadm sslcertview -t 1 -A
```

```
00
```

```
US
```

```
Texas
```

```
Round Rock
```

```
Dell Inc.
```

```
Remote Access Group
```

```
iDRAC default certificate
```

```
US
```

```
Texas
```

```
Round Rock
```

```
Dell Inc.
```

```
Remote Access Group
```

```
iDRAC default certificate
```

```
Jul 8 16:21:56 2005 GMT
```

```
Jul 7 16:21:56 2010 GMT
```

sslcsrgen

Table 133. Details of sslcsrgen

Description	Generates and downloads a CSR file to the client's local file system. The CSR can be used for creating a custom SSL certificate that can be used for SSL transactions on iDRAC.
Synopsis	`racadm sslcsrgen [-g] [-f <filename>]` `racadm sslcsrgen -s`
Input	· **-g** — Generates a new CSR. · **-s** — Returns the status of a CSR generation process (generation in progress, active, or none). · **-f** — Specifies the filename of the location, <*filename*>, where the CSR is downloaded. **NOTE: If the -f option is not specified, the filename defaults to sslcsr in your current directory.**

Table 133. Details of sslcsrgen (continued)

Output	If no options are specified, a CSR is generated and downloaded to the local file system as sslcsr by default. The -g option cannot be used with the -s option, and the -f option can only be used with the -g option. The sslcsrgen -s subcommand returns one of the following status codes: · CSR was generated successfully. · CSR does not exist.

Example	`racadm sslcsrgen -s`
	`or`
	`racadm sslcsrgen -g -f c:\csr\csrtest.txt`

NOTE: Before a CSR can be generated, the CSR fields must be configured in the RACADM cfgRacSecurity group. For example: `racadm config -g cfgRacSecurity -o cfgRacSecCsrCommonName MyCompany`

NOTE: In telnet/ssh console, you can only generate and not download the CSR file.

NOTE: The duration for generating a CSR key depends on the length specified for the key.

sslresetcfg

Table 134. Details of sslresetcfg

Description	Restores the web-server certificate to factory default and restarts web-server. The certificate takes effect 30 seconds after the command is entered. To use this subcommand, you must have the **Chassis Configuration Administrator** privilege for CMC.
Synopsis	`racadm sslresetcfg`
Example	`$ racadm sslresetcfg` `Certificate generated successfully and webserver restarted.`

sslsshresetcfg

Description Generates self-signed SSH SSL keys.

To run this command, you must have the Chassis Configuration Administrator privilege.

Synopsis

```
racadm sslsshresetcfg
```

NOTE: For IOMs, you can only configure SNMPv2 community strings.

set tempprobes

Table 135. Details of set tempprobes

Description	Sets the minimum and maximum warning threshold of temperature probe in the enclosure
Synopsis	`racadm raid set tempprobes:TempSensor.Embedded.0:Enclosure.External.1 0:RAID.ChassisSlot.6-1 -p MinimumWarningThreshold <value>` `racadm raid set tempprobes:TempSensor.Embedded.0:Enclosure.External.1 0:RAID.ChassisSlot.6-1 -p MaximumWarningThreshold <value>`
Input	**-p**— The network password of the share.
Example	

testcifsshare

Description Tests the Common Internet File System (CIFS) share with the current SMB version.

Synopsis

```
racadm testcifsshare -u <username> -p <password> -l <CIFS share>
```

Input The options are:

- `-u`—User name of the CIFS share that must be tested.
- `-p`—Password for the CIFS share that must be tested.
- `-l`—The CIFS share location that must be tested.

Example racadm testcifsshare -u shareme -p shareme -l //100.97.174.77/lccifs

testemail

Table 136. Details of testemail

Description	Sends a test e-mail to a specified destination. Prior to executing the test e-mail command, make sure that the SMTP server is configured and the specified index in the **RACADM cfgEmailAlert** group is enabled and configured properly.
Synopsis	`racadm testemail -i <index>`
Input	-i — Specifies the index of the e-mail alert to test.
Output	`Success: Test e-mail sent successfully` `Failure: Unable to send test e-mail`
Example	Commands for the **cfgEmailAlert** group: • Enable the alert — `racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1`

Table 136. Details of testemail (continued)

	• Set the destination e-mail address —
	`racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 user1@mycompany.com`
	• Set the custom message that is sent to the destination e-mail address —
	`racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 "This is a test!"`
	• Make sure that the SMTP IP address is configured properly —
	`racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr 192.168.0.152`
	• View the current e-mail alert settings —
	`racadm getconfig -g cfgEmailAlert -i <index>`
	where *<index>* is a number from 1 to 4.

testfeature

The following tables describe the **testfeature**subcommand options.

Table 137. Details of testfeature

Option	Description
-f *<feature>*	Specifies the feature name. **testfeature** supports the following features: • ad — Tests Active Directory configuration using simple authentication (user name and password). • adkrb — Tests Active Directory configuration using the Kerberos authentication. • ldap — Tests LDAP configuration and operation (requires user name and password).
-u *<username>*	The user name specified in an appropriate format for the selected authentication method. That is, Active Directory users are specified as user_name@domain_name.
-p *<password>*	The password for the indicated user account.
-d *<bitmask>*	A bitmask (specified as a hexadecimal value) to select various diagnostic messaging levels. This option is optional. **NOTE: -d option is not supported with the remote racadm interface.**

Table 138. testfeature -f ad

Description	Tests Active Directory configuration using simple authentication (user name and password). Use the optional `-d` switch to obtain additional diagnostic information, as needed. This subcommand when executed performs the following: • Checks command syntax. • Verifies whether the required system resources are available. • Validates Active Directory configuration.

Table 138. testfeature -f ad (continued)

	• Verifies the SSL certificate and if the certificate signing request (key) exists. • Acquires LDAP and Global Catalog Service records from DNS. • Acquires user privileges from the Active Directory server. • Checks the time to acquire user privileges with the allotted time to login. **NOTE: In the event of an error, the command displays the test that failed, all the tests performed earlier to the test that failed, and all the error messages.**
Synopsis	`testfeature -f ad -u <username> -p <password> [-d <diagnostic-message-level>]`

Example	• `testfeature -f ad -u user@domain -p secret`
	SUCCESSFUL: User permissions are xxxxxppp.
	The last three digits are the user's permissions.
	• `testfeature -f adkrb -u user_name@domain_name`
	`SUCCESSFUL: User permissions are 80000fff.`
	• `testfeature -f ldap -u harold -p barrel`
	`SUCCESSFUL: User permissions are 0x00000fff.`

Table 139. testfeature -f adkrb

Description	Tests the Active Directory configuration using the Kerberos authentication (single sign-on or Smart Card login). Use the optional **-d** switch to obtain additional diagnostic information, as needed. This subcommand, when run, performs the following: • Checks command syntax. • Verifies if the required system resources are available. • Validates Active Directory configuration. • Verifies if the SSL certificate and certificate signing request (key) exists. • Acquires LDAP and Global Catalog Service records from DNS. • Verifies if the CMC can acquire CMC, LDAP and Global Catalog servers FQDN through reverse IP lookups. • Verifies that the CMC principal name matches the principal name in the uploaded Keytab file. • Verifies that the CMC acquires a Kerberos TGT. • Acquires user privileges from the Active Directory server. • Checks the time to acquire user privileges with the allotted time to login. **NOTE: In the event of an error, the command outputs all tests performed up to and including the test that failed, and all the error messages.**
Synopsis	`testfeature -f adkrb -u <username> [-d <diagnostic-message-level>]`

Table 140. testfeature -f ldap

Description	Tests LDAP configuration and operation, and reports success as each stage of the authentication process proceeds. After successful completion, this command prints the CMC privileges assumed by the specified <*username*>. If a failure occurs, the command stops with an error message that displays the required corrective action. Use the optional **-d** switch to obtain additional diagnostic information, as needed.
Synopsis	`testfeature -f ldap -u <username> -p <password>` `[-d <diagnostic-message-level>]`

testtrap

Table 141. Details of testtrap

Description	Tests the RAC's SNMP trap alerting feature by sending a test trap from iDRAC to a specified destination trap listener on the network. To use this subcommand, you must have the **Test Alerts** privilege. **NOTE: Before you execute the testtrap subcommand, make sure that the specified index in the RACADM cfgAlerting group is configured properly.**
Synopsis	`racadm testtrap -i <index>`
Input	**-i** — Specifies the index of the trap configuration to be used for the test. Valid values are from 1 to 4.

Example	`Commands for the cfgIpmiPet group:`
	· Enable the alert
	`racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 1`
	· Set the destination e-mail IP address
	`racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIpAddr -i 1 192.168.0.110`
	· View the current test trap settings
	`racadm getconfig -g cfgIpmiPet -i <index>`
	where <*index*> is a number from 1 to 4.

traceroute

Table 142. Details of traceroute

Description	Traces the network path of routers that packets take as they are forwarded from your system to a destination IPv4 address. To use this subcommand, you must have the **Administrator** privilege.

Table 142. Details of traceroute (continued)

Synopsis	`racadm traceroute <IPv4 address>`
	
	`racadm traceroute 192.168.0.1`

Input	`racadm traceroute 192.168.0.1`

Output	`traceroute to 192.168.0.1 (192.168.0.1), 30 hops max,`
	
	`40 byte packets`
	
	`1 192.168.0.1 (192.168.0.1) 0.801 ms 0.246 ms 0.253 ms`

traceroute6

Table 143. Details of traceroute6

Description	Traces the network path of routers that packets take as they are forwarded from your system to a destination IPv6 address. To use this subcommand, you must have the **Administrator** privilege.

Synopsis	`racadm traceroute6 <IPv6 address>`
	
	`racadm traceroute fd01::1`

Output	`traceroute to fd01::1 (fd01::1) from fd01::3, 30 hops`
	
	`max, 16 byte packets`
	
	`1 fd01::1 (fd01::1) 14.324 ms 0.26 ms 0.244 ms`

3

CMC Property Database Group and Object Descriptions

The CMC property database contains the configuration information for CMC. Data is organized by associated object, and objects are organized by object group. The IDs for the groups and objects that the property database supports are listed in this section for CMC.

Use the group and object IDs with the RACADM subcommands to configure CMC.

NOTE: You can configure any setting that is not preceded by the hash sign (#) in the output. To modify a configurable object, use the -o option.

NOTE: To view a list of groups that you can use with the database objects, run the command. The -h, or help option, displays a list of all available configuration groups in alphabetical order. This option is useful when you do not have exact group names.

NOTE: RACADM sets the value of objects without performing any functional validation on them. For example, RACADM allows you to set the Certificate Validation object to 1 with the Active Directory object set to 0, even though Certificate Validation can happen only if Active Directory is enabled. Similarly, the cfgADSSOEnable object can be set to 0 or 1 even if the cfgADEnable object is 0, but it takes effect only if Active Directory is enabled.

All string values are limited to displayable ASCII characters, except where otherwise noted.

Topics:

idRacInfo

This group contains display parameters to provide information about the specifics of CMC being queried. One instance of the group is allowed.

Use this object with the `getconfig` subcommand.

To use this object, you must have **CMC Login User** privilege.

The following sections provide information about the objects in the **idRACInfo** group.

idRacProductInfo (Read Only)

Table 144. Details of idRacProductInfo

Description	A text string that identifies the product.
Legal Values	A string of up to 63 ASCII characters.
Default for iDRAC	Integrated Dell Remote Access Controller.
Default for CMC	Chassis Management Controller.

idRacVersionInfo (Read Only)

Table 145. Details of idRacVersionInfo

Description	String containing the current product firmware version.
Legal Values	A string of up to 63 ASCII characters.
Default	The current version number.

idRacBuildInfo (Read Only)

Table 146. Details of idRacBuildInfo

Description	String containing the current RAC firmware build version.
Legal Values	A string of up to 16 ASCII characters.
Default for CMC	The current CMC firmware build version.

idRacName (Read Only)

Table 147. Details of idRacName

Description	A user-assigned name to identify this controller.
Legal Values	A string of up to 15 ASCII characters.
Default for CMC	CMC

cfgLanNetworking

This group contains parameters to configure NIC for IPv4.

One instance of the group is allowed. Some objects in this group may require iDRAC NIC to be reset, which may cause a brief loss in connectivity. Objects that change iDRAC NIC IP address settings close all active user sessions and require users to reconnect using the updated IP address settings.

Use this object with the **config** or **getconfig** subcommands.

To use this object property, you must have the **Chassis Configuration Administrator** privilege.

NOTE: You can configure any setting that is not preceded by the hash sign (#) in the output. To modify a configurable object, use the -o option.

The following sections provide information about the objects in the **cfgLanNetworking** group.

cfgNicIPv4Enable (Read or Write)

Table 148. Details of cfgNicIPv4Enable

Description	Enables or disables the IPv4 stack.
Legal Values	• 1 (TRUE) • 0 (FALSE)
Default	0

cfgNicVLanId (Read or Write)

Table 149. Details of cfgNicVLanId

Description	Specifies the VLAN ID for the network VLAN configuration (in CMC for iDRAC Enterprise on server modules). This property is only valid if **cfgNicVLanEnable** is set to **1** (enabled).
Legal Values	1 – 4000 and 4021 – 4094
Default	1
Example	`racadm config -g cfgLanNetworking -o cfgNicVlanID 1`

cfgDNSDomainNameFromDHCP (Read or Write)

Table 150. Details of cfgDNSDomainNameFromDHCP

Description	Specifies that the DNS domain name should be assigned from the network DHCP server.
Legal Values	• 1 (TRUE) • 0 (FALSE)
Default	0

This property is used only if `cfgNicUseDhcp` is set to 1 (true), or if both **cfgIPv6Enable** and **cfgIPv6AutoConfig** are set to 1 (true).

The CMC can obtain its DNS domain name from either a DHCP or DHCPv6 server, if all of the following properties are set to 1 (true):

- `cfgNicIPv4Enable`
- `cfgNicUseDhcp`
- `cfgIPv6Enable`
- `cfgIPv6AutoConfig`
- `cfgDNSDomainNameFromDHCP`
- `cfgDNSDomainName (Read/Write)`

The network administrator must make sure that these DHCP servers are configured to provide the same DNS domain name to the CMC, otherwise the domain name becomes unpredictable.

cfgDNSDomainName (Read or Write)

Table 151. Details of cfgDNSDomainName

Description	This is the DNS domain name. This parameter is valid only if **cfgDNSDomainNameFromDHCP** is set to 0 (FALSE).
Legal Values	A string of up to 254 ASCII characters. At least one of the characters must be alphabetic. Characters are restricted to alphanumeric, '-', and '.'. **NOTE: Microsoft Active Directory supports only Fully Qualified Domain Names (FQDN) of 64 bytes or fewer.**
Default	*<blank>*

cfgDNSRacName (Read or Write)

Table 152. Details of cfgDNSRacName

Description	Displays the CMC name, which is rac-service tag by default. This parameter is only valid if **cfgDNSRegisterRac** is set to 1 (TRUE).
Legal Values	A string of up to 63 ASCII characters. At least one character must be alphabetic. **NOTE: Some DNS servers only register names of 31 characters or fewer.**
Default	cmc-*<service tag>*

cfgDNSRegisterRac (Read or Write)

Table 153. Details of cfgDNSRegisterRac

Description	Registers the CMC name on the DNS server. When you set this parameter, the CMC registers its DNS name for its IPv4 and IPv6 addresses with the DNS server.
Legal Values	• 1 (TRUE) • 0 (FALSE)
Default	0

NOTE: For IPv6, only the DHCPv6 address or static address is registered.

Example:

```
racadm getconfig -g cfgLanNetworking

cfgNicEnable=1

cfgNicIPv4Enable=1

cfgNicIpAddress=192.168.0.120

cfgNicNetmask=255.255.255.0

cfgNicGateway=192.168.0.1

cfgNicUseDhcp=1

# cfgNicMacAddress=00:00:00:00:00:01

cfgNicVLanEnable=0

cfgNicVLanID=1

cfgNicVLanPriority=0

cfgDNSServersFromDHCP=1

cfgDNSServer1=192.168.0.5

cfgDNSServer2=192.168.0.6

cfgDNSRacName=cmc-frankly

cfgDNSDomainName=fwad.lab

cfgDNSDomainNameFromDHCP=1

cfgDNSRegisterRac=1
```

cfgDNSServersFromDHCP (Read or Write)

Table 154. Details of cfgDNSServersFromDHCP

Description	Specifies if the DNS server IPv4 addresses should be assigned from the DHCP server on the network. For CMC, this property is used only if **cfgNicUseDhcp** is set to 1 (true).
Legal Values	· 1 (TRUE) · 0 (FALSE)
Default	0

cfgDNSServer1 (Read or Write)

Table 155. Details of cfgDNSServer1

Description	Specifies the IPv4 address for DNS server 1. This property is only valid if **cfgDNSServersFromDHCP** is set to **0** (FALSE). **NOTE: cfgDNSServer1 and cfgDNSServer2 may be set to identical values while swapping addresses.**
Legal Values	String representing a valid IPv4 address. For example: 192.168.0.20.
Default	0.0.0.0

cfgDNSServer2 (Read/Write)

Table 156. Details of cfgDNSServer2

Description	Retrieves the IPv4 address for DNS server 2. This parameter is only valid if **cfgDNSServersFromDHCP** is set to 0 (FALSE). **NOTE: cfgDNSServer1 and cfgDNSServer2 may be set to identical values while swapping addresses.**
Legal Values	String representing a valid IPv4 address. For example: 192.168.0.20.
Default	0.0.0.0

cfgNicEnable (Read or Write)

Table 157. Details of cfgNicEnable

Description	Enables or disables CMC network interface controller. If the NIC is disabled, the remote network interfaces to CMC are no longer accessible and CMC are only available through the local or serial RACADM interface.
Legal Values	· 1 (TRUE) · 0 (FALSE)
Default	1

cfgNicIpAddress (Read or Write)

Table 158. Details of cfgNicIpAddress

Description	Specifies the static IPv4 address to be assigned to the RAC or CMC. **NOTE: This parameter is only configurable if the cfgNicUseDhcp parameter is set to 0 (FALSE.)**
Legal Values	String representing a valid IPv4 address. For example: 192.168.0.20.

Table 158. Details of cfgNicIpAddress (continued)

Default	192.168.0.120

cfgNicNetmask (Read or Write)

Table 159. Details of cfgNicNetmask

Description	The subnet mask used for CMC IP address. This property is only valid if **cfgNicUseDhcp** is set to 0 (FALSE). **NOTE: This parameter is only configurable if the cfgNicUseDhcp parameter is set to 0 (FALSE).**
Legal Values	String representing a valid subnet mask. For example: 255.255.255.0.
Default	255.255.255.0

cfgNicGateway (Read or Write)

Table 160. Details of cfgNicGateway

Description	CMC gateway IPv4 address. The gateway IPv4 address used for static assignment of the RAC IP address. This property is only valid if **cfgNicUseDhcp** is set to 0 (FALSE). **NOTE: This parameter is only configurable if the cfgNicUseDhcp parameter is set to 0 (FALSE).**
Legal Values	String representing a valid gateway IPv4 address. For example: 192.168.0.1.
Default	192.168.0.1

cfgNicMacAddress (Read Only)

Table 161. Details of cfgNicMacAddress

Description	The CMC NIC MAC address in the format: dd:dd:dd:dd:dd:dd, where d is a hexadecimal digit in range 0 - 9, A - F
Legal Values	String representing CMC NIC MAC address.
Default	The current MAC address of CMC NIC. For example, 00:12:67:52:51:A3.

cfgRemoteHosts

This group provides properties that allow configuration of the SMTP server for e-mail alerts.

This group enables/disables and configures firmware updates, NTP, remote syslogging, and SMTP email alerting.

Use this object with the `config` or `getconfig` subcommands.

To use this object property, you must have **Chassis Configuration Administrator** privilege.

The following sections provide information about the objects in the **cfgRemoteHosts** group.

cfgRhostsFwUpdateTftpEnable (Read or Write)

Table 162. Details of cfgRhostsFwUpdateTftpEnable

Description	Enables or disables CMC firmware update from a network TFTP server.
Legal Values	· 1 (TRUE) · 0 (FALSE)
Default	1

cfgRhostsFwUpdateIpAddr (Read or Write)

Table 163. Details of cfgRhostsFwUpdateIpAddr

Description	Specifies the network TFTP server IPv4 or IPv6 address that is used for TFTP CMC firmware update operations.
Legal Values	A string representing a valid IPv4 or IPv6 address. For example, `192.168.0.61`
Default	For IPv4, it is 0.0.0.0

cfgRhostsFwUpdatePath (Read or Write)

Table 164. Details of cfgRhostsFwUpdatePath

Description	Specifies TFTP path where CMC firmware image file exists on the TFTP server. The TFTP path is relative to the TFTP root path on the TFTP server. **NOTE: The server may still require you to specify the drive (for example, C:).**
Legal Values	A string with a maximum length of 255 ASCII characters.
Default	*<blank>*

cfgRhostsSmtpServerIpAddr (Read or Write)

Table 165. Details of cfgRhostsSmtpServerIpAddr

Description	The IPv4 or IPv6 address of the network SMTP server. The SMTP server transmits e-mail alerts from CMC if the alerts are configured and enabled.
Legal Values	A string representing a valid SMTP server IPv4 or IPv6 address. For example: 192.168.0.55.
Default	localhost.localdomain

icfgRhostsNtpEnable

Table 166. Details of icfgRhostsNtpEnable

Description	Enables or disables the use of the Network Time Protocol (NTP) for date and time synchronization.
Legal Values	• 1 (true) • 0 (false)
Default	0

cfgRhostsNtpServer1

Table 167. Details of cfgRhostsNtpServer1

Description	Specifies the first of three possible NTP servers.
Legal Values	A string representing a valid NTP server. For example, ntp1.ntp.net. At least one NTP server must be specified and duplicate entries are not allowed.
Default	Null

cfgRhostsNtpServer2

Table 168. Details of cfgRhostsNtpServer2

Description	Specifies the second of three possible NTP servers.
Legal Values	A string representing a valid NTP server. For example, ntp2.ntp.net. At least one NTP server must be specified and duplicate entries are not allowed.
Default	Null

cfgRhostsNtpServer3

Table 169. Details of cfgRhostsNtpServer3

Description	Specifies the third of three possible NTP servers.
Legal Values	A string representing a valid NTP server. For example, ntp3.ntp.net. At least one NTP server must be specified and duplicate entries are not allowed.
Default	Null

cfgRhostsNtpMaxDist

Table 170. Details of cfgRhostsNtpMaxDist

Description	Specifies the NTP maximum distance parameter used to aid in NTP configuration.
Legal Values	1–128
Default	16

cfgRhostsSyslogPort (Read or Write)

Table 171. Details of cfgRhostsSyslogPort

Description	Remote syslog port number to use for writing the RAC and SEL logs to a remote syslog server. This setting takes effect only if the **cfgRhostsSyslogEnable** parameter is set to 1 (enabled).
Legal Values	10–65535 **NOTE: The following port numbers are reserved and cannot be used: 21, 68, 69, 123, 161, 546, 801, 4096, 5988, 5989, 6900, 9000, 60106.**
Default	514

cfgRhostsSyslogEnable (Read or Write)

Table 172. Details of cfgRhostsSyslogEnable

Description	Enables or disables remote syslog to allow the RAC and SEL logs to be written to up to three remote syslog servers.
Legal Values	• 1 (TRUE) • 0 (FALSE)
Default	0

cfgRhostsSyslogServer1 (Read or Write)

Table 173. Details of cfgRhostsSyslogServer1

Description	Specifies the first of three possible remote syslog servers to store the RAC and SEL logs. This property is only valid if **cfgRhostsSyslogEnable** is set to 1 (enabled).
Legal Values	Valid hostname or IPv4 or IPv6 address.
Default	*<blank>*

cfgRhostsSyslogServer2 (Read or Write)

Table 174. Details of cfgRhostsSyslogServer2

Description	Specifies the second of three possible remote syslog servers to store the RAC and SEL logs. This property is only valid if **cfgRhostsSyslogEnable** is set to 1 (enabled).
Legal Values	Valid hostname or IPv4 or IPv6 address.
Default	*<blank>*

cfgRhostsSyslogServer3 (Read or Write)

Table 175. Details of cfgRhostsSyslogServer3

Description	Specifies the third of three possible remote syslog servers to store the RAC and SEL logs. This property is only valid if **cfgRhostsSyslogEnable** is set to 1 (enabled).
Legal Values	Valid hostname or IPv4 or IPv6 address.
Default	*<blank>*

cfgRhostsSyslogPowerLoggingEnabled

Table 176. Details of cfgRhostsSyslogPowerLoggingEnabled

Description	Enables or disables power consumption logging to remote syslog servers. **NOTE: Remote syslog must be enabled and one or more remote syslog servers must be configured for power consumption to be logged.**
Legal Values	• 1 (enabled) • 0 (disabled)
Default	0

cfgRhostsSyslogPowerLoggingInterval

Table 177. Details of cfgRhostsSyslogPowerLoggingInterval

Description	Specifies the power consumption collection/logging interval.
Legal Values	1–1440 (minutes)
Default	5

Example

```
racadm getconfig -g cfgRemoteHosts [-m server-<n>]
```

```
cfgRhostsFwUpdateTftpEnable=1
cfgRhostsFwUpdateIpAddr=0.0.0.0
cfgRhostsFwUpdatePath=
cfgRhostsSmtpServerIpAddr=localhost.localdomain
cfgRhostsNtpEnable=0
cfgRhostsNtpServer1=
cfgRhostsNtpServer2=
cfgRhostsNtpServer3=
cfgRhostsNtpMaxDist=16
cfgRhostsSyslogEnable=0
cfgRhostsSyslogPort=514
cfgRhostsSyslogServer1=
cfgRhostsSyslogServer2=
cfgRhostsSyslogServer3=cfgRhostsSyslogPowerLoggingEnabled=1
cfgRhostsSyslogPowerLoggingInterval=5
```

cfgUserAdmin

This group provides configuration information about the users who are allowed to access CMC through the available remote interfaces.

Up to 16 instances of the user group are allowed. Each instance represents the configuration for an individual user.

NOTE: In the current CMC firmware version, the objects `cfgUserAdminEnable` and `cfgUserAdminPrivilege` are interrelated; changing the value of one property causes the value of the other property to change. For example, if a user does not have login privilege, the user is disabled by default. When you enable the user by changing the value of `UserAdminEnable` to 1, the right most digit of the `UserAdminPrivilege` also becomes 1. On the other hand, if you change the right-most digit of the `UserAdminPrivilege` to 0, the value of `UserAdminEnable` becomes 0.

Use this object with the `config` or `getconfig` subcommands. You must supply an index group number to use these commands as follows: -i <index group>

To use this object property, you must have the **Chassis Configuration Administrator** privilege.

NOTE: You can configure any setting that is not preceded by the hash sign (#) in the output. To modify a configurable object, use the -o option.

The following sections provide information about the objects in the **cfgUserAdmin** group.

cfgUserAdminIndex (Read Only)

Table 178. Details of cfgUserAdminIndex

Description	The unique index of a user. The index number is used to specify a unique group name. Only valid for indexed groups.
Legal Values	The parameter is specified by a decimal integer from 1–16.
Default	*<index of the instance>*

cfgUserAdminPrivilege (Read or Write)

Table 179. Details of cfgUserAdminPrivilege

Description	This property specifies the role-based authority privileges allowed for the user. The value is represented as a bit mask that allows for any combination of privilege values. The table below describes the user privilege bit values that can be combined to create bit masks.
Legal Values	0x0000000-0x0000fff, and 0x0
Default	0x00000000

Example

```
racadm getconfig -g cfgUserAdmin -i 1
```

```
# cfgUserAdminIndex=1
cfgUserAdminUserName=root
# cfgUserAdminPassword=******** (Write-Only)
cfgUserAdminEnable=1
cfgUserAdminPrivilege=0x00000fff
cfgUserAdminSNMPv3Enable=0
cfgUserAdminSNMPv3AuthenticationType=SHA
cfgUserAdminSNMPv3PrivacyType=AES
```

Table 180. Bit masks for user privileges

iDRAC Specific User Privilege	Privilege Bit Mask
Log into iDRAC	0x00000001
Configure iDRAC	0x00000002
Configure Users	0x00000004
Clear Logs	0x00000008
Execute Server Control Commands	0x00000010
Access Virtual Console	0x00000020
Access Virtual Media	0x00000040
Test Alerts	0x00000080
Execute Debug Commands	0x00000100
CMC Specific User Privilege	
CMC Login User	0x0000001
Chassis Configuration Administrator	0x0000002
User Configuration Administrator	0x0000004
Clear Logs Administrator	0x0000008
Chassis Control Administrator	0x0000010
Super User	0x0000020

Table 180. Bit masks for user privileges (continued)

iDRAC Specific User Privilege	Privilege Bit Mask
Server Administrator	0x0000040
Test Alert User	0x0000080
Debug Command Administrator	0x0000100
Fabric A Administrator	0x0000200
Fabric B Administrator	0x0000400
Fabric C Administrator	0x0000800

Table 181. Examples

User Privileges	Privilege Bit Mask
The user is not allowed to access CMC.	0x00000000
The user may only log in to CMC and view CMC and server configuration information.	0x00000001
The user may log in to CMC and change configuration.	0x00000001 + 0x00000002 = 0x00000003
The user may log in, access Virtual Media, and Virtual Console.	0x00000001 + 0x00000040 + 0x00000080 = 0x000000C1

cfgUserAdminUserName (Read or Write)

Table 182. Details of cfgUserAdminUserName

Description	The name of the user for this index. The user index is created by writing a string into this name field if the index is empty. Writing a string of double quotation marks ("") deletes the user at that index. You cannot change the name. You must delete and then recreate the name. The string cannot contain / (forward slash), \ (backslash), . (period), @ (at symbol) or quotation marks. **NOTE: This property value must be unique among user names.**
Legal Values	A string of up to 16 ASCII characters.
Default	• root (User 2) • *<blank>* (All others)

cfgUserAdminPassword (Write Only)

Table 183. Details of cfgUserAdminPassword

Description	The password for this user. User passwords are encrypted and cannot be seen or displayed after the property is written.
Legal Values	A string of up to 20 ASCII characters.
Default	********

cfgUserAdminEnable (Read or Write)

Table 184. Details of cfgUserAdminEnable

Description	Enables or disables an individual user. **NOTE: You can enable a user for a given index, only if you set the password for the same user.**
Legal Values	• 1 (TRUE) • 0 (FALSE)
Default	0

cfgEmailAlert

This group contains parameters to configure e-mail alerting capabilities. Up to four instances of this group are allowed.

Use this object with the `getconfig` and `config` subcommands.

To use this object property, you must have **Chassis Configuration Administrator** privileges.

NOTE: You can configure any setting that is not preceded by the hash sign (#) in the output. To modify a configurable object, use the -o option.

The following sections provide information about the objects in the **cfgEmailAlert** group.

cfgEmailAlertIndex (Read Only)

Table 185. Details of cfgEmailAlertIndex

Description	The unique index of an alert instance.
Legal Values	1-4
Default	*<instance>*

cfgEmailAlertEnable (Read/Write)

Table 186. Details of cfgEmailAlertEnable

Description	Enables or disables the alert instance.
Legal Values	• 1 (TRUE) • 0 (FALSE)
Default	0

cfgEmailAlertAddress (Read/Write)

Table 187. Details of cfgEmailAlertAddress

Description	Specifies the destination email address for email alerts, for example, user1@company.com.

Table 187. Details of cfgEmailAlertAddress (continued)

Legal Values	E-mail address format, with a maximum length of 64 ASCII characters.
Default	*<blank>*

cfgEmailAlertEmailName

Table 188. Details of cfgEmailAlertEmailName

Description	Specifies name or other identifier associated with the destination e-mail address. The e-mail name can refer to an individual, group, location, department, and so on.
Legal Values	A string of up to 32 characters
Default	*<blank>*

Example

```
racadm getconfig -g cfgEmailAlert -i 2
```

```
# cfgEmailAlertIndex=1
cfgEmailAlertEnable=1
cfgEmailAlertAddress=kfulton@dell.com
cfgEmailAlertName=Kevin Fulton
```

cfgSessionManagement

This group contains parameters to configure the number of sessions that can connect to CMC. One instance of the group is allowed. Displays current settings for and configures idle timeout properties for Web server, Telnet, SSH, and RACADM sessions. Changes to idle timeout settings take effect at the next login. To disable idle timeout for a connection, set this property to 0.

The following sections provide information about the objects in the **cfgSessionManagement** group.

cfgSsnMgtRacadmTimeout (Read/Write)

Table 189. Details of cfgSsnMgtRacadmTimeout

Description	Defines the idle timeout in seconds for the Remote RACADM interface. If a remote RACADM session remains inactive for more than the specified timeout, the session is automatically ended.
Legal Values	0, 10 –1920
Default	iDRAC - 60 CMC - 30

Example

```
racadm getconfig -g cfgSessionManagement cfgSsnMgtWebserverTimeout=0
cfgSsnMgtTelnetIdleTimeout=0
cfgSsnMgtSshIdleTimeout=300
cfgSsnMgtRacadmTimeout=0
```

cfgSsnMgtWebserverTimeout (Read/Write)

Table 190. Details of cfgSsnMgtWebserverTimeout

Description	Defines the Web server time-out. This property sets the amount of time (in seconds) that a connection is allowed to remain idle (there is no user input). The session is cancelled if the time limit set by this property is reached. Changes to this setting do not affect the current session. You must log out and log in again to make the new settings effective. An expired Web server session logs out the current session.
Legal Values	60 – 10800
Default	1800

cfgSerial

This group contains configuration parameters for CMC services. One instance of the group is allowed.

Use this object with the `getconfig` or `config` subcommands.

To use this object property, you must have the **Chassis Configuration Administrator** privilege.

The following sections provide information about the objects in the **cfgSerial** group.

NOTE: The cfgSerial object group is applicable for iDRAC Enterprise on server modules for only two properties—cfgSerialTelnetEnable=1 and cfgSerialSshEnable=1.

cfgSerialBaudRate (Read/Write)

Table 191. Details of cfgSerialBaudRate

Description	Sets the baud rate on the serial port.
Legal Values	2400, 4800, 9600, 19200, 28800, 38400, 57600,115200
Default	115200

cfgSerialConsoleEnable (Read/Write)

Table 192. Details of cfgSerialConsoleEnable

Description	Enables or disables the RAC or CMC serial console interface.
Legal Values	• 1 (TRUE) • 0 (FALSE)
Default	1

cfgSerialConsoleIdleTimeout (Read/Write)

Table 193. Details of cfgSerialConsoleIdleTimeout

Description	The maximum number of seconds to wait before an idle serial session is disconnected.

Table 193. Details of cfgSerialConsoleIdleTimeout (continued)

Legal Values	• 0 = No timeout • 60 – 10800
Default	1800

cfgSerialConsoleNoAuth (Read/Write)

Table 194. Details of cfgSerialConsoleNoAuth

Description	Enables or disables the RAC or CMC serial console login authentication.
Legal Values	• 0 (enables serial login authentication) • 1 (disables serial login authentication)
Default	0

cfgSerialConsoleCommand (Read/Write)

Table 195. Details of cfgSerialConsoleCommand

Description	Specifies a serial command that is executed after a user logs into the serial console interface.
Legal Values	A string representing a valid serial command. For example, `connect server-1`.
Default	*<blank>*

cfgSerialConsoleColumns

Table 196. Details of cfgSerialConsoleColumns

Description	Specifies the number of columns in the terminal window command line connected to the serial port. You must log out, then log in again for the changes to take effect. **NOTE: The prompt counts as two characters.** **NOTE: The terminal emulator must be configured with the line wrap mode ON, if a terminal emulator is used.**
Legal Values	0–256
Default	0 (equivalent to 80)

cfgSerialHistorySize (Read/Write)

Table 197. Details of cfgSerialHistorySize

Description	Specifies the maximum size of the serial history buffer.

Table 197. Details of cfgSerialHistorySize (continued)

Legal Values	0 – 8192
Default	8192

cfgSerialSshEnable (Read/Write)

Table 198. Details of cfgSerialSshEnable

Description	Enables or disables the secure shell (SSH) interface on CMC.
Legal Values	· 1 (TRUE) · 0 (FALSE)
Default	1

Example

```
racadm getconfig -g cfgSerial
```

```
cfgSerialBaudRate=115200
cfgSerialConsoleEnable=1
cfgSerialConsoleQuitKey=^\
cfgSerialConsoleIdleTimeout=1800
cfgSerialConsoleNoAuth=0
cfgSerialConsoleCommand=
cfgSerialConsoleColumns=0
cfgSerialHistorySize=8192
cfgSerialTelnetEnable=0
cfgSerialSshEnable=1
```

cfgSerialTelnetEnable (Read/Write)

Table 199. Details of cfgSerialTelnetEnable

Description	Enables or disables the Telnet console interface on CMC.
Legal Values	· 1 (TRUE) · 0 (FALSE)
Default	0

cfgOobSnmp

This group contains parameters to configure the SNMP agent and trap capabilities of CMC. One instance of the group is allowed.

The CMC SNMP agent supports the standard RFC1213 mib-2, and the Dell enterprise-specific MIB.

Use this object with the config or getconfig subcommands.

To use this object property, you must have **Chassis Configuration Administrator** privilege.

NOTE: You can configure any setting that is not preceded by the hash sign (#) in the output. To modify a configurable object, use the -o option.

The following sections provide information about the objects in the **cfgOobSnmp** group.

cfgOobSnmpAgentCommunity (Read/Write)

Table 200. Details of cfgOobSnmpAgentCommunity

Description	Specifies the SNMP Community Name (identical to community string) used for SNMP traps. The community string acts as a password shared between different hosts over the network. This community string value must match with that of the other hosts for any kind of communication through SNMP.
Legal Values	A string of up to 31 characters.
Default	public

Example

```
racadm getconfig -g cfgOobSnmp
```

```
# racadm getconfig -g cfgoobsnmp
cfgOobSnmpAgentEnable=1
cfgOobSnmpAgentCommunity=public
cfgOobSnmpProtocol=ALL
cfgOobSnmpTrapFormat=SNMPv1
```

cfgOobSnmpAgentEnable (Read/Write)

Table 201. Details of cfgOobSnmpAgentEnable

Description	Enables or disables the SNMP agent.
Legal Values	· 1 (TRUE) · 0 (FALSE)
Default	0

cfgOobSnmpProtocol

Table 202. Details of cfgOobSnmpProtocol attribute

Description	Specifies the SNMP protocol used for SNMP traps.
Legal Values	· 0 — All · 1 — SNMPv3
Default	0

cfgOobSnmpTrapFormat

Table 203. Details of cfgOobSnmpTrapFormat attribute

Description	Specifies the format for SNMP traps.
Legal Values	· 0 — SNMPv1 · 1 — SNMPv2 · 2 — SNMPv3

Table 203. Details of cfgOobSnmpTrapFormat attribute (continued)

Default	0

cfgTraps

This group displays information for and configures delivery of SNMP traps for a specific user.

This object property is applicable only to CMC. Use this object with the **config** or **getconfig** subcommands.

To use this object property, you must have **Chassis Configuration Administrator** privilege.

NOTE: You can configure any setting that is not preceded by the hash sign (#) in the output. To modify a configurable object, use the -o option.

cfgTrapsIndex (Read Only)

Table 204. Details of cfgTrapsIndex

Description	Indicates the unique index of an alert instance.
Legal Values	1 - 4
Default	1

cfgTrapsEnable

Table 205. Details of cfgTrapsEnable

Description	Enables or disables event traps.
Legal Values	• 1 (TRUE) • 0 (FALSE)
Default	None

cfgTrapsAlertDestIpAddr

Table 206. Details of cfgTrapsAlertDestIpAddr

Description	Sets the IP address that receives the alert.
Legal Values	A string representing a valid IP address. For example, 192.168.0.20.
Default	None

cfgTrapsCommunityName

Table 207. Details of cfgTrapsCommunityName

Description	Sets the community string (identical to the community name) used for authentication. The community string acts as a password shared between different hosts over the network. This community string value must match with that of the other hosts for any kind of communication through SNMP.

Table 207. Details of cfgTrapsCommunityName (continued)

Legal Values	A string representing the community name.
Default	None

cfgTrapsSNMPv3UserId (Read Only)

Table 208. Details of cfgTrapsSNMPv3UserId attribute

Description	Displays the SNMP user ID of an existing CMC user.
Legal Values	1-16
Default	Empty

cfgTrapsSNMPv3UserName

Table 209. Details of cfgTrapsSNMPv3UserName attribute

Description	Configure SNMPv3 user name.
Legal Values	Any existing CMC user name.
Default	Empty

cfgRacTuning

This group is used to configure various iDRAC or CMC configuration properties, such as valid ports and security port restrictions.

Use this object with the config or getconfig subcommands.

To use this object property for CMC, you must have **Chassis Configuration Administrator** privilege.

NOTE: For CMC, you can configure any setting that is not preceded by the hash sign (#) in the output. To modify a configurable object, use the -o option.

Use the **-m** option to apply this setting to iDRAC.

The following sections provide information about the objects in the **cfgRacTuning** group.

cfgRacTuneSMBVersionEnable

Table 210. Details of cfgUseCMCDNSSettings attribute

Description	Can be used for setting the SMB version.
Legal Values	• SMBv1 • SMBv2 • SMBv3 • 1 • 2 • 3
Default	NA

cfgRacTuneDefCredentialWarningEnable

Use this object with the `getconfig` or `config` subcommands.

Table 211. Details of cfgRacTuneDefCredentialWarningEnable

Description	Enables or disables the display of the default password warning message.
Legal Values	0 and 1
Default	1

cfgRacTuneRemoteRacadmEnable (Read/Write)

Table 212. Details of cfgRacTuneRemoteRacadmEnable

Description	Enables or disables the Remote RACADM interface.
Legal Values	• 1 (TRUE) • 0 (FALSE)
Default	1

cfgRacTuneHttpPort (Read/Write)

Table 213. Details of cfgRacTuneHttpPort

Description	Specifies the port number to use for HTTP network communication.
Legal Values	10–65535 **NOTE: The following port numbers are reserved and cannot be used: 21, 68, 69, 111, 123, 161, 546, 801, 4096, 5988, 5989, 6900, 9000, and 60106.**
Default	80

cfgRacTuneHttpsPort (Read/Write)

Table 214. Details of cfgRacTuneHttpsPort

Description	Specifies the port number to use for HTTPS network communication with.
Legal Values	10–65535 **NOTE: The following port numbers are reserved and cannot be used: 21, 68, 69, 111, 123, 161, 546, 801, 4096, 5988, 5989, 6900, 9000, and 60106.**
Default	443

cfgRacTuneIpRangeEnable (Read/Write)

Table 215. Details of cfgRacTuneIpRangeEnable

Description	Enables or disables the IPv4 Address Range validation feature.
Legal Values	• 1 (TRUE) • 0 (FALSE)
Default	0

cfgRacTuneIpRangeAddr (Read/Write)

Table 216. Details of cfgRacTuneIpRangeAddr

Description	Specifies the acceptable IPv4 address bit pattern in positions determined by the 1s in the range mask property (**cfgRacTuneIpRangeMask**). A login from the incoming IP address is allowed only if the following are identical: • `cfgRacTuneIpRangeMask` bit-wise and with incoming IP address • `cfgRacTuneIpRanbeMask` bit-wise and with `cfgRacTuneIpRangeAddr`.
Legal Values	An IPv4 address formatted string, for example, 192.168.0.44.
Default	192.168.1.1

cfgRacTuneIpRangeMask (Read/Write)

Table 217. Details of cfgRacTuneIpRangeMask

Description	Standard IP mask values with left-justified bits. For example, 255.255.255.0. A login from the incoming IP address is allowed only if both of the following are identical: • `cfgRacTuneIpRangeMask` bit-wise and with incoming IP address • `cfgRacTuneIpRanbeMask` bit-wise and with `cfgRacTuneIpRangeAddr`.
Legal Values	An IPv4 address formatted string, for example, 255.255.255.0.
Default	255.255.255.0

cfgRacTuneIpBlkEnable (Read/Write)

Table 218. Details of cfgRacTuneIpBlkEnable

Description	Enables or disables the IPv4 address blocking feature.
Legal Values	• 1 (TRUE)

Table 218. Details of cfgRacTuneIpBlkEnable (continued)

	• 0 (FALSE)
Default	0

cfgRacTuneIpBlkFailCount (Read/Write)

Table 219. Details of cfgRacTuneIpBlkFailCount

Description	The maximum number of login failures to occur within the window (cfgRacTuneIpBlkFailWindow) before login attempts from the IP address are rejected.
Legal Values	2 – 16
Default	5

cfgRacTuneIpBlkFailWindow (Read/Write)

Table 220. Details of cfgRacTuneIpBlkFailWindow

Description	Defines the time span in seconds that the failed attempts are counted. When failure attempts age beyond this limit, they are dropped from the count.
Legal Values	2–65535
Default	60

cfgRacTuneIpBlkPenaltyTime (Read/Write)

Table 221. Details of cfgRacTuneIpBlkPenaltyTime

Description	Defines the time span in seconds that session requests from an IP address with excessive failures are rejected.
Legal Values	2–65535
Default	300

cfgRacTuneSshPort (Read/Write)

Table 222. Details of cfgRacTuneSshPort

Description	Specifies the port number used for the SSH interface.
Legal Values	10–65535
Default	22

cfgRacTuneTelnetPort (Read/Write)

Table 223. Details of cfgRacTuneTelnetPort

Description	Specifies the port number used for iDRAC or CMC Telnet interface. **NOTE: For CMC, the following port numbers are reserved and cannot be used: 21, 68, 69, 111, 123, 161, 546, 801, 4096, 5988, 5989, 6900, 9000, and 60106.**
Legal Values	• For iDRAC: 1 – 65535 • For CMC: 10 – 65535
Default	23

cfgRacTuneDaylightOffset (Read Only)

Table 224. Details of cfgRacTuneDaylightOffset

Description	Specifies the daylight savings offset (in minutes) to use for the RAC Time. This value is 0 if the time zone is not a Daylight Saving time zone.
Legal Values	0 – 60
Default	0

cfgRacTuneTimezoneOffset (Read Only)

Table 225. Details of cfgRacTuneTimezoneOffset

Description	Specifies the time zone offset (in minutes) from Greenwich Mean Time (GMT)/Coordinated Universal Time (UTC) to use for the RAC Time. Some common time zone offsets for time zones in the United States are: • –480 (PST—Pacific Standard Time) • –420 (MST—Mountain Standard Time) • –360 (CST—Central Standard Time) • –300 (EST—Eastern Standard Time) For CMC: This object property is read only. Specifies the difference in number of seconds, from the UTC/GMT. This value is negative if the current time zone is west of Greenwich.
Legal Values	–720 to 7800
Default	0

cfgRacTuneWebserverEnable (Read/Write)

Table 226. Details of cfgRacTuneWebserverEnable

Description	Enables or disables the Web server. If this property is disabled, CMC is not accessible using client Web browsers. This property has no effect on the Telnet/SSH or RACADM interfaces.
Legal Values	• 1 (TRUE) • 0 (FALSE)

Table 226. Details of cfgRacTuneWebserverEnable (continued)

Default	1

cfgRacTuneFipsModeEnable

Table 227. Details of cfgRacTuneFipsModeEnable attribute

Description	Enables or disables the FIPS mode.
Legal Values	0 and 1
Default	0
Usage	`racadm getconfig -g cfgRacTuning -o cfgRacTuneFipsModeEnableracadm config -g cfgRacTuning -o cfgRacTuneFipsModeEnable 1`

NOTE: The firmware racadm prompts you to confirm whether the FIPS mode has to be enabled, but remote racadm does not prompt you to do so.

cfgRacTuneTLSProtocolVersionEnable

Table 228. Details of cfgRacTuneTLSProtocolVersionEnable attribute

Description	Sets the minimum TLS protocol version.
Legal Values	• 0 - TLSv1.0, TLSv1.1, and TLSv1.2 are enabled. • 1 - TLSv1.1 and TLSv1.2 are enabled. • 2 - only TLSv1.2 is enabled.
Default	1

cfgRacTuneChassisNameInPromptEnable

Table 229. Details of cfgRacTuneChassisNameInPromptEnable attribute

Description	Enables or disables display of the chassis name in the SSH prompt.
Legal Values	• 0—Disable • 1—Enable
Default	0

NOTE: You must have the chassis configuration administrator privilege to set and get the `cfgRacTuneChassisNameInPromptEnable` attribute.

cfgServerInfo

For iDRAC this group allows you to select the BIOS first boot device and provides the option to boot the selected device only once.

For CMC, this group allows you to displays information for and configure a server in the chassis.

Use this object with the config or getconfig subcommands.

To use this object property for CMC, you must have **Chassis Configuration Administrator** privilege.

NOTE: For CMC, you can configure any setting that is not preceded by the hash sign (#) in the output. To modify a configurable object, use the -o option

The following sections provide information about the objects in the **cfgServerInfo** group.

cfgServerInfoIndex (Read Only)

Table 230. Details of cfgServerInfoIndex

Description	Displays the index name of the server.
Legal Values	None
Default	None

cfgServerSlotNumber (Read Only)

Table 231. Details of cfgServerSlotNumber

Description	Specifies the location of the specified server (1–4) in the chassis.
Legal Values	None
Default	None

cfgServerServiceTag (Read Only)

Table 232. Details of cfgServerServiceTag

Description	Displays the service tag of the specified server.
Legal Values	None
Default	None

cfgServerName (Read/Write)

Table 233. Details of cfgServerName

Description	Displays the name of the specified server.
Legal Values	Maximum of 15 non-extended ASCII characters, (ASCII codes 32–126). For more information, see Guidelines to Quote Strings Containing Special Characters when Using RACADM Commands.
Default	SLOT - *<slot number>*

cfgServerFW (Read Only)

Table 234. Details of cfgServerFW

Description	Displays the server's iDRAC management firmware revision.
Legal Values	None
Default	None

cfgServerBIOS (Read Only)

Table 235. Details of cfgServerBIOS

Description	Displays the server's BIOS revision.
Legal Values	None
Default	None

cfgServerBmcMacAddress (Read Only)

Table 236. Details of cfgServerBmcMacAddress

Description	Displays the BMC MAC address of the specified server.
Legal Values	None
Default	None

cfgServerNic1MacAddress (Read Only)

Table 237. Details of cfgServerNic1MacAddress

Description	Displays the MAC address of the server NIC 1.
Legal Values	None
Default	None

cfgServerNic2MacAddress (Read Only)

Table 238. Details of cfgServerNic2MacAddress

Description	Displays the MAC address of the server NIC 2.
Legal Values	None
Default	None

cfgServerNic3MacAddress (Read Only)

Table 239. Details of cfgServerNic3MacAddress

Description	Displays the MAC address of the server NIC 3.
Legal Values	None
Default	None

cfgServerNic4MacAddress (Read Only)

Table 240. Details of cfgServerNic4MacAddress

Description	Displays the MAC address of the server NIC 4.
Legal Values	None
Default	None

cfgServerPriority (Read/Write)

Table 241. Details of cfgServerPriority

Description	Sets the priority level allotted to the server in the chassis for power budgeting purposes.
Legal Values	1–9 in descending priority, where 1 holds the highest priority
Default	1

cfgServerNicEnable (Read/Write)

Table 242. Details of cfgServerNicEnable

Description	Enables or disables LAN channel.
Legal Values	· 1 (Enable) · 0 (Disable)
Default	None

cfgServerIPMIOverLanEnable (Read/Write)

Table 243. Details of cfgServerIPMIOverLanEnable

Description	Enables or disables IPMI LAN channel.
Legal Values	· 1 (enable) · 0 (disable)
Default	None

cfgServerPowerBudgetAllocation (Read Only)

Table 244. Details of cfgServerPowerBudgetAllocation

Description	Displays the current power allocation for the server.
Legal Values	· 1 (Enable) · 0 (Disable)
Default	None

cfgServerDNSRegisterIMC (Read/Write)

Table 245. Details of cfgServerDNSRegisterIMC

Description	Enables or disables DNS name registration for the Integrated System (iDRAC).
Legal Values	• 1 (enable) • 0 (disable)
Default	None

cfgServerDNSIMCName (Read/Write)

Table 246. Details of cfgServerDNSIMCName

Description	Displays the DNS domain name for the integrated Remote Access Controller (iDRAC.)
Legal Values	None
Default	None

cfgServerRootPassword (Write Only)

Table 247. Details of cfgServerRootPassword

Description	Displays the password for iDRAC as a series of asterisks (*). It cannot be seen or displayed after this property is written.
Legal Values	None
Default	None

cfgServerFirstBootDevice (Read/Write)

Table 248. Details of cfgServerFirstBootDevice

Description	Sets or displays the first boot device. This object is read-write. **NOTE: For a vFlash Partition to be configured as First Boot Device, it has to be attached first. When a detached or non-existent VFlash partition or a non-standard boot device is configured as first boot device, the following error message is displayed:** `Invalid object value`
Legal Values	• 0–default • 4–PXE • 8–HDD • 20–DIAG • 28–CD-DVD • 32–BIOS

Table 248. Details of cfgServerFirstBootDevice (continued)

	• 36–vFDD • 40–VCD-DVD • 44–iSCSI • 60–VFLASH partition label
Default	0 (zero)

cfgServerBootOnce (Read/Write)

Table 249. Details of cfgServerBootOnce

Description	Enables or disables the server boot once feature. This object is read-write.
Legal Values	• 1 = TRUE • 0 = FALSE
Default	0

cfgServerPowerConsumption (Read Only)

Table 250. Details of cfgServerPowerConsumption

Description	Displays the current power consumption for a server.
Legal Values	None
Default	None

Example

```
racadm getconfig -g cfgServerInfo -i 8
# cfgServerInfoIndex=8
# cfgServerSlotNumber=8
# cfgServerServiceTag=
cfgServerName=SLOT-08
# cfgServerFW=3.0
# cfgServerBIOS=
# cfgServerBmcMacAddress=00:21:9B:FE:5F:58
# cfgServerNic1MacAddress=00:0D:56:B8:69:63
# cfgServerNic2MacAddress=00:0D:56:B8:69:65
# cfgServerNic3MacAddress=00:0D:56:B8:69:CB
# cfgServerNic4MacAddress=00:0D:56:B8:69:CD
cfgServerPriority=1
cfgServerNicEnable=1
cfgServerIPMIOverLANEnable=1
# cfgServerPowerBudgetAllocation=0
cfgServerDNSRegisterIMC=0
```

```
cfgServerDNSIMCName=iDRAC-
cfgServerRootPassword=******** (Write-Only)
cfgServerFirstBootDevice=0
# cfgServerBootOnce=1
# cfgServerPowerConsumption=0
racadm getconfig -g cfgServerInfo -i 1
# cfgServerInfoIndex=1
# cfgServerSlotNumber=1
# cfgServerServiceTag=1S0M0G1
cfgServerName=SLOT-01
# cfgServerFW=1.40 (Build 12)
# cfgServerBIOS=4.0.2
# cfgServerBmcMacAddress=00:18:8B:FF:41:43
# cfgServerNic1MacAddress=00:1A:A0:FF:D9:F4
# cfgServerNic2MacAddress=00:1A:A0:FF:D9:F6
cfgServerPriority=1
cfgServerNicEnable=1
cfgServerIPMIOverLANEnable=1
# cfgServerPowerBudgetAllocation=0
cfgServerDNSRegisterIMC=0
cfgServerDNSIMCName=iDRAC-1S0M0G1
cfgServerRootPassword=******** (Write-Only)
cfgServerFirstBootDevice=0
# cfgServerBootOnce=1
# cfgServerPowerConsumption=0
```

cfgActiveDirectory

This group contains parameters to configure the Active Directory feature.

Use this object with the `getconfig` or `config` subcommands.

To use this object property, you must have the **Chassis Configuration Administrator** privilege.

NOTE: You can configure any setting that is not preceded by the hash sign (#) in the output. To modify a configurable object, use the -o option.

The following sections provide information about the objects in the **cfgActiveDirectory** group.

cfgADRacName (Read/Write)

Table 251. Details of cfgADRacName

Description	Name of CMC as recorded in the Active Directory forest.
Legal Values	Any printable text string of up to 254 characters, with no white space.
Default	*<blank>*

cfgADCertValidationEnable (Read/Write)

Table 252. Details of cfgADCertValidationEnable

Description	Enables or disables Active Directory certificate validation as a part of the Active Directory configuration process.
Legal Values	• 1 (TRUE) • 0 (FALSE)
Default	1

cfgADRacDomain (Read/Write)

Table 253. Details of cfgADRacDomain

Description	Active Directory Domain in which CMC resides.
Legal Values	Any printable text string of up to 254 characters, with no white space.
Default	1

cfgADRootDomain (Read/Write)

Table 254. Details of cfgADRootDomain

Description	Specifies the root domain of the domain forest.
Legal Values	Any printable text string of up to 254 characters, with no white space.
Default	*<blank>*

cfgADEnable (Read/Write)

Table 255. Details of cfgADEnable

Description	Enables or disables Active Directory user authentication on CMC. If this property is disabled, LDAP authentication may be used for user login.
Legal Values	• 1 (TRUE) • 0 (FALSE)
Default	0

cfgADAuthTimeout (Read/Write)

Table 256. Details of cfgADAuthTimeout

Description	Specifies the number of seconds to wait for Active Directory authentication requests to complete before timing out.

Table 256. Details of cfgADAuthTimeout (continued)

	NOTE: To modify this property, you must have the Configure CMC privilege.
Legal Values	15–300 seconds
Default	120

cfgADSCLEnable

Table 257. Details of cfgADSCLEnable

Description	Enables you to log on to the CMC without enabling the Smart Card login.
Legal Values	• 1 (Enable) • 0 (Disable)
Default	0

cfgADSSOEnable (Read/Write)

Table 258. Details of cfgADSSOEnable

Description	Enables or disables Active Directory single sign-on authentication on CMC.
Legal Values	• 1 (TRUE) • 0 (FALSE)
Default	0

cfgADDomainController1 (Read/Write)

Table 259. Details of cfgADDomainController1

Description	Specifies the LDAP server from which you want the CMC to obtain user names .
Legal Values	A string of up to 254 ASCII characters representing a valid IP address or a fully qualified domain name (FQDN).
Default	None

cfgADDomainController2 (Read/Write)

Table 260. Details of cfgADDomainController2

Description	Specifies the LDAP server from which you want the CMC to obtain user names .
Legal Values	A string of up to 254 ASCII characters representing a valid IP address or a fully qualified domain name (FQDN).

Table 260. Details of cfgADDomainController2 (continued)

Default	None

cfgADDomainController3 (Read/Write)

Table 261. Details of cfgADDomainController3

Description	Specifies the LDAP server from which you want the CMC to obtain user names .
Legal Values	A string of up to 254 ASCII characters representing a valid IP address or a fully qualified domain name (FQDN).
Default	None

cfgADGlobalCatalog1 (Read/Write)

Table 262. Details of cfgADGlobalCatalog1

Description	Specifies the Global Catalog server from which you want the CMC to obtain user names.
Legal Values	A string of up to 254 ASCII characters representing a valid IP address or a fully qualified domain name (FQDN).
Default	None

cfgADGlobalCatalog2 (Read/Write)

Table 263. Details of cfgADGlobalCatalog2

Description	Specifies the Global Catalog server from which you want the CMC to obtain user names.
Legal Values	A string of up to 254 ASCII characters representing a valid IP address or a fully qualified domain name (FQDN).
Default	None

cfgADGlobalCatalog3 (Read/Write)

Table 264. Details of cfgADGlobalCatalog3

Description	Specifies the Global Catalog server from which you want the CMC to obtain user names.
Legal Values	A string of up to 254 ASCII characters representing a valid IP address or a fully qualified domain name (FQDN).
Default	None

cfgADType (Read/Write)

Table 265. Details of cfgADType

Description	Determines the schema type to use with Active Directory.
Legal Values	• 1 (Enables Active Directory with the extended schema) • 2 (Enables Active Directory with the standard schema)
Default	1

cfgADDcSRVLookupbyUserdomain (Read/Write)

Table 266. Details of cfgADDcSRVLookupbyUserdomain

Description	Chooses the way the user domain is looked up for Active Directory.
Legal Values	• 1 (TRUE)—use user domain as the search domain to look up DCs. The user domain is chosen from the user domain list or entered by the login user. • 0 (FALSE)—use the configured search domain **cfgADDcSrvLookupDomainName** to look up DCs.
Default	1

cfgADDcSRVLookupDomainName (Read/Write)

Table 267. Details of cfgADDcSRVLookupDomainName

Description	This is the Active Directory Domain to use when **cfgAddcSrvLookupbyUserDomain** is set to **0**.
Legal Values	String. Maximum length = 254
Default	Null

cfgADDcSRVLookupEnable (Read/Write)

Table 268. Details of cfgADDcSRVLookupEnable

Description	Configures CMC to use pre-configured domain controllers or to use DNS to find the domain controller. If using pre-configured domain controllers, then the domain controllers to use are specified under **cfgAdDomainController1**, **cfgAdDomainController2**, and **cfgAdDomainController3**. CMC does not fail over to the specified domain controllers when DNS lookup fails or none of the servers returned by the DNS lookup works.
Legal Values	• 1 (TRUE)—use DNS to look up domain controllers • 0 (FALSE)—use pre-configured domain controllers
Default	0

cfgADGcRootDomain (Read/Write)

Table 269. Details of cfgADGcRootDomain

Description	The name of the Active Directory root domain used for DNS look up, to locate Global Catalog servers.
Legal Values	String. Maximum character length = 254
Default	Null

cfgADGcSRVLookupEnable (Read/Write)

Table 270. Details of cfgADGcSRVLookupEnable

Description	Determines how the global catalog server is looked up. If using pre-configured global catalog servers, then CMC uses the values **cfgAdGlobalCatalog1**, **cfgAdGlobalCatalog2**, and **cfgAdGlobalCatalog3**.
Legal Values	• 0(FALSE)—use pre-configured Global Catalog Servers (GCS) • 1(TRUE)—use DNS to look up GCS
Default	0

cfgADSpecifyServerEnable

Table 271. Details of cfgADSpecifyServerEnable

Description	Allows you to enable or disable and specify an LDAP server or a global catalog server. Use **cfgADDomainController** or **cfgADGlobalCatalog** to specify the IP address.
Legal Values	• 1 (enabled) • 0 (disabled)
Default	0

cfgLDAP

This group allows you to configure settings related to the Lightweight Directory Access Protocol (LDAP).

Use this object with the **config** or **getconfig** subcommands.

To use this object property for CMC, you must have the **Chassis Configuration Administrator** privilege.

NOTE: For CMC, you can configure any setting that is not preceded by the hash sign (#) in the output. To modify a configurable object, use the -o option.

The following sections provide information about the objects in the **cfgLDAP** group.

cfgLDAPEnable (Read/Write)

Table 272. Details of cfgLDAPEnable

Description	Turns LDAP service on or off.

Table 272. Details of cfgLDAPEnable (continued)

	If this property is disabled, local CMC authentication is used for user logins. **NOTE: For CMC, enabling this option turns off cfgADEnable.**
Legal Values	• 1 (TRUE)— Enable • 0 (FALSE)— Disable
Default	0

cfgLDAPServer (Read/Write)

Table 273. Details of cfgLDAPServer

Description	Configures the address of the LDAP Server. IPv4 and IPv6 are supported. **NOTE: You can specify multiple servers by separating each server with a comma. For example, example.com, sub1.example.com**
Legal Values	String. Maximum length = 254
Default	Null

cfgLDAPPort (Read/Write)

Table 274. Details of cfgLDAPPort

Description	Port of LDAP over SSL. Non-SSL port is not supported.
Legal Values	1 - 65535
Default	636

cfgLDAPBasedn (Read/Write)

Table 275. Details of cfgLDAPBasedn

Description	The Domain Name of the branch of the directory where all searches should start from.
Legal Values	String. Maximum length = 254
Default	Null

cfgLDAPUserAttribute (Read/Write)

Table 276. Details of cfgLDAPUserAttribute

Description	Specifies the user attribute to search for. It is recommended to be unique within the chosen baseDN, otherwise a search filter must be configured to make sure the uniqueness of the login user. If the userDN cannot be uniquely identified, login fails with error.
Legal Values	String. Maximum length = 254
Default	Null *uid* if not configured.

cfgLDAPGroupAttribute (Read/Write)

Table 277. Details of cfgLDAPGroupAttribute

Description	Specifies which LDAP attribute is used to check for group membership. This should be an attribute of the group class. If not specified, then CMC uses the member and unique member attributes.
Legal Values	String. Maximum length = 254
Default	Null

cfgLDAPGroupAttributeIsDN (Read/Write)

Table 278. Details of cfgLDAPGroupAttributeIsDN

Description	If enabled, the CMC performs DN matching; otherwise, the CMC uses the username provided at login for matching.
Legal Values	• 1 (TRUE)—Use the *userDN* from the LDAP Server • 0 (FALSE)—Use the *userDN* provided by the login user
Default	1

cfgLDAPBinddn (Read/Write)

Table 279. Details of cfgLDAPBinddn

Description	The distinguished name of a user used to bind to the server when searching for the login user's DN. If not provided, an anonymous bind is used. This is optional but is required if anonymous bind is not supported. **NOTE: If cfgLDAPBindDN is [null] and cfgLDAPBindPassword is [null], then the CMC attempts an anonymous bind.**
Legal Values	String. Maximum length = 254
Default	Null

cfgLDAPBindpassword (Write Only)

Table 280. Details of cfgLDAPBindpassword

Description	A bind password to use in conjunction with the bindDN. The bind password is sensitive data, and should be protected. This is optional but is required if anonymous bind is not supported.
Legal Values	String. Maximum length = 254
Default	Null

cfgLDAPSearchFilter (Read/Write)

Table 281. Details of cfgLDAPSearchFilter

Description	A valid LDAP search filter. This is used if the user attribute cannot uniquely identify the login user within the chosen baseDN. The search filter only applies to userDN search and not the group membership search.
Legal Values	String of maximum length = 1024 characters
Default	(objectclass=*) Searches for all objects in tree.

cfgLDAPCertValidationEnable (Read/Write)

Table 282. Details of cfgLDAPCertValidationEnable

Description	Controls certificate validation during SSL handshake.
Legal Values	• 1 (TRUE)—CMC uses the CA certificate to validate the LDAP server certificate during SSL handshake. • 0 (FALSE)—CMC does not perform the certificate validation task of SSL handshake.
Default	1

cfgLDAPNetworkTimeout

Table 283. Details of cfgLDAPNetworkTimeout

Description	Configures the network timeout in seconds.
Legal Values	Positive integer
Default	30 seconds

cfgLDAPSearchTimeout

Table 284. Details of cfgLDAPSearchTimeout

Description	Configures the search timeout in seconds.

Table 284. Details of cfgLDAPSearchTimeout (continued)

Legal Values	Positive integer
Default	120 seconds

cfgLDAPSRVLookupDomainName

Table 285. Details of cfgLDAPSRVLookupDomainName

Description	Configures the domain name to be used in the SRV lookup.
Legal Values	String of maximum length of 254 alphanumeric characters and hyphens. The string must begin with a letter.
Default	[null]

cfgLDAPSRVLookupEnable

Table 286. Details of cfgLDAPSRVLookupEnable

Description	Configures the CMC to query a DNS server for SRV records.
Legal Values	• 1 (true) • 0 (false)
Default	0

cfgLDAPSRVLookupServiceName (Read/Write)

Table 287. Details of cfgLDAPSRVLookupServiceName

Description	Configures the service name to be used in the SRV lookup.
Legal Values	String of maximum length of 254 characters.
Default	ldap

cfgLDAPRoleGroup

Use this object with the `getconfig` or `config` subcommands.

To use this object property, you must have the **Chassis Configuration Administrator** privilege.

NOTE: You can configure any setting that is not preceded by the hash sign (#) in the output. To modify a configurable object, use the -o option.

This group configures Generic LDAP Role group descriptions and defines the CMC privileges that LDAP–authenticated users are granted.

cfgLDAPRoleGroup is indexed, containing instances numbered from 1 to 5. Each object instance consists of a pair of properties:

- **cfgLDAPRoleGroupDN**: an LDAP distinguished name (DN)
- **cfgLDAPRoleGroupPrivilege**: a CMC privilege map

Each LDAP–authenticated user assumes the total set of CMC privileges assigned to the matching LDAP distinguished names that the user belongs to.

That is, if the user belongs to multiple role group DNs, the user receives all associated privileges for those DNs.

The following sections provide information about the objects in the **cfgLdapRoleGroup** group.

cfgLDAPRoleGroupDN (Read/Write)

Table 288. Details of cfgLDAPRoleGroupDN

Description	This is the Domain Name of the group in this index. For CMC, configure the LDAP distinguished name (DN) for the role group instance.
Legal Values	String. Maximum length = 1024
Default	None

Example

```
racadm getconfig -g cfgLDAPRoleGroup -o cfgLDAPRoleGroupDN
-i 1 cn=everyone,ou=groups,dc=openldap,dc=com
```

cfgLDAPRoleGroupPrivilege (Read/Write)

Table 289. Details of cfgLDAPRoleGroupPrivilege

Description	A bit–mask defining the privileges associated with this particular group.
Legal Values	0x00000000 to 0x000001ff
Default	0x000

Example

```
racadm getconfig -g cfgLDAPRoleGroup -o cfgLDAPRoleGroupPrivilege
-i 1 0x0
```

cfgLocation

This group defines objects that support physical location properties. Use this object with the `getconfig` or `config` subcommands.

To use this object property, you must have the **Chassis Configuration Administrator** privilege.

cfgLocationDatacenter (Read/Write)

Table 290. Details of cfgLocationDatacenter

Description	Indicates DataCenter name.
Legal Values	String of up to 128 ASCII characters
Default	0

cfgLocationAisle (Read/Write)

Table 291. Details of cfgLocationAisle

Description	Indicates aisle where server is located.
Legal Values	String of up to 128 ASCII characters
Default	0

cfgLocationRack (Read/Write)

Table 292. Details of cfgLocationRack

Description	Indicates rack where server is located.
Legal Values	String of up to 128 ASCII characters
Default	0

cfgLocationRackslot (Read/Write)

Table 293. Details of cfgLocationRackslot

Description	Indicates the slot where a server is located.
Legal Values	Values from 1 - 255 (1 Byte)
Default	0

cfgLocationDevicesize (Read Only)

Table 294. Details of cfgLocationDevicesize

Description	Indicates server chassis size.
Legal Values	Values from 1 - 255
Default	0

cfgStandardSchema

This group contains parameters to configure the Active Directory standard schema settings.

Use this object with the`getconfig` or `config` subcommands.

To use this object property, you must have the **Chassis Configuration Administrator** privilege.

NOTE: You can configure any setting that is not preceded by the hash sign (#) in the output. To modify a configurable object, use the -o option.

The following sections provide information about the objects in the **cfgStandardSchema** group.

cfgSSADRoleGroupIndex (Read Only)

Table 295. Details of cfgSSADRoleGroupIndex

Description	Index of the Role Group as recorded in the Active Directory.
Legal Values	An integer between 1 and 5
Default	*<instance>*

cfgSSADRoleGroupName (Read/Write)

Table 296. Details of cfgSSADRoleGroupName

Description	Name of the Role Group as recorded in the Active Directory forest.
Legal Values	Any printable text string of up to 254 characters with no white space.
Default	*<blank>*

cfgSSADRoleGroupDomain (Read/Write)

Table 297. Details of cfgSSADRoleGroupDomain

Description	Active Directory Domain in which the Role Group resides.
Legal Values	Any printable text string of up to 254 characters, with no white space.
Default	*<blank>*

cfgSSADRoleGroupPrivilege (Read/Write)

Table 298. Details of cfgSSADRoleGroupPrivilege

Description	Use the bit mask numbers listed in the table below to set role-based authority privileges for a Role Group.
Legal Values	0x00000000 0x00000fff
Default	*<blank>*

Example

```
racadm getconfig -g cfgStandardSchema -i 1
```

NOTE: -i <number> is for the index.

```
# cfgSSADRoleGroupIndex=1
cfgSSADRoleGroupName=
cfgSSADRoleGroupDomain=
cfgSSADRoleGroupPrivilege=
```

```
$ config -g cfgStandardSchema -i 1 -o cfgSSADRoleGroupName Charlie
Object value modified successfully
```

Table 299. Bit masks for Role Group privileges

Role Group Privilege	Bit Mask
Login to iDRAC	0x00000001
Configure iDRAC	0x00000002
Configure Users	0x00000004
Clear Logs	0x00000008
Execute Server Control Commands	0x00000010
Access Virtual Console	0x00000020
Access Virtual Media	0x00000040
Test Alerts	0x00000080
Execute Debug Commands	0x00000100

cfgChassisPower

This group is applicable only to CMC and contains parameters to display or configure power for the chassis.

Use this object with the config or getconfig subcommands.

To use this object property, you must have the **Chassis Configuration Administrator** privilege.

The following sections provide information about the objects in the **cfgChassisPower** group.

NOTE: While configuring chassis power from a file, update the value for one chassis power cap property and remove the values for the other chassis power cap properties or, update the last percentage value as it is applicable to all chassis power cap properties. The chassis power cap properties are: `cfgChassisPowerCap`, `cfgChassisPowerCapF`, `cfgChassisPowerCapBTU`, `cfgChassisPowerCapFBTU`, `cfgChassisPowerCapPercent`, and `cfgChassisPowerCapFPercent`.

cfgChassisInPower (Read Only)

Table 300. Details of cfgChassisInPower

Description	Indicates the cumulative input power consumption data (in Watt and BTU/hr) captured from all healthy and functional PSUs in the chassis.
Legal Values	None
Default	None

cfgChassisPeakPower (Read Only)

Table 301. Details of cfgChassisPeakPower

Description	Indicates the maximum system input power consumption (in Watt).

Table 301. Details of cfgChassisPeakPower (continued)

Legal Values	
Default	

cfgChassisPeakPowerTimestamp (Read Only)

Table 302. Details of cfgChassisPeakPowerTimestamp

Description	The timestamp recorded when the peak input power consumption value occurred.
Legal Values	
Default	

cfgChassisMinPower (Read Only)

Table 303. Details of cfgChassisMinPower

Description	The minimum system input power consumption value (in Watt) over the time since the value was last cleared.
Legal Values	None
Default	None

cfgChassisMinPowerTimestamp (Read Only)

Table 304. Details of cfgChassisMinPowerTimestamp

Description	The timestamp recorded when the minimum system power occurred.
Legal Values	None
Default	None

cfgChassisPowerStatus (Read Only)

Table 305. Details of cfgChassisPowerStatus

Description	Indicates the power status of the chassis.
Legal Values	• 1 (other) • 2 (unknown) • 3 (OK) • 4 (non-critical) • 5 (critical) • 6 (non-recoverable)
Default	None

cfgChassisRedundantState (Read Only)

Table 306. Details of cfgChassisRedundantState

Description	Enables or disables power redundancy for the chassis.
Legal Values	• 0 (none) • 1 (full)
Default	None

cfgChassisDefaultPowerCapUpperBound (Read Only)

Table 307. Details of cfgChassisDefaultPowerCapUpperBound

Description	Indicates the maximum default value to which you can set the power cap of a chassis.
Legal Values	5000 Watt
Default	5000 Watt

cfgChassisDefaultPowerCapUpperBoundBTU (Read Only)

Table 308. Details of cfgChassisDefaultPowerCapUpperBoundBTU

Description	Indicates the maximum default value to which you can set the power cap of a chassis.
Legal Values	17060 BTU/h
Default	17060 BTU/h

cfgChassisDefaultPowerCapLowerBound (Read Only)

Table 309. Details of cfgChassisDefaultPowerCapLowerBound

Description	Indicates the minimum default value to which you can set the power cap of a chassis.
Legal Values	Zero Watt
Default	Zero Watt

cfgChassisDefaultPowerCapLowerBoundBTU (Read Only)

Table 310. Details of cfgChassisDefaultPowerCapLowerBoundBTU

Description	Indicates the minimum default value to which you can set the power cap of a chassis.
Legal Values	Zero Watt

Table 310. Details of cfgChassisDefaultPowerCapLowerBoundBTU (continued)

Default	Zero Watt

cfgChassisPowerCap (Read/Write)

Table 311. Details of cfgChassisPowerCap

Description	Indicates the maximum power consumption limit (in Watt) for the entire chassis. The command generates an error if server throttling is necessary to achieve the power goal based on the value for this setting.
Legal Values	2715 – 16685 Watt
Default	16685 Watt

cfgChassisPowerCapF (Read/Write)

Table 312. Details of cfgChassisPowerCapF

Description	Indicates the maximum power consumption limit (in Watt) for the entire chassis. Use **cfgChassisPowerCapF** when power consumption is to be changed regardless of whether server throttling is required. This command generates an error if the value for this setting is lower than the minimum power required for the chassis configuration.
Legal Values	2715 – 16685 Watt
Default	16685 Watt

cfgChassisPowerCapFBTU (Read/Write)

Table 313. Details of cfgChassisPowerCapFBTU

Description	Indicates the maximum power consumption limit (in BTU/hr) for the entire chassis. Use **cfgChassisCapFBTU** when power consumption is to be changed regardless of whether server throttling is required. The command generates an error if the value for this setting is lower than the minimum power required for the chassis configuration.
Legal Values	9264 - 56931 BTU/hr
Default	56931 BTU/hr

cfgChassisPowerCapPercent (Read or Write)

Table 314. Details of cfgChassisPowerCapPercent

Description	Indicates the power consumption limit as a percentage. The percentage is computed mathematically as the minimum power + (percent * (maximum power - minimum power)). The command

Table 314. Details of cfgChassisPowerCapPercent (continued)

	generates an error if server throttling is necessary to achieve the power goal based on the value for this setting.
Legal Values	16 -100 **NOTE: If the specified percent is lower than the minimum value, the CMC will set the value to the minimum value.**
Default	100

cfgChassisPowerCapFPercent (Read/Write)

Table 315. Details of cfgChassisPowerCapFPercent

Description	Indicates the power consumption limit as a percentage. The percentage is computed mathematically as the minimum power + (percent * (maximum power - minimum power)). Use **cfgChassisPowerCapFPercent** when power consumption is to be changed regardless of whether server throttling is required.
Legal Values	16 - 100 **NOTE: If the specified percent is lower than the minimum value, the CMC will set the value to the minimum value.**
Default	100

cfgChassisRedundancyPolicy (Read/Write)

Table 316. Details of cfgChassisRedundancyPolicy

Description	Sets the redundancy policy of the chassis.
Legal Values	• 0 (no redundancy) • 1 (AC redundancy) • 2 (power supply redundancy)
Default	0 (no redundancy)

cfgChassisDynamicPSUEngagementEnable (Read/Write)

Table 317. Details of cfgChassisDynamicPSUEngagementEnable

Description	Enables or disables dynamic engagement.
Legal Values	• 0 (disabled) • 1 (enabled)
Default	0 (disabled)

cfgChassisInMaxPowerCapacity (Read Only)

Table 318. Details of cfgChassisInMaxPowerCapacity

Description	Indicates the total chassis power budget (in watts) available for chassis operation.
Legal Values	None
Default	None

cfgChassisInRedundancyReserve (Read Only)

Table 319. Details of cfgChassisInRedundancyReserve

Description	Indicates the amount of redundant power (in Watt) in reserve that can be utilized in the event of an AC grid or PSU failure. This value is 0 if the Redundancy Policy is set to 0 (no redundancy).
Legal Values	0 (disabled) 1 (enabled)
Default	None

cfgChassisInPowerServerAllocation (Read Only)

Table 320. Details of cfgChassisInPowerServerAllocation

Description	Indicates (in Watt) the cumulative power allocated to servers. There is no default as this parameter is very specific to the particular customer configuration.
Legal Values	None
Default	None

cfgChassisInfrastructureInPowerAllocation (Read Only)

Table 321. Details of cfgChassisInfrastructureInPowerAllocation

Description	Indicates the estimated cumulative DC output power consumption (in watts), determined from a field replaceable unit (FRU) on the hardware modules in the chassis.
Legal Values	None
Default	None

cfgChassisTotalInPowerAvailable (Read Only)

Table 322. Details of cfgChassisTotalInPowerAvailable

Description	Indicates the amount of power (in Watt) available for use by the chassis.
Legal Values	None

Table 322. Details of cfgChassisTotalInPowerAvailable (continued)

Default	None

cfgChassisStandbyInPowerCapacity (Read Only)

Table 323. Details of cfgChassisStandbyInPowerCapacity

Description	Indicates the amount of power (in Watt) available for turning on any hardware modules that are either added to the chassis or if they are already present in the chassis.
Legal Values	None
Default	None

cfgChassisPowerClear (Write Only)

Table 324. Details of cfgChassisPowerClear

Description	Resets **cfgChassisMinPower** and **cfgChassisMaxPowerCapacity**, when set to **1**.
Legal Values	None
Default	None

cfgChassisPowerClearTimestamp (Read Only)

Table 325. Details of cfgChassisPowerClearTimestamp

Description	Time stamp when **cfgChassisMinPower** and **cfgChassisMaxPowerCapacity** were reset.
Legal Values	None
Default	None

cfgChassisPowerButtonEnable (Read/Write)

Table 326. Details of cfgChassisPowerButtonEnable

Description	Indicates if the chassis power button is enabled or disabled.
Legal Values	• 0 (disabled) • 1 (enabled)
Default	None

cfgSystemEnergyConsumptionClear (Write Only)

Table 327. Details of cfgSystemEnergyConsumptionClear

Description	Resets energy statistics when set to 1.

Table 327. Details of cfgSystemEnergyConsumptionClear (continued)

Legal Values	None
Default	None

Examples

- ```
  racadm getconfig -g cfgChassisPower
  # cfgChassisInPower=0 W | 0 BTU/hr
  # cfgChassisPeakPower=0 W
  # cfgChassisPeakPowerTimestamp=06:32:55 01/26/2009
  # cfgChassisMinPower=0 W
  # cfgChassisMinPowerTimestamp=06:32:55 01/26/2009
  # cfgChassisPowerStatus=5
  # cfgChassisRedundantState=0
  cfgChassisPowerCap=16685 W
  cfgChassisPowerCapF=16685 W
  cfgChassisPowerCapBTU=56931 BTU/hr
  cfgChassisPowerCapFBTU=56931 BTU/hr
  cfgChassisPowerCapPercent =100%
  cfgChassisPowerCapFPercent =100%
  cfgChassisRedundancyPolicy=0
  cfgChassisDynamicPSUEngagementEnable=0
  # cfgChassisInMaxPowerCapacity=0 W
  # cfgChassisInRedundancyReserve=0 W
  # cfgChassisInPowerServerAllocation=0 W
  # cfgChassisInfrastructureInPowerAllocation=51 W
  # cfgChassisTotalInPowerAvailable=0 W
  # cfgChassisStandbyInPowerCapacity=0 W
  # cfgChassisPowerClear=******** (Write-Only)
  # cfgChassisPowerClearTimestamp=18:00:00 12/31/1969
  cfgChassisServerBasedPowerMgmtMode=0
  cfgChassisPowerButtonEnable=1
  cfgChassisAllow110VACOperation=0
  cfgChassisMaxPowerConservationMode=0
  cfgChassisPerformanceOverRedundancy=1
  # cfgSystemEnergyConsumptionClear = ****(Write-Only)
  cfgChassisServerBasedPowerMgmtMode=0
  ```
- ```
  racadm config -g cfgChassisPower -o cfgChassisPowerClear 1
  ```

  Clears **cfgChassisMinPower** and **cfgChassisPeakPower**.

cfgChassisServerBasedPowerMgmtMode

Table 328. Details of cfgChassisServerBasedPowerMgmtMode

Description	Indicates the server-based power management mode of a chassis.
Legal Values	• 0 (disabled) • 1 (enabled)
Default	0 (disabled)

cfgChassisPowerCapBTU (Read/Write)

Table 329. Details of cfgChassisPowerCapBTU

Description	Indicates the maximum power consumption limit (in BTU/hr) for the entire chassis. The command generates an error if server throttling is necessary to achieve the power goal based on the value for this setting.

Table 329. Details of cfgChassisPowerCapBTU (continued)

Legal Values	9264 - 56931 BTU/hr
Default	43221 BTU/hr

cfgChassisACPowerRecoveryDisable

Table 330. Details of cfgChassisACPowerRecoveryDisable attribute

Description	If AC power recovery is disabled, the chassis is powered off after power outage is restored.
Legal Values	• 0 — Enable • 1 — Disable
Default	0

cfgKVMInfo

This group is used to view the mapping information for the KVM.

Use this object with the config or getconfig subcommands.

To use this object property, you must have **Chassis Configuration Administrator** privilege.

cfgKvmMapping (Read/Write)

Table 331. Details of cfgKvmMapping

Description	Maps the slots to the KVM.
Legal Values	1, 2, 3, and 4 are the slot numbers that are specified.
Default	1

cfgKvmSlot<num>Enable (Read/Write)

Table 332. Details of cfgKvmSlot<num>Enable

Description	Enable the slots (1 to 4) to access using KVM: • `cfgKvmSlot1Enable` • `cfgKvmSlot2Enable` • `cfgKvmSlot3Enable` • `cfgKvmSlot4Enable`
Legal Values	0 disables the mapping and 1 enables the mapping.
Default	None

cfgDvdInfo

This group is used to view the mapping information for the DVD drive in the chassis.

Use this object with the config or getconfig subcommands.

To use this object property, you must have the **Chassis Configuration Administrator** privilege.

cfgDvdMapping (Read/Write)

Table 333. Details of cfgDvdMapping

Description	Maps the slots to the DVD drive in the chassis:
Legal Values	1, 2, 3, and 4 are the slot numbers that are specified.
Default	1

cfgDvdSlot<num>Enable (Read/Write)

Table 334. Details of cfgDvdSlot<num>Enable

Description	Enable the slots (1 to 4) to access the DVD: • `cfgDvdSlot1Enable` • `cfgDvdSlot2Enable` • `cfgDvdSlot3Enable` • `cfgDvdSlot4Enable`
Legal Values	0 disables the mapping and 1 enables the mapping.
Default	None

cfgLcdInfo

This group is used to view the LCD locale, LCD orientation, and to check if the buttons to navigate through the LCD menu are enabled.

Use this object with the config or getconfig subcommands.

To use this object property, you must have the **Chassis Configuration Administrator** privilege.

The legal values when you run the `getconfig -g cfgLcdInfo` to view information about the following are:

- cfgLcdLocale=es
- cfgLcdOrientation=0
- cfgLcdButtonsEnable=1

cfgAlerting

This group is enables or disables SNMP event trap alerting and sets the event filter.

Use this object with the config or getconfig subcommands.

cfgAlertingEnable

Table 335. Details of cfgAlertingEnable

Description	Enables or disables event traps on the CMC.
Legal Values	• 1 (true) • 0 (false)
Default	None

To use this object property, you must have the **Chassis Configuration Administrator** privilege.

cfgAlertingSourceEmailName

Table 336. Details of cfgAlertingSourceEmailName

Description	Specifies the e-mail address used to send e-mail notifications when an event occurs.
Legal Values	Valid e-mail address
Default	None

Examples

```
racadm getconfig -g cfgAlerting -o cfgAlertingSourceEmailName
```

```
racadm config -g cfgAlerting -o cfgAlertingSourceEmailName user@home.com
```

```
Object value modified successfully.
```

To use this object property, you must have Chassis Configuration Administrator and Test Alert User privileges.

cfgIPv6LanNetworking

This group is used to configure the IPv6 over LAN networking capabilities.

Use this object with the **config** or **getconfig** subcommands.

To use this object property for CMC, you must have the **Chassis Configuration Administrator** privilege.

The following sections provide information about the objects in the **cfgIPv6LanNetworking** group.

cfgIPv6Enable (Read/Write)

Table 337. Details of cfgIPv6Enable

Description	Enables or disables the IPv6 stack.
Legal Values	· 1 (TRUE) · 0 (FALSE)
Default	0

cfgIPv6AutoConfig (Read/Write)

Table 338. Details of cfgIPv6AutoConfig

Description	Enables or disables the **IPv6 Auto Configuration** option. **NOTE: If this value is set to 0, the CMC disables auto configuration and statically assigns IPv6 addresses. If this value is set to 1, the CMC obtains address and route information using stateless auto configuration and DHCPv6.**

Table 338. Details of cfgIPv6AutoConfig (continued)

	NOTE: The CMC uses its MAC address for its DUID (DUID-LL) when communicating with a DHCPv6 server.
Legal Values	• 1 (TRUE) • 0 (FALSE)
Default	1

cfgIPv6Address

Table 339. Details of cfgIPv6Address

Description	Assigns a static IPv6 address to the CMC. This property is used only if **cfgIPv6AutoConfig** is set to 0 (false).
Legal Values	A string representing a valid IPv6 address. For example, 2001:DB8:1234:5678:9ABC:DE11:C00C:BEEF
Default	::

cfgIPv6PrefixLength (Read/Write)

Table 340. Details of cfgIPv6PrefixLength

Description	Specifies the prefix length for IPv6 address. **NOTE: This property is used only if cfgIPv6AutoConfig is set to 0 (false)**
Legal Values	0–128
Default	64

cfgIPv6Gateway (Read/Write)

Table 341. Details of cfgIPv6Gateway

Description	CMC gateway IPv6 address. **NOTE: This property is used only if cfgIPv6AutoConfig is set to 0 (false.)**
Legal Values	Specifies string representing a valid IPv6 entry.
Default	::

cfgIPv6DNSServersFromDHCP6 (Read/Write)

Table 342. Details of cfgIPv6DNSServersFromDHCP6

Description	Specifies whether **cfgIPv6DNSServer1** and **cfgIPv6DNSServer2** are static or DHCP IPv6 addresses.

Table 342. Details of cfgIPv6DNSServersFromDHCP6 (continued)

	NOTE: This property is used only if cfgIPv6AutoConfig is set to 1 (true).
Legal Values	1 (TRUE) 0 (FALSE)
Default	1

cfgIPv6DNSServer1 (Read/Write)

Table 343. Details of cfgIPv6DNSServer1

Description	Specifies the IPv6 DNS server address. NOTE: This property is used only if cfgIPv6DNSServersFromDHCP6 is set to 0 (false).
Legal Values	A string representing a valid IPv6 entry. For example, 2001:DB8:1234:5678:9ABC:DE11:C00C:BEEF
Default	::

cfgIPv6DNSServer2 (Read/Write)

Table 344. Details of cfgIPv6DNSServer2

Description	Specifies the IPv6 DNS server address. NOTE: This property is only valid if cfgIPv6DNSServersFromDHCP6 is set to 0 (false).
Legal Values	A string representing a valid IPv6 entry. For example, 2001:DB8:1234:5678:9ABC:DE11:C00C:BEEF
Default	::

Example

```
$ racadm getconfig -g cfgIPv6LanNetworking

cfgIPv6Enable=1

cfgIPv6AutoConfig=1

cfgIPv6Address=::

cfgIPv6PrefixLength=64

cfgIPv6Gateway=::

cfgIPv6DNSServersFromDHCP6=1

cfgIPv6DNSServer1=::

cfgIPv6DNSServer2=::
```

If both IPv4 and IPv6 are enabled on the CMC, IPv6 DNS servers take priority. The order of preference for DNS servers is:

- cfgIPv6DNSServer1
- cfgIPv6DNSServer2
- cfgDNSServer1
- cfgDNSServer2

cfgCurrentLanNetworking (Read Only)

This group displays the current CMC NIC properties.

Use this object with the **getconfig** subcommand.

To use this object property, you must have the **CMC Login User** privilege.

Synopsis

```
racadm getconfig -g cfgCurrentLanNetworking
```

cfgNicCurrentIPv4Enabled

Table 345. Details of cfgNicCurrentIPv4Enabled

Description	Indicates whether IPv4 is enabled on the CMC. If the current property value is set to 0 (false), the remote network interfaces to the CMC are not accessible over IPv4.
Legal Values	None
Default	None

Example

```
racadm getconfig -g cfgCurrentLanNetworking
# cfgNicCurrentIPv4Enabled=1
# cfgNicCurrentIpAddress=143.166.152.116
# cfgNicCurrentNetmask=255.255.255.0
# cfgNicCurrentGateway=143.166.152.1
# cfgNicCurrentDhcpWasUsed=0
```

```
# cfgNicCurrentVlanEnable=0
# cfgNicCurrentVlanID=1
# cfgNicCurrentVlanPriority=0
# cfgDNSCurrentServer1=192.168.0.5
# cfgDNSCurrentServer2=192.168.0.6
# cfgDNSCurrentDomainName=MYDOMAIN
```

cfgNicCurrentIpAddress

Table 346. Details of cfgNicCurrentIpAddress

Description	Displays the static IP address to the CMC.
Legal Values	None
Default	None

cfgNicCurrentNetmask

Table 347. Details of cfgNicCurrentNetmask

Description	Displays the static subnet mask for the CMC IP address.
Legal Values	None
Default	None

cfgNicCurrentGateway

Table 348. Details of cfgNicCurrentGateway

Description	Displays the static gateway for the CMC IP address.
Legal Values	None
Default	None

cfgNicCurrentDhcpWasUsed

Table 349. Details of cfgNicCurrentDhcpWasUsed

Description	Indicates whether DHCP is used to configure the NIC.
Legal Values	0 – address is static. 1– address was obtained from the DHCP server.
Default	None

cfgNicCurrentVlanEnable (Read Only)

Table 350. Details of cfgNicCurrentVlanEnable

Description	Indicates whether the VLAN is enabled.
Legal Values	0- VLAN is disabled 1- VLAN is enabled
Default	None

cfgNicCurrentVlanID (Read Only)

Table 351. Details of cfgNicCurrentVlanID

Description	Indicates the Current Virtual Lan ID
Legal Values	Integer
Default	None

cfgNicCurrentVlanPriority (Read Only)

Table 352. Details of cfgNicCurrentVlanPriority (Read Only)

Description	Indicates the Current Virtual Lan Priority.
Legal Values	Integer
Default	None

cfgDNSCurrentServer1

Table 353. Details of cfgDNSCurrentServer1

Description	Displays the IP address for DNS server 1.
Legal Values	A Valid IPv4 DNS IP
Default	None

cfgDNSCurrentServer2

Table 354. Details of cfgDNSCurrentServer2

Description	Displays the IP address for DNS server 2.
Legal Values	None
Default	None

cfgDNSCurrentDomainName

Table 355. Details of cfgDNSCurrentDomainName

Description	Displays the DNS domain name.
Legal Values	
Default	

cfgCurrentIPv6LanNetworking (Read Only)

This group displays the current CMC IPv6 properties.

Use this object with the **getconfig** subcommand.

To use this object property, you must have the **CMC Login User** privilege.

cfgCurrentIPv6Enabled

Table 356. Details of cfgCurrentIPv6Enabled

Description	Indicates whether IPv6 is enabled on the CMC. If the current property value is set to 0 (false), the remote network interfaces to the CMC are not accessible over IPv6.
Legal Values	None
Default	None

cfgCurrentIPv6AutoConfigWasUsed

Table 357. Details of cfgCurrentIPv6AutoConfigWasUsed

Description	Indicates whether auto configuration is used to obtain IPv6 settings, including stateless IPv6 address(es) and gateway.
Legal Values	0 (static addressing is used) 1 (address is obtained from the DHCPv6 server and/or stateless auto configuration)
Default	None

cfgCurrentLinkLocalAddress

Table 358. Details of cfgCurrentLinkLocalAddress

Description	Displays the current IPv6 link-local address of the CMC.
Legal Values	None
Default	None

cfgCurrentIPv6Address

Table 359. Details of cfgCurrentIPv6Address

Description	Displays the current IPv6 addresses. This property displays up to 15 global IPv6 addresses, including stateful and stateless addresses.
Legal Values	None
Default	None

cfgCurrentIPv6Gateway

Table 360. Details of cfgCurrentIPv6Gateway

Description	Displays the current IPv6 gateway.
Legal Values	None
Default	None

cfgCurrentIPv6DNSServersFromDHCP6

Table 361. Details of cfgCurrentIPv6DNSServersFromDHCP6

Description	Indicates whether the DNS server addresses are assigned from the DHCPv6 server.
Legal Values	None
Default	None

cfgCurrentIPv6DNSServer1

Table 362. Details of cfgCurrentIPv6DNSServer1

Description	Displays the IPv6 address for DNS server 1.
Legal Values	None
Default	None

cfgCurrentIPv6DNSServer2

Table 363. Details of cfgCurrentIPv6DNSServer2

Description	Displays the IPv6 address for DNS server 2.
Legal Values	None
Default	None

Example

```
racadm getconfig -g cfgCurrentIPv6LanNetworking
# cfgCurrentIPv6Enabled=1
# cfgCurrentIPv6AutoConfigWasUsed=1
# cfgCurrentLinkLocalAddress=fe80::21e:4fff:fe1f:5371/64
# cfgCurrentIPv6Address1=2009:123::e48f:9dd8:6f51:a669/64
# cfgCurrentIPv6Address2=fd88:1::21e:4fff:fe1f:5371/64
# cfgCurrentIPv6Address3=fd88:2::21e:4fff:fe1f:5371/64
# cfgCurrentIPv6Gateway=fe80::21c:23ff:fe77:6215
# cfgCurrentIPv6DNSServersFromDHCP6=1
# cfgCurrentIPv6DNSServer1=2009:123::1
# cfgCurrentIPv6DNSServer2=::
```

cfgNetTuning

This group enables users to configure the advanced network interface parameters for the RAC NIC or CMC. When configured, the updated settings may take up to a minute to become active.

The following sections provide information about the objects in the **cfgNetTuning** group.

CAUTION: Use extra precaution when modifying properties in this group. Inappropriate modification of the properties in this group can result in your RAC NIC become inoperable.

cfgNetTuningNicSpeed

Table 364. Details of cfgNetTuningNicSpeed

Description	Specifies the speed for the CMC NIC. This property is used only if **cfgNetTuningNicAutoNeg** is set to 0.
Legal Values	10, 100, or 1000
Default	100

cfgNetTuningNicFullDuplex (Read/Write)

Table 365. Details of cfgNetTuningNicFullDuplex

Description	Specifies the duplex setting for the RAC or CMC NIC. This property is used only if the **cfgNetTuningNicAutoNeg** is set to 0 (disabled).
Legal Values	• 0 (Half Duplex) • 1 (Full Duplex)
Default	1

cfgNetTuningNicMtu (Read/Write)

Table 366. Details of cfgNetTuningNicMtu

Description	The size in bytes of the maximum transmission unit used by CMC NIC.
Legal Values	576 – 1500

Table 366. Details of cfgNetTuningNicMtu (continued)

Default	1500

NOTE: IPv6 requires a minimum MTU of 1280. If IPv6 is enabled, and cfgNetTuningMtu is set to a lower value, the CMC uses an MTU of 1280.

cfgNetTuningNicAutoneg (Read/Write)

Table 367. Details of cfgNetTuningNicAutoneg

Description	Enables autonegotiation of physical link speed and duplex. If enabled, autonegotiation takes priority over other values set in this group.
Legal Values	• 0 = Auto Negotiation is Disabled • 1 = Auto Negotiation is Enabled
Default	1

Example

```
racadm getconfig -g cfgNetTuning
```

```
cfgNetTuningNicSpeed=100
cfgNetTuningNicFullDuplex=1
cfgNetTuningNicMtu=1500
cfgNetTuningNicAutoneg=1
```

cfgRacSecurity

This group is used to configure settings related to CMC SSL certificate signing request (CSR) feature. The properties in this group must be configured before generating a CSR from CMC.

Use this object with the config or getconfig subcommands.

To use this object property, you must have **Chassis Configuration Administrator** privilege.

For more information on generating certificate signing requests, see the subcommand "sslcsrgen."

The following sections provide information about the objects in the **cfgRacSecurity** group.

cfgRacSecCsrCommonName (Read/Write)

Table 368. Details of cfgRacSecCsrCommonName

Description	Specifies the CSR Common Name (CN) that must be an IP or CMC name as given in the certificate.
Legal Values	A string of up to 64 characters.
Default	<blank>

cfgRacSecCsrOrganizationName (Read/Write)

Table 369. Details of cfgRacSecCsrOrganizationName

Description	Specifies the CSR Organization Name (O).
Legal Values	A string of up to 64 characters.
Default	<blank>

cfgRacSecCsrOrganizationUnit (Read/Write)

Table 370. Details of cfgRacSecCsrOrganizationUnit

Description	Specifies the CSR Organization Unit (OU).
Legal Values	A string of up to 64 characters.
Default	<blank>

cfgRacSecCsrLocalityName (Read/Write)

Table 371. Details of cfgRacSecCsrLocalityName

Description	Specifies the CSR Locality (L).
Legal Values	A string of up to 128 characters.
Default	<blank>

cfgRacSecCsrStateName (Read/Write)

Table 372. Details of cfgRacSecCsrStateName

Description	Specifies the CSR State Name (S).
Legal Values	A string of up to 128 characters.
Default	<blank>

cfgRacSecCsrCountryCode (Read/Write)

Table 373. Details of cfgRacSecCsrCountryCode

Description	Specifies the CSR Country Code (CC).
Legal Values	A string of 2 alphabet country code.
Default	US

cfgRacSecCsrEmailAddr (Read/Write)

Table 374. Details of cfgRacSecCsrEmailAddr

Description	Specifies the CSR email address.
Legal Values	A string of up to 64 characters in email format.
Default	*<blank>*

Example

```
racadm config -g cfgRacSecurity
```

```
cfgRacSecCsrKeySize=1024
cfgRacSecCommonName=CommonName
cfgRacSecOrganizationName=OrgName
cfgRacSecOrganizationUnit=OrgUnit
cfgRacSecLocalityName=LocalityName
cfgRacSecStateName=StateName
cfgRacSecCountryCode=US
cfgRacSecEmailAddr=Name@domain.com
```

cfgRacSecCsrKeySize (Read/Write)

Table 375. Details of cfgRacSecCsrKeySize

Description	Specifies the SSL asymmetric key size for the CSRs.
Legal Values	1024, 2048, and 4096
Default	2048

cfgQuickDeploy

This group is used to configure IDRAC deployment settings. You must have blade administrator privileges for configuring the settings.

cfgActionOnServerInsertion

Table 376. Details of cfgActionOnServerInsertion attribute

Description	Configures settings when a new server is inserted into the slot.
Legal Values	• 0 — No Action • 1 — QuickDeploy Only • 2 — Server Profile Only • 3 — Quick Deploy and Server Profile
Default	0

cfgSetiDRACRootPasswordOnServerInsertion

Table 377. Details of cfgSetiDRACRootPasswordOnServerInsertion attribute

Description	Sets the iDRAC root password when a server is inserted into the chassis.
Legal Values	• 0 (False) — If the value is '1' when the server is inserted, the iDRAC root password is not set. • 1 (True) — If the value is '1' when the server is inserted, the iDRAC root password is set.
Default	0

cfgiDRACRootPassword

Table 378. Details of cfgiDRACRootPassword attribute

Description	The root password is applied when servers are inserted into the chassis.
Legal Values	Up to 64 characters.
Default	calvin

cfgEnableiDRACLAN

Table 379. Details of cfgEnableiDRACLAN attribute

Description	Enables the LAN channel for iDRAC when servers are inserted into the chassis.
Legal Values	• 0 — Disable • 1 — Enable
Default	1

cfgEnableiDRACIPv4

Table 380. Details of cfgEnableiDRACIPv4 attribute

Description	Enables IPv4 for each iDRAC in the chassis. Any iDRAC that is not IPv6 is always IPv4 enabled.
Legal Values	• 0 — Disable • 1 — Enable
Default	1

cfgEnableiDRACIPMIOverLAN

Table 381. Details of cfgEnableiDRACIPMIOverLAN attribute

Description	Enables IPMI over LAN channel for iDRAC when servers are inserted into the chassis.

Table 381. Details of cfgEnableiDRACIPMIOverLAN attribute (continued)

Legal Values	• 0 — Disable • 1 — Enable
Default	0

cfgEnableiDRACIPv4DHCP

Table 382. Details of cfgEnableiDRACIPv4DHCP attribute

Description	Enables DHCP for iDRAC when servers are inserted into the chassis.
Legal Values	• 0 — Disable • 1 — Enable
Default	1

cfgStartingiDRACIPv4Address

Table 383. Details of cfgStartingiDRACIPv4Address attribute

Description	The static IPv4 address for the iDRAC located in the first slot.
Legal Values	IP format
Default	192.168.0.121

cfgiDRACIPv4GateWay

Table 384. Details cfgiDRACIPv4GateWay attribute

Description	IPv4–specific default gateway that is common to all the IPv4–enabled iDRACs present in the chassis.
Legal Values	IP format
Default	0.0.0.0

cfgiDRACIPv4Netmask

Table 385. Details of cfgiDRACIPv4Netmask attribute

Description	IPv4–specific subnet mask that is common to all iDRACs present in the chassis.
Legal Values	IP format
Default	255.255.255.0

cfgEnableiDRACIPv6

Table 386. Details cfgEnableiDRACIPv6 attribute

Description	Enables IPv6 for each IPv6-capable iDRAC present in the chassis.
Legal Values	• 0 — Disable • 1 — Enable
Default	0

cfgEnableiDRACIPv6AutoConfig

Table 387. Details of cfgEnableiDRACIPv6AutoConfig attribute

Description	Enables the IPv6 feature that allows each iDRAC present in the chassis to set its IPv6 address automatically, without manual configuration of the host or DHCP servers.
Legal Values	• 0 — Disable • 1 — Enable
Default	0

cfgiDRACIPv6PrefixLength

Table 388. Details of cfgiDRACIPv6PrefixLength attribute

Description	The length of the subnet in bits that is common to all IPv6-enabled iDRACs present in the chassis.
Legal Values	0–128
Default	64

cfgiDRACIPv6Gateway

Table 389. Details of cfgiDRACIPv6Gateway attribute

Description	IPv6-specific default gateway that is common to all IPv6-enabled iDRACs present in the chassis.
Legal Values	IPv6 format
Default	::

cfgReservedIPAddressNumbers

Table 390. Details of cfgReservedIPAddressNumbers attribute

Description	The number of static IPv4 addresses reserved for iDRACs in the chassis.
Legal Values	32

Table 390. Details of cfgReservedIPAddressNumbers attribute (continued)

Default	32

cfgUseCMCDNSSettings

Table 391. Details of cfgUseCMCDNSSettings attribute

Description	Propagates the CMC DNS Server settings (IPv4 and IPv6) to iDRAC when a blade server is inserted in the chassis.
Legal Values	• 0 — False • 1 — True
Default	0

cfgServerDNSIMCNameEnable

Table 392. Details of cfgServerDNSIMCNameEnable attribute

Description	Enables or disables configuration of the iDRAC DNS name prefix for blade servers that you want to insert in the chassis. **NOTE: You can set the `cfgServerDNSIMCNamePrefix` only if the `cfgServerDNSIMCNameEnable` is set to 1. Else, an error message is displayed.**
Legal Values	• 0—Disable • 1—Enable
Default	0

cfgServerDNSIMCNamePrefix

Table 393. Details of cfgServerDNSIMCNamePrefix attribute

Description	Enables you to specify the iDRAC DNS name prefix for blade servers that you want to insert in the chassis. **NOTE: You can set the `cfgServerDNSIMCNamePrefix` only if the `cfgServerDNSIMCNameEnable` is set to 1. Else, an error message is displayed.** **NOTE: The maximum length of the `cfgServerDNSIMCNamePrefix` is 59 characters. The hyphen (–) is the only special character allowed for setting the prefix.**
Legal Values	N/A
Default	N/A