Dell Chassis Management Controller Version 2.10 for PowerEdge FX2 and FX2s

RACADM CLI Guide

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.

2018 - 06

Rev. A02

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 FX2/FX2s.

NOTE: The terms "storage sled" and "storage module" are used interchangeably in this document.

Topics:

What's new in this release

- Increased the number of support characters in slot names to 24.
- Added a new command, `cfgRacTuneSMBVersionEnable`, to the `cfgRacTuning` group.
- Added a new attribute, `testcifsshare`, to check whether the CIFS share is working with the current SMB version.

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 **dell.com/support**.

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 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.

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 <racIpAddr> -u <username> -p <password> getconfig -g <groupname> [-o
<objectname>] [-i <indexnumber>]
```

```
racadm -r <racIpAddr> -u <username> -p <password> <subcommand>
```

Example

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

```
racadm -r <racIpAddr> -u myuser -p mypass getsysinfo
```

RACADM Command Options

Table 1. Command options and their deception

Option	Description
-r *<racIpAddr>*	Specifies the controller's remote IP address.
-u *<usrName>*	Specifies the user name that is used to authenticate the command transaction. If the **-u** option is used, the **-p** option must be used, and the **-i** option 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 used to authenticate the command transaction. If the **-p** option is used, the **-i** option is not allowed.
-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.

Table 2. RACADM interfaces

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

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

Displayable Characters

Displayable characters include the following set:

```
abcdefghijklmnopqrstuvwxwz

ABCDEFGHIJKLMNOPQRSTUVWXYZ

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

Supported RACADM Subcommands

Table 3. Details of Subcommands

Subcommand	CMC	
	Telnet/SSH/Serial	Remote RACADM
“?” and “?<subcommand>”	Yes	Yes
chassisaction	Yes	Yes
chassislog	Yes	Yes
closessn	Yes	Yes
clrsel	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	Yes	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

Subcommand	CMC	
getpminfo	Yes	Yes
getraclog	Yes	Yes
getractime	Yes	Yes
getsel	Yes	Yes
getsleduplinkstatus	Yes	Yes
getsensorinfo	Yes	Yes
getslotname	Yes	Yes
getssninfo	Yes	Yes
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
racresetcfg	Yes	Yes
remoteimage	Yes	Yes
serveraction	Yes	Yes
set	Yes	Yes
setassettag	Yes	Yes
setflexaddr	Yes	Yes
setled	Yes	Yes
setniccfg	Yes	Yes
setractime	Yes	Yes
setslotname	Yes	Yes
setsysinfo	Yes	Yes
sshpkauth	Yes	Yes
sslkeyupload	No	Yes
sslcertview	Yes	Yes
sslcsrgen	Yes	Yes

Subcommand	CMC	
sslresetcfg	Yes	Yes
testemail	Yes	Yes
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 *CMC FX2/FX2s 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 FX2/FX2s User's Guide* provides information about using the FX2/FX2s–related Web interface features.
- The *Dell Chassis Management Controller (CMC) for Dell PowerEdge FX2/FX2s 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 7 (iDRAC7) 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.
- 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 FX2/FX2s 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 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.

2

RACADM Subcommand Details

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

Topics:

- getsensorinfo
- getssninfo
- getstoragemoduleinfo
- getsvctag
- getsysinfo
- gettracelog
- getversion
- ifconfig
- jobqueue
- krbkeytabupload
- license
- netstat
- ping
- ping6
- racdump
- racreset
- racresetcfg
- remoteimage
- serveraction
- set
- setassettag
- setchassisname
- setflexaddr
- setled
- setniccfg
- setractime
- setslotname
- setsysinfo
- SSH or Telnet RACADM
- sshpkauth
- sslkeyupload
- sslcertupload
- sslcertview
- sslcsrgen
- sslresetcfg
- 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 double quotation marks:

- $ (dollar sign)
- " (double quotation mark)
- ` (backward quotation mark)
- \ (backward slash)
- ~ (tilde)
- | (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 double quotation marks.

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

For using double quotation marks:

The following characters must be escaped by prepending a backward slash:

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

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

For using 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).

Question mark and question mark with subcommand

Table 4. Details of Question mark and question mark with subcommand

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
clrraclog        -- clear the CMC log
clrsel           -- clear the System Event Log (SEL)
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 with subcommand

Table 5. Details of help and help with subcommand

Description	Lists all the subcommands available for use with **RACADM** and provides a short description for each. You may also type a subcommand, group, object, or FQDD alternate name after **help**.
Synopsis	• `racadm help` • `racadm help <subcommand>`
Input	None

Output

- The **help** command displays a complete list of subcommands.
- The racadm **help <*subcommand*>** command displays information for the specified subcommand only.
- The racadm **help -g <*groupname*>** command displays information for the specified group.
- The racadm **help -o <*objectname*>** command displays information for the specified object.
- The racadm **help <*FQDD Alias*>.<*Group*>** command displays information for the specified group.
- The racadm **help <*FQDD Alias*>.<*Object*>** command displays information for the specified object.
- The racadm **help <*FQDD Alias*>.<*Group*>.<*Object*>** command displays information for the specified object.

Example

```
racadm help system.power
```

```
racadm help system.power.supply
```

chassislog

Table 6. Details of 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.

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
  - Updates
  - Audit
  - Config
- `-b` — The subcategory used to filter the records. Provide multiple subcategories using a "," as the delimiter. The value is case-insensitive.
- `-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.
- `-s` — The severity used to filter the records. Provide multiple severities using a "," as the delimiter. The value is case-insensitive. Valid Severity values:
  - 1. Warning
  - 2. Critical
  - 3. Info

NOTE: To view or export the Chassis log, only CMC Login User permission is required.

Example

- Display the number of records present in the Chassis Log:

```
racadm chassislog view -i
```

- 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. Details of chassislog export

Description

Exports the Chassis log to a remote share.

Synopsis

```
racadm chassislog export -f<filename> -u<username> -p<password> -
l<CIFS or NFS share>
racadm -r<cmcip> -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.
- `-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. Details of 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 <cmcip> -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 192.168.0.1 -u root -p <default root user password> chassislog clear`
	
	NOTE: The default local account credential is root (user name) and calvin (user password).

chassisaction

Table 9. Details of chassisaction

Description	Runs a power action on the chassis or a switch. To use this subcommand, you must have the **Chassis Control Administrator** privilege.
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. – **switch-n**, where n=1 to 2 • <*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. Details of 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 executing 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. Details of 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 [-m <module>]`
Input	`-m` — The `<module>` option can have the following values: • `server-<n>` where, n = 1 to 4 • `server-<nx>` where n = 1 to 4 and x = a to d (lower case) **NOTE: n= 2 and 4 are valid only for multinode sleds.**

Example	• Clear cmc sel log:
	`racadm clrsel`
	• Clear sel log on server 1:
	`racadm clrsel -m server-1`

- Clear sel log on server 2a:

```
racadm clrsel -m server-2a
```

config

Table 12. Details of 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 <*group name*> -o <*object name*> [-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.
- `-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 running 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 192.168.0.1.`

  Sets the **cfgNicIpAddress** configuration parameter (object) to the value 192.168.0.1. 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 13. 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 to 4
- `server –<nx>`: where `n` = 1 to 4 and `x` = a to d (lower case)

  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>

Examples

- 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 14. Details of deploy

Description

Deploys blade server or IOM by specifying the required properties.

To use this subcommand, you must have the **Server Administrator** privilege.

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>`

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, HDD, CD-DVD, vFDD, vCD-DVD, 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** — server/switch. Applies options to all modules present in the chassis of the given module type. Specify the value as server or switch. Default value is `server`. Switches must support Ethernet Management.
- **-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. Required **Username** when you are setting IOA values.
- **-m** < *module* > — Specifies the server you want to configure.

  Legal value must be one of the following values:
  - server-n where *n*=1–4
  - switch-n where *n*=1–2.
- **-p** < *password* > — Specifies the password for the root user on the server or switch.

  Legal values: For switches, valid passwords are 6 - 32 ASCII characters in length, ranging in value 32–125 (decimal). For servers, valid passwords are 1 – 20 ASCII characters in length, ranging in value 32 – 126 (decimal).
- **-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.
  - 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).
- **-v** —SNMPv2 community string. Valid community strings are 1–20 characters in length, with valid ASCII characters in the range [33–125] (decimal). Protocol version set to SNMPv2. Permission on community string is read-only.

  NOTE: This input is available in IOA only.
- **-q**— Displays or modifies the quick deploy parameters.
- **-n**— 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-1 -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-2 192.168.0.11 255.255.255.0 192.168.0.1`

  ERROR: Server in slot 9 is an extension of the server in slot 1.
- `racadm deploy -m server-1 -u root -p <default root user password> -s -6 ::/64 :: 10`

eventfilters

Table 15. 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.

Valid category values are:

- System
- Config
- Updates
- 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, 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: racra

  ```
  racadm eventfilters set -c cmc.alert.all -n none
  ```

- 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 16. 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`

feature

Table 17. 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 the 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 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 18. 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
```

```
CMC: The feature card inserted is valid, serial number =
CN0H871T137401112222A00 The feature card contains the following
feature(s):
FlexAddress: bound
FlexAddressPlus: bound
ExtendedStorage: bound
```

fwupdate

Table 19. Details of fwupdate

Description

Allows you to update the CMC firmware, chassis infrastructure firmware. You can:

- Check the firmware update process status.
- Update the firmware from an 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 CMC firmware resets the CMC, causing all network connections to get logged off.

NOTE: The subcommand generates an error, when used on the extension slot of a multi-slot server.

The CMC firmware performs a signature verification step to ensure the authenticity of the uploaded firmware. The firmware update process is successful only if CMC authenticates the firmware image from the service provider as valid image. The firmware update process is stopped, if CMC cannot verify the signature of the uploaded firmware image. A warning event is then logged, and an appropriate error message is displayed.

NOTE: Run the firmware update command through only one remote racadm session at a time.

Synopsis

- Using Remote RACADM:

  ```
  racadm fwupdate -p -u -d <firmware image>
  ```

  NOTE: iDRAC7 targets are not supported from CMC racadm. 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, the remote RACADM session logs off with the error message `ERROR: Specified path is too long`.

  NOTE: While performing firmware CMC firmware upgrade if the uploaded firmware image file does not contain a verification signature or it contains a verification signature, which is not valid or corrupted, the following message is displayed:

  ```
  Invalid firmware: The firmware image validation was unsuccessful
  ```

  NOTE: While performing CMC firmware downgrade, if the current CMC firmware does not recognize the computed signature of the earlier version, the following message is displayed:

  ```
  Firmware downgrade is unsuccessful: a downgrade to this firmware
  version is not supported
  ```

- `racadm fwupdate -g -u -a 192.168.0.100 -d fx2_cmc.bin -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
  – iominf-n, where n = 1
  – main-board
  – 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 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.

Output

Displays a message indicating the operation that is being performed.

Example

NOTE: The following commands apply to CMC update.

- Upload a firmware image from the client and start firmware update:

```
racadm -r 192.168.0.120 -u root -p calvin fwupdate -p -u -d firmimg.cmc
```

- Upload the firmware image from the TFTP server and start the firmware update:

```
racadm fwupdate -g -u -a 192.168.0.100 -d fx2_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 root <default root password> -d
fx2_cmc.bin -m
```

- Start IOM infrastructure firmware update.

```
racadm fwupdate -u -m iominf-1
```

- View the current firmware update status of all firmware targets:

```
racadm fwupdate -s -m all
```

- View the current firmware update status of a particular module:

```
racadm fwupdate -s -m cmc-active
```

- Cancel a firmware update in progress:

```
racadm fwupdate -c
```

- Signed CMC Firmware Image:

```
racadm fwupdate -g -u -a <TFTP IP> -d <Firmware Path> -m
```

```
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.
```

Table 20. Firmware update methods

FW Update Method	CMC
Local RACADM	No
Local RACADM—TFTP	No
Local RACADM—FTP	No
Remote RACADM	Yes
Remote RACADM—TFTP	Yes
Remote RACADM—FTP	Yes
Firmware RACADM—TFTP	Yes
Firmware RACADM—FTP	Yes

get

Table 21. 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 cannot export the chassis configuration profile to a remote network share with proxy using the `get` command. But, you can export the chassis configuration profile to the local management station.

Synopsis

```
racadm get -f <filename>
```

```
racadm -r <CMC IP> -u <username> -p <password> get -f <filename>
```

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

Input

- `-f`: save 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.
- `-t`: specify the file type that has to be exported. Valid value is “XML”.
- `--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

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
```

getactiveerrors

Table 22. 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 to 2 cmc-n, where n = 1 fan-n, where n = 1 to 8 ps-n, where n = 1 or 2 chassis

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 23. 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 24. 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 25. 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 CMC 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.
- **-m** — Indicates the module on which you want to carry out the action. The —m or *<module>* displays the following information for a particular server, group of servers, individual storage, or storage groups:
  - session
  - WEB/SSH/Telnet
  - remote system log
  - storage mode
  - service tag
  - asset tag

  The *<module>* must have one of the following values:
  - *server-<n>* — where n = 1 to 4
  - *server-<nx>* — where n = 1 to 4 and x = a to d (lower case). The n = 2 and 4 are valid for multi-node sleds only.
  - *storage-<n>* — where n = 1 to 4

  NOTE: The -m option is available only for `cfgRemoteHosts`, `cfgRacTuning`, `cfgSerial`, `cfgSessionManagement`, `cfgLanNetworking`, and `cfgIPv6LanNetworking` commands.
- **-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
  ```
- Saves all group configuration objects from CMC to **myrac.cfg**.

  ```
  racadm getconfig -f myrac.cfg
  ```

  If you do not configure the following key attributes in their respective groups for a particular index, the groups are not saved in to the file. This is applicable for all the index groups.

Table 26. Key attributes

Group	Key Attribute
cfgEmailAlert	cfgEmailAlertAddress
cfgLDAPRoleGroup	cfgLDAPRoleGroupDN
cfgServerInfo	cfgServerBmcMacAddress

Group	Key Attribute
cfgStandardSchema	cfgSSADRoleGroupName
cfgTraps	cfgTrapsAlertDestIPAddr
cfgUserAdmin	cfgUserAdminUserName

- Displays a list of the available configuration groups on CMC 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
```

- Displays the storage sled information.

```
racadm getconfig –g cfgStoragemodule –m storage-3
```

getdcinfo

Table 27. Details of getdcinfo

Description	Displays general I/O module and daughter card configuration information. Only the CMC controls daughter cards. 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 28. Example

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

Table 29. Server- state

<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

getsleduplinkstatus

Table 31. Details of getsleduplinkstatus

Description

Displays multi-node sled network switch uplink status.

Synopsis

```
racadm getsleduplinkstatus
```

Examples

```
racadm getsleduplinkstatus
```

```
Sled No : 2
  Port No               = 3
  A1 Link Status        = Up
  A2 Link Status        = Down

  Port No               = 4
  A1 Link Status        = Up
  A2 Link Status        = Up

Sled No : 3
  Port No               = 5
  A1 Link Status        = Up
  A2 Link Status        = Down

  Port No               = 4
  A1 Link Status        = Up
  A2 Link Status        = Up
```

getflexaddr

Table 32. Details of getflexaddr

Description

Displays enabled or disabled status for the entire chassis. If used with -i, the command displays 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.

Synopsis

```
racadm getflexaddr [-i <slotNum>]
```

Input

-i < *slotNum* > — Specifies the slot information to be displayed. < *slotNum* > must be from 1 to 4.

Table 33. Example

<*Slot#*>	<*Status*>	<*Server Presence*>
1a	Enabled	Present
1b	Enabled	Present
1c	Enabled	Present
1d	Enabled	Not Present
2	Enabled	Present
3a	Disabled	Present
3b	Disabled	Present
3c	Disabled	Present
3d	Disabled	Present
4	Disabled	Present

Table 34. Details

<*Fabric*>	<*Type*>	<*Server-Assigned*>	<*Chassis-Assigned*>
slot1a-idrac	Controller	18:A9:9B:FD:C3:FF	F0:1F:AF:88:21:A0(active)
slot1-A1	10 GbE KR	00:90:FA:51:31:E2	F0:1F:AF:88:21:A1(active)
	10 GbE KR/3	00:90:FA:51:31:E3	F0:1F:AF:88:21:A3(active)
	FCoE-WWN	10:00:00:90:FA:51:31:E3)	20:01:F0:1F:AF:88:21:A3(active)
	10 GbE KR/3	00:90:FA:51:31:E5	F0:1F:AF:88:22:75(active)
	FCoE-WWN	10:00:00:90:FA:51:31:E5	20:01:F0:1F:AF:88:22:75(active)
	10 GbE KR	00:90:FA:51:31:E5	20:01:F0:1F:AF:88:22:73(active)

	10 GbE KR/3	00:90:FA:51:31:E5	F0:1F:AF:88:22:75(active)
	FCoE-WWN	10:00:00:90:FA:51:31:E5	20:01:F0:1F:AF:88:22:75(active)
	10 GbE KR	10:00:00:90:FA:51:31:E5	20:01:F0:1F:AF:88:22:75(active)
	10 GbE KR	00:90:FA:51:31:E7	F0:1F:AF:88:22:77(active)
	10 GbE KR	00:90:FA:51:31:E7	F0:1F:AF:88:22:7B(active)
	10 GbE KR	00:90:FA:51:31:E9	F0:1F:AF:88:22:7D(active)
slot1-A2	10 GbE KR	00:90:FA:51:31:EA	F0:1F:AF:88:21:A2(active)
	10 GbE KR	00:90:FA:51:31:EB	F0:1F:AF:88:21:A4(active)
	10 GbE KR/3	00:90:FA:51:31:EB	F0:1F:AF:88:21:A4(active)
	FCoE-WWN	10:00:00:90:FA:51:31:EB	20:01:F0:1F:AF:88:21:A4(active)
	10 GbE KR/3	00:90:FA:51:31:EC	F0:1F:AF:88:22:74(active)
	10 GbE KR/3	00:90:FA:51:31:EC	F0:1F:AF:88:22:74(active)
	FCoE-WWN	10:00:00:90:FA:51:31:EC	20:01:F0:1F:AF:88:22:74(active)
	10 GbE KR/3	10:00:00:90:FA:51:31:EC	20:01:F0:1F:AF:88:22:74(active)
	10 GbE KR/3	00:90:FA:51:31:ED	F0:1F:AF:88:22:76(active)
	FCoE-WWN	10:00:00:90:FA:51:31:ED	20:01:F0:1F:AF:88:22:76(active)
	10 GbE KR	00:90:FA:51:31:EE	F0:1F:AF:88:22:78(active)
	10 GbE KR	00:90:FA:51:31:EF	F0:1F:AF:88:22:7A(active)
	10 GbE KR	00:90:FA:51:31:EF	F0:1F:AF:88:22:7A(active)
	10 GbE KR	00:90:FA:51:31:F0)	F0:1F:AF:88:22:7C(active)
	10 GbE KR	00:90:FA:51:31:F1	F0:1F:AF:88:22:7E(active)

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

getioinfo

Table 35. Details of getioinfo

Description	Displays general information about the stack and 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 [-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 36. Example 1

<IO>	*<Name>*	*<Type>*	*<Presence>*	*<POST>*	*<Power>*	*<Role>*	*<Secure Mode>*	*<Mode>*
switch-1	N/A	None	Not Present	N/A	N/A	N/A	No	N/A
switch-2	PE	10 Gigabit KR	Present	OK	ON	Master	No	N/A

Table 37. Example 2

<IO>	*<Name>*	*<Type>*	*<Presence>*	*<POST>*	*<Power>*	*<Role>*	*<SecureMode>*	*<Mode>*
Switch-1	1GBE PASS-THROUGH MODULE	Gigabit Ethernet	Present	OK	ON	Master	No	N/A

getled

Table 38. 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 values: • server-<n> where n=1-4

- server-<nx> where n=1-4; x=a-d (lower case)
- switch-n where n=1 or 2
- cmc-active

Example

For CMC:

- `racadm getled -m server-4`
  <*module*> <*LED state*> server-4 Blinking
- `racadm getled -m chassis`
  <*module*> <*LED state*> server-4 Not blinking
- `racadm getled -m server-1`
  <*module*> <*LED state*> server-1 ON
- `racadm getled -m server-1`
  <*module*> <*LED state*> server-1 Extension(1)

getmacaddress

Table 39. Details of getmacaddress

Description

Displays the MAC/WWN addresses for all modules or for a specified module.

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 the **CMC Login User** privilege.

Synopsis

- `racadm getmacaddress`
- `racadm getmacaddress -m chassis`
- `racadm getmacaddress -m switch-<n>`
- `racadm getmacaddress [-m <module>] [-t iscsi] [-x]`
- `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*=1–2
- **-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.
- **-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 `-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 40. MAC address for Chassis

<Name>	*<Presence>*	*<BMC MAC Address>*	*<NIC1 MAC Address>*	*<NIC2 MAC Address>*
CMC	Present	N/A	74:86:7A:D5:33:44	N/A

Table 41. MAC address for switch 1

<Name>	*<Presence>*	*<BMC MAC Address>*	*<NIC1 MAC Address>*	*<NIC2 MAC Address>*
Switch-1	Present	Not Installed	00:00:00:00:00:00	Not Installed

Table 42. MAC address for switch 1

<Name>	*<Presence>*	*<BMC MAC Address>*	*<NIC1 MAC Address>*	*<NIC2 MAC Address>*
Server-1a	Present	F8:DB:88:3E:01:80	F8:DB:88:3E:01:81	F8:DB:88:3E:01:84

Server-1b	Present	F8:DB:88:3E:02:50	F8:DB:88:3E:02:6F	F8:DB:88:3E:02:72
Server-1c	Present	F8:DB:88:3E:08:09	F8:DB:88:3E:01:E9	F8:DB:88:3E:01:EC
Server-1b	Not Present	Not Installed	Not Installed	Not Installed

Table 43. 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
			00:11:43:FD:B7:2C	00:11:43:FD:B7:2D

Table 44. RACADM MAC address

<Name>	*<Type>*	*<Presence>*	*<BMC MAC Address>*	*<NIC1 MAC Address>*	*<NIC2 MAC Address>*
CMC	N/A	Present	N/A	74:86:7A:D5:33:44	N/A
Server-1-A	Gigabit Ethernet	Present	74:86:7A:D6:CF:22	Not Installed	Not Installed
Server-2	Not Installed	Not Present	Not Installed	Not Installed	Not Installed
Server-3-A	10 GbE KR iSCSI FCoE-FIP FCoE-WWN 10 GbE KR	Present Present Present Present Present	74:86:7A:D6:D0:38	E0:DB: 55:25:65:9C E0:DB: 55:25:65:9D E0:DB: 55:25:65:9D 20:01:E0:DB: 55:25:65:9D E0:DB:55:25:65:A0	E0:DB:55:25:65:9E E0:DB:55:25:65:9E E0:DB:55:25:65:9F 20:01:E0:DB: 55:25:65:9F E0:DB:55:25:65:A2
Server-4	Not Installed	Not Present	Not Installed	Not Installed	Not Installed
Switch-1	Gigabit Ethernet	Present	Not Installed	00:00:00:00:00:00	Not Installed

Table 45. Ethernet and iSCSI 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 46. 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 47. MAC/WWN addresses for all LOMs or mezzanine cards

<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	IO-Identity
	Gigabit Ethernet	Present	84:8F:69:FC:E8:F1	Unknown	IO-Identity
Switch-1	10 GbE KR	Present	F8:B1:56:45:DD:BD	N/A	Factory

Table 48. 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	N/A	FlexAddress

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

Table 49. console assigned MAC/WWN of all LOMs or mezzanine cards

<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 50. Details of getmodinfo

Description

Displays configuration and status information for all modules or a specified module (server, storage sled, switch, CMC, fan unit, blower, power supply unit, chassis, 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]ra
```

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
  - `server-nx` , where n = 1 to 4; x = a to d
  - `switch-n` , where n = 1 or 2
  - `pcie-n` , where n = 1 to 8
  - `CMC-n` , where n = 1
  - `fan-n` , where n = 1 to 8
  - `ps-n` , where n = 1 to 2
  - `chassis`
  - `main-board`
  - `io-cable`
  - `fpc cable`

- **-A —** Does not display the headers and labels in the output.

Example

Table 51. Details

<module>	<presence>	<pwrState>	<health>	<svcTag>	<node Id>
Chassis	Present	ON	OK	ST0MP19	N/A
Main-Board	Present	ON	OK	N/A	N/A
Storage-2	Present	OFF	Not OK	6666666	N/A
Storage-3	Present	OFF	Not OK	6666666	N/A
Storage-4	Present	OFF	OK	6666666	N/A
Fan-1	Present	ON	OK	N/A	N/A
Fan-2	Present	ON	Unknown	N/A	N/A
Fan-3	Present	ON	Unknown	N/A	N/A
Fan-4	Present	ON	Unknown	N/A	N/A
Fan-5	Present	ON	OK	N/A	N/A
Fan-6	Present	ON	Unknown	N/A	N/A
Fan-7	Present	ON	Unknown	N/A	N/A
Fan-8	Present	ON	Unknown	N/A	N/A
PS-1	Present	Online	OK	N/A	N/A
PS-2	Present	Online	OK	N/A	N/A
CMC	Present	Primary	OK	N/A	N/A
Switch-1	Present	ON	OK	0000000	N/A
Switch-2	Present	ON	OK	N/A	N/A
Server-1	Present	OFF	OK	H23H23Z	H23H23Z
Server-2a	Present	OFF	OK	JD3FRTW	JD3FRTWa
Server-2b	Present	OFF	OK	JD3FRTW	JD3FRTWb
Server-2c	Present	OFF	OK	JD3FRTW	JD3FRTWc
Server-2d	Present	OFF	OK	JD3FRTW	JD3FRTWd
Cable-IO	Present	ON	OK	STOMP11	N/A
Cable-CP	Present	ON	OK	STOMP11	N/A

getniccfg

Table 52. Details of 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:
	• `chassis`
	: default state if -m is not specified
	• `server-n`
	: where n = 1 to 4
	• `switch-n`
	: where n = 1 or 2

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 = 192.168.0.12 Current Subnet Mask = 255.255.254.0 Current Gateway = 192.168.0.1 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-1
```

LOM Model Name = BRCM 10GbE 2P 57810s bNDC

LOM Fabric Type = 10 GbE KR

IPv4 Enabled = 1

DHCP Enabled = 1

IP Address = 192.168.0.18

Subnet Mask = 255.255.255.0

Gateway = 192.168.0.1

IPv6 Enabled = 0

Autoconfiguration Enabled = 0

Link local Address =

IPv6 Gateway = ::

VLAN Enable = 0

VLAN ID = 1

VLAN priority = 0

```
racadm getniccfg -m switch-1
```

DHCP Enabled = 1

IP Address = 192.168.0.12

Subnet Mask = 255.255.255.0

Gateway = 0.0.0.0

Output

The **getniccfg** subcommand displays an appropriate error message if the operation is not successful. Otherwise, the output is displayed in the following format:

```
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
```

getpbinfo

Table 53. 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                          = 90 W
Peak System Power                           = 93 W
Peak System Power Timestamp                 = 20:28:32 03/04/2014
Minimum System Power                        = 83 W
Minimum System Power Timestamp              = 20:28:02 03/04/2014
Overall Power Health                        = OK
Redundancy                                  = Yes
System Input Power Cap                      = 3371 W
Redundancy Policy                           = Redundancy Alerting Only
System Input Max Power Capacity             = 2382 W
Input Redundancy Reserve                    = 0 W
Max Power Conservation Mode                 = 11:20:08 02/27/2014
Power Available for Server Power-on         = 1965 W
```

```
[Chassis Power Supply Status Table]
<name>     <Model>  <Power State> <Input Current> <Input Volts> <Output Rated Power>
PS1     0CC6WF   Online        0.3 A           208.0 V       1100 W
PS2     0GYH9V   Online        0.3 A           209.0 V       1100 W
```

getpciecfg

Table 54. Details of getpciecfg

Description	Displays the FQDD of the PCIe slots and their mapping information and properties.

NOTE: To use this subcommand, you must have CMC Login User privilege.

NOTE: Lengthy PCIe card names and server slot names are truncated when the assignments for all PCIe slots are displayed.

Synopsis

```
racadm getpciecfg [-c <FQDD>]
```

Input

- **-a** — Use this option to display the assignment of the PCIe slots .
- **-c** — Use this option to select a specific PCIe adapter or virtual adapter.
- **FQDD** — FQDD of the selected PCIe slot

Example

- Displays FQDDs of all the PCIe slots:

```
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
```

- Displays the assignment of PCIe slots and virtual adapters:

```
racadm getpciecfg -a
<PCIe Slot#> <Name>  <pwrState> <Server Slot Name> <Server Slot#>
PCIe slot-1          PCIe Card 1           ON
SLOT-04          4

PCIe slot-2          Not Present           N/A
UNMAPPED         N/A

PCIe slot-3          PCIe Card 3           OFF
SLOT-03          3

PCIe slot-4          Extension PCIe Card 3 ON
SLOT-03          3

PCIe slot-5          PCIe Card 5               OFF
SLOT-02          2

PCIe slot-6          Not Present            N/A
UNMAPPED         N/A

PCIe slot-7          PCIe Card 7            ON
localhost        1

PCIe slot-8          Not Present            N/A
UNMAPPED         N/A
```

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

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

getpminfo

Table 55. Details of getpminfo

Description Displays power management status information.

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

Synopsis

```
racadm getpminfo
```

Example

```
racadm getpminfo
```

```
[Real-Time Power Statistics]
System Input Power                      = 89 W (303 BTU/h)
Peak System Power                       = 93 W (317 BTU/h)
Peak System Power Start Time            = 20:26:06 03/04/2014
Peak System Power Timestamp             = 20:28:32 03/04/2014
Minimum System Power                    = 83 W (283 BTU/h)
Minimum System Power Start Time         = 20:26:06 03/04/2014
Minimum System Power Timestamp          = 20:28:02 03/04/2014
System Idle Power                       = 89 W (303 BTU/h)
System Potential Power                  = 417 W (1422 BTU/h)
System Input Current Reading            = 0.6 A
```

```
[Real-Time Energy Statistics]
System Energy Consumption               = 62.2 kWh
System Energy Consumption Start Time = 15:56:11 02/12/2014
System Energy Consumption Timestamp  = 06:07:07 03/05/2014
```

```
[System Power Status]
Chassis Power State                     = ON
Overall Power Health                    = OK
Redundancy                              = Yes
```

```
[System Power Policy Configuration]
System Input Power Cap                  = 3371 W (11502 BTU/h | 100%)
Redundancy Policy                       = Redundancy Alerting Only
```

```
[Power Budgeting]
System Input Max Power Capacity         = 2382 W
Input Redundancy Reserve                = 0 W
Power Available for Server Power-on     = 1965 W
```

gettracelog

Table 56. 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 CMC 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 192.68.157.103: session timeout
sid 0be0aef4
```

getractime

Table 57. Details of getractime

Description

Displays the current CMC time.

Synopsis

- `racadm getractime [-d]`
- `racadm getractime [-d] [-z] [-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 CMC time is displayed.

Example

- `racadm getractime`
  Thu Dec 8 20:15:26 2005
- `racadm getractime -d`
  20051208201542.000000

getsel

Table 58. Details of getsel

Description

Displays all sensor event log entries in the iDRAC.

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
```

getslotname

Table 59. Details of getslotname

Description

Displays the name, host name, 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, iDRAC DNS name, or the host name (if available). The values are:
  - 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               Webserver01                  WXP-8GRB221
   3               Webserver3                   WXP-319QWEecet5
   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.

getsensorinfo

Table 60. Details of getsensorinfo

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

Table 61. Examples

<Sensor Name>	<Status>	<Reading>	<LC>	UC
CPU1 VCORE PG	OK	0	600	N/A
System Board 12V PG	OK	0	600	N/A
System Board 3.3V PG	OK	4037	600	N/A
System Board 5V PG	OK	4045	600	N/A
CPU1 PLL PG	OK	4107	600	N/A
System Board 1.5V PG	OK	0	600	N/A
System Board 1.1V PG	OK	0	600	N/A
CPU1 M01 VTT PG	OK	0	600	N/A
CPU1 M23 VDDQ PG	OK	0	600	N/A
CPU1 M23 VTT PG	OK	0	600	N/A
CPU1 VSA PG	OK	0	600	N/A
CPU1 M01 VDDQ PG	OK	0	600	N/A
NDC PG	OK	0	600	N/A
CPU1 VTT PG	OK	0	600	N/A
MEZZB PG	OK	0	600	N/A
MEZZC PG	OK	0	600	N/A
PERC1 PG	OK	0	600	N/A

Table 62. Current sensor

<Sensor Name>	<Status>	<Reading>	<LW>	<LC>	<UW>	<UC>
System Board Current	OK	22	3	-7	42	47

```
Sensor Type: Processor
<Sensor Name> <Status> <AC-OK status>         <lc> <uc>
CPU1 Status              OK                          Presence Detected         N/
A                N/A
CPU2 Status              N/A                      Absent                         N/
A                N/A
```

```
Sensor Type: Memory
<Sensor Name> <Status>        <State>         <lc> <uc>
DIMM SLOT A1              OK                                        Presence
```

```
Detected           N/A                                  N/A
DIMM SLOT A2               OK                        Presence Detected          N/
A                                  N/A
DIMM SLOT A3               OK                                          Presence
Detected           N/A                                  N/A
DIMM SLOT A4               OK                        Presence Detected               N/
A                                  N/A
DIMM SLOT A5               OK
Absent                                                  N/A                                  N/A
DIMM SLOT A6               OK                     Absent                                     N/
A                                  N/A
DIMM SLOT A7               OK                           Absent                          N/
A                                  N/A
DIMM SLOT A8               OK
Absent                                                  N/A                        N/A
DIMM SLOT A9               OK                           Absent                               N/
A                                  N/A
DIMM SLOT A10              OK
Absent                                                  N/A                           N/A
DIMM SLOT A11              OK                           Absent                               N/
A                                  N/A
DIMM SLOT A12              OK
Absent                                                  N/A                           N/A
DIMM SLOT B1               OK                           Absent                               N/
A                                  N/A
DIMM SLOT B2               OK
Absent                                                  N/A                           N/A
DIMM SLOT B3               OK                           Absent                               N/
A                                  N/A
DIMM SLOT B4               OK
Absent                                                  N/A                           N/A
DIMM SLOT B5               OK                           Absent                               N/
A                                  N/A
DIMM SLOT B6               OK
Absent                                                  N/A                           N/A
DIMM SLOT B7               OK                           Absent                               N/
A                                  N/A
DIMM SLOT B8               OK
Absent                                                  N/A                           N/A
DIMM SLOT B9               OK                           Absent                               N/
A                                  N/A
DIMM SLOT B10              OK
Absent                                                  N/A                           N/A
DIMM SLOT B11              OK                             Absent                                  N/
A                                  N/A
DIMM SLOT B12              OK                Absent                                           N/
A                            N/A
```

```
Sensor Type: Battery
<Sensor Name>       <Status>  <Reading>  <lc> <uc>
System Board CMOS Battery       OK                                Present                 N/
A                                N/A
```

```
racadm getsensorinfo -c
```

Table 63. FanSpeed

<Num>	<sensorName>	<status>	<reading>	<LW>	<LC>	<UW>	<UC>	<PWM>
A	Fan-1A	OK	1800 rpm	960	840	N/A	N/A	17
B2	Fan-1B	OK	1560 rpm	960	840	N/A	N/A	17
	Fan-2	OK	2640 rpm	1800	1560	N/A	N/A	17
		OK						
	Fan-3	OK	2640 rpm	1800	1560	N/A	N/A	17

<Num>	<sensorName>	<status>	<reading>	<LW>	<LC>	<UW>	<UC>	<PWM>
	Fan-4	OK	2640 rpm	1800	1560	N/A	N/A	17
A	Fan-5A	OK	1920 rpm	960	840	N/A	N/A	17
B	Fan-5B	OK	1560 rpm	960	840	N/AN/A	N/A	17
	Fan-6	OK	2640 rpm	1800	1560		N/A	17
		OK						
	Fan-7	OK	2640 rpm	1800	1560	N/A	N/A	17
	Fan-8	OK	2640 rpm	1800	1560	N/A	N/A	17

Table 64. Temp sensor

<Num>	<sensorName>	<Status>	<reading>	<LW>	<LC>	<UW>	<UC>
1	Chassis Ambient	OK	23 C	3	-7	42	47
2	Server-1a	OK	N/A	N/A	N/A	N/A	N/A
3	Server-1b	OK	N/A	N/A	N/A	N/A	N/A
4	Server-1c	OK	N/A	N/A	N/A	N/A	N/A
5	Server-3a	OK	N/A	N/A	N/A	N/A	N/A
6	Server-3b	OK	N/A	N/A	N/A	N/A	N/A
7	Server-3c	OK	N/A	N/A	N/A	N/A	N/A
8	Server-3d	OK	N/A	N/A	N/A	N/A	N/A

Table 65. Battery sensor

<Num>	*<sensorName>*	*<status>*	*<health>*
1	PS-1	Online	OK
2	PS-2	Online	OK

Table 66. Cable sensor

<Num>	*<sensorName>*	*<status>*
1	IO-Cable	OK
2	FPC-Cable	OK

getssninfo

Table 67. Details of getssninfo

Description	Displays a list of users that are connected to CMC. 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

NOTE: Based on the Session ID (SSNID) or the user name (User), the CMC 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" "192.68.174.19" "Telnet" "NONE"

racadm getssninfo -A -u *

"root" "192.68.174.19" "Telnet" "NONE"

"bob" "192.68.174.19" "GUI" "NONE"
```

getstoragemoduleinfo

Table 69. Details of getstoragemoduleinfo

Description

Displays the storage module configuration and status information.

Synopsis

- `racadm getstoragemoduleinfo`
- `racadm getstoragemoduleinfo <FQDD>`

Input

-c — The **-c** *<FQDD>* option can be used to view the details of a storage sled. The availability of this option is based on the *<FQDD>* input. This command is supported only when a storage sled is present in the CMC FX2/FX2s chassis.

Examples

Table 70. Details

<Storage Slot>	<FQDD>
Storage-1	N/A
Storage-2	System.Modular.02
Storage-3	System.Modular.03

```
Storage-4                          System.Modular.04
```

Display format of storage sled information when the storage mode is “joined” or has a single controller.

```
racadm getstoragemoduleinfo -c System.Modular.02
```

```
Storage-2 FQDD               = System.Modular.02
Chassis Slot                 = 2
Name                         = SLOT-02
Model                        = PowerEdge FD332
Status                       = Not OK
Service Tag                  = 2435678
Asset Tag                    = ABCD12345
Intrusion State              = Open
Storage Mode                 = Joined
Number of Controllers        = 1
FQDD                         = RAID.Modular.2-1
     Physical Disk Slots          = 0-15
     Connected Server             = SLOT-01
     Controller Mode Capability   = HBA and RAID
```

Display format of storage sled information when the storage mode is “split single host”.

```
racadm getstoragemoduleinfo -c System.Modular.03
```

```
Storage-2 FQDD               = System.Modular.03
Chassis Slot                 = 3
Name                         = SLOT-03
Model                        = PowerEdge FD332
Status                       = Not OK
Service Tag                  = 8748596
Asset Tag                    = KLOP98656
Intrusion State              = Closed
Storage Mode                 = Split single host
Number of Controllers        = 2
FQDD                         = RAID.Modular.3-1
     Physical Disk Slots          = 0-7
     Connected Server             = SLOT-01
     Controller Mode Capability   = HBA
FQDD                         = RAID.Modular.3-2
     Physical Disk Slots          = 8-15
     Connected Server             = SLOT-1
     Controller Mode Capability   = HBA
```

Display format of storage sled information when the storage mode is “Split dual host”.

```
racadm getstoragemoduleinfo -c System.Modular.03
```

```
Storage-3 FQDD               = System.Modular.03
Chassis Slot                 = 3
Name                         = SLOT-03 (Storage)
Model                        = PowerEdge FD332
Status                       = OK
Service Tag                  = 4657248
Asset Tag                    = ERHJ57834
Intrusion State              = Closed
Storage Mode                 = Split dual host
Number of Controllers        = 1
FQDD                         = RAID.Modular.3-1
     Physical Disk Slots          = 0-7
     Connected Server             = SLOT-01
     Controller Mode Capability   = RAID
FQDD                         = RAID.Modular.2-1
     Physical Disk Slots          = 8-15
     Connected Server             = SLOT-2
     Controller Mode Capability   = HBA and RAID
```

Display format when storage sleds are not installed on the CMC FX2 or CMC FX2s system.

```
racadm getstoragemoduleinfo
```

```
This command is not supported on this configuration.
```

getsvctag

Table 71. Details of getsvctag

Description	Displays the Service Tag of the host system.
Synopsis	`racadm getsvctag`
Input	`getsvctag`
Output	<Module> <ServiceTag> <NodeId> Chassis STPST02 N/A Switch-1 0000000 N/A Switch-2 N/A N/A Server-1 FC830 FC830 Server-2 Extension(1) N/A Storage-3 7647563 N/A Storage-4 7654321 N/A
Example	`racadm getsvctag`

getsysinfo

Table 72. Details of getsysinfo

Description	Displays information related to CMC and chassis. **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 = Tue Jan 29 2013 23:00 CMC Location = CMC-1 Primary CMC Location = 4.40 CMC Version = 1.10 Last Firmware Update = Mon Jan 28 2013 08:41 Hardware Version = A04 CMC Network Information:

```
NIC Enabled                = 1
MAC Address                = D4:AE:52:AC:CA:C6
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         = 192.168.164.115
Current IP Gateway         = 192.168.164.1
Current IP Netmask         = 255.255.255.0
DHCP Enabled               = 1
Current DNS Server 1       = 192.168.165.80
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 FX2s
System AssetTag            = 00000
Service Tag                = STPST06
Express Service Code       = 62746758870
Chassis Name               = CMC-STPST06
Chassis Location           = [UNDEFINED]
Chassis Midplane Version   = 1.0
Power Status               = ON
System ID                  = 1488
PCIe Switch Board Type     = Gen 3
```

NOTE: In the Chassis Information output, the `PCIe Switch Board Type` information is displayed only for PowerEdge FX2s chassis model.

Examples

```
racadm getsysinfo -d
```

```
racadm getsysinfo -c
```

```
racadm getsysinfo -A
```

```
racadm getsysinfo -4
```

```
racadm getsysinfo -6
```

gettracelog

Table 73. 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 CMC 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 192.68.157.103: session timeout
sid 0be0aef4
```

getversion

Table 74. Details of getversion

Description

Displays the current software version, model and generation information, and whether the target device can be updated.

NOTE: To use this subcommand, you must have CMC Login User privilege.

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-1a   2.15.15.15 (18)        PowerEdge FC430
iDRAC8       Y
server-1b   2.40.40.40 (13)        PowerEdge FC430
iDRAC8       Y
server-1c   2.10.10.10 (49)        PowerEdge FC430
iDRAC8       Y
server-1d   2.40.40.40 (13)        PowerEdge FC430
iDRAC8       Y
server-3a   2.10.10.10 (27)        PowerEdge FC430
iDRAC8       Y
server-3b   2.10.10.10 (49)        PowerEdge FC430
iDRAC8       Y
```

```
server-3c   2.30.30.30 (10)        PowerEdge FC430
iDRAC8       Y
server-3d   2.10.10.10 (49)        PowerEdge FC430
iDRAC8       Y
```

```
<Switch>       <Model Name>                        <HW Version>
<FW Version>
switch-1    1GBE PASS-THROUGH MODULE           A00              N/A
```

```
<CMC>           <CMC
Version>                                          <Updatable>
cmc
2.00.000.20161003sahu                                        Y
```

```
<Chassis Infrastructure>         <FW Version>             <FQDD>
Main Board                       1.20.A00.201502058
System.Chassis.
1#Infra
                                              structure.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 **-l** 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.
- **-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.
  - `switch-n` , where n = 1 to 2.
  - `CMC`
  - `mainboard`

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 75. Details of ifconfig

Description	Displays the contents of the network interface table.

To use this subcommand, you must have the **Administrator** privilege.

Synopsis

```
racadm ifconfig
```

Example

```
$ racadm ifconfig

eth0      Link encap:Ethernet  HWaddr 00:1D:09:FF:DA:23

          inet addr:192.168.0.1  Bcast:192.168.0.120
 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 76. 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.
- **– –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]
------------------------------------------------------------
```

- Delete the specified job:

  ```
  racadm jobqueue delete -i RID_860202993201
  ```

- racadm jobqueue delete -i <JobID>

krbkeytabupload

Table 77. Details of krbkeytabupload

Description	Uploads a Kerberos keytab file. To run this subcommand, you must have the **Configure Chassis Administrator** privilege.

Synopsis	`racadm krbkeytabupload [-f <filename>]`
	
	`<filename> is the name of the file including the path.`

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 78. Details of license

Description	Manages the CMC and storage sled 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 view -c <storage sled FQDD>` • Import the license: `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: 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.
- **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.

Examples

- View licenses:
  - View all the license information in the chassis.

```
racadm license view
```

```
CMC.Integrated.1
        Status               = OK
        Device               = CMC.Integrated.1
        Device Description   = Chassis Management Controller for
PowerEdge FX2/FX2s
        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
```

– View the storage sled license information in the chassis.

```
racadm license view -c <FQDD>
```

```
System.Modular.03
        Status              = OK
        Device              = System.Modular.03
        Device Description  = Dual PERC Controller for PowerEdge
FD332
        Unique Identifier   = PQR123
                License #1
                        Status              = OK
                        Transaction ID      = 522
                        License Description = PowerEdge FD332
Dual RAID License
                        License Type        = PERPETUAL
                        Entitlement ID      =
Q3nJiS1xnX4rdRlat24qjdfb
                        License Bound       = PQR243
                        Expiration          = Never Expires
```

- Import a license:
  – Import a license from a CIFS share to a device (for example, Integrated CMC):

    ```
    racadm license import -u admin -p passwd -f License.xml -l //
    x.x.x.x/licshare -c cmc.integrated.1
    ```

  – Import a license from an NFS share to a device (for example, Integrated CMC):

    ```
    racadm license import -f License.xml -l x.x.x.x:/share -c
    cmc.integrated.1
    ```

  – Import a license from the local file system using Remote RACADM:

    ```
    racadm license import -u admin -p passwd -r x.x.x.x -f C:
    \Mylicdir\License.xml -c cmc.integrated.1
    ```

- Export a license file:
  – Export license to an NFS share using transaction ID (for example, transaction 27).

    ```
    racadm license export -f License.xml -l x.x.x.x:/licshare -t 27
    ```

  – 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 //
    x.x.x.x/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 may 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 <default root user password> -f
    LicenseFile.xml  -l //x.x.x.x/licshare -c cmc.embedded.1
    ```

- Delete a license:
  – Delete licenses on a particular device. For example. Embedded CMC:

    ```
    racadm license delete -c cmc.embedded.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
    ```

  – Delete a storage sled license. For example, System.Modular.03

    ```
    racadm license delete -c System.Modular.03
    ```

- 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 x.x.x.x:/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 //
x.x.x.x/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
```

– Replace a storage sled license

```
racadm license replace -f
nfs/"CfDuqtnJTobaSYGNzmdA4Buz_xyz_dual.xml" -| x.x.x.x:/nfs -t 8
```

netstat

Table 79. Details of netstat

Description	Displays the routing table and the current connections. To use this subcommand, you must have the **Execute Diagnostic Commands** permission.
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 80. Details of ping

Description	Verifies that the destination IP address is reachable from CMC with the current routing-table contents. A destination IP address 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.
Synopsis	`racadm ping <ipaddress>`

ping6

Table 81. Details of

Description	Verifies that the destination IPv6 address is reachable from a 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 based on the current routing-table contents.

To use this subcommand for CMC, you must have the Administrator privilege.

Synopsis

```
racadm ping6 <ipv6address>
```

Example

```
racadm iping6 192.168.0.2
```

```
IPING6 192.168.0.2 (192.168.0.2): 56 data bytes
```

```
64 bytes from 192.168.0.2: icmp_seq=0 ttl=121 time=2.9
ms
```

```
--- 192.168.0.2 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 82. 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 **CMC Login User** 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              = Mon Jul 04 2016 18:50
Primary CMC Location       = CMC
Primary CMC Version        = 2.00
Last Firmware Update       = Mon Jul 03 2016 20:06
Hardware Version           = A00

CMC Network Information:
NIC Enabled                = 1
MAC Address                = F8:BC:12:32:E6:80
Register DNS CMC Name      = 0
DNS CMC Name               = cmc-grapple
Current DNS Domain         = SSEFW.COM
VLAN ID                    = 1
VLAN Priority              = 0
VLAN Enabled               = 0

CMC IPv4 Information:
IPv4 Enabled               = 1
Current IP Address         = 10.94.224.187
Current IP Gateway         = 10.94.224.1
Current IP Netmask         = 255.255.255.0
DHCP Enabled               = 1
Current DNS Server 1       = 10.116.2.250
Current DNS Server 2       = 10.116.2.251
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 FX2s
System AssetTag            = 00000
Service Tag                = grapple
Express Service Code       = 108126335602
Chassis Name               = CMC-grapple
Chassis Location           = [UNDEFINED]
Chassis Midplane Version   = 1.0
Power Status               = ON
System ID                  = 1488
PCIe Switch Board Type     = Gen 3

================================================================================
 Session Information
================================================================================
SSNID Type   User   IP Address  Login Date/Time
49580 SSH    root   10.94.78.51 07/04/2016 18:07:40

================================================================================
 Sensor Information
================================================================================

<senType>       <Num>   <sensorName>    <status>        <reading>       <units>         <LC>
<UC>    <PWM>
FanSpeed        1A      Fan-1A          OK              8040            rpm             3720
```

```
N/A     67
FanSpeed        1B      Fan-1B          OK              7080            rpm             3720
N/A     67
FanSpeed        2       Fan-2           OK              11040           rpm             5520
N/A     67
FanSpeed        3       Fan-3           OK              11040           rpm             5520
N/A     67
FanSpeed        4       Fan-4           OK              11160           rpm             5520
N/A     67
FanSpeed        5A      Fan-5A          OK              8040            rpm             3720
N/A     67
FanSpeed        5B      Fan-5B          OK              7080            rpm             3720
N/A     67
FanSpeed        6       Fan-6           OK              11040           rpm             5520
N/A     67
FanSpeed        7       Fan-7           OK              11040           rpm             5520
N/A     67
FanSpeed        8       Fan-8           OK              10920           rpm             5520
N/A     67

<senType>       <Num>   <sensorName>        <status>        <reading>       <units>
<LC>    <UC>
Temp            1       Chassis Ambient         OK              23              Celsius
-7      47
Temp            2       Server-1a               OK              N/A             Celsius
N/A     N/A
Temp            3       Server-1b               OK              N/A             Celsius
N/A     N/A
Temp            4       Server-1c               OK              N/A             Celsius
N/A     N/A
Temp            5       Server-1d               OK              N/A             Celsius
N/A     N/A
Temp            6       Server-3a               OK              N/A             Celsius
N/A     N/A
Temp            7       Server-3b               OK              N/A             Celsius
N/A     N/A
Temp            8       Server-3c               OK              N/A             Celsius
N/A     N/A
Temp            9       Server-3d               OK              N/A             Celsius
N/A     N/A

<senType>       <Num>   <sensorName>    <status>        <health>
PWR             1       PS-1            Online          OK
PWR             2       PS-2            Online          OK

<senType>       <Num>   <sensorName>    <status>
Cable           1       Cable-IO        OK
Cable           2       Cable-CP        OK

================================================================================
 Switches Information
================================================================================
<IO      Name                          Type             Presence   POST       Power
Role          SecureMode   Mode
Switch-1  1GBE PASS-THROUGH MODULE       Gigabit Ethernet   Present      OK
ON          Master         No             N/A
Switch-2  N/A                            None               Not Present  N/A          N/
A         N/A            N/A            N/A

================================================================================
 Daughter Card Information
================================================================================
Group A I/O Type : Gigabit Ethernet
Group B I/O Type : PCIe
Group C I/O Type : PCIe

<IO#>      <Type>                  <State>     <Role>
switch-1   Gigabit Ethernet        OK          Master
switch-2   None                    N/A         N/A
```

```
<Server#>      <Presence>            <DC1 Type>    <DC1 State>   <DC2 Type>   <DC2 State>
server-1a          Present               None           N/A          PCIe         OK
server-1b          Present               PCIe           OK           None         N/A
server-1c          Present               None           N/A          PCIe           OK
server-1d          Present               PCIe           OK           None            N/A
server-2           Extension(1)          None           N/A          None         N/A
server-3a          Present               None            N/A          PCIe         OK
server-3b          Present               PCIe           OK           None         N/A
server-3c          Present               None           N/A          PCIe         OK
server-3d          Present               PCIe           OK           None         N/A
server-4           Extension(3)          None           N/A          None         N/A

================================================================================
 All Modules Information
================================================================================
<module>        <presence>      <pwrState>      <health>        <svcTag>        <nodeId>
Chassis         Present         ON              OK              grapple         N/A
Main-Board      Present         ON              OK              N/A             N/A
Fan-1           Present         ON              OK              N/A             N/A
Fan-2           Present         ON              OK              N/A             N/A
Fan-3           Present         ON              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
Fan-7           Present         ON              OK              N/A             N/A
Fan-8           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
CMC             Present         Primary         OK              N/A             N/A
Switch-1        Present         ON              OK              N/A             N/A
Switch-2        Not Present     N/A             N/A             N/A             N/A
Server-1a       Present         OFF             OK              1111111         1111111
Server-1b       Present         OFF             OK              6P3RG52         6P3RG52
Server-1c       Present         OFF             OK              HP3RG52         HP3RG52
Server-1d       Present         OFF             OK              DN3RG52         DN3RG52
Server-2        Extension(1)    N/A             N/A             N/A             N/A
Server-3a       Present         OFF             OK              N/A             N/A
Server-3b       Present         OFF             OK              6Q3RG52         6Q3RG52
Server-3c       Present         OFF             OK              N/A             N/A
Server-3d       Present         OFF             OK              1FXSG52         1FXSG52
Server-4        Extension(3)    N/A             N/A             N/A             N/A
Cable-IO        Present         ON              OK              grapple         N/A
Cable-CP        Present         ON              OK              grapple         N/A

================================================================================
 Power Budget Information
================================================================================

[Power Budget Status]
System Input Power                          = 186 W
Peak System Power                           = 195 W
Peak System Power Timestamp                 = 21:16:21 10/03/2016
Minimum System Power                        = 140 W
Minimum System Power Timestamp              = 20:08:27 10/03/2016
Overall Power Health                        = OK
Redundancy                                  = No
System Input Power Cap                      = 3371 W
Redundancy Policy                           = None
System Input Max Power Capacity             = 3371 W
Input Redundancy Reserve                    = 0 W
Max Power Conservation Mode                 = No
Power Available for Server Power-on         = 2712 W

[Chassis Power Supply Status Table]
<Name>          <Model>         <Power State>      <Input Current>         <Input Volts>
<Output Rated Power>
PS1             095HR5          Online                0.4 A              239.8 V           1600
W
```

```
PS2             095HR5          Online                  0.4 A             240.0 V           1600
W

================================================================================
 Nic Information
================================================================================
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        = 10.94.224.187
Current Subnet Mask       = 255.255.255.0
Current Gateway           = 10.94.224.1
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
Redundant mode            = 0
VLAN Enable               = 0
VLAN ID                   = 1
VLAN priority             = 0

================================================================================
 Tracelog Information
================================================================================

Jul  4 17:13:00 CMC-grapple systemd[1]: Stopping Rotate Logs...
Oct  4 17:14:00 CMC-grapple systemd[1]: logrotate.service holdoff time over, scheduling restart.
Oct  4 17:14:00 CMC-grapple systemd[1]: Stopping Rotate Logs...
Oct  4 17:14:07 CMC-grapple ssnmgrd: root from 10.94.78.51: session timeout sid 25332
Oct  4 17:14:07 CMC-grapple ssnmgrd: root from 10.94.78.51: session timeout sid 25332
Oct  4 17:14:07 CMC-grapple sshd[11379]: Session close PID succeeds: sid=25332, User: root, IP:
10.94.78.51
Oct  4 17:14:07 CMC-grapple sshd[11379]: Session close PID succeeds: pid=11379 sid=25332
Oct  4 18:47:43 CMC-grapple systemd[1]: Stopping System Logging Service...
Oct  4 18:48:08 CMC-grapple systemd[1]: logrotate.service holdoff time over, scheduling restart.
Oct  4 18:48:08 CMC-grapple systemd[1]: Stopping Rotate Logs...
Oct  4 18:49:08 CMC-grapple systemd[1]: logrotate.service holdoff time over, scheduling restart.
Oct  4 18:49:08 CMC-grapple systemd[1]: Stopping Rotate Logs...
Oct  4 18:50:08 CMC-grapple systemd[1]: logrotate.service holdoff time over, scheduling restart.
Oct  4 18:50:08 CMC-grapple systemd[1]: Stopping Rotate Logs...

================================================================================
 Raclog Information
================================================================================
SeqNumber       = 7
Message ID      = USR8513
Category        = Audit
AgentID         = CMC
Severity        = Information
Timestamp       = 2016-07-04 20:25:07
Message Arg   1 = root
Message Arg   2 = 10.94.18.232
Message Arg   3 = SSH
Message         = root login successful from 10.94.18.232 (type=SSH).
--------------------------------------------------------------------------------
SeqNumber       = 6
Message ID      = PSU8517
Category        = Audit
AgentID         = CMC
Severity        = Information
Timestamp       = 2016-07-04 20:24:39
```

```
Message         = PSU redundancy policy changed.
-------------------------------------------------------------------------------
SeqNumber       = 4
Message ID      = USR8513
Category        = Audit
AgentID         = CMC
Severity        = Information
Timestamp       = 2016-07-04 20:23:46
Message Arg   1 = root
Message Arg   2 = 10.94.18.232
Message Arg   3 = GUI
Message         = root login successful from 10.94.18.232 (type=GUI).
-------------------------------------------------------------------------------
SeqNumber       = 3
Message ID      = USR8501
Category        = Audit
AgentID         = CMC
Severity        = Information
Timestamp       = 2016-07-04 20:22:06
Message Arg   1 = 7990
Message Arg   2 = 41269
Message         = Successfully closed Session process: pid=7990 sid=41269
-------------------------------------------------------------------------------
SeqNumber       = 2
Message ID      = USR8501
Category        = Audit
AgentID         = CMC
Severity        = Information
Timestamp       = 2016-07-04 20:22:06
Message Arg   1 = 7990
Message Arg   2 = 48120
Message         = Successfully closed Session process: pid=7990 sid=48120
-------------------------------------------------------------------------------

===============================================================================
 sel Information
===============================================================================
Mon Oct 03 2016 20:21:57 Normal Log cleared.
Mon Oct 03 2016 20:24:39 Normal The power supplies are not redundant.
```

racreset

Table 83. 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, CMC may require up to two minutes to return to a usable state.**
Synopsis	`racadm racreset [-m <module>]`
Input	`-m<module>` — This option can have one of the following values: · `server <-n>`, where n= 1–4 · `server <-nx>`, where n=1–4 and x=a-d (lower case) · `sled-n` , where n=1–4 **NOTE: The `-m sled-n` option is available only for multinode servers.** **NOTE: You can use the `-f` option to force the reset. This option is available only with the `-m` option.**

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
  ```
- Racreset on multinode server
  ```
  racadm racreset -m sled-1
  ```
- Force racreset on multinode server
  ```
  racadm racreset -m sled-1 -f
  ```

racresetcfg

Table 84. 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
  - server-<nx> — where n=1–4 and x=a-d (lower case)

  NOTE: The values n= 2 and 4 are valid for multi-node sleds only
- -c : <feature> — Must be one of the following values:
  - ad — Reset Active Directory and LDAP 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 "disabled".

  NOTE: The –c option is valid with only <module=chassis> only.

  NOTE: If the `racresetcfg` is performed on a chassis, the CMC resets after the task.

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
  ```

remoteimage

Table 85. Details of remoteimage

Description

Connects, disconnects, or deploys a media file on a remote server.

To use this subcommand, you must have the **Administrator** permission.

Synopsis

- `racadm remoteimage [-m <module> | -a]`
- `racadm remoteimage -d -m <module>`
- `racadm remoteimage -d -a`
- `racadm remoteimage -s [-m <module> | -a]`
- `racadm remoteimage -c -m <module> -u <username> -p <password> -l <image_path>`
- `racadm remoteimage -c -a -u <username> -p <password> -l <image_path>`
- `racadm remoteimage -e -m module -u <username> -p <password> -l <image_path>`
- `racadm remoteimage -e -a -u <username> -p <password> -l <image_path>`

Input

- `-c` — Connect a remote image.
- `-d` — Disconnect the remote image.
- `-e` — Deploys a remote image
- `-s` — Display the connection status; –a is assumed, if not specified.
- `-m` <*module*> — The `<module>` option can have the following values:
  - `server-<n>`, where n=1–4
  - `server-<nx>`, where n=1–4 and x=a-d (lower case)
- `-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.

NOTE: The `-u`, `-p`, and `-l` options are applicable only to connect and deploy actions.

Example

- `racadm remoteimage -c -u "user" -p "pass" -l //shrloc/foo.iso`

  Remote Image is now Configured.
- `racadm remoteimage -d`

  Disable Remote File Started. Please check status using -s option to verify if the Remote File Share is ENABLED or DISABLED.
- `racadm remoteimage -s`

  Remote File Share is Enabled.

  UserName

  Password

  ShareName //192.168.0.1/xxxx/dtk_3.3_73_Linux.iso

serveraction

Table 86. 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 -m <module> <action>
```

```
racadm serveraction -a <action>
```

Input

- `-m<module>` — server-n, where *n*=1–4
- `-a` — Performs action on all servers. Not allowed with the powerstatus 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 shut down, this operation is not 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 resettig the iDRAC on a server.

  NOTE: The reseat option is not available for individual FM120 servers.

NOTE: The `-f` option is required to force the 'reseat' action.

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 turned off on that server.

  ```
  racadm serveraction -m server-3 powerdown
  ```

  Server is already powered OFF.
- Turn off the server from CMC when power is already turned 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 action on multinode server:

  ```
  racadm serveraction -m server-1a powerstatus
  ```

- Get Power Status on iDRAC

  ```
  racadm serveraction powerstatus
  ```

  Server Power Status: ON
- Reseat action on a multinode sled

  ```
  racadm serveraction -f -m sled-1 reseat
  ```
- Explanation of Support
  CMC needs to support graceful shutdown

  The support of address individual blades is expected on the CMC

set

Table 87. Details of set

Description

Import saved CMC 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.

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>
```

Input

- `-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".

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
  ```

setassettag

Table 88. 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 " (double quote), ` (back quote), & (ampersand), and \ (backslash) 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 89. Details of setchassisname

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

setflexaddr

Table 90. 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* > = A1 or A2

< *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
  ```
- ```
  racadm setflexaddr -f A 1
  ```

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

setled

Table 91. 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=1–2

  — 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 -1 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-2 -1 1`
  ERROR: Server in slot 9 is an extension of the server in slot 1.

setniccfg

Table 92. Details of setniccfg

Description

Sets the CMC 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 Chassis Administrator** permission.

NOTE: The terms NIC and Ethernet management port may be used interchangeably.

Synopsis

- `racadm getniccfg`
- `racadm getniccfg –m <module>`,
  where –m must be one of the following values:
  - `chassis`: default state if -m is not specified
  - `server-n`: where n = 1 to 4
  - `switch-n`: where n = 1 or 2
- `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`
- `racadm setniccfg –p [-6}`
- `racadm setniccfg [-m <module>] –k [<speed> <duplex>]`
- `racadm setniccfg [-i <slot>] –v [<vlan_id> <vlan_priority>]`

Input

- `-d` — Enables DHCP for the NIC (default is “DHCP disabled”.)
- `-d -6` — 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
- `-s -6` — Enables static IPv6 settings. The IPv6 address, Prefix Length, and the IPv6 gateway can be specified.
- `-o` — Enable or disable NIC.
- -m<module> — Must be one of the following values:
  - `chassis`: Default state if - m is not specified.
  - `server-n`: where n=1–4
  - `server-nx`: where n=1–4; x=a-d (lower case)

  - `switch-n`: where n=1–2
- `-i <slot>` — Must be number n, where n=1 to 4
- `-v` — When performing on a switch, release and renew any DHCP lease on that port for the changes to be effective. The VLAN settings must be one of the following legal values:
  - no arguments imply remove vlan tag, not compatible with server-nx. For example ("server-4b") notation
  - `<vlan_id>` 1 to 4000, 4021, and 4094 inclusive
  - `vlan_priority>` 0 to 7, inclusive
- `-p` — Disables IPV4 (default)/IPV6 protocol
- `-k` — Must be one of the following legal values:
  - no arguments imply autonegotiate
  - `<speed>` = 10, 100
  - `<duplex>` = half, full
- `-r` — Enable or disable redundant mode. The legal values are:
  - 1 — Enable
  - 0 — Disable

NOTE: The options -o, -k, -p, and -r can be specified for chassis only.

- `-6`:
  - Sets static IPv6 addresses (w/ -s option).
  - Enables autoconfig for IPv6 (w/ -d option).
  - Disables IPv6 (w/ -p option).
  - Can be specified for chassis or servers.

Example

- `racadm setniccfg -s 192.168.0.120 255.255.255.0 192.168.0.1`
- `racadm setniccfg -d`
- `racadm setniccfg -d6`
- Configuration of speed = 100Mbps and duplex= full duplex:

  `racadm setniccfg -k 100 full`
- Configuration of speed and duplex to autonegotiate:

  `racadm setniccfig -k`
- Configuration of redundant mode:

  `racadm setniccfg -r 1`
- Configuration of VLAN id and priority of a slot or all blades in a sleeve:

  `racadm setniccfg -i 5 -v 1000 7`
- Configuration of CMC to a static IPv6 address:

  `racadm setniccfg -m chassis -s -6 2001:DB8::2 64 2001:DB8::1`
- Configuration of server to use stateless autoconfiguration address:

  `racadm setniccfg -m server-1 -d -6`
- Configuration of VLAN id and priority for a switch:

  `racadm setniccfg -m switch-1 -v 1000 7`
- Removal of VLAN configuration from a switch:

  `racadm setniccfg -m switch-1 -v`

setractime

Table 93. 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 • racadm setractime -z {?|timezone|timezone-prefix*}
Input	• -d — Sets the time in the string yyyymmddhhmmss.mmmmmmsoff where: — 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 94. Details of setslotname

Description

Sets the name of the slot and enables the feature to display the host name (if available) or 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 set whether the 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 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 " (double quote), ` (back quote), & (ampersand), \ (backslash), ; (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 <value>`

Input

- `-i <Slot_Number>`—Specify the slot number in the chassis. Valid values: 1-4.
- `<Slot_Name_To_Be_Set>` —The new name to be assigned to the slot.
- —h `<values>`—Displays the Hostname, Slotname, or iDRAC DNS name. The legal values are:
  - `0`—Displays the Slotname
  - `1`—Displays the Hostname
  - `2`—Displays the iDRAC DNS name

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 95. 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 " (double quote), ` (back quote), &(ampersand), > (greater than), < (less than), and \ (backslash) are not supported for this subcommand.**
Synopsis	`racadm setsysinfo [-c chassisname|chassislocation] <string>`
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 96. Details of sshpkauth

Description	Enables you to upload and manage up to four different SSH public keys per user. You can upload a key file or key text, view keys, or delete keys.
	
	RSA key size should be between 768 and 4096 and the recommended DSA key size is 1024.
	
	This command has three mutually exclusive modes—upload, view, and delete that are determined by the options.
	
	Upload
	
	The upload mode allows you to upload a keyfile or to copy the key text on the command line. You cannot upload and copy a key at the same time.
	
	Remote RACADM:
	
	`racadm sshpkauth -i <2 to 16> -k <1 to 4> -f <filename>`
	
	`racadm sshpkauth -i <2 to 16> -k <1 to 4> -t`
	
	`<key-text>`

Telnet/ssh/serial RACADM:

```
racadm sshpkauth -i <2 to 16> -k <1 to 4> -t
```

```
<key-text>
```

View

The view mode allows the user to view a key specified by the user or all keys.

```
racadm sshpkauth -i <2 to 16> -v -k <1 to 4>
```

```
racadm sshpkauth -i <2 to 16> -v -k all
```

Delete

The delete mode allows the user to delete a key specified by the user or all keys.

```
racadm sshpkauth -i <2 to 16> -d -k <1 to 4>
```

```
racadm sshpkauth -i <2 to 16> -d -k all
```

Synopsis

```
racadm sshpkauth
```

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 <default root user password>
sshpkauth -i svcacct -k 1 -p 0xfff -f dsa_2048.pub
```

Input

- **-i** < *user index* > - Index for the user. <*user index*> must be between 2 and 16 on iDRAC.
- **-k** [< *key index* > | all] - Index to assign the PK key being uploaded. *all* only works with the -v or -d options. <*key index*> must be between 1 and 4 or *all* on iDRAC.
- **-t** < *PK Key Text* > - Key text for the SSH Public key.
- **-f** < *filename* > - File containing the key text to upload. The -f option is not supported on Telnet/ssh/serial RACADM.
- **-v** - View the key text for the index provided.
- **-d** - Delete the key for the index provided.

Examples :

- Upload an invalid key to iDRAC User 2 in the first key space using a string:

```
$ racadm sshpkauth -i 2 -k 1 -t "This is invalid key
Text"
```

```
ERROR: Key text appears to be corrupt
```

- Upload a valid key to iDRAC User 2 in the first key space using a file:

```
$ racadm sshpkauth -i 2 -k 1 -f pkkey.key
```

```
Key file successfully uploaded.
```

- Get all keys for User 2 on iDRAC:

```
$ racadm sshpkauth -v -i 2 -k all
```

```
******************** User ID 2 ******************
```

```
Key ID 1:
```

```
ssh-rsa    AAAAB3NzaC1yc2EAAAABIwAAAIEAzzy+k2npnKqVEXGXIzo0sbR6JgA5YNbWs3ekoxXV
               fe3yJVpVc/5zrrr7XrwKbJAJTqSw8Dg3iR4n3vUaP+lPHmUv5Mn55Ea6LHUslAXFqXmOdlThd
```

```
                wilU2VLw/iRH1ZymUFnut8ggbPQgqV2L8bsUaMqb5PooIIvV6hy4isCNJU=
1024-bit RSA, converted from OpenSSH by xx_xx@xx.xx

Key ID 2:

Key ID 3:

Key ID 4:
```

sslkeyupload

Table 97. Details of sslkeyupload

Description	Uploads SSL key from the client to CMC. To use this subcommand, you must have **Server Administrator** permission.
Synopsis	`racadm sslkeyupload -t <type> -f <filename>`
Input	• **-t** — Specifies the key to upload. 1 = SSL key used to generate the server certificate • **-f** — Specifies the file name of the SSL key to be uploaded.
Output	Returns 0 when successful and a nonzero number when unsuccessful.
Example	`racadm sslkeyupload -t 1 -f c:\sslkey.txt`

sslcertupload

Table 98. Details of sslcertupload

Description	Uploads a custom SSL server or CA certificate for Directory Service from the client to CMC. To use this subcommand, you must have the **Server Administrator** 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 • -f — Specifies the file name of the certificate to be uploaded. • -e — Allows for upload of multiple certificate format types. – 1 = Base64 – 2 = PKCS12 The current release does not support this option. • -p — Pin for decrypting the PKCS12 file uploaded. If <*format type*> is selected as 2, it is mandatory to specify -p option. The current release does not support this option.

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 99. Details of sslcertview

Description	Displays the SSL server or CA certificate that exists on CMC.. To use this subcommand, you must have the **CMC Login User** privilege.
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 100. Output

Serial Number	00
Subject 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)	CMC 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)	CMC Default certificate
Common Name (CN)	CMC 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
CMC default certificate
US
Texas
Round Rock
Dell Inc.
Remote Access Group
CMC default certificate
Jul 8 16:21:56 2005 GMT
Jul 7 16:21:56 2010 GMT
```

sslcsrgen

Table 101. 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 CMC. To use this subcommand, you must have the **Chassis Configuration Administrator•** permission.
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.**
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 102. 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.
```

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 103. Details of testemail

Description

Sends a test e-mail from CMC 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
  ```

- 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 104. 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 105. Details of 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.

- 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 106. Details of 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 107. Details of 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 108. Details of testtrap

Description	Tests the RAC's SNMP trap alerting feature by sending a test trap from CMC to a specified destination trap listener on the network. To use this subcommand, you must have the **Test Alerts** permission. **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 109. 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** permission.
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 110. 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** permission.
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: 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 111. 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.

idRacDescriptionInfo - Read only

Table 112. Details of idRacDescriptionInfo

Description	A text description of the RAC type.
Legal Values	A string of up to 255 ASCII characters.
Default	This system component provides a complete set of remote management functions for the PowerEdge servers.

idRacVersionInfo - Read only

Table 113. 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 114. 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 115. 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 CMC NIC for IPv4.

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

For CMC, 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 a setting that does not have a hash sign (#) prefixed 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 116. Details of cfgNicIPv4Enable

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

Default	• For iDRAC: 0 • For CMC: 1

cfgNicVLanEnable - Read or Write

Table 117. Details of cfgNicVLanEnable

Description	Enables or disables the VLAN capabilities. All chassis management traffic, including the CMC and all iDRACs, resides on this external VLAN when enabled. No iDRAC configuration change is required to use this external management network VLAN.
Legal Values	• 1 (TRUE) • 0 (FALSE)
Default	**0**
Example	• `racadm config -g cfgLanNetworking -o cfgNicVLanEnable 1` • `racadm config -g cfgLanNetworking -o cfgNicVLanEnable 0`

cfgNicVLanId - Read or Write

Table 118. Details of cfgNicVLanId

Description	Specifies the VLAN ID for the network VLAN configuration in CMC. 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`

cfgNicVLanPriority - Read or Write

Table 119. Details of cfgNicVLanPriority

Description	Specifies the VLAN Priority for the network VLAN configuration in CMC. This property is only valid if `cfgNicVLanEnable` is set to `1` (enabled).
Legal Values	0 – 7
Default	0
Example	`racadm config -g cfgLanNetworking -o`

```
cfgNicVLanPriority 7
```

cfgDNSDomainNameFromDHCP - Read or Write

Table 120. 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 **cfgCurrentIPv6Enabled** 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`
- `cfgCurrentIPv6Enabled`
- `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 121. Details of cfgDNSDomainName

Description	In the DNS domain name, parameter is only valid 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 only supports Fully Qualified Domain Names (FQDN) of 64 bytes or fewer.**
Default	`<blank>`

cfgDNSRacName - Read or Write

Table 122. 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 123. 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 124. 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 125. 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 or Write

Table 126. 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 127. 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 128. 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.
Default	192.168.0.120

cfgNicNetmask - Read or Write

Table 129. 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 130. 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

cfgNicUseDhcp - Read or Write

Table 131. Details of cfgNicUseDhcp

Description	Specifies whether DHCP is used to assign the CMC IPv4 address. If this property is set to 1(TRUE), then CMC IPv4 address, subnet mask and gateway are assigned from the DHCP server on the network. If this property is set to `0` (FALSE), the user can configure the `cfgNicIpAddress`, `cfgNicNetmask` and `cfgNicGateway` properties.
Legal Values	• `1` (TRUE) • `0` (FALSE)
Default	0

cfgNicMacAddress - Read only

Table 132. 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.

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 **User Configuration Administrator** privilege.

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

cfgUserAdminIndex - Read only

Table 133. 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 134. 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

Table 135. Example

iDRAC Specific User Privilege	**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
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
Server Administrator	0x0000040
Test Alert User	0x0000080

Debug Command Administrator	0x0000100
Fabric A Administrator	0x0000200
Fabric B Administrator	0x0000400
Fabric C Administrator	0x0000800

Table 136. Examples

User Privilege(s)	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 137. 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), \ (backward slash), . (period), @ (at symbol), " (quotation marks), (semicolon), or ' (backward quote) **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 138. 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 139. 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

cfgUserAdminSNMPv3Enable (Read or Write)

NOTE: The `cfgUserAdminSNMPv3Enable` attribute is deprecated and replaced with `cfgUserAdminSNMPv3Enable` attribute.

Table 140. Details of `cfgUserAdminSNMPv3Enable` attribute

Description	Enables or disables SNMPv3 support for a CMC user.
Legal Values	• 0 — Disabled • 1 — Enabled
Default Value	0 — Disabled
Dependency	None

cfgUserAdminSNMPv3AuthenticationType (Read or Write)

NOTE: The `cfgUserAdminSNMPv3AuthenticationType` attribute is deprecated and replaced with `cfgUserAdminSNMPv3AuthenticationType` attribute.

Table 141. Details of `cfgUserAdminSNMPv3AuthenticationType` attribute

Description	Configure SNMPv3 authentication type.
Legal Values	• 0—None • 1—MD5 • 2—SHA
Default Value	2 — SHA
Dependency	None

cfgUserAdminSNMPv3PrivacyType (Read or Write)

NOTE: The `cfgUserAdminSNMPv3PrivacyType` attribute is deprecated and replaced with `cfgUserAdminSNMPv3PrivacyType` attribute.

Table 142. Details of `cfgUserAdminSNMPv3PrivacyType` attribute

Description	Configure SNMPv3 privacy protocol type.
Legal Values	• 0 — None • 1 — DES • 2 — AES
Default Value	2 — AES
Dependency	None

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 for, you must have **Chassis Configuration Administrator** privileges.

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

cfgEmailAlertIndex - Read only

Table 143. Details of cfgEmailAlertIndex

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

cfgEmailAlertEnable - Read or Write

Table 144. Details of cfgEmailAlertEnable

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

Default	0

cfgEmailAlertAddress - Read or Write

Table 145. Details of cfgEmailAlertAddress

Description	Specifies the destination email address for email alerts, for example, user1@company.com.
Legal Values	E-mail address format, with a maximum length of 64 ASCII characters.
Default	*<blank>*

cfgEmailAlertEmailName

Table 146. 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 or iDRAC. 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 147. 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 sessions, the session closes.
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 148. 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.

cfgSerialBaudRate (Read/Write)

Table 149. 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 150. Details of cfgSerialConsoleEnable

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

cfgSerialConsoleQuitKey (Read or Write)

Table 151. Details of cfgSerialConsoleQuitKey attribute

Description

Legal value:

NOTE: The CTRL key is represented by using the ^ (carat) character.

NOTE: The CTRL key does not generate a character by itself, but must be struck simultaneously with another key to generate a character.

For example, striking both the CTRL key and the \ key simultaneously (rather than sequentially) is denoted as ^\.

Configuration options: The value must start with the ^ character, and must follow one of the characters — a-z, A-Z, [,], \

In the input command, use \ without the quotes. For example:

```
config -g cfgSerial -o cfgSerialConsoleQuitKey "SHIFT+6"\\
```

Default:

cfgSerialConsoleIdleTimeout (Read/Write)

Table 152. Details of cfgSerialConsoleIdleTimeout

Description	The maximum number of seconds to wait before an idle serial session is disconnected.
Legal Values	• 0 = No timeout • 60 – 1920
Default	1800

cfgSerialConsoleNoAuth (Read/Write)

Table 153. 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 154. 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 155. 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 156. Details of cfgSerialHistorySize

Description	Specifies the maximum size of the serial history buffer.
Legal Values	0 – 8192

Default	8192

cfgSerialSshEnable (Read/Write)

Table 157. Details of cfgSerialSshEnable

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

cfgSerialTelnetEnable (Read/Write)

Table 158. 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.

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

cfgOobSnmpAgentCommunity (Read/Write)

Table 159. 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
```

```
cfgOobSnmpTrapsEnable=1
cfgOobSnmpAgentCommunity=public
```

cfgOobSnmpAgentEnable (Read/Write)

Table 160. Details of cfgOobSnmpAgentEnable

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

cfgOobSnmpProtocol

Table 161. Details of cfgOobSnmpProtocol attribute

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

cfgOobSnmpTrapFormat

Table 162. Details of cfgOobSnmpTrapFormat attribute

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

cfgTrapsIndex (Read Only)

Table 163. Details of cfgTrapsIndex

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

cfgTrapsEnable

Table 164. Details of cfgTrapsEnable

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

cfgTrapsAlertDestIpAddr

Table 165. 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 166. 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.
Legal Values	A string representing the community name.
Default	None

Example

```
racadm getconfig -g cfgTraps -i 2
```

```
# cfgTrapsIndex=2
cfgTrapsEnable=1
cfgTrapsAlertDestIpAddr=
cfgTrapsCommunityName=public
```

cfgTrapsSNMPv3UserId (Read Only)

Table 167. Details of cfgTrapsSNMPv3UserId attribute

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

cfgTrapsSNMPv3UserName

Table 168. 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.

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

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

cfgRacTuneSMBVersionEnable

Table 169. Details of cfgUseCMCDNSSettings attribute

Description	Can be used for setting the SMB version.
Legal Values	• SMBv1 • SMBv2

	• SMBv3 • 1 • 2 • 3
Default	NA

cfgRacTuneDefCredentialWarningEnable

Table 170. 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 171. Details of cfgRacTuneRemoteRacadmEnable

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

cfgRacTuneChassisMgmtAtServer

Table 172. Details of cfgRacTuneChassisMgmtAtServer

Description	Modify the Rack System Management Mode
Legal Values	• 0 — Disable • 1 — Monitor • 2 — Manage and Monitor
Default	2

cfgRacTuneHttpPort (Read/Write)

Table 173. Details of cfgRacTuneHttpPort

Description	Specifies the port number to use for HTTP 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, 60106.**
Default	80

cfgRacTuneHttpsPort (Read/Write)

Table 174. 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, 4003, 4096, 5988, 5989, 6900, 9000, 60106.**
Default	443

cfgRacTuneIpRangeEnable (Read/Write)

Table 175. 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 176. 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 177. 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 178. Details of cfgRacTuneIpBlkEnable

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

cfgRacTuneIpBlkFailCount (Read/Write)

Table 179. 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 180. 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 181. 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 182. Details of cfgRacTuneSshPort

Description	Specifies the port number used for the SSH interface.
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, 60106.**
Default	22

cfgRacTuneTelnetPort (Read/Write)

Table 183. 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, 60106.**
Legal Values	• For CMC: 10 – 65535

- For iDRAC: 1 – 65535

Default	23

cfgRacTuneDaylightOffset (Read Only)

Table 184. 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

Example

```
racadm getconfig -g cfgRacTuning [-m server-<n>] -o
<
object name
> <
object value
>
```

```
cfgRacTuneRemoteRacadmEnable=1
cfgRacTuneWebserverEnable=1
cfgRacTuneHttpPort=80
cfgRacTuneHttpsPort=443
cfgRacTuneTelnetPort=23
cfgRacTuneSshPort=22
cfgRacTuneIpRangeEnable=0
cfgRacTuneIpRangeAddr=192.168.1.1
cfgRacTuneIpRangeMask=255.255.255.0
cfgRacTuneIpBlkEnable=0
cfgRacTuneIpBlkFailCount=5
cfgRacTuneIpBlkFailWindow=60
cfgRacTuneIpBlkPenaltyTime=300
# cfgRacTuneTimezoneOffset=-18000
# cfgRacTuneDaylightOffset=3600
```

cfgRacTuneTimezoneOffset

Table 185. 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) • - 480 (PST — 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	- 720–7800
Default	0

cfgRacTuneSledNetworkUplink

Table 186. Details of cfgRacTuneSledNetworkUplink

Description	Configuration of all the sleds that contain an internal network switch (for example, the FM120).
Legal Values	• 1 - Standard (aggregated) • 2 - Network Adaptor Isolation (Enhanced Security) • 3 - Isolated Networks
Default	1

cfgRacTuneUserBlkEnable

Table 187. Details of cfgRacTuneUserBlkEnable

Description	Blocks the login for maximum of 5 minutes after 5 unsuccessful login attempts. The login using any interface such as **WSMAN** or **GUI** is blocked after 5 unsuccessful attempts. **NOTE: This is applicable only to configure the user privilege.**
Legal Values	• 1 – Enabled • 0 – Disabled
Default	0 — Disabled

Example

```
racadm getconfig -g cfgRacTuning [-m server-<n>] -o
<
object name
> <
object value
>
```

```
cfgRacTuneRemoteRacadmEnable=1
cfgRacTuneWebserverEnable=1
cfgRacTuneHttpPort=80
cfgRacTuneHttpsPort=443
cfgRacTuneTelnetPort=23
cfgRacTuneSshPort=22
cfgRacTuneIpRangeEnable=0
cfgRacTuneIpRangeAddr=192.168.1.1
cfgRacTuneIpRangeMask=255.255.255.0
cfgRacTuneIpBlkEnable=0
cfgRacTuneIpBlkFailCount=5
cfgRacTuneIpBlkFailWindow=60
```

```
cfgRacTuneIpBlkPenaltyTime=300
# cfgRacTuneTimezoneOffset=-18000
# cfgRacTuneDaylightOffset=3600
```

cfgRacTuneWebserverEnable (Read/Write)

Table 188. 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)
Default	1

cfgRacTuneFipsModeEnable

Table 189. 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 190. 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

cfgServerInfo

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

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

Use this object with the config or getconfig subcommands.

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

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

cfgServerInfoIndex (Read Only)

Table 191. Details of cfgServerInfoIndex

Description	Displays the index name of the server.

cfgServerSlotNumber (Read Only)

Table 192. Details of cfgServerSlotNumber

Description	Specifies the location of the specified server (1–4) in the chassis.

cfgServerServiceTag (Read Only)

Table 193. Details of cfgServerServiceTag

Description	Displays the service tag of the specified server.

cfgServerName (Read/Write)

Table 194. 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.
Default	SLOT - *<slot number>*

cfgServerFW (Read Only)

Table 195. Details of cfgServerFW

Description	Displays the server's CMC management firmware revision.

cfgServerBIOS (Read Only)

Table 196. Details of cfgServerBIOS

Description	Displays the server's BIOS revision.

cfgServerBmcMacAddress (Read Only)

Table 197. Details of cfgServerBmcMacAddress

Description	Displays the BMC MAC address of the specified server.

cfgServerNic1MacAddress (Read Only)

Table 198. Details of cfgServerNic1MacAddress

Description	Displays the MAC address of the server NIC 1.

cfgServerNic2MacAddress (Read Only)

Table 199. Details of cfgServerNic2MacAddress

Description	Displays the MAC address of the server NIC 2.

cfgServerNic3MacAddress (Read Only)

Table 200. Details of cfgServerNic3MacAddress

Description	Displays the MAC address of the server NIC 3.

cfgServerNic4MacAddress (Read Only)

Table 201. Details of

Description	Displays the MAC address of the server NIC 4.

cfgServerNicEnable (Read/Write)

Table 202. Details of cfgServerNic4MacAddress

Description	Enables or disables LAN channel.
Legal Values	• 1 (Enable) • 0 (Disable)

cfgServerNodeId

Table 203. Details of cfgServerNodeId

Description	Unique identification for a server provided by Dell for support and maintenance.

cfgServerIPMIOverLanEnable (Read/Write)

Table 204. Details of cfgServerIPMIOverLanEnable

Description	Enables or disables IPMI LAN channel.
Legal Values	• 1 (enable) • 0 (disable)

cfgServerDNSRegisterIMC (Read/Write)

Table 205. Details of cfgServerDNSRegisterIMC

Description	Enables or disables DNS name registration for the CMC.
Legal Values	• 1 (enable) • 0 (disable)

cfgServerDNSIMCName (Read/Write)

Table 206. Details of cfgServerDNSIMCName

Description	Displays the DNS domain name for the CMC.

cfgServerRootPassword (Write Only)

Table 207. Details of cfgServerRootPassword

Description	Displays the password for CMC as a series of asterisks (*). It cannot be seen or displayed after this property is written.

cfgServerFirstBootDevice (Read/Write)

Table 208. 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 = None • 0 = Default • 4 = PXE • 8 = HDD • 20 = CD-DVD • 24 = BIOS • 28 = vFDD • 32 = vCD-DVD • 40 = SD • 44 = RFS • 48 = F11 • 52 = F10 • 60 = FDD
Default	0 = None

cfgServerBootOnce (Read/Write)

Table 209. 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

cfgStorageModule

This group contains the parameters to configure storage sleds.
Use this command with the `config` and `getconfig` commands.

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

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

cfgStorageModuleStorageMode (Read/Write)

Table 210. Details of cfgStorageModuleStorageMode

Description	Displays the configuration mode of the storage sled.
Legal Values	• 2 — Split-single • 1 — Split-dual • 0 — Joined

cfgStorageModuleServiceTag (Read Only)

Table 211. Details of cfgStorageModuleServiceTag

Description	Displays the Service Tag of the storage sled.
Legal Values	Any printable string of up to seven alpha-numeric characters, without white space.

cfgStorageModuleAssetTag (Read/Write)

Table 212. Details of cfgStorageModuleAssetTag

Description	Displays the Asset Tag of the storage sled.
Legal Values	Any printable alpha-numeric string of up to 254 characters, without white space.

ConnectedServer (Read Only)

Table 213. Details of ConnectedServer

Description	Displays the name of the compute sled to which storage sled is connected.
Legal Values	None
Default Value	None

RAID-EnabledControllers (Read Only)

Table 214. Details of RAID-EnabledControllers

Description	Displays the name of the RAID-enabled controller. This property is updated when the single RAID or dual RAID license is applied.
Legal Values	None
Default Values	None

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.

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

cfgADRacName (Read/Write)

Table 215. 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 216. 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 or Write)

Table 217. 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	<blank>

cfgADRootDomain

Table 218. 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 219. 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 220. Details of cfgADAuthTimeout

Description	Specifies the number of seconds to wait for Active Directory authentication requests to complete before timing out. **NOTE: To modify this property, you must have the Configure CMC permission.**
Legal Values	15–300 seconds
Default	120

cfgADSCLEnable

Table 221. 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 222. Details of cfgADSSOEnable

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

cfgADDomainController

Table 223. Details of cfgADDomainController

Description	Specifies the AD server from which you want the CMC to obtain user names. Must be used with **cfgADSpecifyServerEnable.**
Legal Values	Valid IP address or fully qualified domain name (FQDN).

cfgADDomainController1 (Read/Write)

Table 224. 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).

cfgADDomainController2 (Read/Write)

Table 225. 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).

cfgADDomainController3 (Read/Write)

Table 226. 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).

cfgADGlobalCatalog1 (Read/Write)

Table 227. 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).

cfgADGlobalCatalog2 (Read/Write)

Table 228. 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).

cfgADGlobalCatalog3 (Read/Write)

Table 229. 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).

cfgADType (Read/Write)

Table 230. 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

cfgADDcSRVLookupDomainName (Read/Write)

Table 231. 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

cfgADDcSRVLookupDomainName (Read/Write)

Table 232. 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 233. 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

cfgADSpecifyServerEnable

Table 234. 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.

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

cfgLdapEnable (Read/Write)

Table 235. Details of cfgLdapEnable

Description	Turns LDAP service on or off. 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 236. 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 237. Details of cfgLdapPort

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

cfgLdapBasedn (Read/Write)

Table 238. 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 239. 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 240. 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 241. 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 242. 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 243. 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 244. 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 245. 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 246. Details of cfgLDAPNetworkTimeout

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

cfgLDAPSearchTimeout

Table 247. Details of cfgLDAPSearchTimeout

Description	Configures the search timeout in seconds.
Legal Values	Positive integer

Default	120 seconds

cfgLDAPSRVLookupDomainName

Table 248. 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 249. 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 250. 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.

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 251. 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 252. 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 253. Details of cfgLocationDatacenter

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

cfgLocationAisle (Read/Write)

Table 254. 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 255. 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 256. 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 257. Details of cfgLocationDevicesize

Description	Indicates server chassis size.
Legal Values	Values from 1 - 255
Default	2U

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.

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

cfgSSADRoleGroupIndex (Read Only)

Table 258. 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 259. 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 260. 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 261. 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>*

Table 262. Example

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 263. Details of cfgChassisInPower

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

cfgChassisPeakPower (Read Only)

Table 264. Details of cfgChassisPeakPower

Description	The maximum system input power consumption (in Watts), because the value was last cleared by a user.
Legal Values	None
Default	None

cfgChassisPeakPowerTimestamp (Read Only)

Table 265. Details of cfgChassisPeakPowerTimestamp

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

cfgChassisMinPower (Read Only)

Table 266. Details of cfgChassisMinPower

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

cfgChassisMinPowerTimestamp (Read Only)

Table 267. Details of cfgChassisMinPowerTimestamp

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

cfgChassisPowerStatus (Read Only)

Table 268. 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 269. Details of cfgChassisRedundantState

Description	Indicates the power supply redundancy status.
Legal Values	• 0 (none)

- 1 (full)

Default	None

cfgChassisMaxPowerConservationMode (Read/Write)

Table 270. Details of cfgChassisMaxPowerConservationMode

Description	Enables or disables maximum power conservation mode. When enabled, all servers are immediately reduced to their minimum power levels, and all subsequent server power allocation requests are denied. In this mode, performance of the servers that are turned on may be degraded, and additional servers cannot be turned on, regardless of the server priority.
Legal Values	• 0 (disabled) • 1 (enabled)
Default	0 (disabled)

cfgChassisPowerCapUpperBound (Read Only)

Table 271. Details of cfgChassisPowerCapUpperBound

Description	Indicates the minimum chassis thermal capacity, power supply capacity, and server maximum input.
Legal Values	None
Default	None

cfgChassisPowerCapLowerBound (Read Only)

Table 272. Details of cfgChassisPowerCapLowerBound

Description	Indicates the minimum power required to operate the chassis with the servers running.
Legal Values	None
Default	None

cfgChassisSledPowerButtonEnable

Table 273. Details of cfgChassisSledPowerButtonEnable

Description	Permits to use the power button on all multi-node Sleds (such as the FM120).
Legal Values	• 1 — Enable • 0 — Disable
Default	1

cfgChassisPowerCap (Read/Write)

Table 274. Details of cfgChassisPowerCap

Description	Indicates the maximum power consumption limit (in Watts) 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	539 – 3371 Watts
Default	3371 Watts

cfgChassisPowerCapF (Read/Write)

Table 275. Details of cfgChassisPowerCapF

Description	Indicates the maximum power consumption limit (in Watts) 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	539 – 3371 Watts
Default	3371 Watts

cfgChassisPowerCapBTU (Read/Write)

Table 276. 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.
Legal Values	1839-11501 BTU/hr
Default	11501 BTU/hr

cfgChassisPowerCapFBTU (Read/Write)

Table 277. 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/Write)

Table 278. 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 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 279. 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 280. Details of cfgChassisRedundancyPolicy

Description	Sets the redundancy policy of the chassis.
Legal Values	• 0 — No redundancy • 1 — Grid redundancy • 3 — Redundancy alerting only • 4 — Fault tolerant redundancy
Default	3 — Redundancy alerting only

cfgChassisInMaxPowerCapacity (Read Only)

Table 281. 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 282. Details of cfgChassisInRedundancyReserve

Description	Indicates the amount of redundant power (in Watts) 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

cfgChassisPowerClear (Write Only)

Table 283. Details of cfgChassisPowerClear

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

cfgChassisPowerClearTimestamp (Read Only)

Table 284. Details of cfgChassisPowerClearTimestamp

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

cfgChassisPowerButtonEnable (Read/Write)

Table 285. Details of cfgChassisPowerButtonEnable

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

cfgChassisPowerCapBTU (Read/Write)

Table 286. 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.
Legal Values	9264 - 56931 BTU/hr
Default	43221 BTU/hr

cfgChassisACPowerRecoveryDisable

Table 287. 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.

cfgKvmEnable

Table 288. Details of cfgKvmEnable

Description	Enable KVM operation for all slots
Legal Values	• 0 — Disable • 1 — Enable
Default	1

cfgKvmMapping

Table 289. Details of cfgKvmMapping

Description	Selects the server to which the KVM connects
Legal Values	1[a-d]-4[a-d]
Default	0 (Unmapped)

cfgAlerting

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

Use this object with the config or getconfig subcommands.

cfgAlertingEnable

Table 290. 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 291. Details of cfgAlertingSourceEmailName

Description	Specifies the e-mail address used to send e-mail notifications when an event occurs.
Legal Values	None
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 Chassis Configuration Administrator privilege.

NOTE: To apply this setting to iDRAC, use the `-m` option.

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

cfgIPv6Enable (Read or Write)

Table 292. Details of cfgIPv6Enable

Description	Enables or disables `CMC IPv6` stack.
Legal Values	• `1` (TRUE) • `0` (FALSE)
Default	0

cfgIPv6AutoConfig (Read/Write)

Table 293. 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.** **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 294. 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 295. 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 296. 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	::

cfgCurrentIPv6DNSServersFromDHCP6

Table 297. Details of cfgCurrentIPv6DNSServersFromDHCP6

Description	Indicates whether the DNS server addresses are assigned from the DHCPv6 server.

cfgIPv6DNSServer1 (Read/Write)

Table 298. 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 299. 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
cfgCurrentIPv6Enabled=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
```

cfgNicCurrentIpAddress

Table 300. Details of cfgNicCurrentIpAddress

Description	Displays the IP address the CMC is currently using.
Legal Values	Valid IPv4 addresses. For example: 192.168.0.20.

cfgNicCurrentNetmask

Table 301. Details of cfgNicCurrentNetmask

Description	Displays the subnet mask the CMC is currently using.
Legal Values	Valid IPv4 addresses. For example: 192.168.0.20.

cfgNicCurrentGateway

Table 302. Details of cfgNicCurrentGateway

Description	Displays the Gateway address the CMC is currently using.
Legal Values	Valid IPv4 addresses. For example: 192.168.0.20.

cfgNicCurrentDhcpWasUsed

Table 303. 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 304. Details of cfgNicCurrentVlanEnable

Description	Indicates whether the VLAN is enabled.
Legal Values	0—VLAN is disabled 1—VLAN is enabled

cfgNicCurrentVlanID (Read Only)

Table 305. Details of cfgNicCurrentVlanID

Description	Indicates the Current Virtual Lan ID
Legal Values	Integer

cfgNicCurrentVlanPriority (Read Only)

Table 306. Details of cfgNicCurrentVlanPriority

Description	Indicates the Current Virtual Lan Priority.
Legal Values	Integer

cfgDNSCurrentServer1

Table 307. Details of cfgDNSCurrentServer1

Description	Displays the IP address for DNS server 1.
Legal Values	A Valid IPv4 DNS IP

cfgDNSCurrentServer2

Table 308. Details of cfgDNSCurrentServer2

Description	Displays the IP address for DNS server 2.

cfgDNSCurrentDomainName

Table 309. Details of cfgDNSCurrentDomainName

Description	Displays the DNS domain name.

cfgNicCurrentIPv4Enabled

Table 310. 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.

Example

```
racadm getconfig -g cfgCurrentLanNetworking
# cfgNicCurrentIPv4Enabled=1
# cfgNicCurrentIpAddress=192.68.152.116
# cfgNicCurrentNetmask=255.255.255.0
# cfgNicCurrentGateway=192.68.152.1
# cfgNicCurrentDhcpWasUsed=0
# cfgNicCurrentVlanEnable=0
# cfgNicCurrentVlanID=1
# cfgNicCurrentVlanPriority=0
# cfgDNSCurrentServer1=192.168.0.5
# cfgCurrentIPv6DNSServer2=192.168.0.6
# cfgDNSCurrentDomainName=MYDOMAIN
```

cfgCurrentIPv6LanNetworking (Read Only)

This group displays the current CMC IPv6 properties.

This group is applicable only for CMC. Use this object with the **getconfig** subcommand.

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

cfgCurrentIPv6Enabled (Read/Write)

Table 311. Details of cfgCurrentIPv6Enabled

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

cfgCurrentIPv6AutoConfigWasUsed

Table 312. 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 313. Details of cfgCurrentLinkLocalAddress

Description	Displays the current IPv6 link-local address of the CMC.

cfgCurrentIPv6Address

Table 314. Details of cfgCurrentIPv6Address

Description	Displays the current IPv6 addresses. This property displays up to 15 global IPv6 addresses, including stateful and stateless addresses.

cfgCurrentIPv6Gateway

Table 315. Details of cfgCurrentIPv6Gateway

Description	Displays the current IPv6 gateway.

cfgCurrentIPv6DNSServersFromDHCP6

Table 316. Details of cfgCurrentIPv6DNSServersFromDHCP6

Description	Indicates whether the DNS server addresses are assigned from the DHCPv6 server.

cfgCurrentIPv6DNSServer1

Table 317. Details of cfgCurrentIPv6DNSServer1

Description	Displays the IPv6 address for DNS server 1.

cfgCurrentIPv6DNSServer2

Table 318. Details of cfgCurrentIPv6DNSServer2

Description	Displays the IPv6 address for DNS server 2.

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 319. 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

cfgNetTuningNicAutoneg (Read/Write)

Table 320. 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
```

cfgNetTuningNicFullDuplex (Read/Write)

Table 321. 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 322. Details of cfgNetTuningNicMtu

Description	The size in bytes of the maximum transmission unit used by CMC NIC.
Legal Values	576 – 1500
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.

cfgNetTuningNicRedunadant

Table 323. Details of cfgNetTuningNicRedunadant

Description	Specifies either Stacking or Redundant mode for CMC Management Port 2.
Legal Values	• 0 – Stacking • 1 – Redundant
Default	0 – Stacking

NOTE: When Management Port 2 is set for Redundant but is cabled for Stacking, the downstream CMCs (further from the top-of-rack switch) will not have a network link.

NOTE: When Management Port 2 is set for Stacking but is cabled for Redundant (two connections to the TOR switch), routing loops could cause a network storm.

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 324. 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 254 characters.
Default	*<blank>*

cfgRacSecCsrOrganizationName (Read/Write)

Table 325. Details of cfgRacSecCsrOrganizationName

Description	Specifies the CSR Organization Name (O).
Legal Values	A string of up to 254 characters.
Default	*<blank>*

cfgRacSecCsrOrganizationUnit (Read/Write)

Table 326. Details of cfgRacSecCsrOrganizationUnit

Description	Specifies the CSR Organization Unit (OU).
Legal Values	A string of up to 254 characters.
Default	*<blank>*

cfgRacSecCsrLocalityName (Read/Write)

Table 327. Details of cfgRacSecCsrLocalityName

Description	Specifies the CSR Locality (L).
Legal Values	A string of up to 254 characters.
Default	*<blank>*

cfgRacSecCsrStateName (Read/Write)

Table 328. Details of cfgRacSecCsrStateName

Description	Specifies the CSR State Name (S).
Legal Values	A string of up to 254 characters.
Default	*<blank>*

cfgRacSecCsrCountryCode (Read/Write)

Table 329. 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 330. Details of cfgRacSecCsrEmailAddr

Description	Specifies the CSR email address.
Legal Values	A string of up to 254 characters.
Default	*<blank>*

Example

```
racadm config -g cfgRacSecurity
```

```
cfgRacSecCsrKeySize=1024
cfgRacSecCommonName=
```

```
cfgRacSecOrganizationName=
cfgRacSecOrganizationUnit=
cfgRacSecLocalityName=
cfgRacSecStateName=
cfgRacSecCountryCode=
cfgRacSecEmailAddr=
```

cfgRacSecCsrKeySize (Read/Write)

Table 331. Details of cfgRacSecCsrKeySize

Description	Specifies the SSL asymmetric key size for the CSRs.
Legal Values	1024, 2048, 4096
Default	2048

cfgPCIe

Displays the PCIe reassignment information.

Use this sub command with the `getconfig` and `config` commands.

The following section provides information about the objects in the **cfgPCIe** group.

cfgPCIeReassignmentEnable (Read/Write)

Table 332. Details of cfgPCIeReassignmentEnable

Description	Indicates whether the PCIe reassignment is enabled or disabled.
Legal Values	• 0 — Disable • 1 — Enable

NOTE: Power off all the servers in the FX2s chassis before changing the PCIe reassignment.

cfgQuickDeploy

This group is used to configure IDRAC deployment settings. You must have blade administrator privileges for configuring the settings.

cfgActionOnServerInsertion

Table 333. 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 334. 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 335. 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 336. 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 337. 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 338. Details of cfgEnableiDRACIPMIOverLAN attribute

Description	Enables IPMI over LAN channel for iDRAC when servers are inserted into the chassis.
Legal Values	• 0 — Disable • 1 — Enable
Default	0

cfgEnableiDRACIPv4DHCP

Table 339. 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 340. 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 341. 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 342. 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 343. 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 344. 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 345. 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 346. 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 347. Details of cfgReservedIPAddressNumbers attribute

Description	The number of static IPv4 addresses reserved for iDRACs in the chassis.
Legal Values	32
Default	32

cfgUseCMCDNSSettings

Table 348. 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