iDRAC with Lifecycle Controller Version 3.36.36.36

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.

2019 - 09

Rev. A00

Contents

1

Introduction

This document provides information about the RACADM subcommands, supported RACADM interfaces, and property database groups and object definitions for iDRAC for the Dell EMC servers.

Topics:

New in this release

- Added support for `System.ThermalSettings DriveTemperaturePolling` attribute.

Supported RACADM Interfaces

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

The RACADM utility supports the following interfaces:

- Local—Supports running RACADM commands from the managed server's operating system. To run local RACADM commands, install the OpenManage software on the managed server. Only one instance of Local RACADM can be executed on a system at a time. If you try to open another instance, an error message is displayed and the second instance of Local RACADM closes immediately. To download the local RACADM tool from www.dell.com/support, select **Drivers and Downloads**, select a server, and then select **Systems Management** > **Dell Toolkit**.

  NOTE: Local RACADM and local RACADM proxy runs with root user privilege.
- SSH or Telnet—Also known as Firmware RACADM. Firmware RACADM is accessible by logging in to iDRAC using SSH or Telnet. Similar to Remote RACADM, at the RACADM prompt, directly run the commands without the RACADM prefix.
- Remote—Supports running RACADM commands from a remote management station such as a laptop or desktop. To run Remote RACADM commands, install the DRAC Tools utility from the OpenManage software on the remote computer. To run Remote RACADM commands:

  - Formulate the command as a SSH or Telnet RACADM command.

  NOTE: You must have administrator privileges to run RACADM commands using Remote RACADM.

  For more information about the options, see RACADM Subcommand Details. To download the local RACADM tool, go to www.dell.com/poweredgemanuals, select the desired server. and then click **Drivers & downloads**.

RACADM Syntax Usage

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

SSH, Telnet, or Remote RACADM

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

```
racadm -r <racIPAddr> -u username -p password getconfig -g <group name> -o <object name>
```

```
racadm <subcommand>
```

Example

```
racadm getsysinfo
```

```
racadm -r 192.168.0.2 -u username -p xxx getsysinfo
```

```
racadm -r 192.168.0.2 -u username -p xxx getconfig -g cfgchassispower
```

Remote RACADM

NOTE: By default, TLS version 1.0 is enabled on Windows 2012 R2 which is not supported on the Remote RACADM. Install the latest Windows update available, to updgrade TLS to version 1.1 or higher. Also, set the TLS version in the `iDRAC.Webserver.TLSProtocol` as appropriate. For more information about Windows update see, support.microsoft.com/en-us/help/3140245/update-to-enable-tls-1-1-and-tls-1-2-as-default-secure-protocols-in-wi

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

Example

```
racadm -r 192.168.0.2 -u root -p xxxx getsysinfo
Security Alert: Certificate is invalid - Certificate is not signed by Trusted Third Party
Continuing execution.
```

NOTE: The following command does not display a security error:

```
racadm -r 192.168.0.2 -u noble -p xxx getsysinfo --nocertwarn
```

The remote RACADM commands must link to the libssl library on the HOST, which corresponds to the version of OpenSSL package installed on the HOST. Perform the following steps to verify and link the library.

- Check the openssl version installed in the HOST:

```
[root@localhost ~]# openssl
OpenSSL> version
OpenSSL 1.0.1e-fips 11 Feb 2013
OpenSSL>
```

- Locate the openSSL libraries are in the HOST machine (/usr/lib64/ in case of RHEL), and to check the various versions of the libraries:

```
[root@localhost ~]# ls -l /usr/lib64/libssl*
-rwxr-xr-x. 1 root root 249368 Oct 15  2013 /usr/lib64/libssl3.so
lrwxrwxrwx. 1 root root     16 Oct 29  2014 /usr/lib64/libssl.so.10 -> libssl.so.1.0.1e
-rwxr-xr-x. 1 root root 439912 Sep 27  2013 /usr/lib64/libssl.so.1.0.1e
```

- Link the library libssl.so using ln -s command to the appropriate OpenSSL version in the HOST:

```
[root@localhost ~]# ln -s /usr/lib64/libssl.so.1.0.1e /usr/lib64/libssl.so
```

- Verify if the libssl.so soft linked to libssl.so.1.0.1e:

```
[root@localhost ~]# ls -l /usr/lib64/libssl*
-rwxr-xr-x. 1 root root 249368 Oct 15  2013 /usr/lib64/libssl3.so
```

```
lrwxrwxrwx. 1 root root     27 Aug 28 13:31 /usr/lib64/libssl.so -> /usr/lib64/
libssl.so.1.0.1e
lrwxrwxrwx. 1 root root     16 Oct 29  2014 /usr/lib64/libssl.so.10 -> libssl.so.1.0.1e
-rwxr-xr-x. 1 root root 439912 Sep 27  2013 /usr/lib64/libssl.so.1.0.1e
```

Accessing Indexed-Based Device Groups and Objects

- To access any object, run the following syntax:

```
device.<group name>.[<index>].<object name>
```

- To display the supported indexes for a specified group, run:

```
racadm get device.<group name>
```

Example

```
racadm get nic.nicconfig
NIC.nicconfig.1 [Key=NIC.Integrated.1-1-1#nicconfig]
NIC.nicconfig.2 [Key=NIC.Integrated.1-2-1#nicconfig]
NIC.nicconfig.3 [Key=NIC.Integrated.1-3-1#nicconfig]
NIC.nicconfig.4 [Key=NIC.Integrated.1-4-1#nicconfig]
```

- To display the object list for the specified group, run:

```
racadm get device.<group name>.<index>
```

Example

```
racadm get nic.nicconfig.2
[Key=NIC.Integrated.1-2-1#nicconfig]
BannerMessageTimeout=5
BootStrapType=AutoDetect
HideSetupPrompt=Disabled
LegacyBootProto=NONE
LnkSpeed=AutoNeg
#VLanId=1
VLanMode=Disabled
```

- To display a single object for the specified group, run:

```
racadm get device.<group name>.<index>.<object name>
```

Example

```
racadm get nic.nicconfig.3.legacybootproto
[Key=NIC.Integrated.1-3#NICConfig]
Legacybootproto=PXE
```

RACADM Command Options

The following table lists the options for the RACADM command:

Table 1. RACADM Command Options

Option	Description
`-r <racIpAddr>` `-r <racIpAddr> : <port number>`	Specifies the controller's remote IP address. Use `<port number>` if the iDRAC port number is not the default port (443).
`-u <username>`	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 (interactive) is not allowed.

Option	Description
	NOTE: If you delete a user account using the iDRAC web interface and then use RACADM to create a new account with the same user name, you are not prompted to enter a password. However, you must manually provide a password for the account to be able to log into iDRAC using that account.
`-p <password>`	Specifies the password used to authenticate the command transaction. If the `-p` option is used, the `-i` option is not allowed.
`--nocertwarn`	Does not display certificate related warning message.

Using autocomplete feature

Use the autocomplete feature in firmware RACADM to:

- Display all the available RACADM commands in the alphabetical order on pressing the tab key at the prompt.
- View the complete list, enter the starting letter of the command at the prompt and press tab key.
- Navigate the cursor within a command, press:

  Home key: Directs to the starting of the command.

  End key: Directs to the end of the command.
- View the history of the commands that were run in the current session, press up and down arrow key.
- Exit the Autocomplete mode, enter `Quit`, `Exit`, or press Ctrl+D key.

For example:

- Example 1: `racadm> <press tab>`

```
arp
autoupdatescheduler
clearasrscreen
clearpending
closessn
clrraclog
.
.
.
.
.
.
.
vflashsd
vflashpartition
vmdisconnect
cd
quit
```

- Example 2: `racadm> get <press tab>`

```
get
getconfig
getled
getniccfg
getraclog
getractime
getsel
getsensorinfo
getssninfo
getsvctag
getsysinfo
gettracelog
getversion
```

- Example 3:

```
racadm> getl<press tab>
```

```
racadm> getled <press enter> or <racadm getled>
LEDState: Not-Blinking
```

- Example 4:

```
racadm>> get bios.uefiBootSettings
BIOS.UefiBootSettings
BIOS.UefiBootSettings.UefiBootSeq
BIOS.UefiBootSettings.UefiPxeIpVersion
```

NOTE: In the RACADM autocomplete mode, certain RACADM commands may not be listed inline with the platforms. In such scenarios, execute the RACADM command in the normal execution mode.

NOTE: In the RACADM autocomplete mode, type the commands directly without giving racadm as prefix.

NOTE: The RACADM get or set attributes with value length up to 512 characters are supported from autocomplete mode. If the value length is 512 characters or more, execute the RACADM command in the normal execution mode.

Lifecycle Controller Log

Lifecycle Controller logs provide the history of changes related to components installed on a managed system. You can also add work notes to each log entry.

The following events and activities are logged:

- System events
- Storage devices
- Network devices
- Configuration
- Audit
- Updates

You can view and filter logs based on the category and severity level. You can also export and add a work note to a log event.

If you initiate configuration jobs using RACADM CLI or iDRAC web interface, the Lifecycle log captures the information about the user, interface used, and the IP address of the system from which you initiate the job.

Unsupported RACADM Subcommands

The following table provides the list of RACADM subcommands which are not supported.

Table 2. Unsupported RACADM Subcommands

Subcommand	iDRAC on Blade Servers
	Telnet/SSH/Serial
krbkeytabupload	No
sslcertupload	No
sslkeyupload	No
usercertupload	No

Proxy parameters

Some commands do not support setting the proxy parameters if the share location (-l) is HTTP/HTTPS. To perform the operation with HTTP or HTTPS through a proxy, the proxy parameters must be first configured using the lifecyclecontroller.lcattributes. Once these proxy parameters are configured, they become the part of default configuration; the proxy attributes should be cleared to end use of the HTTP/HTTPS proxy.

The valid lifecyclecontroller.lcattributes HTTP/HTTPS proxy parameters are:

- `UserProxyUserName`
- `UserProxyPassword`
- `UserProxyServer`
- `UserProxyPort`
- `UserProxyType`

To view the list of proxy attributes, use `racadm get lifecycleController.lcAttributes`.

NOTE: Squid proxy configuration is not supported to access HTTP/HTTPS shares.

Other Documents You May Need

In addition to this guide, you can access the following guides available on the Dell Support website at www.dell.com/esmmanuals. To access the documents, click the appropriate product link.

- The *Integrated Dell Remote Access Controller User's Guide* provides information about configuring and using an iDRAC to remotely manage and monitor your system and its shared resources through a network.
- The *iDRAC9 with Lifecycle Controller Attribute Registry* provides information about all attributes to perform get and set operations using RACADM interface.
- Documentation specific to your third-party management console application.
- The *Dell OpenManage Server Administrator's User's Guide* provides information about installing and using Dell OpenManage Server Administrator.
- The *Dell Update Packages User's Guide* provides information about obtaining and using Dell Update Packages as part of your system update strategy.
- The *Glossary* provides information about the terms used in this document.

The following system documents are also available to provide more information about the system in which iDRAC is installed:

- The *Hardware Owner's Manual* provides information about system features and describes how to troubleshoot the system and install or replace system components.
- Documentation for any components you purchased separately provides information to configure and install the options.
- Release notes or readme files may be included to provide last-minute updates to the system or documentation or advanced technical reference material intended for experienced users or technicians.

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.

See the *Safety and Regulatory* information that is shipped with your system.

NOTE: Warranty information may be included within this document or as a separate document.

Accessing documents from Dell support site

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

- Using the following links:
  - For all Enterprise Systems Management documents — www.dell.com/esmmanuals
  - For OpenManage documents — www.dell.com/openmanagemanuals
  - For iDRAC and Lifecycle Controller documents — www.dell.com/idracmanuals
  - For OpenManage Connections Enterprise Systems Management documents — www.dell.com/omconnectionsclient
  - For Serviceability Tools documents — www.dell.com/ServiceabilityTools
  - For Client Command Suite Systems Management documents — www.dell.com/DellClientCommandSuiteManuals
- From the Dell Support site:
  1. Go to www.dell.com/support/home.
  2. Under **Browse all products** section, click **Software**.
  3. In the **Software** group box, click the required link from the following:
     - **Enterprise Systems Management**
     - **Client Systems Management**
     - **Serviceability Tools**

4. To view a document, click the required product version.

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

Contacting Dell

NOTE: If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues:

1. Go to www.dell.com/support.
2. Select your support category.
3. Verify your country or region in the **Choose a Country/Region** drop-down list at the bottom of the page.
4. Select the appropriate service or support link based on your need.

2

RACADM Subcommand Details

This section provides detailed description of the RACADM subcommands including the syntax and valid entries.

Topics:

- ping
- ping6
- RACADM Proxy
- racdump
- racreset
- racresetcfg
- recover
- remoteimage
- rollback
- sensorsettings
- serveraction
- set
- setled
- setniccfg
- sshpkauth
- sslcertdownload
- sslcertupload
- sslcertview
- sslcertdelete
- sslcsrgen
- sslkeyupload
- sslresetcfg
- Storage
- SupportAssist
- swinventory
- switchconnection
- systemconfig
- systemerase
- systemperfstatistics
- techsupreport
- testemail
- testtrap
- testalert
- traceroute
- traceroute6
- update
- usercertupload
- usercertview
- vflashsd
- vflashpartition
- vmdisconnect

Guidelines to Quote Strings Containing Special Characters When Using RACADM Commands

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

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

- $ (dollar sign)
- " (double quotation marks)
- ` (backward quotation marks)
- \ (backward slash)
- ~ (tilde)
- | (vertical bar)
- ((left parentheses)
-) (right parentheses)

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

There are different escaping rules for double quotation marks.

For using double quotation marks:

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

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

help and help subcommand

Table 3. help and help subcommand

Description	Lists all the subcommands available for use with **RACADM** and provides a short description about each subcommand. You may also type a subcommand, group, object or Fully Qualified Descriptor (FQDD) name after `help`.
Synopsis	• `racadm help` • `racadm help <subcommand>`
Input	• `<subcommand>` — specifies the subcommand for which you need the help information. • `<device name>` — specifies the device name such as iDRAC, BIOS, NIC, LifecycleController, FC, system, or Storage. • `<group>` — specifies the group name supported by the corresponding device. • `<object>` — specifies the object for the entered group.
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 <device name> <Group>` command displays information for the specified group. • The `racadm help <device name> <Group> <Object>` command displays information for the specified object.

arp

Table 4. Details of arp sub command

Description	Displays the contents of the Address Resolution Protocol (ARP) table. ARP table entries cannot be added or deleted. To use this subcommand, you must have Debug privilege.
Synopsis	`racadm arp`
Input	N/A
Example	`racadm arp`

Output

Table 5. Details of output

Address	HW Type	HW Address	Mask	Device
192.168.1.1	Ether	00:0d:65:f3:7c:bf	C	eth0

autoupdatescheduler

Table 6. Details of the autoupdatescheduler command

Description

You can automatically update the firmware of the devices on the server.

To run this subcommand, you must have the Server Control privilege.

NOTE:

- **The `autoupdatescheduler` subcommand can be enabled or disabled.**
- **Lifecycle Controller and CSIOR may not be enabled to run this subcommand.**
- **The autoupdatescheduler can be enabled or disabled.**
- **The minimum Lifecycle Controller version required is Lifecycle Controller 1.3.**
- **When a job is already scheduled and the `clear` command is run, the scheduling parameters are cleared.**
- **If the network share is not accessible or the catalog file is missing when the job is scheduled, then the job is unsuccessful.**

Synopsis

- To create the AutoUpdateScheduler, run the command.

```
racadm autoupdatescheduler create -u <user> -p <password> -l <location> -f
<filename> -time <time> -dom <DayOfMonth> -wom <WeekOfMonth> -dow
<DayofWeek> -rp <repeat> -a <applyreboot> -ph <proxyHost> -pu <proxyUser> -
pp <proxyPassword> -po <proxyPort> -pt <proxyType>
```

- To view AutoUpdateScheduler parameter, run the command.

```
racadm autoupdatescheduler view
```

- To clear and display AutoUpdateScheduler parameter, run the command.

```
racadm autoupdatescheduler clear
```

NOTE: After the parameters are cleared, the AutoUpdateScheduler is disabled. To schedule the update again, enable the AutoUpdateScheduler.

Input

Valid options:

- `-u` — Specifies the user name of the remote share that stores the catalog file.

  NOTE: For CIFS, enter the domain name as domain or username.
- `-p` — Specifies the password of the remote share that stores the catalog file.
- `-l` — Specifies the network share (NFS, CIFS, FTP, TFTP,HTTP, or HTTPS) location of the catalog file. IPv4 and IPv6 addresses are supported.
- `-f` — Specifies the catalog location and the filename. If the filename is not specified, then the default file used is `catalog.xml`.

  NOTE: If the file is in a subfolder within the share location, then enter the network share location in the `-l` option and enter the subfolder location and the filename in the `-f` option.
- `-ph` — Specifies the FTP/HTTP proxy host name.
- `-pu` — Specifies the FTP/HTTP proxy user name.
- `-pp` — Specifies the FTP/HTTP proxy password.
- `-po` — Specifies the FTP/HTTP proxy port.
- `-pt` — Specifies the FTP/HTTP proxy type.
- `-time` — Specifies the time to schedule an autoupdate in the HH:MM format. This option must be specified.
- `-dom` — Specifies the day of month to schedule an autoupdate. Valid values are 1–28, L (Last day) or '*' (default — any day).

- `-wom` — Specifies the week of month to schedule an autoupdate. Valid values are 1–4, L (Last week) or '*' (default — any week).
- `-dow` — Specifies the day of week to schedule an autoupdate. Valid values are sun, mon, tue, wed, thu, fri, sat, or '*' (default — any day).

NOTE: The `-dom`, `-wom`, or `-dow` option must be included in the command for the autoupdate schedule. The * value for the options must be included within ' ' (single quotation mark).

- **If the `-dom` option is specified, then the `-wom` and `-dow` options are not required.**
- **If the `-wom` option is specified, then the `-dow` is required and `-dom` is not required.**
- **If the `-dom` option is non-'*', then the schedule repeats by month.**
- **If the `-wom` option is non-'*', then the schedule repeats by month.**
- **If the `-dom` and `-wom` options are '*' and the `-dow` option is non-'*', then the schedule repeats by week.**
- **If all the three `-dom`, `-wom` and `-dow` options are '*', then the schedule repeats by day.**

- `-rp` — Specifies the repeat parameter. This parameter must be specified.
  - If the `-dom` option is specified, then the valid values for `-rp` are 1–12.
  - If the `-wom` option is specified, then the valid values for `-rp` are 1–52.
  - If the `-dow` option is specified, then the valid values for `-rp` are 1–366.
- `-a` — Applies reboot (1 — Yes, 0 — No). This option must be specified.

Example

Usage examples:

- To configure autoupdate feature settings.
  - For CIFS, run the command:

```
racadm autoupdatescheduler create -u domain/admin -p xxx -l //1.2.3.4/
share -f cat.xml -time 14:30 -wom 1 -dow sun -rp 1 -a 1
```

  - For NFS, run the command:

```
 racadm autoupdatescheduler create -u nfsadmin -p nfspwd -l 1.2.3.4:/
share -f cat.xml -time 14:30 -dom 1 -rp 5 -a 1
```

  - For FTP, run the command:

```
racadm autoupdatescheduler create -u ftpuser -p ftppwd -l ftp.test.com -f
cat.xml.gz -ph 10.20.30.40 -pu padmin -pp ppwd -po 8080 -pt http -time
14:30 -dom 1 -rp 5 -a 1
```

  - For HTTP, run the command:

```
racadm autoupdatescheduler create -u httpuser -p httppwd   -l http://
test.com -f cat.xml -ph 10.20.30.40 -pu padmin -pp ppwd   -po 8080 -pt
http -time 14:30 -dom 1 -rp 5 -a 1
```

  - For TFTP, run the command:

```
 racadm autoupdatescheduler create -l tftp://1.2.3.4 -f cat.xml.gz -
time 14:30 -dom 1
-rp 5 -a 1
```

  - To view AutoUpdateScheduler parameter:

```
racadm autoupdatescheduler view
hostname    = 192.168.0
sharename   = nfs
sharetype   = nfs
catalogname = Catlog.xml
time        = 14:30dayofmonth =1
repeat      = 5
applyreboot = 1
idracuser   = racuser
```

- To clear and display AutoUpdateScheduler parameter:

```
racadm autoupdatescheduler clear
RAC1047: Successfully cleared the Automatic Update (autoupdate) feature
settings
```

bioscert

Table 7. Details of the bioscert subcommand

Description

Allows you to

- View the installed Secure Boot Certificates. To view, you must have the Login privilege
- Export the Secure Boot Certificate to a remote share or local system. To export, you must have the Login privilege
- Import the Secure Boot Certificate from a remote share or local system. To import, you must have login and system control privilege
- Delete the installed Secure Boot Certificate. To delete, you must have login and system control privilege
- Restore the installed Secure Boot Certificate Sections. To restore, you must have login and system control privilege

Synopsis

- To view the installed Secure Boot Certificates

```
racadm bioscert view -all
```

- To export the Secure Boot Certificate to a remote share or local system.

```
racadm bioscert view -t <keyType> -k <KeySubType> -v <HashValue or
ThumbPrintValue>
```

- ```
  racadm bioscert export -t <keyType> -k <KeySubType> -v <HashValue or
  ThumbPrintValue> -f <filename> -l <CIFS/NFS/HTTP/HTTPS share> -u <username>
  -p <password>
  ```
- ```
  racadm bioscert import -t <keyType> -k <KeySubType> -f <filename> -l
  <CIFS/NFS/HTTP/HTTPS share> -u <username> -p <password>
  ```
- ```
  racadm bioscert delete -all
  ```
- ```
  racadm bioscert delete -t <keyType> -k <KeySubType> -v <HashValue or
  ThumbPrintValue>
  ```
- ```
  racadm bioscert restore -all
  ```
- ```
  racadm bioscert restore -t <keyType>
  ```

Input

- `-t`— Specifies the key type of the Secure Boot Certificate to be exported.
  - 0— Specifies the PK (Platform Key)
  - 1— Specifies the KEK (Key Exchange Key)
  - 2— Specifies the DB (Signature Database)
  - 3— Specifies the DBX (Forbidden signatures Database)
- `-k` — Specifies the Certificate type or the Hash type of the Secure Boot Certificate file to be exported.
  - 0— Specifies the Certificate type
  - 1— Specifies the Hash type (SHA - 256)
  - 2— Specifies the Hash type (SHA - 384)
  - 3— Specifies the Hash type (SHA - 512)
- `-v`— Specifies the Thumbprint value or the Hash value of the Secure Boot Certificate file to be exported.Filename of the exported.

- `-f`—Specifies the file name of the exported Secure Boot Certificate.
- `-l`—Specifies the network location to where the Secure Boot Certificate file must be exported.
- `-u`—Specifies the username for the remote share to where the Secure Boot Certificate file must be exported.
- `-p`—Specifies the password for the remote shre to where the Secure Boot Certificate file must be exported.

Example

- To view the installed Secure boot Certificates.

```
 racadm bioscert view -all
```

- To view an installed PK Certificate

```
racadm bioscert view -t 0 -k 0 -v
AB:A8:F8:BD:17:1E:35:12:90:67:CD:0E:69:66:79:9B:BE:64:52:0E
```

- To view installes DBX certificate of HASH type SHA-256

```
 racadm bioscert view -t 3 -k 1 -v
416e3e4a6722a534afba9040b6d6a69cc313f1e48e7959f57bf248d543d00245
```

- Export the KEK certificate to a remote CIFS share

```
 racadm bioscert export -t 1 -k 0 -v
AB:A8:F8:BD:17:1E:35:12:90:67:CD:0E:69:66:79:9B:BE:64:52:0E
-f kek_cert.der -l //10.94.161.103/share -u admin -p mypass
```

- Export the DBX (Hash Type SHA-256) to a remote NFS share

```
 racadm bioscert export -t 3 -k 1 -v
416e3e4a6722a534afba9040b6d6a69cc313f1e48e7959f57bf248d543d00245
-f kek_cert.der -l 192.168.2.14:/share
```

- Export the KEK certificate to a local share using the local racadm

```
 racadm bioscert export -t 1 -k 0 -v
AB:A8:F8:BD:17:1E:35:12:90:67:CD:0E:69:66:79:9B:BE:64:52:0E   -f
kek_cert.der
```

- Export the KEK certificate to a local share using remote racadm

```
racadm -r 10.94.161.119 -u root -p calvin bioscert export -t 1 -k 0 -v
AB:A8:F8:BD:17:1E:35:12:90:67:CD:0E:69:66:79:9B:BE:64:52:0E -f kek_cert.der
```

- Import the KEK certificate from the CIFS share to the embedded iDRAC

```
racadm bioscert import -t 1 -k 0 -f kek_cert.der -l //10.94.161.103/share -
u admin -p mypass
```

- Import KEK (Hash Type SHA-256) from a CIFS share to the embedded iDRAC

```
racadm bioscert import -t 1 -k 1 -f kek_cert.der -l //192.168.2.140/
licshare -u admin -p passwd
```

- Import KEK certificate from a NFS share to the embedded iDRAC

```
 racadm bioscert import -t 1 -k 0 -f kek_cert.der -l 192.168.2.14:/share
```

- Import KEK certificate from a local share using Local RACADM

```
racadm bioscert import -t 1 -k 0 -f kek_cert.der
```

- Import KEK certificate from a local share using remote RACADM

```
racadm -r 10.94.161.119 -u root -p calvin bioscert import -t 1 -k 0 -f
kek_cert.der
```

- To delete an installed KEK Secure Boot Certificate

```
racadm bioscert delete -t 3 -k 0 -v
416e3e4a6722a534afba9040b6d6a69cc313f1e48e7959f57bf248d543d00245
```

- To delete an installed DBX Secure Boot Certificate of HASH type SHA-256

```
racadm bioscert delete -t 3 -k 1 -v
416e3e4a6722a534afba9040b6d6a69cc313f1e48e7959f57bf248d543d00245
```

- To delete all the installed KEK Secure Boot Certificates

```
racadm bioscert delete --all
```

- To restore the installed KEK Secure Boot Certificates

```
racadm bioscert restore -t 1
```

- To restore all the installed Secure Boot Certificates

```
racadm bioscert restore --all
```

cd

Table 8. cd

Description	To change the current working object, use this command.
Synopsis	`racadm> cd <object>`
Input	`racadm> cd <object>`
Output	Displays the new prompt.

Example	• **Example 1:** To navigate to the system device type directory:
	`racadm>>cd system`
	`racadm/system>`
	• **Example 2**: To run all the power-related `get` or `set` commands:
	`racadm/system>cd power`
	`racadm/Power>`

cd..

Table 9. cd..

Description	To go back to the previous directory, use this command.
Synopsis	`racadm> cd..`
Input	`racadm> cd..`
Output	To traverse back to the previous directory, use the command.
Example	• **Example 1**: To traverse back from power to system object:

- Input: racadm/power> cd..
- Output:

```
system>>
```

- **Example 2**: To traverse back from system object to the prompt:
  - Input: racadm/system> cd..
  - Output:

```
racadm>>
```

clearasrscreen

Table 10. Details of the clearasrscreen attribute

Description	Clears the last crash (ASR) screen that is in memory. For more information, see "Enabling Last Crash Screen" section in the *iDRAC User's Guide*. **NOTE: To run this subcommand, you must have the Clear Logs permission.**
Synopsis	`racadm clearasrscreen`
Input	None
Output	Clears the last crash screen buffer.
Example	`racadm clearasrscreen`

clearpending

Table 11. clearpending

Description	Deletes the pending values of all the attributes (objects) in the device (NIC, BIOS, FC, and Storage). **NOTE: If any attribute is not modified or a job is already scheduled for the same device, then the pending state is not cleared or deleted.**
Synopsis	`racadm clearpending <FQDD>`
Input	<FQDD> — The values are: • BIOS FQDD • NIC FQDD • FC FQDD • Storage controller FQDD
Output	A message is displayed indicating that the pending state is cleared or deleted.
Example	`racadm clearpending NIC.Integrated.1-1`

closessn

Table 12. Details of closessn

Description

Closes a communication session on the device. Use `getssninfo` to view a list of sessions that can be closed using this command.

To run this subcommand, you must have the Administrator permission.

NOTE: This subcommand ends all the sessions other than the current session.

Synopsis

- `racadm closessn –i <session_ID>`
- `racadm closessn -a`
- `racadm closessn -u <username>`

Input

- `–i <session_ID>` — The session ID of the session to close, which can be retrieved using RACADM `getssninfo` subcommand.

  Session running this command cannot be closed.
- `–a` — Closes all sessions.
- `–u <username>` — Closes all sessions for a particular user name.

Output

Successful or error message is displayed.

Example

- Closes the session 1234.

  ```
  racadm closessn -i 1234
  ```
- Closes all the sessions other then the active session for root user.

  ```
  racadm closessn –u root
  ```
- Closes all the sessions.

  ```
  racadm closessn –a
  ```

clrsel

Table 13. Details of clrsel

Description

Removes all the existing records from the System Event Log (SEL).

To use this subcommand, you must have **Clear Logs** permission.

Synopsis

```
racadm clrsel
```

Example

- `racadm clrsel`

  The SEL was cleared successfully

config

Table 14. Details of config

Description

Allows you to set iDRAC configuration parameters individually or to batch them as part of a configuration file and then modify iDRAC configuration properties. If the data is different, the iDRAC object is written with a new value.

NOTE: This subcommand is deprecated. For viewing the configuration objects and its values, use set subcommand. For more information, see *iDRAC RACADM CLI Guide* available at www.dell.com/idracmanuals .

Synopsis

- `racadm config -g <group> -o <object> <value>`
- `racadm config -g <group> -o <object> -i <index> <value>`
- `racadm config -f <filename> -o [-c] [-p] [-continue]`

NOTE:

- **The configuration file retrieved using remote RACADM is not interoperable. For the config `racadm -r 192.168.0 -u root -p xxx config -f c:\config.txt` command, use the configuration file retrieved from the same interface. For example, for the config `racadm -r 192.168.0 -u root -p xxx config -f c:\config.txt` , use the file generated from getconfig command `racadm -r 192.168.0 -u root -p xxx getconfig -f c:\config.txt`.**
- **-f is only applicable for remote RACADM.**

Input

- `-f`—The `-f <filename>` option causes `config` to read the contents of the file specified by `<filename>` and configure iDRAC. The file must contain data in the format specified in the section Parsing Rules in the *iDRAC User's Guide* available at www.dell.com/idracmanuals .

  NOTE: The `-f` option is not supported for the Serial or telnet or SSH console.
- `-continue`—This option is used with `-f` option only. If configuration through file is unsuccessful for a group, then configuration continues with the next group in the file. If this option is not used, then configuration stops when it is unsuccessful for a particular group. After the unsuccessful group, the rest of the groups are not configured.
- `-p`—This option must be used with the `-f` option. It directs `config` to delete the password entries contained in the config file `-f <filename>` after the configuration is complete.

  To apply the password, you must remove the preceding read-only marker '#' in the config file before executing the `config -f` command.
- `-g`—The `-g <groupName>`, or `group` option, must be used with the `-o` option. The `<group>` specifies the group containing the object that is to be set.
- `-o`—The `-o <objectName>`, or `object` option, must be used with the `-g` option. This option specifies the object name that is written with the string.
- `<value>`—Value to set to configuration object.
- `-i`—The `-i <index>`, or `index` option, is valid only for indexed groups and can be used to specify a unique group—used with -g and -o. 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.

  'nx' is allowed for servers.
- `-c`—This option performs validation but do not configure.

Output

This subcommand generates error output for any of the following reasons:

- Invalid syntax, group name, object name, index or other invalid database members.
- If the RACADM command-line interface is unsuccessful.

Examples

- To configure a single property of a group:

  ```
  racadm config -g cfgSerial -o cfgSerialBaudRate
  ```
- Modify a user password:

  ```
  racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 3 newpassword
  ```

- Configure a RAC from a configuration file:

```
racadm config -f config.txt
```

- Configure a RAC from a configuration file and continue if a group fails to get configured:

```
racadm set -f config.txt --continue
```

coredump

Table 15. Details of coredump

Description

Displays detailed information related to any recent critical issues that have occurred with iDRAC. The coredump information can be used to diagnose these critical issues.

If available, the coredump information is persistent across iDRAC power cycles and remains available until either of the following conditions occur:

The coredump information is deleted using the coredumpdelete subcommand.

For more information about clearing the `coredump`, see the coredumpdelete.

NOTE: To use this subcommand, you must have the Execute Debug privilege.

Synopsis

```
racadm coredump
```

Example

```
racadm coredump
There is no coredump currently available.
```

```
racadm coredump
Feb 19 15:51:40 (none) last message repeated 5 times
Feb 19 15:52:41 (none) last message repeated 4 times
Feb 19 15:54:12 (none) last message repeated 4 times
Feb 19 15:56:11 (none) last message repeated 2 times
Feb 22 11:46:11 (none) kernel:
```

coredumpdelete

Table 16. Details of coredumpdelete

Description

Deletes any currently available coredump data stored in the RAC.

To use this subcommand, you must have **Execute Debug** Command permission.

NOTE: If a `coredumpdelete` command is issued and a `coredump` is not currently stored in the RAC, the command displays a success message. This behavior is expected. See the `coredump` subcommand for more information about viewing a coredump.

Synopsis

```
racadm coredumpdelete
```

Output

Coredump is deleted.

Example

```
racadm coredumpdelete
```

```
Coredump request completed successfully
```

diagnostics

Table 17. Details of diagnostics

Description

Collects and exports remote diagnostics report from iDRAC.

The results of the latest successfully run remote diagnostics are available and retrievable remotely through an NFS, CIFS, HTTP, or HTTPS) share.

Synopsis

To run a remote diagnostic report:

```
racadm diagnostics run -m <mode> -r <reboot type> -s <start time> -e
<expiration time>
```

To export a remote diagnostic report:

```
racadm diagnostics export -f <file name> -l <NFS,CIFS,HTTP,or HTTPS share
location> -u <username> -p <password>
```

Input

- `–m <mode>`—Specifies the type of diagnostic mode. The types are:
  - Collect and export remote diagnostics report from the iDRAC.

    The results of the latest successfully executed remote Diagnostics will be available and retrievable remotely through the NFS, CIFS, HTTP, and HTTPS share.
  - `0`(Express)—The express mode executes a subset of diagnostic tests.
  - `1`(Extended)—The extended mode executes all available diagnostics tests.
  - `2`(Both)—Runs express and extended tests serially in sequence.
- `-f <filename>`—Specifies the name of the configuration file.
- `-l`—Specifies the location of the network share (NFS, CIFS, HTTP, and HTTPS).
- `-u <username>`—Specifies the user name of the remote share to import the file.
- `-p <password>`—Specifies the password of the remote share to import the file.
- `-r <reboot type>`—Specifies the reboot type. The type can be one of the following:
  - `pwrcycle`—Power cycle
  - `Graceful` —Graceful reboot without forced shutdown
  - `Forced`—Graceful reboot with forced shutdown
- `-s <start time>`—Specifies the start time for the scheduled job in yyyymmddhhmmss format. The default value `TIME_NOW` starts the job immediately.
- `-e <expiration time>`—Specifies the expiry time for the scheduled job in yyyymmddhhmmss format. The default value `TIME_NA` does not apply the waiting time.

NOTE: For the diagnostic report run operation, the time difference between the `-s` and `-e` options must be more than five minutes.

Output

Provides the Job ID for the diagnostic operation.

Examples

- To initiate the remote diagnostic operation:

  ```
  racadm diagnostics run -m 1 -r forced -s 20121215101010 -e TIME_NA
  ```

- To export a remote diagnostics report to CIFS share:

  ```
  racadm diagnostics export -f diagnostics -l //192.168.0/cifs -u
  administrator -p xxx
  ```

- To export a remote diagnostics report to NFS share:

  ```
  racadm diagnostics export -f diagnostics -l 192.168.0:/nfs -u
  administrator -p xxx
  ```

- To export a remote diagnostics report to the HTTP share:

```
racadm diagnostics export -f diags.txt -u httpuser -p httppwd -l http://
test.com
```

- To export a remote diagnostics report to the HTTPS share:

```
  racadm diagnostics export -f diags.txt -u httpsuser -p httpspwd -l
https://test.com
```

- To export a remote diagnostics report to a local share:

```
racadm diagnostics export -f diags.txt
```

driverpack

Table 18. Details of driverpack

Description

Installs the driver pack for the operating system.

Synopsis

To get information about the available driver packs

```
racadm driverpack getinfo
```

To attach the driver pack that matches the operating system

```
Racadm driverpack attach -i <index> -t <expose duration>
```

To detach the driver pack

```
Racadm driverpack detach
```

Input

- `-i`—index of the operating system
- `-t`—exposed time duration in seconds. It is an optional parameter and the default value is 64800 seconds.

Output

- `racadm driverpack getinfo`—<OS name>
- `Racadm driverpack attach`—Job Id details
- `Racadm driverpack detach`—detach successful

```
racadm driverpack getinfo—<OS name>
```

```
Racadm driverpack attach—Job Id details
```

```
Racadm driverpack detach—detach successful
```

Example

- To attach the driver pack with operating system index and exposed time

```
 racadm driverpack attach -i <OS Index> [-t <exposed time>]
```

- To check the job status

```
racadm jobqueue view -i JID_000000000000
```

- To detach the operating system

```
racadm driverpack detach
```

eventfilters

Table 19. Details of eventfilters

Description

Displays the list of event filter settings.

To use this subcommand with the `set` and `test` option, you must have the **Administrator** privilege.

Synopsis

```
racadm eventfilters <eventfilters command type>
```

```
racadm eventfilters get -c <alert category>
```

```
racadm eventfilters set -c <alert category> -a <action> -n <notifications>
```

```
racadm eventfilters set -c <alert category> -a <action> -r <recurrence>
```

```
racadm eventfilters test -i <Message ID to test>
```

NOTE: The general format of an alert category:

```
idrac.alert.category.[subcategory].[severity]
```

where category is mandatory, but subcategory and severity are optional. A severity cannot precede a subcategory.

Valid Category values are:

- `All`
- `System`
- `Storage`
- `Updates`
- `Audit`
- `Config`
- `Worknotes`

Definitions of the values are:

- System Health—System Health category represents all the alerts that are related to hardware within the system chassis. Examples include temperature errors, voltage errors, and device errors.
- Storage Health—Storage Health category represents alerts that are related to the storage subsystem. Examples include, controller errors, physical disk errors, and virtual disk errors.
- Updates—Update category represents alerts that are generated when firmware/drivers are upgraded or downgraded.

  NOTE: This does not represent firmware inventory.
- Audit—Audit category represents the audit log. Examples include, user login/logout information, password authentication failures, session info, and power states.
- Configuration—Configuration category represents alerts that are related to hardware, firmware, and software configuration changes. Examples include, PCIe card added/removed, RAID configuration changed, iDRAC license changed.
- Work notes—Work notes represents an entry in the Lifecycle log. You can add a work note to the Lifecycle Log to record comments for your reference. You can enter comments such as scheduled downtime or changes that are made by administrators who work in different shifts for the later reference.

NOTE: `idrac.all.all` is not a valid sub category.

Valid Severity values are:

- `Critical`
- `Warning`
- `Info`

Valid examples of alert queries are:

- `idrac.alert.all`
- `idrac.alert.audit`
- `idrac.alert.audit.lic`
- `idrac.alert.audit.warning`
- `idrac.alert.audit.lic.critical`

This command does not support setting the proxy parameters if the share location (-l) is HTTP/HTTPS. For more information, see Proxy parameter section.

Input

- `get`—Displays the list of eventfilter settings
- `set`—Configures the actions and notifications for a given eventfilter configuration
- `-i`—Message ID for which the simulation is needed
- `-c`—Alert category of the specific event filter
- `-a`—The action that must be invoked when the event occurs. Valid values are `none`, `powercycle`, `power off`, or `systemreset`
- `-n`—The notification is sent when the event occurs. Valid values are `all`, `snmp`, `ipmi`, `ws-events`, `redfish-events`, `oslog`, `email`, `remotesyslog`, or `none`. You can append multiple notifications that are separated by a comma. You cannot enter the values `all` or `none` with other notifications. If incorrect notification is specified along with other valid notifications, the valid and invalid notification set is failed.
- `-r`—Event generation interval. This option is applicable only to the temperature statistics subcategory `tmps`. You can use this option as a stand-alone or with `-n` and `-a`.

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 0–365. 0 disables the event generation.

Example

- Display all available event filter configurations.

```
racadm eventfilters get -c idrac.alert.all
```

- Display eventfilter configurations for a specific category. For example, audit

```
racadm eventfilters get -c idrac.alert.audit
```

- Display eventfilter configurations for a specific subcategory. For example, licensing under the audit category

```
racadm eventfilters get -c idrac.alert.audit.lic
```

- Display eventfilter configurations for a specific severity. For example, warning under the audit category

```
racadm eventfilters get -c idrac.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 idrac.alert.audit.lic.warning
```

- Clear all available alert settings.

```
racadm eventfilters set -c idrac.alert.all -a none -n none
```

- Configure using severity as a parameter. For example, all informational events in storage category are assigned power off as action, and email and SNMP as notifications.

```
racadm eventfilters set -c idrac.alert.storage.info -a poweroff -n
email,snmp
```

- Configure using subcategory as a parameter. For example, all configurations under the licensing subcategory in the audit category are assigned power off as action and all notifications are enabled.

```
racadm eventfilters set -c idrac.alert.audit.lic -a poweroff -n all
```

- Configure using subcategory and severity as parameters. For example, all information events under the licensing subcategory in the audit category are assigned power off as action and all notifications are disabled:

```
racadm eventfilters set -c idrac.alert.audit.lic.info -a poweroff -n none
```

- Configure the event generation interval for temperature statistics.

```
racadm eventfilters set -c idrac.alert.system.tmps.warning -r 10
```

- Configure the event generation interval and notifications for temperature statistics.

```
racadm eventfilters set -c idrac.alert.system.tmps -r 5 -a none -n snmp
```

- Send a test alert for the fan event.

```
racadm eventfilters test -i FAN0001
```

- To configure the proxy parameter.

```
racadm set lifecyclecontroller.lcattributes.UserProxyUsername admin1
```

- To remove the proxy parameter.

```
racadm set lifecyclecontroller.lcattributes.UserProxyUsername
```

- To view the list of proxy attributes.

```
racadm get lifecycleController.lcAttributes
```

exposeismInstallertohost

Table 20. Details of exposeismInstallertohost

Description	Exposes the ISM installer to host OS
Synopsis	`racadm exposeismInstallertohost`
Input	Not Applicable
Example	Not Applicable

fcstatistics

Table 21. Details of fcstatistics

Description	Displays a list of FCs (FQDDs), managed server for which statistics is available.
Synopsis	`racadm fcstatistics <FC fqdd>`
Input	`<FC fqdd>` — Specify the FQDD of the target FC device.
Example	`racadm fcstatistics <FC fqdd>`

frontpanelerror

Table 22. Details of frontpanelerror

Description	Enables or disables the live-feed of the errors currently being displayed on the LCD screen. For error acknowledge use `hide`, and error assert use `show`.

Synopsis

```
racadm frontpanelerror show
```

```
racadm frontpanelerror hide
```

Input

- `show` — to view the errors currently being displayed on the LCD screen.
- `hide` — to hide the errors currently being displayed on the LCD screen.

Example

- ```
  racadm frontpanelerror show
  Front Panel Error—Show Enabled.
  ```
- ```
  racadm frontpanelerror hide
  Front Panel Error—Hide Enabled.
  ```

fwupdate

Table 23. Details of fwupdate

Description

Allows you to update the firmware. You can:

- Check the firmware update process status.
- Update iDRAC firmware from FTP or TFTP server by providing an IP address and optional path.
- Update iDRAC firmware from the local file system using Local and Remote RACADM.
- Roll back to the standby firmware.

To use this subcommand, you must have Configure iDRAC permission.

NOTE: This command is only for iDRAC firmware update. For any other firmware update like BIOS or DUPs, use Update subcommand.

NOTE: If the iSM is exposed on the host server, you may see the `Firmware update operation is already in progress` error.

Synopsis

```
racadm fwupdate -s
```

```
racadm fwupdate -g -u -a <TFTP_Server_IP_Address>
[-d <path> [--clearcfg]
```

```
racadm -r <iDRAC IP_Address> -u <username> -p <password> fwupdate -f
<ftpserver ip> <ftpserver username> <ftpserver password> -d <path> where path
is the location on the ftp server where firmimg.d7 is stored.
```

```
racadm fwupdate -r
```

```
racadm fwupdate -p -u [-d <path>]
```

NOTE: When attempting to run firmware update task, if the firmware image path length is greater than 256 characters, remote RACADM client exits with the error message "`ERROR: Specified path is too long`".

Input

- `–u`—The update option performs a checksum of the firmware update file and starts the update process. This option may be used along with the `–g` or `–p` options. At the end of the update, iDRAC performs a soft reset.
- `–s`—This option returns the status of the update process.
- `-a`—The `-a` option specifies TFTP server IP address that is used for firmware image. This option must be used with the `-g` option.
- `-clearcfg`—The `-clearcfg` option removes the previous iDRAC configuration after firmware update.

- `-g`—The get option instructs the firmware to get the firmware update file from the TFTP server. Specify the `-a -u`, and `—d` options. In the absence of the `—a` option, the defaults are read from properties in the group `cfgRemoteHosts`, using properties `cfgRhostsFwUpdateIpAddr` and `cfgRhostsFwUpdatePath`.
- `-p`—The `-p`, or put, option is used to update the firmware file from the managed system to iDRAC. The `-u` option must be used with the `-p` option.
- `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.

NOTE: The `-p` option is supported on local and remote RACADM and is not supported with the `serial/Telnet/ssh` console and on the Linux operating systems.

NOTE: The `-p` option is applicable for both remote and local RACADM proxy commands. However, this option is not supported for local RACADM running on Linux operating systems.

- `-r`—The rollback option is used to roll back to the standby firmware.
- —Specifies the FTP server IP address or FQDN, username, and password used for firmware image. Applies FTP download process for firmware update.

Output

Displays a message indicating the operation that is being performed.

Example

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

```
racadm fwupdate -p -u -d /tmp/images
```

- Upload firmware image from FTP server and start firmware update:

```
racadm fwupdate -f 192.168.0.10 test test -d firmimg.d7
```

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

```
racadm fwupdate -g -u -a 192.168.0.100 -d /tmp/images
```

- Query the current status of the firmware update process:

```
racadm fwupdate -s
```

- Rollback to the standby firmware:

```
racadm fwupdate -r
```

- Upload firmware image from TFTP server, start firmware update. After firmware update is complete, delete previous iDRAC configuration:

```
racadm fwupdate -g -u -a 192.168.0.100 -d /tmp/images --clearcfg
```

NOTE: Firmware update from local RACADM (using `-p -u -d` options) is not supported on Linux operating system.

The following table describes the firmware update method that is supported for each interface:

Table 24. Details of fwupdate methods

FW Update Method	iDRAC on Blade Servers	iDRAC on Rack and Tower Servers
Local RACADM	Yes	Yes
Local RACADM-TFTP	Yes	Yes
Local RACADM-FTP	Yes	Yes
Remote RACADM	Yes	Yes
Remote RACADM-TFTP	Yes	Yes

FW Update Method	iDRAC on Blade Servers	iDRAC on Rack and Tower Servers
Remote RACADM-FTP	Yes	Yes
Firmware RACADM-TFTP	Yes	Yes
Firmware RACADM-FTP	Yes	Yes

get

Table 25. Details of get

Description

Displays the value of one or more objects. The `get` subcommand has two forms.

- Displays the value of a single object.
- Exports the value of multiple objects to a file.

It supports multiple object value exports in two file formats

- JSON format— SCP JSON files can be exported to a network share file.
- INI format—The INI format files can be exported to a local file only.
- Server Configuration Profile XML format-XML format files can be exported to a local/NFS/CIFS/FTP/TFTP network share.

  NOTE: To run the `Get` sub-command for Server Configuration Profile XML files, use the Lifecycle Controller version 1.1 or later.

NOTE: Some objects may have a pending value if a `Set` operation is performed on the object through a reboot job. To complete the pending operation, schedule the job using a jobqueue command, and then check for completion of the job using the returned Job ID. For more information, see jobqueue.

Synopsis

Single-object Get

```
racadm get <FQDD Alias>.<group>
```

```
racadm get <FQDD Alias>.<group>.<object>
```

```
racadm get <FQDD Alias>.<group>.[<index>].<object>
```

```
racadm get <FQDD Alias>.<index>.<group>.<index>.<object>
```

Multi-object Get

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

```
racadm get -f <filename> -t xml -l <NFS share> [--clone | --replace ] [--
includeph]
```

```
racadm get -f <filename> -t xml -l <NFS share> -c <FQDD>[,<FQDD>*]
```

```
racadm get -f <filename> -t xml -u <username> -p <password> -l <FTP share> -c
<FQDD>
```

```
racadm get -f <filename> -t xml -l <TFTP share> -c <FQDD>
```

```
racadm get -f <filename> -t xml -u <username> -p <password> -l <CIFS share>
[--clone | --replace ] [--includeph]
```

```
racadm get -f <filename> -t xml -u <username> -p <password> -l <CIFS share> -
c <FQDD>[,<FQDD>*]
```

```
racadm get -f <filename> -t xml -u <username> -p <password> -l <HTTP share> -
c <FQDD>
```

```
racadm get -f <filename> -t xml -u <username> -p <password> -l <HTTPS share> -
c <FQDD>
```

Input

- `<FQDD Alias>`
  - Examples for FQDDs
    - `System.Power`
    - `System.Power.Supply`
    - `System.Location`
    - `LifecycleController.LCAttributes`
    - `System.LCD`
    - `iDRAC.Serial`

For the list of supported groups and objects under the get command, see Database objects with get and set commands.

- `<group>`—Specifies the group containing the object that must be read.
- `<object>`—Specifies the object name of the value that must be read.
- `<index>`—Specifies where FQDD Aliases or Groups must be indexed.
- `-f <filename>`—This option enables you to export multiple object values to a file. This option is not supported in the Firmware RACADM interface.
- `-u`—Specifies user name of the remote CIFS share to which the file must be exported.
- `-p`—Specifies password for the remote CIFS share to which the file must be exported.
- `-l`—Specifies network share location to which the file is exported.
- `-t`—Specifies the file type to be exported.

  The valid values are:

  - `JSON`—It exports the SCP JSON file to a network share file.
  - `xml`—It exports the SCP xml format file, either to a local or network share file.
  - `ini`—It exports the legacy configuration file. If -t is not specified, then the ini format file is exported. It can only be exported to a local file.

  NOTE: To import or export Server Configuration Profile xml files, Lifecycle Controller version 1.1 or later is required.

- `--clone`—Gets the configuration `.xml` files without system-related details such as service tag. The `.xml` file received does not have any virtual disk creation option.
- `--replace`—Gets the configuration `.xml` files with the system-related details such as service tag.
- `-c`—Specifies the FQDD or list of FQDDs separated by ',' of the components for which the configurations should be exported. If this option is not specified, the configuration related to all the components are exported.
- `--includeph`—Specifies that the output of the passwords included in the exported configuration `.xml` file are in the hashed format.

  NOTE: if --includeph is not used, the output of the passwords are in the .xml file in clear text.

NOTE: For `--clone` and `--replace` options, only `.xml` file template is received. These options `--clone` and `--replace` cannot be used in the same command.

This command does not support proxy parameters. To perform the operation with http and https, the proxy parameters has to be configured in the lifecyclecontroller.lcattributes. Once these proxy parameters are configured, they become the part of default configuration. They have to be removed to ignore the proxy parameters.

This command does not support setting the proxy parameters if the share location (-l) is HTTP/HTTPS. To perform the operation with HTTP or HTTPS through a proxy, the proxy parameters must be first configured using the lifecyclecontroller.lcattributes. Once these proxy parameters are configured, they become the part of default configuration; the proxy attributes should be cleared to end use of the HTTP/HTTPS proxy.

The valid lifecyclecontroller.lcattributes HTTP/HTTPS proxy parameters are:

- `UserProxyUserName`
- `UserProxyPassword`
- `UserProxyServer`
- `UserProxyPort`
- `UserProxyType`

To view the list of proxy attributes, use `racadm get lifecycleController.lcAttributes`.

Examples

- Get system LCD information.

```
racadm get system.lcdLCDUserString
```

- Display an entire group, in this case the topology configuration.

```
racadm get system.location
```

- Display a single object from a particular group.

```
racadm get system.location.rack.name
```

- Export the xml configuration to a CIFS share.

```
racadm get -f file -t xml -u myuser -p xxx -l //192.168.0/share
```

- Export the xml configuration to an NFS share.

```
racadm get -f file -t xml -l 192.168.0:/myshare
```

- Export a “cloned” xml configuration to a CIFS share

```
racadm get -f xyz_temp_clone -t xml -u Administrator -p xxx -l //192.168.0/
xyz --clone
```

- Export a “replace” xml configuration to a CIFS share

```
racadm get -f xyz_temp_replace -t xml -u Administrator -p xxx -l //
192.168.0/xyz --replace
```

- Export the xml configuration of the iDRAC component to FTP share.

```
racadm get -f file -t xml -u username -p password -l ftp://192.168.10.24/
```

- Export the JSON configuration of the iDRAC component to FTP share.

```
racadm get -f file -t json -u username -p password -l ftp://192.168.10.24/
```

- Export the xml configuration of the iDRAC component to TFTP share.

```
racadm get -f file -t xml  -l tftp://192.168.10.24/
```

- Export the JSON configuration of the iDRAC component to TFTP share.

```
racadm get -f file -t json -l ftp://192.168.10.24/
```

- Export the xml configuration of the iDRAC component to a CIFS share.

```
racadm get -f file -t xml -u myuser -p xxx -l //192.168.0/share  -c
iDRAC.Embedded.1
```

- Export the xml configuration of the iDRAC component to NFS share.

```
racadm get -f file -t xml -l 10.1.12.13:/myshare
```

- Export the xml configuration of the iDRAC component to HTTP share.

```
racadm get -f file -t xml -u httpuser -p httppwd -l http://test.com/myshare
```

- Export the xml configuration of the iDRAC component to HTTPS share.

```
racadm get -f file -t xml -u httpuser -p httppwd -l https://test.com/myshare
```

- Export the JSON configuration of the iDRAC component to HTTP share.

```
racadm get -f file -t json -u httpuser -p httppwd -l http://test.com/myshare
```

- Export the JSON configuration of the iDRAC component to HTTPS share.

```
racadm get -f file -t json -u httpuser -p httppwd -l https://test.com/
myshare
```

- Include password hash in the configuration `.xml` file.

```
racadm get -f<filename> -t xml -l<NFS or CIFS share> -u<username> -
p<password> -t xml --includeph
```

- Configure proxy parameters.

```
racadm set lifecyclecontroller.lcattributes.UserProxyUsername admin1
```

```
racadm set lifecyclecontroller.lcattributes.UserProxyUsername
```

- View the list of proxy attributes

```
racadm get lifecycleController.lcAttributes
```

getconfig

Table 26. Details of getconfig subcommand

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

NOTE: This subcommand is deprecated. For viewing the configuration objects and its values, use `get` subcommand. For more information, see the *iDRAC RACADM CLI Guide* available at www.dell.com/idracmanuals.

Synopsis

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

```
racadm getconfig -g <groupName> [-i <index>]
```

```
racadm getconfig -u <username>
```

```
racadm getconfig -h
```

```
racadm getconfig -g <groupName> -o <objectName> [-i index]
```

Input

- `-f` — The `-f <filename>` option directs `getconfig` to write the entire iDRAC configurations to a configuration file. This file can be used for batch configuration operations using the `config` subcommand.

  NOTE: This option is supported only on remote interfaces.
- `-g` — The `-g <groupName>` or group option, is 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, then 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 remember exact group names.
- `-i` — The `-i <index>` or index option, is valid only for indexed groups and is 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, then a value of 1 is assumed for groups, which are tables that have multiple entries. The `-i` option enters the index value and not a *named* value
- `-o` — The `-o <objectname>` or object option specifies the object name that is used in the query. This option is optional and can be used with the `-g` option.
- `-u` — The `-u <username>` or user name option, is used to display the configuration for the specified user. The `<username>` option is the login name for the user.
- `-v` — The `-v` option displays more information with the display of the properties and is used with the `-g` option.

Output

The subcommand displays error message when:

- Invalid syntax, group name, object name, index, or any other invalid database members are entered.
- The RACADM CLI transport is unsuccessful.

If errors are not encountered, this subcommand displays the content of the specified configuration.

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

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

cfgUserAdmin cfgUserAdminUserName

Example

- Displays the configuration properties (objects) that are contained in the group `cfgLanNetworking`.

```
racadm getconfig -g cfgLanNetworking
```

- Saves all group configuration objects from iDRAC 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.

Saves all group configuration objects from iDRAC to `myrac.cfg`.

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

Saves all group configuration objects from iDRAC 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 27. Details of groups and key attributes

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

- Displays a list of the available configuration groups on iDRAC in an alphabetical order.

```
racadm getconfig -h
```

- Displays the configuration properties for the user named **root**.

```
racadm getconfig -u root
```

- Displays the user group instance at index 2 with verbose information for the property values.

```
racadm getconfig -g cfgUserAdmin -i 2 -v
```

- Displays an entire group of serial configuration.

```
racadm getconfig -g cfgSerial
```

- Displays a single object from a particular group.

```
racadm getconfig -g cfgSerial -o cfgSerialBaudRate
```

- Displays an indexed group.

```
racadm getconfig -g cfgUserAdmin -o cfgUserAdminUserName -i 2
```

- Displays the current Enhanced Cooling Mode property configuration.

```
racadm getconfig -g cfgThermal
```

gethostnetworkinterfaces

Table 28. Details of gethostnetworkinterfaces

Description

Displays host network interface details.

NOTE: To run this subcommand, you must have iDRAC Service Module installed on the server operating system.

Synopsis

```
racadm gethostnetworkinterfaces
```

```
racadm gethostnetworkinterfaces <NIC FQDD>
```

Examples

- To display the details of all the network interfaces on the server.

```
racadm gethostnetworkinterfaces

Local Area Connection 12
Description               : iDRAC Virtual NIC USB Device #8
Status                    : Up
Interface Type            : Ethernet
DHCP                      : Enabled
DHCPServerV4              : 169.254.0.1
MAC Address               : 00-25-64-F9-7A-E7
IPv4 Address              : 169.254.0.2
Subnet Mask               : 255.255.255.0
IPv6 Address              : fe80::1cce:a0a7:f30e:54fc
Prefix Length             : 64
IPv6 DNSServer Address  0: fec0:0:0:ffff::1
IPv6 DNSServer Address  1: fec0:0:0:ffff::2
IPv6 DNSServer Address  2: fec0:0:0:ffff::3
```

- To display the details of a particular NIC on the server.

```
racadm gethostnetworkinterfaces NIC.Integrated.1-1-1

Local Area Connection
Description               : Broadcom NetXtreme Gigabit Ethernet
Status                    : Up
Interface Type            : Ethernet
DHCP                      : Enabled
DHCPServerV4              : 10.94.224.25
MAC Address               : 14-FE-B5-FF-B1-9C
FQDD                      : NIC.Integrated.1-1-1
IPv4 Address              : 10.94.225.189
Subnet Mask               : 255.255.255.128
IPv6 Address              : fe80::7c5f:a114:84d4:17f6
Prefix Length             : 64
IPv4 Gateway Address      : 10.94.225.129
IPv4 DNSServer Address  0: 10.116.2.250
IPv4 DNSServer Address  1: 10.116.2.251
```

getled

Table 29. Details of getled

Description

Displays the LED settings on a module: blinking, not blinking, or unknown (for empty slots).

To run this subcommand, you must have the Login User privilege.

Synopsis

```
racadm getled
```

Input

Output

- LED is blinking
- LED is not-blinking

Example

```
racadm getled
LED State : Blinking
racadm getled
LED State : Not-Blinking
```

getniccfg

Table 30. Details of getniccfg

Description

Displays the current and static NIC settings for iDRAC.

Synopsis

```
racadm getniccfg
```

Input

Output

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

Table 31. Details of IPV4 settings

```
IPv4 settings:
NIC Enabled                     =1
IPv4 Enabled                    =1
DHCP Enabled                    =0
IP Address                      =10.94.227.207
Subnet Mask                     =255.255.255.0
Gateway                         =10.94.227.1
IPv6 settings:
IPv6 Enabled                    =Disabled
DHCP6 Enabled                   =Enabled
IP Address 1                    =::
Gateway                         =::
Link Local Address              =::
IP Address 2                    =::
IP Address 3                    =::
IP Address 4                    =::
IP Address 5                    =::
IP Address 6                    =::
IP Address 7                    =::
IP Address 8                    =::
IP Address 9                    =::
IP Address 10                   =::
IP Address 11                   =::
IP Address 12                   =::
```

```
IP Address 13                =::
IP Address 14                =::
IP Address 15                =::
LOM Status:
NIC Selection                =dedicated
Link Detected                =Yes
Speed                        =1Gb/s
Duplex Mode                  =Full Duplex
Active NIC                   =Dedicated
Static IPv4 settings:
Static IP Address            =10.94.227.207
Static Subnet Mask           =255.255.255.0
Static Gateway               =10.94.227.1
Static IPv6 settings:
Static IP Address 1          =::
Static Prefix Length         =64
Static Gateway               =::
```

NOTE: IPv6 information is displayed only if IPv6 is enabled in iDRAC.

NOTE: IPv6 Address 1 field indicates static IP and IPv6 Address 2 field indicates dynamic IP.

NOTE: LOM Status is displayed only for iDRAC on Rack and Tower servers and is not displayed for iDRAC Enterprise on Blade servers.

Example

- Display iDRAC network settings in server slot 1

```
racadm getniccfg
```

getraclog

Table 32. Details of getraclog

Description

The `getraclog` command displays RAC log entries.

Synopsis

- `racadm getraclog [-i]`
- `racadm getraclog [-s <start>] [-c <count>]`

```
racadm getraclog [-c <count>] [-s <start-record>]
```

NOTE: If options are not provided, the entire log is displayed.

Input

- `-c` — Specifies the number of records to display.

  NOTE: On Local RACADM, the number of logs are restricted to 100 by default.
- `-s` — Specifies the starting record used for the display.

NOTE: When Enhanced Chassis Logging and Events feature is enabled, then -i and --more options are not displayed.

Output

```
SeqNumber = 286
Message ID = USR0005
Category = Audit
AgentID = RACLOG
Severity = Information
Timestamp = 2017-05-15 06:25:27
Message = Login failed from processdisco06a: 192.168.0
Message Arg 1 = processdisco06a
Message Arg 2 = 10.92.68.245
FQDD = iDRAC.Embedded.1
```

Example

Display the recent 2 records for RAC log

```
racadm getraclog -c
2
SeqNumber = 4102
Message ID = LIC201
Category = Audit
AgentID = DE
Severity = Warning
Timestamp = 2017-05-15 06:30:20
Message = License yPMRJGuEf7z5HG8LO7gh assigned to device iDRAC expires in 4
days.
Message Arg 1 = yPMRJGuEf7z5HG8LO7ghMessage Arg 2 = iDRACMessage Arg 3 = 4
--------------------------------------------------------------------------------
-----
SeqNumber = 4101
Message ID = USR0032
Category = Audit
AgentID = RACLOG
Severity = Information
Timestamp = 2017-05-15 06:25:27
Message = The session for root from 192.168.0 using RACADM is logged off.
Message Arg 1 = root
Message Arg 2 = 10.94.98.92
Message Arg 3 = RACADM
FQDD = iDRAC.Embedded.1
--------------------------------------------------------------------------------
-------
```

getractime

Table 33. Details of getractime

Description Displays the current iDRAC time.

Synopsis

- `racadm getractime [-d]`

Input

- `-d` — Displays the time in the format, YYYYMMDDhhmmss.

Output The current iDRAC time is displayed.

Example

- ```
  racadm getractime
  Mon May 13 17:17:12 2013
  ```
- ```
  racadm getractime -d
  20141126114423
  ```

getremoteservicesstatus

Table 34. Details of getremoteservicesstatus

Description	Displays the status of a system.
Synopsis	`racadm getremoteservicesstatus`
Input	`racadm getremoteservicesstatus`
Output	Possible values for the host system status • Powered Off • In POST • Out of POST • Collecting System Inventory • Automated Task Execution • Lifecycle Controller Unified Server Configurator • Server has halted at F1/F2 error prompt because of a POST error • Server has halted at F1/F2/F11 prompt because there are no bootable devices available • Server has entered F2 setup menu • Server has entered F11 Boot Manager menu Possible values for the for LifeCycle controller(LC) status • Ready • Not Initialized • Reloading data • Disabled • In Recovery • In Use Possible values for the real time status • Ready • Not ready Possible values for the overall status status • Ready • Not ready
Example	• `racadm getremoteservicesstatus`

getsel

Table 35. Details of getsel

Description	Displays all system event log (SEL) entries in iDRAC.
Synopsis	• `racadm getsel [-i]` • `racadm getsel [-s <start>][-c <count>]` **NOTE: If no arguments are specified, the entire log is displayed.**
Input	• `–i` — Displays the number of entries in the SEL. • `-s` — Displays the starting record number. • `-c` — Specifies the number of records to display. • `--more` — Displays a screen. • `-A` — Does not display headers or labels. • `-o` — Displays each record on a single line.. • `-E` — Displays RAW SEL data along with the other data. • `-R` — Displays only the RAW SEL data for each record

Example

- Display entire log.

```
racadm getsel
```

- Display number of records in log.

```
racadm getsel -i
```

getsensorinfo

Table 36. Details of getsensorinfo

Description	Displays the status for system sensors. **NOTE: For the Dell PowerEdge FX2 chassis with the FM120x4 server, the power-related information is not displayed.**
Synopsis	• `racadm getsensorinfo` • `racadm getsensorinfo -c`
Input	`-c`—Compact output format.

NOTE: Chassis Controller is supported only on Dell PowerEdge FX2, and GPU sensors are displayed only on PowerEdge C4130 servers.

Example

```
racadm getsensorinfo
Sensor Type : POWER
```

Table 37. racadm getsensorinfo Sensor Type : POWER

<Sensor Name>	<Status>	<Type>
PS1 Status	Present	AC

```
Sensor Type : TEMPERATURE
```

Table 38. Sensor Type : TEMPERATURE

<Sensor Name>	<Status>	<Reading>	<lc>	<uc>	<lnc>[R/W]	<Unc>[R/W]
System Board Inlet Temp	Ok	20 C	-7 C	47 C	3 C [Y]	42C [Y]
System Board Exhaust Temp	Ok	19 C	0 C	75 C	0 C [N]	70 C [N]
CPU1 Temp	Ok	59 C	3 C	97 C	8 C [N]	92 C [N]

```
Sensor Type : FAN
```

Table 39. Sensor Type : FAN

<Sensor Name>	<Status>	<Reading>	<lc>	<uc>	<PWM %>
System Board Fan1 RPM	Ok	5880 RPM	600 RPM	NA	21%
System Board Fan2 RPM	Ok	6000 RPM	600 RPM	NA	0%

System Board Fan3 RPM	Ok	5880 RPM	600 RPM	NA	0%
System Board Fan4 RPM	Ok	5880 RPM	600 RPM	NA	0%
System Board Fan5 RPM	Ok	5640 RPM	600 RPM	NA	144%
System Board Fan6 RPM	Ok	5880 RPM	600 RPM	NA	152%

```
Sensor Type : VOLTAGE
```

Table 40. Sensor Type : VOLTAGE

<Sensor Name>	<Status>	<Reading>	<lc>	<uc>
CPU1 VCORE PG	Ok	Good	NA	NA
System Board 3.3V PG	Ok	Good	NA	NA
System Board 5V AUX PG	Ok	Good	NA	NA
CPU1 M23 VPP PG	Ok	Good	NA	NA
System Board 1.05V PG	Ok	Good	NA	NA
CPU1 M23 VDDQ PG	Ok	Good	NA	NA
CPU1 M23 VTT PG	Ok	Good	NA	NA
System Board 5V SWITCH PG	Ok	Good	NA	NA
System Board VCCIO PG	Ok	Good	NA	NA
System Board 2.5V AUX PG	Ok	Good	NA	NA
CPU1 M01 VDDQ PG	Ok	Good	NA	NA
System Board NDC PG	Ok	Good	NA	NA
CPU1 M01 VPP PG	Ok	Good	NA	NA
System Board 1.5V PG	Ok	Good	NA	NA
System Board PS2 PG Fail	Ok	Good	NA	NA
System Board PS1 PG Fail	Ok	Good	NA	NA
System Board 1.5V AUX PG	Ok	Good	NA	NA
CPU1 M01 VTT PG	Ok	Good	NA	NA
PS1 Voltage 1	Ok	240 V	NA	NA
System Board DIMM PG	Ok	Good	NA	NA

```
Sensor Type : CURRENT
```

Table 41. Sensor Type : CURRENT

<Sensor Name>	<Status>	<Reading>	<lc>	<uc>	<lnc> [R/W]	<unc> [R/W]
PS1 Current 1	Ok	0.4 Amps	NA	NA	0 Amps [N]	0 Amps [N]
System Board Pwr Consumption	Ok	56 Watts	NA	1386 Watts	0 Watts [N]	1260 Watts [N]

```
Sensor Type : PROCESSOR
```

Table 42. Sensor Type : PROCESSOR

<Sensor Name>	<Status>	<State>	<lc>	<uc>
CPU1 Status	Ok	Presence Detected	NA	NA
CPU2 Status	N/A	Absent	NA	NA

```
Sensor Type : MEMORY
```

Table 43. Sensor Type : MEMORY

<Sensor Name>	<Status>	<State>	<lc>	<uc>
DIMM A1	N/A	Presence Detected	NA	NA
DIMM A2	N/A	Absent	NA	NA
DIMM A3	Ok	Absent	NA	NA
DIMM A4	N/A	Absent	NA	NA
DIMM A5	N/A	Absent	NA	NA
DIMM A6	N/A	Absent	NA	NA
DIMM A7	N/A	Absent	NA	NA
DIMM A8	N/A	Absent	NA	NA
DIMM A9	N/A	Absent	NA	NA
DIMM A10	N/A	Absent	NA	NA
DIMM A11	N/A	Absent	NA	NA
DIMM A12	N/A	Absent	NA	NA
DIMM B1	N/A	Absent	NA	NA
DIMM B2	N/A	Absent	NA	NA
DIMM B3	N/A	Absent	NA	NA
DIMM B4	N/A	Absent	NA	NA
DIMM B5	N/A	Absent	NA	NA
DIMM B6	N/A	Absent	NA	NA
DIMM B7	N/A	Absent	NA	NA
DIMM B8	N/A	Absent	NA	NA
DIMM B9	N/A	Absent	NA	NA
DIMM B10	N/A	Absent	NA	NA
DIMM B11	N/A	Absent	NA	NA

```
DIMM B12            N/A                 Absent              NA                  NA
```

```
Sensor Type : Chassis Controller
```

Table 44. Sensor Type : Chassis Controller

<Sensor Name>	<Status>	<State>
Chassis Controller	OK	OK

```
/tmp # vi idraclogs
4 23:09:39 idrac8 L4, S3 [2440]: sessionmanagement_dmmapping_thread() confd (2)
4 23:09:39 idrac8 L4, S3 [2440]: request.command is 13
4 23:09:39 idrac8 L4, S3 [10297]: AddMessageToLclogEI() Obtained MUT Flag
4 23:09:39 idrac8 L4, S3 [10297]: ___ AddMessageToLclogEI : DCLCLWRAPCreateTLVLi
4 23:09:39 idrac8 L4, S3 [10297]: GetSledType() shmStatus 0 shmData0
4 23:09:39 idrac8 L5, S3 [10297]: RacadmcheckRSMStatus: This is RSM capable syst
4 23:09:40 idrac8 L4, S3 [10297]: ret is 0
4 23:09:40 idrac8 L4, S3 [10297]: probename is Chassis Controller
4 23:09:40 idrac8 L4, S3 [10297]: pCMCStatusobj->offsetKey is 24
4 23:09:40 idrac8 L4, S3 [10297]: pCMCStatusobj->sensorValue is 0
4 23:09:40 idrac8 L4, S3 [10297]: MAP Uninitialized, time to uninit = 0 millisec
4 23:09:40 idrac8 L4, S3 [10297]: RACADM total execution time: 1680 milliseconds
```

```
Sensor Type : BATTERY
```

Table 45. Sensor Type : BATTERY

<Sensor Name>	<Status>	<Reading>	<lc>	<uc>
System Board CMOS Battery	Ok	Present	NA	NA
PERC1 ROMB Battery	Ok	Unknown	NA	NA
PERC2 ROMB Battery	Ok	Unknown	NA	NA

```
Sensor Type : PERFORMANCE
```

Table 46. Sensor Type : PERFORMANCE

<Sensor Name>	<Status>	<Status>	<lc>	<uc>
System Board Power Optimized	Ok	Not Degraded	NA	NA

```
Sensor Type : INTRUSION
```

Table 47. Sensor Type : INTRUSION

<Sensor Name>	<Intrusion>	<Status>
System Board Intrusion	Closed	Power ON

```
Sensor Type : REDUNDANCY
```

Table 48. Sensor Type : REDUNDANCY

<Sensor Name>	<Status>	<Type>
System Board Fan Redundancy	Full Redundant	Fan

```
System Board PS Redundancy      Disabled                        PSU
```

```
Sensor Type : SYSTEM PERFORMANCE
```

Table 49. Sensor Type : SYSTEM PERFORMANCE

<Sensor Name>	<Status>	<Reading>	<lc>	<uc>	<lnc> [R/W]	<unc> [R/W]
System Board CPU Usage	Non-Critical	0%	0%	100%	0% [N]	99% [Y]
System Board IO Usage	Non-Critical	0%	0%	100%	0% [N]	99% [Y]
System Board MEM Usage	Non-Critical	0%	0%	100%	0% [N]	99% [Y]
System Board SYS Usage	Non-Critical	0%	0%	100%	0% [N]	99% [Y]

getssninfo

Table 50. Details of getssninfo

Description

Displays a list of users that are connected to iDRAC. The following information is displayed:

- Session ID
- Username
- IP address (if applicable)
- Session type (for example, serial or Telnet)
- Login date and time in MM/DD/YYYY HH:MM:SS format

NOTE: Based on the Session ID (SSNID) or the user name (User), the iDRAC administrator can close the respective sessions or all the sessions using the `closessn` subcommand. For more information, see closessn.

Synopsis

```
racadm getssninfo [-u <username>] [-A]
```

Input

- `-u` — displays only sessions associated with a specific user.
- `-A` — does not display headers or labels.

Example

```
racadm getssninfo
```

Table 51. racadm getssninfo

SSNID	Type	User	IP Address	Login Date/Time
58999	SSH	root	192.168.0.10	04/07/2016 12:00:34

Display the details of sessions without header

```
racadm getssninfo -A
```

```
"43584" "SSH" "root" "192.168.0.10" "04/07/2016 12:00:34"
```

getsvctag

Table 52. Details of getsvctag

Description

Displays the service tag of the host system.

Synopsis

```
racadm getsvctag
```

Output Any system tag as applicable.

Example

- Display the service tag of the host system.

```
racadm getsvctag
```

getsysinfo

Table 53. Details of getsysinfo

Description Displays information related to iDRAC, managed system, and watchdog configuration.

NOTE: The hostname and OS Name fields in the `getsysinfo` output display accurate information only if the OpenManage Server Administrator (OMSA) is installed on the managed system. If OMSA is not installed these fields may be blank or inaccurate. An exception to this are VMware operating system names, which are displayed even if OMSA is not installed on the managed system.

Synopsis `racadm getsysinfo [-d] [-A] [-c] [-4] [-6]`

Input

- `–4`—Displays IPv4 settings
- `–6`—Displays IPv6 settings
- `–c`—Displays common settings
- `–d`—Displays iDRAC information
- `–A`—Eliminates the printing of headers or labels

Output

```
RAC Information:
RAC Date/Time           = Fri May  5 10:56:23 2017

Firmware Version        = 3.00.00.00
Firmware Build          = 62
Last Firmware Update    = 05/02/2017 06:49:43
Hardware Version        = 0.01
MAC Address             = 84:7b:eb:d5:03:e0
SVC Tag                                                    = BDC14GH

Common settings:
Register DNS RAC Name   = 1
DNS RAC Name            = ipmierrata
Current DNS Domain      = sha512.com
Domain Name from DHCP   = Disabled

IPv4 settings:
Enabled                 = 1
Current IP Address      = 10.94.195.33
Current IP Gateway      = 10.94.195.1
Current IP Netmask      = 255.255.255.0
DHCP Enabled            = 1
Current DNS Server 1    = 10.94.192.67
Current DNS Server 2    = 0.0.0.0
DNS Servers from DHCP   = Disabled

IPv6 settings:
Enabled                 = 1
Current IP Address 1    = 2011:de11:bdc:195::16e/64
Current IP Gateway      = fe80::21c:23ff:fe6a:1106
Autoconfig              = 1
Link Local IP Address   = fe80::ba2a:72ff:fefc:4fb0/64
Current IP Address 2    = ::
Current IP Address 3    = ::
Current IP Address 4    = ::
Current IP Address 5    = ::
```

```
Current IP Address 6    = ::
Current IP Address 7    = ::
Current IP Address 8    = ::
Current IP Address 9    = ::
Current IP Address 10   = ::
Current IP Address 11   = ::
Current IP Address 12   = ::
Current IP Address 13   = ::
Current IP Address 14   = ::
Current IP Address 15   = ::
DNS Servers from DHCPv6 = Disabled
Current DNS Server 1    = 2011:de11:bdc:192::67/64
Current DNS Server 2    = ::

System Information:
System Model            = PowerEdge R630
System Revision         = I
System BIOS Version     = 1.3.6
Service Tag             = 62T3232
Express Svc Code        = 13230477902
Host Name               = WIN-2TA05N3JSLD
OS Name                 = Microsoft Windows Server 2008 R2, Enterprise x64 Edition
OS Version              = Version 6.1 (Build 7601 : Service Pack 1) (x64) Server Full In
Power Status            = OFF
Fresh Air Capable       = Yes
```

Example

- Display system information

```
racadm getsysinfo -c
```

- Display iDRAC information

```
racadm getsysinfo -d
```

- Display IPv4 details without header

```
racadm getsysinfo -A
```

```
"RAC IPv4 Information:"
"1"
"10.94.195.33"
"10.94.195.1"
"255.255.255.0"
"1"
"10.94.192.67"
"0.0.0.0"
"1"
```

- Display svctag information

```
racadm -r 10.94.95.96 getsysinfo -d
```

gettracelog

Table 54. Details of gettracelog

Description	Lists all the trace login entries of iDRAC.
Synopsis	• `racadm gettracelog [-i]` • `racadm gettracelog [-s <start>] [-c <count>]`
Input	• `–i` — Displays the number of entries in iDRAC trace log.

- `-c` — Specifies the number of records to display.
- `-s` — Specifies the starting record to display.

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 starts. After the system starts, the system's timestamp is used.

Example

- Display entire log

```
racadm gettracelog
```

- Display number of records in log

```
racadm gettracelog -i
```

```
Total Records: 228
```

getversion

Table 55. Details of getversion

Description	Displays the current software version, model and generation information, and whether the target device can be updated.
Synopsis	• `racadm getversion` • `racadm getversion [-b | -c | –i]` • `racadm getversion [-f <filter>]`

Input	• `-c` — Displays the server's current CPLD version.
	• `-b` — Displays the server's current BIOS version.
	• `-i` — Displays the server's current IDSDM version.
	• `-f <filter>` — Filters the components and must be one of the following values:
	  • `bios`: BIOS
	  • `idrac`: iDRAC
	  • `lc`: Lifecycle Controller
	  • `idsdm`: SD card

```
racadm getversion -c
```

Table 56. Details of `racadm getversion -c`

<Server>	*<CPLD Version>*	*<Blade Type>*
server-1	1.0.5	PowerEdgeM520
server-2	1.0.3	PowerEdgeM610x
server-4	1.0.0	PowerEdgeM710HD
server-5	1.0.3	PowerEdgeM710
server-7	1.0.6	PowerEdgeM620

server-9	1.0.5	PowerEdgeM520

```
racadm getversion
Bios Version = 2.0.18
iDRAC Version = 2.00.00.00
Lifecycle Controller Version = 2.00.00.00
```

```
racadm getversion -b
```

Table 57. Details of `racadm getversion -b`

<Server>	*<BIOS Version>*	*<Blade Type>*
server-1	1.6.0	PowerEdgeM520
server-2	6.3.0	PowerEdgeM610x
server-4	7.0.0	PowerEdgeM710HD
server-5	6.3.0	PowerEdgeM710
server-7	1.7.1	PowerEdgeM620
server-9	1.7.1	PowerEdgeM520

Table 58. Details

<Switch>	*<Model Name>*	*<HW Version>*	*<FW Version>*
switch-1	MXL 10/40GbE	X01	9-2(0-296)
switch-2	M8024-k 10GbE SW	A00	5.0.1.3
switch-3	Dell PowerConnect M8024	X00	
switch-4	Dell PowerConnect M8024	X00	
switch-5	Dell PowerConnect M6348	X02	
switch-6	Dell PowerConnect M6220	A01	

GroupManager

Table 59. Details of GroupManager

Description

Allows you to:

- Delete the group from the group manager.
- Remove the iDRAC from group by itself by using admin previleges.
- Join the group using administrator privileges.

NOTE: This subcommand is supported only on iDRAC9.

Synopsis

- To delete the group from the group manager.

```
groupmanager delete -g <groupname>
```

- To remove the iDRAC from group by itself by using administrator privileges.

```
groupmanager removeself -g <groupname>
```

- To join the group using administrator privileges.

```
groupmanager joingroup -g <groupname> -uid <uuid> -pcode < grouppasscode>
```

Input

- `-g`— Specifies the name of the iDRAC member group
- `-uid` — Specifies the group user id
- `-pcode`— Specifies the group passcode

Example

- To delete the group from the groupmanager:

```
racadm groupmanager delete -g <groupname>
```

- To remove the iDRAC from the group by itself:

```
racadm groupmanager removeself -g <groupname>
```

- To join server to the local iDRAC group:

```
racadm groupmanager joingroup -g <mygrpxyz> -uid <uid1234> -pcode <12345>
```

hwinventory

Table 60. Details of hwinventory

Description

Allows you to display or export current internal hardware inventory or shipped hardware inventory by device.

NOTE: iDRAC supports a maximum of 12 parallel sessions of hardware inventory.

Synopsis

- `racadm hwinventory`
- `racadm hwinventory NIC|FC`
- `racadm hwinventory <FQDD>`
- `racadm hwinventory export -f <filename> -u <username> -p <password> -l <CIFS, NFS, HTTP, or HTTPS share>`

Input

- `<FQDD>` — Specifies the FQDD of the target device.
  - `FQDD` — NIC.Slot.1–2

  NOTE: The hwinventory subcommand supports NIC and FC FQDDs only.
- `-f` — Exported Hardware Inventory filename.

- `-u` — Username of the remote share to where the file must be exported. Specify user name in a domain as **domain/username**
- `-p` — Password for the remote share to where the file must be exported.
- `-l` — Network share location to where the Hardware Inventory must be exported.

Examples

- To get the hwinventory, run the following command:

```
racadm hwinventory
[InstanceID: DIMM.Socket.B1]
Device Type = Memory
RemainingRatedWriteEndurance = 0 %
SystemEraseCapability = Not Supported
CacheSize = 0 MB
NonVolatileSize = 0 MB
VolatileSize = 32768 MB
MemoryTechnology = NVDIMM-F
Rank = Double Rank
PrimaryStatus = OK
ManufactureDate = Mon Jun 12 07:00:00 2017 UTC
Model = DDR4 DIMM
PartNumber = M393A4K40BB2-CTD
SerialNumber = 35F0538B
Manufacturer = Samsung
BankLabel = B
Size = 32768 MB
CurrentOperatingSpeed = 2133 MHz
Speed = 2666 MHz
MemoryType = DDR-4
DeviceDescription = DIMM B1
FQDD = DIMM.Socket.B1
InstanceID = DIMM.Socket.B1
LastUpdateTime = 2018-05-21T14:25:36
LastSystemInventoryTime = 2018-06-04T03:53:01
----------------------------------------------------------------------

[InstanceID: DIMM.Socket.A2]
Device Type = Memory
SystemEraseCapability = Not Supported
CacheSize = 0 MB
NonVolatileSize = 0 MB
VolatileSize = 32768 MB
MemoryTechnology = NVDIMM-F
Rank = Double Rank
PrimaryStatus = OK
ManufactureDate = Mon Jun 12 07:00:00 2017 UTC
Model = DDR4 DIMM
PartNumber = M393A4K40BB2-CTD
SerialNumber = 35F045C3
Manufacturer = Samsung
BankLabel = A
Size = 32768 MB
CurrentOperatingSpeed = 2133 MHz
Speed = 2666 MHz
MemoryType = DDR-4
DeviceDescription = DIMM A2
FQDD = DIMM.Socket.A2
InstanceID = DIMM.Socket.A2
LastUpdateTime = 2018-05-21T14:25:36
LastSystemInventoryTime = 2018-06-04T03:53:01
----------------------------------------------------------------------

[InstanceID: DIMM.Socket.A7]
Device Type = Memory
SystemEraseCapability = Not Supported
CacheSize = 0 MB
NonVolatileSize = 16384 MB
VolatileSize = 0 MB
MemoryTechnology = NVDIMM-P
Rank = Single Rank
```

```
PrimaryStatus = OK
ManufactureDate = Mon Mar 13 07:00:00 2017 UTC
Model = DDR4 DIMM
PartNumber = 18ASF2G72XF12G6V21AB
SerialNumber = 1648DCC4
Manufacturer = Micron Technology
BankLabel = A
Size = 16384 MB
CurrentOperatingSpeed = 2133 MHz
Speed = 2666 MHz
MemoryType = DDR-4
DeviceDescription = DIMM A7
FQDD = DIMM.Socket.A7
InstanceID = DIMM.Socket.A7
LastUpdateTime = 2018-05-21T14:25:36
LastSystemInventoryTime = 2018-06-04T03:53:01
----------------------------------------------------------------------
```

- To get the list of NIC FQDDs, run the following command:

```
racadm hwinventory nic
NIC.Slot.2-1-1:Emulex OCe14102-U1-D - 00:90:FA:4C:FE:C2
PartitionCapable :                          1

NIC.Slot.2-1-2:Emulex OCe14102-U1-D - 00:90:FA:4C:FE:C3
PartitionCapable :                          2

NIC.Slot.2-1-3:Emulex OCe14102-U1-D - 00:90:FA:4C:FE:C4
PartitionCapable :                          3

NIC.Slot.2-1-4:Emulex OCe14102-U1-D - 00:90:FA:4C:FE:C5
PartitionCapable :                          4
```

- To display the statistics for the NIC FQDD, type the following command:

```
$racadm hwinventory <NIC FQDD>
```

```
Total RDMA Packets Received:            0

Total RDMA Packets Transmitted:            0

Total RDMA Bytes Transmitted:            0

Total RDMA Bytes Received:            0

Total RDMA Transmitted ReadRequest Packets:    0

Total RDMA Transmitted Send Packets:        0

Total RDMA Transmitted Write Packets:        0

Total RDMA Protocol Errors:            0

Total RDMA Protection Errors:            0
```

- To get the complete details for NIC.Integrated.1-4-1, type the following command:

```
racadm hwinventory NIC.Integrated.1-4-1
Device Description:                         Integrated NIC 1 Port 4 Partition 1
PCI Vendor ID:                                14e4
PCI Sub Vendor ID:                            1028
PCI Device ID:                                165F
PCI Sub Device ID:                            1f5b
Current MAC Address:                          74:86:7A:D6:E0:EF
Permanent MAC Address:                        74:86:7A:D6:E0:EF
Virtual iSCSI MAC Address:                    Unavailable
Permanent iSCSI MAC Address:                  Unavailable
Virtual FIP MAC Address:                      Unavailable
Permanent FIP MAC Address:                    Unavailable
Permanent FCoE MAC Address:                   Unavailable
Slot Type:                                    Not Applicable
Data Bus Width:                               Unknown
```

```
Slot Length:                                Not Applicable
Bus Number:                                 2
DeviceNumber:                               0
Function Number:                            1
Last Update Time:                           20140508190902.000000+000
Last System Inventory Time:                 20140515163940.000000+000
ProductName:                                BRCM GbE 4P 5720-t rNDC
WWN:                                        Unavailable
VirtWWN:                                    Unavailable
WWPN:                                       Unavailable
VirtWWPN:                                   Unavailable
Family Version:                             7.8.16
Controller BIOS Version:                    1.32
EFI Version:                                16.2.4
Max Bandwidth:                              0
Min Bandwidth:                              0
FCoE WWNN:
Vendor Name:                                Broadcom Corp
Number of PCI-e Functions
Supported per Port:                         1
Number of PCI-e Functions
Currently Enabled per Port:                 1
Family Driver Version:                      Unavailable
Protocol:                                   1
Link Duplex:                                Not Applicable
Link Speed:                                 Not Applicable
Auto Negotiated:                            Disabled
Transmit Flow Control:                      Off
Receive Flow Control:                       Off
Media Type:                                 Unavailable
NIC Mode:                                   Disabled
FCoE Offload Mode:                          Disabled
iSCSI Offload Mode:                         Disabled
Max Number of IOs per session supported:    0
Number of Max LOGINs per port:              0
Max Number of exchanges:                    0
Max NPIV WWN per port:                      0
Number of Targets Supported:                0
Max Number of outstanding commands
supported across all sessions:              0
Flex Addressing:                            Capable
UEFI:                                       Capable
iSCSI Offload:                              Not Capable
iSCSI Boot:                                 Capable
TCP OffloadEngine:                          Not Capable
FCoE:                                       Not Capable
FCoE Boot:                                  Not Capable
PXE Boot:                                   Capable
SRIOV:                                      Not Capable
Wake on LAN:                                Capable
Network Management Pass Through:            Capable
OS2BMC PassThrough:                         Capable
Energy Efficient Ethernet:                  Capable
On Chip Thermal Sensor:                     Capable
NPar:                                       Not Capable
Remote PHY:                                 Not Capable
Feature Licensing:                          Not Capable
IPSec Offload:                              Not Capable
MAC Sec:                                    Not Capable
RDMA:                                       Not Capable
Enhanced Transmission Selection:            Not Capable
Priority Flow Control:                      Not Capable
DCB Exchange Protocol:                      Not Capable
Congestion Notification:                    Not Capable
VEB-VEPA Single Channel:                    Not Capable
VEB-VEPA Multi Channel:                     Not Capable
EVB:                                        Not Capable
BPE:                                        Not Capable
Open Flow:                                  Not Capable
Partition WOL Support:                      Not Capable
Virtual Link Control                        Not Capable
Partition RX Flow Control:                  Not Capable
Partition TX Flow Control:                  Not Capable
```

```
TX Bandwidth Control Maximum:                  Not Capable
TX Bandwidth Control Minimum:                  Not Capable
```

- To export the inventory to a remote CIFS share, type the following command:

```
racadm hwinventory export -f Myinventory.xml -u admin -p xxx
  -l //1.2.3.4/share
```

- To export the inventory to a remote NFS share, type the following command:

```
racadm hwinventory export -f Myinventory.xml -u admin -p xxx
  -l 1.2.3.4:/share
```

- To export the inventory to local file system using local Racadm, type the following command:

```
racadm hwinventory export -f Myinventory.xml
```

- To export the inventory to a remote HTTP share:

```
racadm hwinventory export -f Myinventory.xml -u httpuser -p httppass -l http://test.com/
share
```

- To export the inventory to a remote HTTPS share:

```
racadm hwinventory export -f Myinventory.xml -u httpuser -p httppass -l http://test.com/
share
```

- To display the Standard hardware inventory verbose description for the FC.Slot.2–1, type the following command:

```
racadm hwinventory FC.Slot.2-1
PCI Vendor ID:                                 1077
PCI Sub Vendor ID:                             1077
PCI Device ID:                                 2532
PCI Sub Device ID:                             015c
PCI Bus:                                       67
PCI Device:                                    0
PCI Function:                                  0
Vendor Name:                                   Unavailable
Device Name:                                   QLogic QLE2560 8Gb Fibre Channel Adapter -
21000024FF089D8A
WWN:                                           20:00:00:24:FF:08:9D:8A
VirtWWN:                                       20:00:00:24:FF:08:9D:8A
WWPN:                                          21:00:00:24:FF:08:9D:8A
VirtWWPN:                                      21:00:00:24:FF:08:9D:8A
Chip Type:                                     ISP2532
Family Version:                                02.57.14
EFI Version:                                   2.34
OS Driver Version:                             Unavailable
First FC Target WWPN:                          50:06:01:60:44:60:28:8C
First FC Target LUN:                           0
Second FC Target WWPN:                         00:00:00:00:00:00:00:00
Second FC Target LUN:                          0
Hard Zone Address:                             0
Hard Zone Enable:                              Disabled
FC Tape Enable:                                Disabled
Loop reset Delay:                              5
Frame Payload Size :                           2048
Fabric Login Retry Count:                      0
Fabric Login Timeout:                          0
Port Login Retry Count:                        8
Port Login Timeout:                            3000
Port Down Retry Count:                         45
Port Down Timeout:                             0
Link Down Timeout:                             45000
Port Number:                                   1
Port Speed:                                    0
No capabilities found for FQDD "FC.Slot.2-1"
/admin1-> racadm hwinventory FC.Slot.3-1
PCI Vendor ID:                                 1077
PCI Sub Vendor ID:                             1077
PCI Device ID:                                 2031
PCI Sub Device ID:                             0256
PCI Bus:                                       4
```

```
PCI Device:                                    0
PCI Function:                                  0
Vendor Name:                                   QLogic
Device Name:                                   QLogic QLE2660 16Gb FC Adapter -
2001000E1E091075
WWN:                                           20:00:00:0E:1E:09:10:75
VirtWWN:                                       20:00:00:0E:1E:09:10:75
WWPN:                                          20:01:00:0E:1E:09:10:75
VirtWWPN:                                      20:01:00:0E:1E:09:10:75
Chip Type:                                     8324, Rev. 02
Family Version:                                02.00.84
EFI Version:                                   5.30
OS Driver Version:                             9.1.10.27
First FC Target WWPN:                          00:00:00:00:00:00:00:00
First FC Target LUN:                           0
Second FC Target WWPN:                         00:00:00:00:00:00:00:00
Second FC Target LUN:                          0
Hard Zone Address:                             0
Hard Zone Enable:                              Disabled
FC Tape Enable:                                Disabled
Loop reset Delay:                              5
Frame Payload Size :                           2048
Fabric Login Retry Count:                      0
Fabric Login Timeout:                          0
Port Login Retry Count:                        8
Port Login Timeout:                            3000
Port Down Retry Count:                         30
Port Down Timeout:                             0
Link Down Timeout:                             30000
Port Number:                                   1
Port Speed:                                    0
Max Number of IOs per connection supported:    9
Maximum number of Logins per port:             8
Maximum number of exchanges:                   9
Maximum NPIV per port:                         1
Maximum number of FC Targets supported:        8
Maximum number of outstanding commands across  all connections: 9
Flex Addressing:                               Capable
UEFI:                                          Capable
FC Start:                                       Capable
On Chip Thermal Sensor:                        Capable
Feature Licensing:                             Not Capable
```

ifconfig

Table 61. Details of ifconfig

Description	Displays the contents of the network interface table. To use this subcommand, you must have the Execute Diagnostic Commands permission.
Synopsis	`racadm ifconfig`
Input	N/A

Table 62. Example

`eth0`	`Link encap:Ethernet  HWaddr 00:1D:09:FF:DA:23`
	`inet addr:192.168.0.0 Bcast:192.168.0.255 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)`

inlettemphistory

Table 63. Details of inlettemphistory

Description

Displays the average and the peak temperatures during the last hour, day, week, month, or year. Also Exports the inlet temperature history data file. The file can be exported to a remote file share, local file system, or the management station.

NOTE: For FM120x4 systems, this subcommand provides the historical data for system board temperature.

Synopsis

- `racadm inlettemphistory export -f <filename> -t <type> [-u <username of the network share>] [-p <password for the remote share>] [-i <network share location>]`
- `racadm inlettemphistory get`

This command does not support setting the proxy parameters if the share location (-l) is HTTP/HTTPS. To perform the operation with HTTP or HTTPS through a proxy, the proxy parameters must be first configured using the lifecyclecontroller.lcattributes. Once these proxy parameters are configured, they become the part of default configuration; the proxy attributes should be cleared to end use of the HTTP/HTTPS proxy.

The valid lifecyclecontroller.lcattributes HTTP/HTTPS proxy parameters are:

- `UserProxyUserName`
- `UserProxyPassword`
- `UserProxyServer`
- `UserProxyPort`
- `UserProxyType`

To view the list of proxy attributes, use `racadm get lifecycleController.lcAttributes`.

Input

- `-f` — Exports inlet temperature history filename. The maximum length of this parameter is 64 characters.
  NOTE: If a file with the specified filename exists, then the older file is replaced with the new history file.
- `-u` — User name of the remote share to export the file. Specify user name in a domain as domain or username.
- `-p` — Password for the remote share to where the file must be exported.
- `-l` — Network share location to where the inlet temperature history must be exported. The maximum length of this parameter is 256 characters.
  NOTE: The supported network locations are CIFS, NFS, HTTP, and HTTPS.
- `-t` — Specifies the exported file type. Valid values are `xml` and `csv`. These values are case-insensitive.

NOTE: From firmware RACADM, only export to a remote share is supported. The behavior of remote share is not defined when the path specified (`-l`) contains special characters.

Example

- Export the log to a remote CIFS share.

```
racadm inlettemphistory export -f Mylog.xml -u admin -p xxx -l //1.2.3.4/
share -t xml
```

- Export the log to a remote HTTP share.

```
racadm inlettemphistory export -f Mylog.xml -u httpuser -p httppwd\n  -l
http://test.com -t xml
```

- Export the log to a remote HTTPS share.

```
racadm inlettemphistory export -f Mylog.xml -u httpsuser -p httpspwd\n  -l
https://test.com -t xml
```

- Export the log to local file system using Local RACADM.

```
racadm inlettemphistory export -f Mylog.xml -t xml
```

- Export the log to management station using Remote RACADM.

```
racadm -r 1.2.3.4 -u user -p xxx inlettemphistory export -f Mylog.csv -t csv
```

- View the inlet temperature history.

```
racadm inlettemphistory get
```

```
Duration Above Warning Threshold as Percentage = 0.0%
Duration Above Critical Threshold as Percentage = 0.0%

Average Temperatures
Last Hour  = 23C ( 73.4F )
Last Day   = 24C ( 75.2F )
Last Week  = 24C ( 77.0F )
Last Month = 25C ( 77.0F )
Last Year  = 23C ( 73.4F )

Peak Temperatures
Last Hour  = 23C ( 73.4F ) [At Wed, 21 May 2017 11:00:57]
Last Day   = 25C ( 77.0F ) [At Tue, 21 May 2017 15:37:23]
Last Week  = 27C ( 80.6F ) [At Fri, 20 May 2017 10:38:20]
Last Month = 29C ( 84.2F ) [At Wed, 16 May 2017 15:34:13]
Last Year  = 29C ( 84.2F ) [At Wed, 16 May 2017 15:34:13]
```

- Configure the proxy parameter.

```
racadm set lifecyclecontroller.lcattributes.UserProxyUsername admin1
```

- Remove the the proxy parameter.

```
racadm set lifecyclecontroller.lcattributes.UserProxyUsername
```

- View the list of proxy attributes.

```
racadm get lifecycleController.lcAttributes
```

jobqueue

Table 64. Details of jobqueue

Description

Enables you to view and delete a job or jobs in the current Job Queue.

NOTE:

- **To run this subcommand, you must have the Server control privilege.**
- **If an unexpected error message is displayed for any operation, ensure you delete some jobs in the jobqueue and retry the operation.**
- **Use jobqueue create command after applying a pending device configuration. Else, you may see a job creation and deletion in the lclog.**
- **Multi-object Set commands using INI, XML, or JSON files do NOT require a jobqueue create command; jobs will be automatically created by the Set command.**

Synopsis

```
racadm jobqueue view -i<jobid>
```

```
racadm jobqueue delete [-i<jobid>][--all]
```

where valid options are `-i` and `--all`.

```
racadm jobqueue create <fqdd> [-r <reboot type> ] [-s <start
time> ] [-e <expiry time>]
```

```
racadm jobqueue create <fqdd> [-r <reboot type>] [-s <start time>]
[-e <expiration time>] [--realtime]
```

Input

- `-i` — Specifies a job ID that is displayed or deleted.

  NOTE: The value `JID_CLEARALL` will force delete all the possible jobs in the queue.
- `--all` — The job IDs that are not applicable are deleted.
- `-fqdd` — Specifies an FQDD for which a job should be created.
- `–r <reboot type>` — Specifies a reboot type.
  - `none` — No Reboot Job. This option is the default value.
  - `pwrcycle` — Power cycle.
  - `graceful` — Graceful Reboot without forced shut down.
  - `forced` — Graceful Reboot with forced shut down.
- `start time` — Specifies a start time for job scheduled in the yyyymmddhhmmss format. TIME_NOW means immediate. Next Reboot means job is in scheduled state until the next manual restart.
- `expiry time` — Specifies expiry time for the job execution in the yyyymmddhhmmss format. The job must start by this time. TIME_NA means expiry time is not applicable.
- `--realtime` — Specifies the real time job.

  NOTE:
  - **`--realtime` is applicable for storage configuration commands run on systems with PowerEdge RAID Controller 9 cards with firmware version 9.1 and later.**
  - **`-r` option is not valid for real time configuration.**

Example

- View jobs in the current job queue.

  ```
  racadm jobqueue view
  ```
- View status of a specific job ID.

  ```
  racadm jobqueue view -i <JobID>
  ```
- Issue configuration changes for a PowerEdge RAID controller then start a real time job to execute the changes.

  ```
  racadm set RAID.Slot.3-1.RAIDdefaultWritePolicy WriteBack
  racadm set RAID.Slot.3-1.Name “Prod Workload”
  racadm jobqueue create RAID.Slot.3-1 –realtime
  ```
- Delete all possible jobs from the current job queue.

  ```
  racadm jobqueue delete --all
  ```
- Delete a specific job from the current job queue.

  ```
  racadm jobqueue delete -i <JobID>
  ```
- To clear all the jobs in the job queue.

  ```
  racadm jobqueue delete –i JID_CLEARALL
  ```
- Create a Job for the provided FQDD and add to the job queue.

  ```
  racadm jobqueue create NIC.Integrated.1-1 -r pwrcycle -s
  TIME_NOW -e 20120501100000
  ```

- Create a real time configuration job for the specified RAID controller.

```
racadm jobqueue create RAID.Integrated.1-1 -s TIME_NOW --realTime
RAC1024: Successfully scheduled a job.
Verify the job status using "racadm jobqueue view -i JID_xxxxx"
command.
Commit JID = JID_927008261880
```

krbkeytabupload

Table 65. details of krbkeytabupload

Description	Uploads a `Kerberos keytab` file to iDRAC. To run this subcommand, you must have the Server Control privilege.
Synopsis	`racadm krbkeytabupload [-f <filename>]` `<filename>` is the name of the file including the path.
Input	`-f` — Specifies the filename of the keytab uploaded. If the file is not specified, the keytab file in the current directory is selected.
Output	When successful `Kerberos Keytab successfully uploaded to the RAC` message is displayed. If unsuccessful, appropriate error message is displayed.
Example	`racadm krbkeytabupload -f c:\keytab\krbkeytab.tab`

lclog

Table 66. Details of lclog

Description

Allows you to:

- Export the lifecycle log history. The log exports to remote or local share location.
- View the lifecycle log for a particular device or category
- Add comment to a record in lifecycle log
- Add a work note (an entry) in the lifecycle log
- View the status of a configuration job.

NOTE:

- **When you run this command on Local RACADM, the data is available to RACADM as a USB partition and may display a pop-up message.**
- **While Lifecycle Controller is running for racadm commands, you cannot perform other operation which needs Lifecycle Controller Partition. If the Lifecycle Controller Partition is unreleased (because of improper closure of racadm command in the partition), then you must wait 20-35 minutes to clear the Lifecycle Controller Partition**

Synopsis

```
racadm lclog comment edit -q <sequence number> -m <Text to be added>
```

```
racadm lclog view -i <number of records> -a <agent id>  -c <category> -s
<severity> -b <sub-category> -q <sequence no> -n <number of records> -r
<start timestamp> -e <end timestamp>
```

```
racadm lclog export -f <filename> -u <username> -p <password> -l <CIFS or NFS
or HTTP or HTTPS or TFTP or FTP share>
```

```
racadm lclog export -f <filename> -u <username> -p <password> -l <CIFS or NFS
or HTTP or HTTPS or TFTP or FTP share> --complete
```

```
racadm -r <idracip> -u <idrac username> -p <idrac password> lclog export\ -f
<filename> -u <username> -p <password> -l <CIFS or NFS or HTTP or HTTPS or
TFTP or FTP share>
```

```
racadm -r <idracip> -u <idrac username> -p <idrac password> lclog export\ -f
<filename> -u <username> -p <password> -l <CIFS or NFS or HTTP or HTTPS or
TFTP or FTP share> -- complete
```

```
racadm lclog viewconfigresult -j <job ID>
```

```
racadm lclog worknote add -m <text to be added>
```

Input

- `-i`—Displays the number of records present in the active log.
- `-a`—The agent ID used to filter the records. Only one agent ID is accepted. The value is case-insensitive. Valid Agent-ID values:
  - `UEFI_SS_USC`
  - `CusOsUp`
  - `UEFI_Inventory`
  - `iDRAC`
  - `UEFI_DCS`
  - `SEL`
  - `RACLOG`
  - `DE`
  - `WSMAN`
  - `RACADM`
  - `iDRAC_GUI`
- `-k`—Filters the records based on the filter string provided in **racadm lclog view** command.
- `-c` — The category used to filter the records. Provides multiple categories using a "," as the delimiter. The value is case-insensitive. Valid category values:
  - `System`
  - `Storage`
  - `Worknotes`
  - `Config`
  - `Updates`
  - `Audit`
- `-b` —The subcategory used to filter the records. Provides multiple subcategories using a "," as the delimiter.
- `-q`—The sequence number from which the records must be displayed. Records older than this sequence number is displayed.

  NOTE: This parameter input is an integer. If an alphanumeric input is provided, then invalid subcommand syntax error is displayed.
- `-n`—Specifies the n number of records that must be displayed. On Local RACADM, if this parameter is not specified, by default 100 logs are retrieved.

- `-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 quotation marks.
- `-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 quotation marks.
- `-f <filename>`—Specifies the file location and name where lifecycle log is exported.
- `-a <name>`—Specifies the FTP Server IP address or FQDN, user name, and password.
- `-l <location>`—Specifies the location of the network share or area on file system where lifecycle log is exported. Two types of network shares are supported:
  - SMB-mounted path: `//<ipaddress or domain name>/<share_name>/<path to image>`
  - NFS-mounted path: `<ipaddress>:/<path to image>`.
- `-u <user>`—Specifies the user name for accessing the FTP server, or Domain and user name for accessing network share location.
- `-p <password>`—Specifies the password for accessing the FTP server or share location.
- `-s`—The severity used to filter the records. Provide multiple severities using a "," as the delimiter. The value is case-insensitive. Valid Severity values:
  - `Warning`
  - `Critical`
  - `Info`
- `–m <Comment>` —User comment string for a record that must be inserted in the Lifecycle Controller log. This comment string must be less than 128 characters. The text must be specified within double quotation mark.
  NOTE: HTML-specific characters may appear as escaped text.
- `-m <Worknote>`—Adds a worknote (an entry) in the Lifecycle log. This worknote must be less than 256 characters. The text must be specified within double quotation mark.
  NOTE: HTML-specific characters may appear as escaped text.

NOTE: For `-m <worknote>` and `–m <comment>` options, you need test alert privilege.

- `--complete`—Export the complete Lifecycle log as a compressed file. The exported file is of the type `.xml.gz`.
- `-j<Job ID>`—Specifies the Job ID.

Example

- Display the number of records present in the Lifecycle log.

```
racadm lclog view -i
```

- Display the records containing the string `session`

```
racadm lclog view -k session
```

- Display the iDRAC agent `idrac` records, under the storage category and storage physical disk drive subcategory, with severity set to `warning`.

```
racadm lclog view -a idrac -c storage -b pdr -s warning
```

- Display the records under storage and system categories with severities set to `warning` or `critical`.

```
racadm lclog view -c storage,system -s warning,critical
```

- Display the records having severities set to `warning` or `critical`, starting from sequence number 4.

```
racadm lclog view -s warning,critical -q 4
```

- Display 5 records starting from sequence number 20.

```
racadm lclog 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 lclog view -r "2011-01-02 23:33:40" -e "2011-01-03 00:32:15"
```

- Display all the available records from the active Lifecycle log.

```
racadm lclog view
```

NOTE: If output is not returned when this command is used remotely, then retry increasing the remote RACADM timeout value. To increase the timeout value, run the command `racadm set iDRAC.Racadm.Timeout <value>`. Alternatively, you can retrieve few records.

- Add a comment to record number 5 in the Lifecycle log.

```
racadm lclog comment edit –q 5 –m “This is a test comment.”
```

- Add a worknote to the Lifecycle log.

```
racadm lclog worknote add –m "This is a test worknote."
```

- Export the complete Lifecycle log in gzip format to a remote FTP share

```
racadm lclog export -f log.xml.gz –u ftppuser -p ftppwd –l ftp://192.168.0/
share
```

- Export the complete Lifecycle log in gzip format to a remote TFTP share

```
racadm lclog export -f log.xml.gz tftp://192.168.0.1/
```

- Export the Lifecycle log to a remote FTP share

```
racadm lclog export -f Mylog.xml –u ftppuser -p ftppwd –l ftp://192.168.0/
share
```

- Export the Lifecycle log to a remote TFTP share

```
racadm lclog export -f Mylog.xml tftp://192.168.0.1/
```

- Export the Lifecycle log to a remote CIFS share.

```
racadm lclog export -f Mylog.xml –u admin -p xxx -l //192.168.0/share
```

- Export the complete Lifecycle log in gzip format to a remote CIFS share.

```
racadm lclog export -f log.xml.gz –u admin -p xxx -l //192.168.0/share --
complete
```

- Export the Lifecycle log to a remote NFS share.

```
racadm lclog export -f Mylog.xml -l 192.168.0:/home/lclog_user
```

- Export the Lifecycle log to a local share using Local RACADM.

```
racadm lclog export -f Mylog.xml
```

- Export the complete Lifecycle log in gzip format to a local share using Local RACADM.

```
racadm lclog export -f log.xml.gz --complete
```

- Export the Lifecycle log `lclog` to a local share using Remote RACADM.

```
racadm -r 192.168.0 -u admin -p xxx lclog export -f Mylog.xml
```

- Display the status of the specified Job ID with Lifecycle Controller.

```
racadm lclog viewconfigresult -j JID_123456789012
```

- Export the complete Lifecycle Log in gzip format to a remote HTTP share:

```
racadm lclog export -f log.xml.gz –u httpuser -p httppwd -l http://test.com
```

- Export the complete Lifecycle Log in gzip format to a remote HTTPS share

```
racadm lclog export -f log.xml.gz -u httpsuser -p httpspwd -l https://
test.com
```

- Export the Life Cycle Log to a remote HTTP share

```
racadm lclog export -f Mylog.xml -u httpuser -p httppwd -l http://test.com
```

- Export the Life Cycle Log to a remote HTTPS share

```
racadm lclog export -f Mylog.xml -u httpsuser -p httpspwd -l https://
test.com
```

NOTE: Squid proxy configuration is not supported to access http/https shares.

license

Table 67. license

Description

Manages the hardware licenses.

Synopsis

- `racadm license view [-c <component>]`
- `racadm license import [-f <licensefile>] -l <location> -u <username> -p <password> -c <component> [-o]`
- `racadm license export -f <license file> [-l <location>] [-u <username>] [-p <password>] -e <ID> -c <component>`
- `racadm license delete -t <transaction ID> [-o]`
- `racadm license delete -e <entitlement ID> [-o]`
- `racadm license delete -c <component> [-o]`

Input

- `view` — View license information.
- `import` — Installs a new license.
- `export` — Exports a license file.
- `delete` — Deletes a license from the system.
- `-l <remote share location>` — Network share location from where the license file must be imported.

  If the file is on a shared location, then `-u <share user>` and `-p <share password>` must be used.
- `-f` — Filename or path to the license file
- `-e <ID>` — Specifies the entitlement ID of the license file that must be exported
- `-t <ID>` — Specifies the transaction ID.
- `-c <component>` — Specifies the component name on which the license is installed.
- `-o` — Overrides the End User License Agreement (EULA) warning and imports, replaces or deletes the license.

NOTE: Only a user with Server Control and Configure iDRAC privilege can run the `import`, `delete`, and `replace` commands.

NOTE: For export license, you need Login and Configure iDRAC privilege.

Examples

- View all License Information on System.

```
$racadm license view
```

```
iDRAC.Embedded.1
        Status               = OK
        Device               = iDRAC.Embedded.1
        Device Description   = iDRAC
        Unique Identifier    = H1VGF2S
                License #1
                        Status               = OK
                        Transaction ID       = 5
                        License Description  = iDRAC Enterprise License
                        License Type         = PERPETUAL
                        Entitlement ID       = Q3XJmvoxZdJVSuZemDehlcrd
                        License Bound        = H1VGF2S
                        Expiration           = Not Applicable
```

- Import a new license to a specific device in a known location.

```
$racadm license import -f license.xml -l //shareip/sharename
-u <share user> -p <share user password> -c idrac.embedded.1
```

- Import a license from a CIFS share to a device, in this case Embedded iDRAC.

```
 racadm license import -u admin -p xxx -f License.xml
-l //192.168.0/licshare -c idrac.embedded.1
```

- Import a license from an NFS share to a device, in this case Embedded iDRAC.

```
 racadm license import -f Licen.xml -l 192.168.0:/share
-c idrac.embedded.1
```

- Import a license by overriding the EULA warning.

```
racadm license import -u admin -p passwd -f License.xml -l //192.168.0/licshare -c
idrac.embedded.1 -o
```

```
-Import a license from the local filesystem using local racadm: racadm license import -f
License.xml -c idrac.embedded.1
```

```
-Import a license from the local filesystem using remote racadm: racadm license import -f
C:\Mylicdir\License.xml -c idrac.embedded.1
```

- Import a license from the local file system using Local RACADM.

```
 racadm license import -f License.xml -c idrac.embedded.1
```

- Import a license from the local file system using Remote RACADM.

```
 racadm -r 192.168.0.1 -u admin -p xxx license import -f C:\Mylicdir\License.xml -c
idrac.embedded.1
```

- Export a license file.

```
racadm license export -f license.xml -l 192.168.0:/share -u uname -p xxx -c
iDRAC.Embedded.1
```

Instead of `-c`, you can use `-e <ID>` or `-t <ID>`

For Remote RACADM, if filename is not specified, the files are exported to the directory where RACADM is running.

- Export license to an NFS share using transaction ID, in this case transaction 27.

```
racadm license export -f License.xml -l 192.168.0:/licshare
-t 27
```

- Export license to a CIFS share specifying the entitlement ID, in this case abcdxyz.

```
racadm license export -u admin -p passwd -f License.xml -l //192.168.0/licshare -e abcdxyz
```

```
racadm license export -u httpuser -p httppwd -f License.xml -l http://test.com -e abcdxyz
```

```
racadm license export -u httpsuser -p httpspwd -f License.xml -l https://test.com -e
abcdxyz
```

- Export license to a CIFS share specifying the FQDD. While using the `-c` option and exporting a license from a device, more than one license file may be exported. Therefore if a filename is given, an index is appended to the end of the filename such as`LicenseFile0.xml`, `LicenseFile1.xml`. In this case, the device is Embedded iDRAC.

```
racadm license export -u admin -p xxx -f LicenseFile.xml -l //192.168.0/licshare -c
idrac.embedded.1
```

```
racadm license export -u httpuser -p httppswd -f LicenseFile.xml -l http://test.com -c
idrac.embedded.1
```

```
racadm license export -u httpsuser -p httpspswd -f LicenseFile.xml -l https://test.com -c
idrac.embedded.1
```

- Delete licenses on a particular device, in this case Embedded iDRAC.

```
racadm license delete -c idrac.embedded.1
```

- Delete a license using entitlement ID, in this case xYZabcdefg.

```
racadm license delete -e xYZabcdefg
```

- Delete a license using transaction ID, in this case 2.

```
racadm license delete -t 2
```

netstat

Table 68. Details of netstat

Description	Display the routing table and network statistics.
Synopsis	`racadm netstat`
Privilege Required	Debug

Examples

- To display the routing table and network statistics, type the following command:

```
$ racadm netstat
```

nicstatistics

Table 69. Details of nicstatistics

Description	Displays the statistics for the NIC FQDD.
Synopsis	- `racadm nicstatistics`

- `racadm nicstatistics <NIC FQDD>`
- `racadm hwinventory NIC.Integrated.1-1`

Examples

- To displays the statistics for the NIC FQDD, type the following command:

```
$racadm nicstatistics <NIC FQDD>
```

```
Total RDMA Packets Received:            0
Total RDMA Packets Transmitted:            0
Total RDMA Bytes Transmitted:            0
Total RDMA Bytes Received:           0
Total RDMA Transmitted ReadRequest Packets:    0
Total RDMA Transmitted Send Packets:        0
Total RDMA Transmitted Write Packets:        0
Total RDMA Protocol Errors:           0
Total RDMA Protection Errors:            0
```

- To display the statistics for the integrated NIC, type the following command:

```
$ racadm nicstatistics NIC.Integrated.1-1
```

```
Total Bytes Received:            0
Total Bytes Transmitted:        0
Total Unicast Bytes Received:        0
Total Multicast Bytes Received:        0
Total Broadcast Bytes Received:        0
Total Unicast Bytes Transmitted:    0
```

- To get the network statistics, type the following command:

```
$ racadm nicstatistics
```

```
NIC.Slot.5-2-1 : QLogic CNA Gigabit Ethernet-B8:AC:6F:B3:BF:10
```

```
NIC.Slot.5-2-1 : QLogic CNA Gigabit Ethernet-B8:AC:6F:B3:BF:11
```

```
NIC.Slot.5-2-1 : QLogic CNA Gigabit Ethernet-B8:AC:6F:B3:BF:12
```

```
NIC.Slot.5-2-1 : QLogic CNA Gigabit Ethernet-B8:AC:6F:B3:BF:13
```

```
NIC.Slot.5-2-1 : QLogic CNA Gigabit Ethernet-B8:AC:6F:B3:BF:14
```

ping

Table 70. Details of ping

Description

Verifies if the destination IP address is reachable from iDRAC with the current routing-table contents. A destination IP address is required. Based on the current routing-table contents, an ICMP echo packet is sent to the destination IP address.

To run this subcommand, you must have the **Debug** privilege.

Synopsis

```
racadm ping <ipaddress>
```

Input

`<ipaddress>` — The IP address of the remote endpoint to ping.

Output

```
PING 192.168.0 (192.168.0): 56 data bytes64 bytes from 192.168.0: seq=0
ttl=64 time=4.121 ms
192.168.0 ping statistics
1 packets transmitted, 1 packets received, 0 percent packet lossround-trip
min/avg/max = 4.121/4.121/4.121 ms
```

ping6

Table 71. Details of ping6

Description

Verifies if the destination IPv6 address is reachable from iDRAC or with the current routing-table contents. A destination IPv6 address is required. Based on the current routing-table contents, an ICMP echo packet is sent to the destination IPv6 address.

To run this subcommand, you must have **Debug** privilege.

Synopsis

```
racadm ping6 <ipv6address>
```

Input

`<ipv6address>` — the IPv6 address of the remote endpoint to ping.

Example

```
Pinging 2011:de11:bdc:194::31 from 2011:de11:bdc:194::101 with 32 bytes of
data:
Reply from 2011:de11:bdc:194::31: time<1ms
Reply from 2011:de11:bdc:194::31: time<1ms
Reply from 2011:de11:bdc:194::31: time<1ms
Reply from 2011:de11:bdc:194::31: time<1ms

Ping statistics for 2011:de11:bdc:194::31:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

RACADM Proxy

Table 72. Details of RACADM Proxy

Description

On the PowerEdge FX2/FX2s systems, you can manage the compute sleds and CMC using the iDRAC's RACADM Proxy feature that redirects commands from iDRAC to CMC. You can return the CMC response to local or remote RACADM.to access the CMC configuration and reporting features without placing the CMC on the management network. The CMC configuration commands are supported through local proxy when local configuration is enabled on iDRAC.

NOTE: Local racadm and local racadm proxy runs with root user privilege.

Synopsis

Local RACADM proxy usage

```
racadm <CMC racadm subcommand> --proxy
```

Remote RACADM proxy usage

```
racadm <CMC racadm subcommand> -u <username> -p <password> -r <idrac-ip
connected to cmc> --proxy
```

NOTE:

- **The attribute `racadm getconfig -g cfgractuning -o cfgRacTuneChassisMgmtAtServer` must be set as non-zero in CMC.**
- **The attribute `racadm get system.ChassisControl.ChassisManagementMonitoring` attribute must be enabled in iDRAC.**
- **`--proxy` must be entered at the end of the command.**
- **The root privilege is the default privilege for Local RACADM proxy.**
- **The user privilege in the Remote RACADM proxy for CMC maps to iDRAC privilege.**

Table 73. Details of CMC and iDRAC privilege for an operation

Required CMC Privilege for an operation	Required iDRAC Privilege for proxy operation
CMC Login User	Login
Chassis Configuration Administrator	Configure
User Configuration Administrator	Configure User
Clear Logs Administrator	Logs
Chassis Control Administrator	System Control
Server Administrator	System Control
Test Alert User	System Operations
Debug Command Administrator	Debug
Fabric x Administrator (where x is A, B, or C)	System Control

- **When CMC is not placed on the network, the import, export, and file operation commands to CIFS, NFS, or FTP will fail.**
- **When the Remote or Local RACADM Proxy operation is in progress, if the iDRAC is reset, then the Proxy operation fails and the output is not displayed in Remote or Local RACADM.**
- **When racadm `getsystem.ChassisControl.ChassisManagementMonitoring` attribute is set to `monitor`, all the users including root users can only view the attribute.**

  To configure, set the attribute to `monitor and manage` in CMC.

Input

- `-u` — Specifies the user name of the remote share that stores the catalog file.
- `-p` — Specifies the password of the remote share that stores the catalog file.
- `-r` — Specifies the iDRAC IP address connected to CMC.

Example

Local RACADM

```
racadm getractime --proxy
```

Remote RACADM

```
racadm getractime -u root -p xxx -r 192.168.0 getractime --proxy
```

racdump

Table 74. Details of racdump

Description	Provides a single command to get dump, status, and general iDRAC board information. To run this subcommand, you must have the Debug permission. • General System/RAC Information • Coredump Information • Network Interface Statistics • Session Information • Process Information • RAC Firmware Build Log **NOTE: The RAC debug logs are not part of Local and Remote RACADM. It is available only on Firmware RACADM**
Synopsis	`racadm racdump`
Input	N/A

Example

```
================================================================================ General
System/RAC Information
================================================================================ RAC Information:
RAC Date/Time = Thu May 18 13:35:32 2017 Firmware Version = 3.00.00.00 Firmware Build = 12 Last
Firmware Update = 04/04/2017 19:41:38 Hardware Version = 0.01 MAC Address = 18:03:73:F7:B7:CA
Common settings: Register DNS RAC Name = 0 DNS RAC Name = idrac Current DNS Domain = Domain Name
from DHCP = Disabled IPv4 settings: Enabled = 1 Current IP Address = 192.168.0.1 Current IP
Gateway = 192.168.0.1 Current IP Netmask = 192.168.0.1 DHCP Enabled = 0 Current DNS Server 1 =
0.0.0.0 Current DNS Server 2 = 0.0.0.0 DNS Servers from DHCP = Disabled IPv6 settings: Enabled =
0 Current IP Address 1 = :: Current IP Gateway = :: Autoconfig = 1 Link Local IP Address = ::
Current IP Address 2 = :: Current IP Address 3 = :: Current IP Address 4 = :: Current IP Address
5 = :: Current IP Address 6 = :: Current IP Address 7 = :: Current IP Address 8 = :: Current IP
Address 9 = :: Current IP Address 10 = :: Current IP Address 11 = :: Current IP Address 12 = ::
Current IP Address 13 = :: Current IP Address 14 = :: Current IP Address 15 = :: DNS Servers
from DHCPv6 = Disabled Current DNS Server 1 = :: Current DNS Server 2 = :: System Information:
System Model = PowerEdge R720 System Revision = I System BIOS Version = 3.0.00 Service Tag =
Express Svc Code = Host Name = localhost.localdomain OS Name = OS Version = Power Status = ON
Fresh Air Capable = No Watchdog Information: Recovery Action = None Present countdown value =
478 seconds Initial countdown value = 480 seconds Embedded NIC MAC Addresses:
NIC.Integrated.1-3-1 Ethernet = 78:2B:CB:4B:C2:ED NIC.Integrated.1-1-1 Ethernet =
78:2B:CB:4B:C2:EB
================================================================================ Coredump
Information ================================================================================
There is no coredump currently available.
================================================================================ Network
Interface Statistics
================================================================================ Kernel IPv6
routing table Destination Next Hop Flags Metric Ref Use Iface ::1/128 :: U 0 1 1 lo ::1/128 :: U
256 0 0 lo fe80::1a03:73ff:fef7:b7ca/128 :: U 0 0 1 lo fe80::/64 :: U 256 0 0 eth1 ff00::/8 :: U
256 0 0 eth1 Kernel IP routing table Destination Gateway Genmask Flags MSS Window irtt Iface
0.0.0.0 192.168.0.1 0.0.0.0 UG 0 0 0 bond0 192.168.0.1 0.0.0.0 192.168.0.1 U 0 0 0 bond0 Active
Internet connections (w/o servers) Proto Recv-Q Send-Q Local Address Foreign Address State tcp 0
0 192.168.0.1:53986 192.168.0.1:199 ESTABLISHED tcp 0 0 192.168.0.1:53985 192.168.0.1:199
ESTABLISHED tcp 0 0 192.168.0.1:199 192.168.0.1:53986 ESTABLISHED tcp 0 0 192.168.0.1:199
192.168.0.1:53985 ESTABLISHED
================================================================================ Session
Information ================================================================================ No
active sessions currently exist.
================================================================================ Process
Information ================================================================================ PID
USER VSZ STAT COMMAND 1 root 5236 S {systemd} /sbin/init 2 root 0 SW [kthreadd] 3 root 0 SW
```

```
[ksoftirqd/0] 6 root 0 SW [watchdog/0] 7 root 0 SW< [khelper] 8 root 0 SW [kdevtmpfs] 9 root 0
SW< [netns] 153 root 0 SW [sync_supers] 155 root 0 SW [bdi-default] 157 root 0 SW< [kblockd] 166
root 0 SW [khubd] 16233 root 40916 S racadm racdump 16246 root 3824 S sh -c /bin/ps 16247 root
3828 R /bin/ps 26851 root 0 SW [kworker/u:3]
================================================================================ RAC Firmware
Build Log ================================================================================
BLD_TAG=idracfw_bldtag_3.00.00.00_691231_1800_00 BLD_VERSION=3.00.00.00 BLD_NUMBER=69.12.31
BLD_DATE=2.00.00.00.733 BLD_TYPE=idrac BLD_KERNEL=ZIMAGE
```

racreset

Table 75. Details of racreset

Description

Resets iDRAC. The reset event is logged in the iDRAC log.

To run this subcommand, you must have the Configure iDRAC permission and configure user privilege.

NOTE: After you run the `racreset` subcommand, iDRAC may require up to two minutes to return to a usable state.

Synopsis

```
racadm racreset soft
```

```
racadm racreset hard
```

```
racadm racreset soft -f
```

```
racadm recreset hard -f
```

Input

- `-f` — This option is used to force the reset.

Output

```
racadm racreset
RAC reset operation initiated successfully. It may take up to a minute for
the RAC to come online again.
```

Example

- iDRAC reset

```
racadm racreset
```

racresetcfg

Table 76. Details of racresetcfg

Description

Deletes your current iDRAC configuration and resets iDRAC to the factory default settings based on the options provided.

If you run `racresetcfg` from a network client for example, a supported web browser, TELNET or SSH, or Remote RACADM), use the default IP address which is 192.168.0.120. The `racresetcfg` subcommand does not reset the **cfgDNSRacName** object.

To run this subcommand, you must have the `Configure iDRAC` privilege and `Configure User` privilege.

NOTE: Certain firmware processes must be stopped and restarted to complete the reset to defaults. iDRAC becomes unresponsive for about 30 seconds while this operation completes.

Synopsis

- RAC reset operation initiated successfully. It may take several minutes for the RAC to come online again.

```
racadm racresetcfg
```

- `racadm racresetcfg -f`
- `racadm racresetcfg [-all]`
- `racadm racresetcfg [-rc]`

Input

- `-f`—Force `racresetcfg`. If any vFlash partition creation or formatting is in progress, iDRAC returns a warning message. You can perform a force reset using this option.
- `-all`—Discard all settings and reset user to shipping value.
- `-rc`—Discard all settings and reset user to default user name and password.

NOTE: When you perform `racresetcfg -rc` on Stomp and Noble/VRTX servers, by default, the DHCP is disabled.

Example

- Reset the configuration on iDRAC.

```
racadm racresetcfg
```

The RAC configuration has initiated restoration to factory defaults.

Wait up to a minute for this process to complete before accessing the RAC again.

- Reset when vFlash partition creation is in progress.

```
racadm racresetcfg
```

A vFlash SD card partition operation is in progress. Resetting the iDRAC may corrupt the vFlash SD card. To force `racresetcfg`, use the `-f` flag.

- Reset all iDRAC's configurations to default, and preserve the user and network settings.

```
racadm racresetcfg -f
```

- Reset all iDRAC's configurations to default, and reset the user to shipping value.

```
racadm racresetcfg -all
```

- Reset all iDRAC's configurations to default, and reset the user to root/calvin.

```
racadm racresetcfg -rc
```

recover

Table 77. Details of Recover sub-command

Description

Allows you to recover the previous version of the firmware.

NOTE: To run this subcommand, you must have the Server Control privilege.

Synopsis

- To recover the BIOS firmware:

```
racadm recover <FQDD>
```

NOTE: BIOS.Setup.1-1 is the supported FQDD

Input

- `FQDD`— Specify the FQDD of the device for which the recovery is required.

Examples

- To recover the BIOS firmware:

```
racadm recover BIOS.Setup.1-1
```

RAC1234: Recovery operation initiated successfully. Check the Lifecycle logs for the status of the operation by running RACADM command "racadm lclog view".

remoteimage

Table 78. Details of remoteimage

Description

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

To run this subcommand, you must log in with virtual media privilege for iDRAC.

Synopsis

- `racadm remoteimage -d`
- `racadm remoteimage -s`
- `racadm remoteimage -c [-u <username> -p <password> -l <image_path>]`

Input

- `-c`—Connect the image.
- `-d`—Disconnect image.
- `-u`—User name to access shared folder.
- `-p`—Password to access shared folder.
- `-l` —Image location on the network share; use single quotation marks around the location.
- `-s` —Display current status.

NOTE: Use a forward slash (/) when providing the image location. If backward slash (\) is used, override the backward slash for the command to run successfully.

For example:

```
racadm remoteimage -c -u user -p xxx -l /\/\192.168.0.2/\CommonShare/
\diskette
```

NOTE: The following options only apply to connect and deploy actions

- `-u` —Username.

  User name to access the network share. For domain users, you can use the following formats:

  - domain/user
  - domain\user
  - user@domain
- `-p` —Password to access the network share.

Example

- Disable Remote File Sharing.

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

- Check Remote File Share status.

```
racadm remoteimage -s
Remote File Share is Enabled
UserName
Password
ShareName //192.168.0/xxxx/dtk_3.3_73_Linux.iso
```

- Deploy a remote image on iDRAC CIFS Share.

```
racadm remoteimage -c -u admin -p xxx -l //192.168.0.32/dev/OM840.iso
```

- Deploy a remote image on iDRAC NFS Share.

```
racadm remoteimage -c -u root -p password -l '192.168.1.113:/opt/nfs/
OM840.iso
```

- Deploy a remote image on iDRAC HTTP Share.

```
racadm remoteinage -c -u "user" -p "xxx" -l http://shrloc/foo.iso
```

- Deploy a remote image on iDRAC HTTPS Share.

```
racadm remoteinage -c -u "user" -p "xxx" -l https://shrloc/foo.iso
```

NOTE: -p and -u options are not mandatory in case of HTTP/HTTPS based remoteimage commands.

rollback

Table 79. Details of rollback

Description

Allows you to roll back the firmware to an earlier version.

Synopsis

```
racadm rollback <FQDD> [--reboot]
```

NOTE: To get the list of available rollback versions and FQDDs, run the `racadm swinventory` command.

Input

- `<FQDD>`: Specify the FQDD of the device for which the rollback is required.
- `--reboot`: Performs a graceful system reboot after the BIOS firmware rollback.

Example

- To perform BIOS firmware rollback:

```
racadm rollback iDRAC.Embedded.1-1
RAC1056: Rollback operation initiated successfully.
```

- To perform a graceful system reboot after BIOS firmware rollback:

```
racadm rollback BIOS.Setup.1-1 --reboot
```

sensorsettings

Table 80. sensorsettings

Description

Allows you to perform threshold settings of the sensor.

To run this subcommand, you must have **Configure iDRAC** privilege.

NOTE: An error message is displayed when the following is performed:

- **A set operation is performed on an unsupported FQDD.**
- **Out of range settings is entered.**
- **Invalid sensor FQDD is entered.**
- **Invalid threshold level filter is entered.**

Synopsis

```
racadm sensorsettings set <FQDD> -level Min <value>
```

Input

- `<FQDD>` — Sensor or corresponding sensor FQDD which needs a threshold configuration. Run the command, `racadm getsensorinfo` to view the sensor FQDD. The `R/W` field in the output getsensorinfo indicates if

the sensor thresholds can be configured. Replace the <FQDD> field with the corresponding sensor FQDD that needs a threshold configuration.

- -level — threshold level for the sensor setting. Values are Max or Min.

Examples

To set the minimum noncritical threshold level for a power sensor type.

```
racadm sensorsettings set iDRAC.Embedded.1#SystemBoardCPUUsage -level Max 95
```

NOTE: The entered value must be lesser or higher than the sensor critical threshold limit.

serveraction

Table 81. serveraction

Description

Enables you to perform power management operations on the blade system.

To run this subcommand, you must have the Execute Server Control Commands permission.

Synopsis

```
racadm serveraction <action> -f
```

Input

<action> — Specifies the power management operation to perform. The options are:

- hardreset — Performs a force reset (reboot) operation on the managed system.
- powercycle — Performs 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 — Powers down the managed system.
- powerup — Powers up the managed system.
- powerstatus — Displays the current power status of the server (ON or OFF).
- graceshutdown — Performs a graceful shutdown of the server. If the operating system on the server cannot shut down completely, then this operation is not performed.
- nmi — Generates the Non-masking interrupt (NMI) to halt the system operation. The NMI sends a high-level interrupt to the operating system, which causes the system to halt the operation to allow critical diagnostic or troubleshooting activities.

  NOTE:

  The halt system operation does not occur on systems running the Linux operating system.
- -f — Force the server power management operation.

  This option is applicable only for the PowerEdge-VRTX platform. It is used with powerdown,powercycle, and hardreset options.

NOTE: The actionpowerstatus is not allowed with -a option.

Output

Displays an error message if the requested operation is not completed, or a success message if the operation is completed.

Example

Get Power Status on iDRAC

```
racadm serveraction powerstatus
Server Power Status: ON
```

```
racadm serveraction powercycle
Server power operation successful
```

set

Table 82. Details of set

Description

Modifies the value of configuration objects on a component. The `Set` sub-command has two forms:

- The modification of a single object to a new value specified in the command line.
- The modification of multiple objects to new values using a configuration file.

  It supports multi-object value import from two configuration file formats.

  - INI format — The INI format files can be imported from a local file only
  - Server Configuration Profile(SCP) XML and JSON format - XML and JSON format files can be imported from a local file, from an NFS, CIFS, HTTP, HTTPS, FTP and TFTP network share.

    NOTE: To run the `Set` sub-command for Server Configuration Profile XML files, use the Lifecycle Controller version 1.1 or later.

  Depending on the type of configuration object being modified, the new values could be applied immediately (in "real-time") or require staging and a reboot of the system to apply the new values. The following components support either real-time or staged application of new values:

  - iDRAC with Lifecycle Controller
  - PowerEdge RAID controllers

    NOTE: Use PowerEdge RAID controllers with firmware version 9.1 or later. The real-time support is provided only while performing hardware RAID configuration.

The following components require staging and system reboot for application of new values:

- BIOS
- Other PowerEdge RAID controllers — For software RAID configuration
- Networking devices – Ethernet and Fibre Channel

NOTE:

- **To modify the value of staged objects such as BIOS or NIC, commit and reboot job creation must be used to apply the pending values. When single object `Set` operations are used to stage value modification, use the jobqueue command to schedule a job to reboot the server and apply the new values. For staged multi-object `Set` operations using ini and xml configuration files, a job will automatically be created by the `Set` command; use the –b, -w and -s options to specify how the staged reboot will be performed. For more information, see jobqueue.**

Synopsis

Single-object Set

```
racadm set <FQDD Alias>.<group> <value>
```

```
racadm get <FQDD Alias>.<group>.<object> <value>
```

```
racadm get <FQDD Alias>.<group>.[<index>].<object> <value>
```

```
racadm get <FQDD Alias>.<index>.<group>.<index>.<object> <value>
```

Multi-object Set

```
racadm set -f <filename> [-t ini] [--continue]
```

```
racadm set -f <filename> -t xml -l <NFS share> [--preview] [--continue]
```

```
racadm set -f <filename> -t xml -l <NFS share> -c <FQDD>[,<FQDD>*]
```

```
racadm set -f <filename> -t xml -u <username> -p <password> -l <CIFS share>
[--preview] [--continue]
```

```
racadm set -f <filename> -t xml -u <username> -p <password> -l <CIFS share>
-c <FQDD>[,<FQDD>*]
```

- Configure a RAC from an XML configuration file located on a remote NFS share

```
racadm set -f <filename> -t xml -l <NFS> 10.1.2.3:/myshare
```

- Configure a RAC from an XML configuration file located on a remote HTTP share.

```
racadm set -f <filename> -t xml -u <httpuser> -p <httppwd> -l <HTTP> http://
test.com/myshare
```

- Configure a RAC from an XML configuration file located on a remote HTTPS share.

```
racadm set -f <filename> -t xml -u <httpsuser> -p <httpspwd> -l <HTTPS>
https://test.com/myshare
```

- Configure a RAC from an XML configuration file located on a remote FTP share

```
racadm set -f <filename> -t xml -u <username> -p <password> -l <FTP share> -
c <FQDD>
```

- Configure a RAC from an XML configuration file located on a remote TFTP share.

```
racadm set -f <filename> -t xml -l <TFTP share> -c <FQDD>
```

Input

- `<FQDD Alias>`

  Examples for FQDDs:

  - System.Power
  - System.Power.Supply
  - System.Location
  - LifecycleController.LCAttributes
  - System.LCD
  - iDRAC.Serial
- `<group>` — Specifies the group containing the object that must be written.
- `<object>` — Specifies the object name of the value that must be written.
- `<index>` — This option is specified where FQDD Aliases or Groups must be indexed.
- `-f <filename>` — Enables set to configure the device from a specified file. This option is not supported in the Firmware RACADM interface.
- `--continue` — This option is used with –f only and is applicable for only for INI file operation.. If a multi-object `Set` is unsuccessful for a <group>, then `Set` continues with the next <group> in the file. If this option is not used, then `Set` stops when it is unsuccessful for a particular <group>. After the unsuccessful <group>, the remaining <group>s are not configured.

  NOTE:

  This option is applicable only for INI file operation.
- `-u` — Specifies user name of the CIFS remote share from which the file must be imported
- `-p` — Specifies password for the remote CIFS share from which the file must be imported.
- `-l` — Specifies network share location from where the file must be imported.
- `-t` — Specifies the file type to be imported.

  The valid values are:

  - `xml`—Imports the Server Configuration Profile in XML format either from a local or network share file.
  - `JSON`—Specifies a JSON file.
  - `INI`— files can only be imported from a local file.

  NOTE: To import or export Server Configuration Profile . `xml`, use the Lifecycle Controller version 1.1 or later.

Staging and reboot control options

The following options control when and how system reboots are performed when using the –f option. As noted above, some `FQDD`s require a system reboot to apply the new values; other `FQDD`s optionally support immediate application of new values. If the imported file contains ONLY immediate application-capable `FQDD`s such as iDRAC, do NOT use the –b option and the Set command will schedule a real-time job to immediately apply the new values.

NOTE: The –b, -w, –s, and --preview options are applicable only with –f option.

- `-b` — . Specifies the type of shutdown for the system after a file import operation completes. The parameters are `Graceful`, `Forced`, and `NoReboot` for graceful shutdown, forced shutdown, and no reboot respectively. If -b is not specified, graceful shutdown is taken as the default except as noted above for files containing new values for immediate application-capable <FQDD>s.

  NOTE: If the operating system is in use, then the `graceful` shutdown option may time out within 300 seconds. If this operation is unsuccessful, then retry with the `force` option.
- `-w` — Maximum time to wait for the graceful shutdown to occur. The value must be entered in seconds. Minimum accepted value is 300 seconds and the maximum accepted value is 3600 seconds. The default value is 1800 seconds.
- `-s` — Power state of the host when the import operation completes. The parameters are "On" for powered ON and "Off" for powered OFF. If this parameter is not specified, power ON is taken as default.
- `--preview` — Validates the configuration `.xml` file and view the status.

  The `--preview` option provides the **Job ID** to verify the status of the file preview operation. The **Job ID** can be tracked by running the `racadm jobqueue view -I <JID>` command.

  NOTE:
  - **The `--preview` option does not restart the system.**
  - **The `-b`,`-w` options cannot be included with the `--preview` option.**
  - **A scheduled job or pending configuration should not be running while using the `--preview` option.**
- `-c` — Specifies the FQDD or list of FQDDs separated by ',' of the components for which the configurations should be imported. If this option is not specified, configuration related to all the components are imported.

NOTE: To use the `-c` or `--preview` option, the minimum Lifecycle Controller version required is 1.2.

NOTE: On certain devices, importing the server configuration profile requires two imports to apply the configuration to all the devices. The first import of the profile enables hidden devices which are then configured with a second import. The devices that require two imports are as follows:

- **PERC S110 and PERC S130 controllers**
- **PERC S110 and PERC S130 controllers**
- **BIOS and PCIe device: enabling PCIe slots in the system that are disabled and configuring the PCIe device**
- **BIOS: enabling processor trusted execution (TXT) when server has Trusted Platform Module (TPM) 2.0 installed**
- **BIOS: if SCP contains only a BIOS section that includes switching boot mode to UEFI and configuration of UEFI PXE network settings**
- **BIOS: if SCP contains only a BIOS section that includes switching boot mode to legacy BIOS or UEFI along with changes to the boot order sequence using changes to BootSeq, HddSeq, or UefiBootSeq attributes.**
- **BIOS: changing TPM 2.0 cryptographic support from the default of SHA-1**

  NOTE: Boot mode and boot order sequence can be changed with a single SCP import if the SetBootOrderFqddN and SetLegacyHddOrderFqddN attributes are used.

This command does not support setting the proxy parameters if the share location (-l) is HTTP/HTTPS. For more information, see Proxy parameter section.

Example

Single-object Set of real-time objects

- Configure LCD String.

```
$ racadm set system.lcd.LCDUserString test
```

- - Configure iDRAC name.

```
racadm set iDRAC.Info.Name idrac-server100
```

Single-object Set of staged objects

- Configure several BIOS settings, create a job to initiate application of new values, reboot the system, then wait for the job to complete.

  ```
  racadm set BIOS.SysProfileSettings.ProcTurboMode Disabled
  racadm set BIOS.ProcSettings.ProcVirtualization Enabled
  racadm set BIOS.ProcSettings.ControlledTurbo Enabled
  racadm jobqueue create BIOS.Setup.1-1 –r Graceful
  ```

  - Note of the Job ID output by the jobqueue command
  - After reboot, wait for the job to complete by checking the job status

    ```
    racadm jobqueue view –i <Job ID>
    ```

Multi-object Set of real-time objects

- Configure the iDRAC using a local INI file.

  ```
  racadm set –f myidrac.ini
  ```
- Configure the iDRAC using a local Server Configuration Profile XML file containing only iDRAC settings.

  ```
  racadm set –f myidrac.xml –t xml
  ```
- Configure the iDRAC using a Server Configuration Profile XML file stored on an NFS share containing only iDRAC settings.

  ```
  racadm set –f myidrac.xml –t xml –l 10.1.2.3:/myshare
  ```
- Import a Server Configuration Profile from a CIFS share, using only the iDRAC component.

  ```
  racadm set –f file –t xml –u myuser –p mypassword –l //192.168.0/share –c
  iDRAC.Embedded.1
  ```

Multi-object Set of staged objects

- Configure a systems using a local Server Configuration Profile XML file containing a mix of real-time and staged objects; reboot the server gracefully with a wait time of ten minutes, leaving the server powered on after the reboot.

  ```
  racadm set –f myfile.xml –t xml –b "graceful" –w 600 –s "on"
  ```

  - Make note of the Job ID output by the Set command.
  - After reboot, wait for the job to complete by checking the job status.

    ```
    racadm jobqueue view –i <Job ID>
    ```
- Configure a systems using a local Server Configuration Profile XML file containing a mix of real-time and staged objects; postpone reboot until other operations have been completed.

  ```
  racadm set –f myfile.xml –t xml –b NoReboot
  ```

  - Make note of the Job ID output by the Set command; because of the NoReboot option, the job will be pending until the server is rebooted
  - Complete other operations, then perform a reboot
  - After reboot, wait for the job to complete by checking the job status

    ```
    racadm jobqueue view –i <Job ID>
    ```
- Verify the Server Configuration Profile XML file content located in a remote CIFS share.

  ```
  racadm set –f temp_Configuration_file –t xml –u Administrator –p Password –
  l //192.168.0/xyz –preview
  ```
- Configure a RAC from an XML configuration file located on a remote FTP share.

  ```
  racadm set –f myfile.xml –t xml –u username –p password –l ftp://
  192.168.10.24/
  ```
- Configure a RAC from a JSON configuration file located on a remote FTP share.

  ```
  racadm set –f myfile.xml –t json –u httpsuser –p httpspwd –l ftp://
  192.168.10.24/
  ```

- Configure a RAC from an XML configuration file located on a remote TFTP share.

```
racadm set -f myfile.xml -t xml -l tftp://192.168.10.24/
```

- Configure a RAC from a JSON configuration file located on a remote TFTP share.

```
racadm set -f myfile.xml -t json -l tftp://192.168.10.24/
```

- Configure a RAC from an XML configuration file located on a remote HTTP share.

```
racadm set -f myfile.xml -t xml -u httpuser -p httppwd -l http://test.com/
myshare
```

- Configure a RAC from an XML configuration file located on a remote HTTPS share.

```
racadm set -f myfile.xml -t xml -u httpsuser -p httpspwd -l https://
test.com/myshare
```

- Configure a RAC from a JSON configuration file located on a remote HTTPS share.

```
racadm set -f myfile.xml -t json -u httpsuser -p httpspwd -l https://
test.com/myshare
```

- Configure the proxy parameter.

```
racadm set lifecyclecontroller.lcattributes.UserProxyUsername admin1
```

- Remove the the proxy parameter.

```
racadm set lifecyclecontroller.lcattributes.UserProxyUsername
```

- View the list of proxy attributes.

```
racadm get lifecycleController.lcAttributes
```

setled

Table 83. Details of setled

Description

Sets the state (blinking or not blinking) of the LED on the specified module.

To run this subcommand, you must have the Configure iDRAC permission.

Synopsis

```
racadm setled -l <ledState>
```

Input

- `-l <ledState>` — Specifies the LED state. The values are:
  - 0 — No Blinking
  - 1 — Blinking

Example

- From iDRAC stop LED from blinking.

```
racadm setled -l 0
RAC0908: System ID LED blink off.
```

- From iDRAC start LED to blink.

```
racadm setled -l 1
RAC0907: System ID LED blink on.
```

setniccfg

Table 84. Details of setniccfg

Description

Sets the iDRAC IP address for static and DHCP modes.

To run this subcommand, you must have the **Configure iDRAC** privilege.

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

Synopsis

- `racadm setniccfg -d`
- `racadm setniccfg -d6`
- `racadm setniccfg -s <IPv4Address> <netmask> <IPv4 gateway>`
- `racadm setniccfg -s6 <IPv6 Address> <IPv6 Prefix Length> <IPv6 Gateway>`
- `racadm setniccfg -o`

Input

- `-d` — Enables DHCP for the NIC. It is enabled by default.
- `-d6` — Enables AutoConfig for the NIC (default is disabled).
- `-s` — Enables static IP settings. The IPv4 address, netmask, and gateway must be specified. Otherwise, the existing static settings are used. `<ipaddress>`, `<netmask>`, and `<gateway>` must be typed as dot-separated strings.

```
racadm setniccfg -s 192.168.0 255.255.255.0 192.168.0
```

- `-s6` — Enables static IPv6 settings. The IPv6 address, Prefix Length, and the IPv6 Gateway can be specified.
- `-o` — Enable or disable NIC.

Example

- To Configure static IPv4 address for iDRAC NIC

```
racadm setniccfg -s 192.168.0 255.255.255.0 192.168.0
Static IP configuration enabled and modified successfully
```

- Configure DHCP mode for iDRAC IPv4

```
racadm setniccfg -d
DHCP is now ENABLED
```

- Configure DHCP mode for iDRAC IPv6

```
racadm setniccfg -d6
DHCP6 is now ENABLED
```

sshpkauth

Table 85. Details of sshpkauth

Description

Enables you to upload and manage up to 4 different SSH public keys for each user. You can upload a key file or key text, view keys, or delete keys.

This command has three mutually exclusive modes determined by the options — `upload`, `view`, and `delete`.

To run this subcommand, you must have Configure user privilege.

Synopsis

- `racadm sshpkauth -i svcacct -k <key_index> -p <privilege> -t <PK_key_text>`
- `racadm sshpkauth -i svcacct -k <key_index> -p <privilege> -f <PK_key_text>`

- `racadm sshpkauth -v -i svcacct -k all|<key_index>`
- `racadm sshpkauth -d -i svcacct -k all|<key_index>`

Input

- `-i <user_index>` — Index for the user.
- `-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 to 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.

  NOTE: The `-f` option is not supported on Telnet or SSH or serial RACADM.
- `-v` — View the key text for the index provided.
- `-d` — Delete the key for the index provided.

Example

- 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:
```

sslcertdownload

Table 86. Details of sslcertdownload

Description

Downloads an SSL certificate from iDRAC to the client's file system.

To run this subcommand, you must have the **Server Control** privilege.

NOTE: This subcommand is only supported on the remote interface(s).

Synopsis `racadm sslcertdownload -f <filename> -t <type>`

Input

- `-f` — Specifies the target filename on local file system to download the certificate.
- `-t <type>`—Specifies the type of certificate to download, either the CA certificate for Directory Service or the server certificate.
  - `1`—Server Certificate
  - `2`—Active Directory
  - `3`—Custom Signing Certificate
  - `4`—Client Trust Certificate for SSL
  - `5`—Factory Identity Certificate

Output Returns 0 when successful and non-zero number when unsuccessful.

Example

- Download server certificate:

```
racadm -r 192.168.0 -u root -p xxx sslcertdownload -t 1 -f cert.txt
```

- Download Active Directory certificate:

```
racadm -r 192.168.0 -u root -p xxx sslcertdownload -t 2 -f ad_cert.txt
```

NOTE: This command is not supported in the firmware RACADM interface as it is not a file system.

sslcertupload

Table 87. Details of sslcertupload

Description Uploads a custom SSL server or CA certificate for Directory Service from the client to iDRAC.

To run this subcommand, you must have the following privilege:

- Active Directory certificate - Privilege required Configure iDRAC + Configure User
- Public Key Cryptography Standards (PKCS) format - Privilege required Configure iDRAC
- Client Trust certificate for SSL format and Factory Identity Certificate format - Privilege required Configure iDRAC

Synopsis `racadm sslcertupload -t <type> -f <filename> -p <passphrase>`

Input

- `-f`—Specifies the source filename in the local file system of the certificate uploaded.
- `-p`—Pass phrase for the Public Key Cryptography Standards file.
- `-t`—Specifies the type of certificate to upload. The type of certificate must be:
  - `1`—Server certificate
  - `2`—CA certificate for Directory Service
  - `3`—Public Key Cryptography Standards (PKCS) format
  - `4`—Client Trust certificate for SSL format
  - `5`—Factory Identity Certificate format

Output `racadm -r 192.168.0.2 -u root -p xxx sslcertupload -t 2 -f cert.txt` Certificate that is successfully uploaded to the RAC.

Example

- Uploading a server certificate.

```
racadm -r 192.168.0.2 -u root -p xxx sslcertupload -t 1 -f cert.txt
```

- Uploading web server certificate and key

```
racadm -r 192.168.0.2 -u root -p xxx sslcertupload -t 6 -f cert.txt -k
key.txt
```

- Uploading Active Directory certificate

```
racadm -r 192.168.0.2 -u root -p xxx sslcertupload -t 2 -f ad_cert.txt
```

- Uploading Client Trust certificate for SSL

```
racadm -r 192.168.0.2 -u root -p xxx sslcertupload -t 4 -f
https_cert.cer
```

- Uploading Factory Identity certificate

```
racadm -r 192.168.0.2 -u root -p xxx sslcertupload -t 5 -f fi_cert.cer
```

sslcertview

Table 88. Details of sslcertview

Description	Displays the SSL server or CA certificate that exists on iDRAC.
Synopsis	`racadm sslcertview -t <type> [-A]`

Input	• `-t`—Specifies the type of certificate to view, either the CA certificate or server certificate.
	  • `1`—Server Certificate
	  • `2`—Active Directory
	  • `3`—Factory Identity Certificate
	  • `4`—Client Trust certificate for SSL
	• `-A`—Prevents printing headers or labels.
	NOTE: If a certificate is generated using a comma ',' as one of the parameters, command displays the partial name in the following fields only until the comma:
	• **Organization Name**
	• **Common Name**
	• **Location Name**
	• **State Name**
	The rest of the string is not displayed.

Table 89. Output

`Serial Number`	`01`
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)`	`iDRAC Default certificate`
Issuer Information:	
`Country Code (CC)`	`US`
`State (S)`	`Texas`
`Locality (L)`	`Round Rock`
`Organization (O)`	`Dell Inc.`
`Organizational Unit (OU)`	`Remote Access Group`

```
Common Name (CN)                        iDRAC Default certificate
Valid From                              May 15 23:54:19 2017 GMT
Valid To                                May 12 23:54:19 2027 GMT
```

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

```
00

US

Texas

Round Rock

Dell Inc.

Remote Access Group

iDRAC default certificate

US

Texas

Round Rock

Dell Inc.

Remote Access Group

iDRAC default certificate

May 15 23:54:19 2017 GMT

May 12 23:54:19 2027 GMT
```

sslcertdelete

Table 90. Details of sslcertdelete

Description	Command to delete a custom signing certificate from iDRAC. To run this subcommand, you must have the **Configure iDRAC** privilege.
Synopsis	`racadm sslcertdelete -t <type>`
Input	`-t`—Specifies the type of certificate to delete. The type of certificate is: • `3`—Custom signing certificate • `4`—Client trust certificate for SSL
Output	The following information is displayed: • The custom signing certificate was deleted. • The iDRAC resets and may be offline temporarily.

Example

Use Remote RACADM to delete the custom signing certificate.

```
$ racadm -r 192.168.0 -u root -p xxx sslcertdelete -t 3
```

Use Remote RACADM to delete the Client Trust certificate for SSL.

```
$ racadm -r 192.168.0 -u root -p xxx sslcertdelete -t 4
```

sslcsrgen

Table 91. Details of sslcsrgen

Description

Generates and downloads a certificate signing request (CSR) file to the client's local file system. The CSR can be used for creating a custom SSL certificate that can be used for SSL transactions on iDRAC.

To run this subcommand, you must have the Configure iDRAC privilege.

Synopsis

- `racadm sslcsrgen -g`
- `racadm sslcsrgen [-g] [-f <filename>]`
- `racadm sslcsrgen -s`
- `racadm sslcsrgen -g -t <csr_type>`
- `racadm sslcsrgen -g -f <filename> -t <csr_type>`
- `racadm sslcsrgen -s -t <csr_type>`

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: The `-f` option is only supported on the remote interfaces.
- `-t` —Specifies the type of CSR to be generated. The options are:
  - 1—SSL cert
  - 2—Factory Identity Cert

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

- Display the status of CSR operation:

  ```
  racadm sslcsrgen -s
  ```
- Generate and download a CSR to local file system using remote RACADM

  ```
  racadm -r 192.168.0.120 -u <username> -p <password> sslcsrgen -g -f
  csrtest.txt
  ```
- Generate and download a CSR to local file system using local RACADM

  ```
  racadm sslcsrgen -g -f c:\csr\csrtest.txt
  ```
- Generate a new certificate signing request for Factory Identity type

  ```
  racadm sslcsrgen -g -t 2
  ```

- Display the status of the current CSR operation for Factory Identity type

```
racadm sslcsrgen -s -t 2
```

- Generate and download a CSR for Factory Identity type to local file system using remote RACADM

```
racadm -r 192.168.0.120 -u root -p calvin sslcsrgen -g -f csrtest.txt -t 2
```

- Generate and download a CSR for Factory Identity type to local file system using local RACADM

```
racadm sslcsrgen -g -f c:\csr\csrtest.txt -t 2
```

NOTE: Before a CSR can be generated, the CSR fields must be configured in the RACADM `iDRAC.Security` group. For example:

```
racadm set iDRAC.security.commonname MyCompany
```

NOTE: In Telnet or SSH console, you can only generate and not download the CSR file.

sslkeyupload

Table 92. Details of sslkeyupload

Description	Uploads SSL key from the client to iDRAC. To run this subcommand, you must have the **Server Control** privilege.
Synopsis	`racadm sslkeyupload -t <type> -f <filename>`
Input	• `-t` — Specifies the key to upload. The value is: • `1` — SSL key used to generate the server certificate. • `-f` — Specifies the filename of the SSL key that must be uploaded.
Output	If upload is successful, the message `SSL key successfully uploaded to the RAC` is displayed. if upload is unsuccessful, error message is displayed.
Example	`racadm sslkeyupload -t 1 -f c:\sslkey.txt`

sslresetcfg

Table 93. Details 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 run this subcommand, you must have the Configure iDRAC privilege.
Synopsis	`racadm sslresetcfg`
Input	N/A
Example	`racadm sslresetcfg` `Certificate generated successfully and webserver restarted.`

Storage

Table 94. Details of storage

Description

Allows you to run the commands to control storage arrays.

To run this subcommand for configuring the storage properties, you must have the server control permission.

Synopsis

Inventory

NOTE: You can also run the command using `raid` in place of the `storage` command.

- To view the help details for get command, run the following command:

```
racadm storage help get
```

- To generate and view information about the inventory of storage root node, run the following command:

```
racadm storage get status
```

- To generate and view information about the inventory of controllers, run the following command:

```
racadm storage get controllers -o
```

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

- To get the list of controllers, run the following command:

```
racadm storage get controllers
```

- To get the properties of PCIeSSD controller, run the following command:

```
racadm storage get controllers:<PcieSSD controller FQDD>
```

- To generate and view information about the inventory of batteries, run the following command:

```
racadm storage get batteries -o
```

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

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

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

- To generate and view information about the inventory of virtual disks, run the following command:

```
racadm storage get vdisks
```

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

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

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

- To generate and view information about the inventory of enclosures, run the following command:

```
racadm storage get enclosures -o
```

```
racadm storage get enclosures --refkey <connector FQDDs separated by comma>
```

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

- To get the list of enclosures, run the following command:

```
racadm storage get enclosures
```

- To get the properties of the PCIeSSD enclosure, run the following command:

```
racadm storage get enclosures:<PCIeSSD enclosure FQDD>
```

- To generate and view information about the inventory of physical disk drives, run the following command:

```
racadm storage get pdisks
```

```
racadm storage get pdisks -o
```

```
racadm storage get pdisks -o -p <property names separated by comma>
```

```
racadm storage get pdisks --refkey <enclosure/Backplanes FQDDs separated by
comma>
```

```
racadm storage get pdisks --refkey <enclosure/Backplanes FQDDs separated by
comma> -o
```

```
racadm storage get pdisks --refkey <enclosure/Backplanes FQDDs separated by
comma> -o -p <property names separated by comma>
```

- To get the list of physical disks, run the following command:

```
racadm storage get pdisks
```

- To get the properties of PCIeSSD physical disk, run the following command:

```
racadm storage get pdisks:<PCIeSSD FQDD>
```

- To rename, expansion and raid level migration of the virtual disks. To rebuild, cancel rebuild and cancel the background initialization.

```
racadm storage renamevd:<VirtualDisk FQDD > -name <new_vd_name>
```

```
racadm storage capacityexpansion:<VirtualDisk FQDD > -size <new size VD> -
pdkey <PhysicalDisk FQDDs>
```

```
racadm storage capacityexpansion:<VD FQDD> -size <new size>.
```

```
racadm storage discardcache:<Controller FQDD>
```

```
racadm storage raidlevelmigration:<VirtualDisk FQDD > -new_rl <raid_level> -
pdkey:<pdisk_fqdd separated by commas>
```

```
racadm storage rebuild:<PD FQDD>
```

```
racadm storage cancelrebuild:<PD FQDD>
```

```
racadm storage cancelbgi:<VD FQDD>
```

- To generate and view information about the inventory of fans, run the following command:

```
racadm storage get fans --refkey <enclosure FQDDs separated by comma>
```

```
racadm storage get fans --refkey <enclosure FQDDs separated by comma > -o
```

```
racadm storage get fans --refkey <enclosure FQDDs separated by comma> -o -p
<property names separated by comma>
```

- To generate and view information about the inventory of EMMs, run the following command:

```
racadm storage get emms -refkey <enclosure FQDDs separated by comma>
```

```
racadm storage get emms --refkey <enclosure FQDDs separated by comma> -o
```

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

- To generate and view information about the inventory of PSU, run the following command:

```
racadm storage get psus -refkey <enclosure FQDDs separated by comma>
```

```
racadm storage get psus --refkey <enclosure FQDDs separated by comma> -o
```

```
racadm storage get psus --refkey <enclosure FQDDs separated by comma> -o -p
<property names separated by comma>
```

Configuration

- To view the help details for a configuration command, run the following command:

```
racadm storage help <command>
```

```
where command can take below values
converttoraid, converttononraid, controllers, clearconfig,
createsecuritykey, createvd, deletesecuritykey,
 deletevd, encryptvd, enclosures, emms, fans, hotspare, importconfig,
```

```
ccheck, cryptographicerase, preparetoremove, blink, unblink, cancelcheck,
renamevd, cancelbgi, rebuild, cancelrebuild, capacityexpanon,
raidlevelmigrationinit, modifysecuritykey, psus, pdisks, resetconfig,
tempprobes, vdisks, patrolread, forceonline,
forceoffline,replacephysicaldisk,unlock,and setbootvd.
```

NOTE: iSM must be running on the operating system to run the preparetoremove method:

- To create, delete, and secure the virtual disks. To start or stop the consistency check on the specified virtual disk, run the following command:

```
racadm storage createvd:<Controller FQDD> -rl {r0|r1|r5|r6|r10|r50|r60}[-wp
{wt|wb|wbf}] [-rp {nra|ra|ara}] [-ss {1k|2k|4k|8k|16k|32k|64k|128k|256k|
512k|1M|2M|4M|8M|16M}]-pdkey:<comma separated PD FQDD> [-dcp {enabled|
disabled|default}] [-name <VD name>] [-size <VD size>{b|k|m|g|t}] [-
T10PIEnable]
```

NOTE: T10PI is no longer supported on PERC9 and PERC10 controllers:

```
racadm storage init:<VD FQDD> -speed {fast|full}
```

```
racadm storage deletevd:<VD FQDD>
```

```
racadm storage encryptvd:<VD FQDD>
```

```
racadm storage createsecuritykey:<Controller FQDD> -key <Key id> -xxx
<passphrase>
```

```
racadm storage modifysecuritykey:<Controller FQDD> -key <Key id>-xxx <old
passphrase> -xxx <new passphrase>
```

```
racadm storage deletesecuritykey:<Controller FQDD>
```

```
racadm storage ccheck:<vdisk fqdd>
```

```
racadm storage cancelcheck:<vdisk fqdd>
```

- To set virtual disk as bootvd and replace physical disk in virtual disk:

```
racadm storage setbootvd:<controller FQDD> -vd <VirtualDisk FQDD >
```

```
racadm storage replacephysicaldisk:<Source PD FQDD > -dstpd <Destination
PD  FQDD>
```

- To convert the physical disk drives and assign or delete a hotspare. To scan physical disks that are connected to a controller and detect problem, run the following command:

```
racadm storage converttononraid:<PD FQDD>
```

```
racadm storage converttoraid:<PD FQDD>
```

NOTE: Convert to RAID or Non RAID is not supported on PERC 10 and BOSS controller cards:

```
-mdtype <metadataType>
```

```
racadm storage hotspare:<Physical Disk FQDD> -assign yes -type dhs -vdkey:
<FQDD of VD>
```

```
racadm storage hotspare:<Physical Disk FQDD> -assign yes -type ghs
```

```
racadm storage hotspare:<Physical Disk FQDD> -assign no
```

```
racadm storage patrolread:<controller FQDD> -state start|stop
```

NOTE: If the `-assign` option is `no`, you cannot add other options. If the `-assign` option is `yes` and if the `-type` option is not present, the global hotspare (ghs) is created by default.

- To reset, clear, and import the storage configuration to the controller, run the following command:

```
racadm storage importconfig:<Controller FQDD>
```

```
racadm storage resetconfig:<Controller FQDD>
```

```
racadm storage clearconfig:<Controller FQDD>
```

- To unlock foreign configuration:

```
racadm storage unlock:<Controller FQDD> -key <Key id> -passwd <passphrase>
```

- To start or stop a blink or identify operation on the specified or PCIeSSD device, run the following command:

```
racadm storage blink:<FQDD>
```

```
racadm storage blink:<PCIeSSD FQDD>
```

```
racadm storage unblink:<FQDD>
```

```
racadm storage unblink:<PCIeSSD FQDD>
```

NOTE: The Start or Stop a Blink feature is not supported for HHHL PCIe SSD devices:

- To force a physical disk online, offline

```
racadm storage forceonline:<PD FQDD>
```

```
racadm storage forceoffline:<PD FQDD>
```

- To prepare the PCIeSSD drive for removal:

```
racadm storage preparetoremove <PCIeSSD FQDD>
```

NOTE: The Prepare to Remove task is not supported for HHHL PCIe SSD devices.

- To perform a cryptographic erase operation on PCIeSSD device, run the following command:

```
racadm storage cryptographicerase:<PCIeSSD FQDD>
```

- To set the encryption mode:

```
racadm storage setencryptionmode:<Controller FQDD> -mode <KEY Management
Mode>
```

- To request iDRAC to rekey all devices:

```
racadm storage rekey:<Controller FQDD>
```

Input

- `-o`—Specifies the optimized version.
- `-p`—Specifies the property name.
- `--refkey`—Specifies the controller or enclosure FQDDs.
- `-name`—Specifies the new name for the virtual disk.
- `-size`—Specifies the new size for the virtual disk. It should be more than the current size.
  - `b`—Specifies the size in bytes
  - `k`—Specifies the size in kilobytes
  - `m`—Specifies the size in megabytes
  - `g`—Specifies the size in gigabytes
  - `t`—Specifies the size in terabytes
- `-rl`—Sets the storage level.
  - `r0`—storage 0-Striping
  - `r1`—storage 1-Mirroring
  - `r5`—storage 5-Striping with Parity
  - `r6`—storage 6-Striping with Extra Parity
  - `r10`—storage 10-Spanned Striping with Mirroring
  - `r50`—storage 50-Spanned Striping with Parity
  - `r60`—storage 60-Spanned Striping with Extra Parity
- `-new_rl`—Specifies the new possible raid level for the virtual disk
  - `r0`—RAID0
  - `r1`—RAID1
  - `r5`—RAID5
  - `r6`—RAID6

  NOTE: This is a mandatory option must provide with RLM operation. Possible raid migrations with disk addition are R0-R1, R0-R5/R6,R1-R0/R5/R6, R5-R0/R6, R6-R0/R5. Possible raid migrations without disk addition are R1-R0, R5-R0, R6-R0/R5.
- `-wp{wt|wb|wbf}`—Sets the write policy to Write Through, Write Back, or Write Back Force
- `-rp {nra|ra|ara}`—Sets the read policy to No Read Ahead, Read Ahead, Adaptive Read Ahead
- `-ss`—Specifies the stripe size to use.
- `-pdkey:<PD FQDD list>`—Specifies the physical disk drive to use in the virtual disk.
- `-dcp`—Sets the Disk Cache Policy in the Virtual Disk.
  - `enabled`—Allows the virtual disk to use the cache.
  - `disabled`—Does not allow the virtual disk to use the cache.
  - `default`—Uses the default cache policy. For SAS drives, use the `disabled` option and for SATA drives, use the `enabled` option by default.
- `-name <VD name>`—Specifies the name of the virtual disk.
- `-size <VD size>`—Specifies the size of each virtual disk.
  - `b`—Specifies the size in bytes
  - `k`—Specifies the size in kilobytes
  - `m`—Specifies the size in megabytes
  - `g`—Specifies the size in gigabytes
  - `t`—Specifies the size in terabytes
- `-sc`—Number of spans in a virtual disk (required for multi-span RAID level)

  NOTE:
  - **For PERC9, if the value of `controller.SupportRAID10UnevenSpans` is `supported`, you can enter only `0` for this option while creating RAID level 10. The created RAID10 virtual disk displays the spandepth as `1` (default).**
  - **For other controllers:**

- **The default value for multi-span RAID levels is 2 and for basic RAID level is 1.**
- **For hybrid RAID levels such as RAID10, RAID50, and RAID60, this option is mandatory.**
- **The value for `-sc` option can be 0 only for RAID10.**

- `-T10PIEnable`—Creates a virtual disk with protection information.
- `-key <Key id>`—Specifies the key id.
- `-passwd <passphrase>`—Specifies the passphrase.
- `-newpasswd <passphrase>`—Specifies the new passphrase.
- `-assign {yes | no}`—Assigns or unassigns the disk as a hotspare.
- `-type { ghs | dhs}`—Assigns a global or dedicated hotspare.
- `-vdkey:<VD FQDD>`—Assigns the dedicated hotspare to the specified virtual disk. This option is required for dedicated hotspare.
- `-state <start|stop>`—`start` value starts a patrol read operation. `stop` value stops a running patrol read operation.

  NOTE: To start the operation, the `Controller.PatrolReadMode` must be in `Manual` mode.
- `-speed`—Specifies the initialization of the Virtual disk.
  - `fast`—Performs fast initialization.
  - `full`—Performs slow initialization.
- `blink: <FQDD>` or `unblink: <FQDD>`—`<FQDD>` can be physical disk drives, virtual disks, or PCIeSSD.
- `<PCIeSSD FQDD>`—Specifies the PCIeSSD FQDD.
- `<PCIeSSD controller|enclosure FQDD>`—Specifies the PCIeSSD controller or enclosure FQDD.
- `preparetoremove`—Specifies the PCIeSSD drive to prepare for removal.

  NOTE: Ensure that ISM is installed and running to perform the `preparetoremove` operation.
- `cryptographicerase`—Specifies the PCIeSSD drive to perform the cryptographic erase operation.-
- `-mdtype { windows | linux}`—Specifies the metadata type for the physical disk conversion to RAID

  NOTE: SWRAID only supports mdtype.
- `-mode`—Specifies the PERC key management type.

Example

Inventory

- To view the help details for get command, run the following command:

```
racadm>>storage help get
racadm storage help get
Storage monitoring and inventory of hardware RAID connected to the system.

Usage :
racadm storage get status
racadm storage help <Object type I/II>
racadm storage get <Object type I>
racadm storage get <Object type I> -current
racadm storage get <Object type I> -pending
racadm storage get <Object type I> -o
racadm storage get <Object type I> -o -p <property names separated by comma>
racadm storage get <Object type I>:<FQDDs of Object type I separated by comma> -p
<property names separated by comma>
racadm storage get <Object type I>:<FQDDs of Object type I separated by comma>
racadm storage get <Object type II> --refkey <reference keys separated by comma>
racadm storage get <Object type II> --refkey <reference keys separated by comma> -o
racadm storage get <Object type II> --refkey <reference keys separated by comma> -o
-p <property names separated by comma>
-------------------------------------------------------------------------------

Valid Options:
Object type I      : controllers, batteries, vdisks, pdisks, fans, emms, tempprobes, psus,
enclosures.
Object type II     : batteries, vdisks, pdisks, fans, emms, psus, tempprobes, enclosures.
-current <optional>: Displays only the current Raid objects from storage.If -pending not
mentioned it will consider as the default option
-pending           : Displays only the Pending Raid Objects from Storage.
-o                 : Displays all the properties of the selected Key or Object.
```

```
-p                : Displays the property names with filter.
FQDD's            : Displays all the properties of the FQDD's Key.
--refkey          : Displays all the reference key of Object type.
help              : Displays each object type help.
NOTE: Maximum Property names can be specified in -p option is = 10.
NOTE: Maximum FQDD's or refkey can be specified is = 3.
-------------------------------------------------------------------------------

Usage Examples :
racadm storage get controllers
racadm storage get psus
racadm storage get controllers -o
racadm storage get controllers -o -current
racadm storage get controllers -o -pending
racadm storage get enclosures -o
racadm storage get controllers -o -p name,status
racadm storage get vdisks -o -p layout,status
racadm storage get controllers:RAID.INTEGRATED.0
racadm storage get emms:EMM.Slot.0:ENCLOSURE.EXTERNAL.0-0:RAID.INTEGRATED.0
racadm storage get controllers:RAID.INTEGRATED.0 -p status
racadm storage get emms:EMM.Slot.0:ENCLOSURE.EXTERNAL.0-0:RAID.INTEGRATED.0 -p status
racadm storage get batteries --refkey RAID.INTEGRATED.0
racadm storage get pdisks --refkey ENCLOSURE.EXTERNAL.0-0:RAID.INTEGRATED.0
racadm storage get batteries --refkey RAID.INTEGRATED.0 -o -p status,state,name
racadm storage get fans --refkey RAID.INTEGRATED.0 -o -p status,speed,name
```

- To rename, expansion and raid level migration of the virtual disks. To rebuild, cancel rebuild and cancel the back-ground initialization.

```
racadm storage renamevd:<VirtualDisk FQDD > -name <new_vd_name>
```

```
racadm storage capacityexpansion:<VirtualDisk FQDD > -size <new size VD> -pdkey
<PhysicalDisk FQDDs>
```

```
racadm storage raidlevelmigration:<VirtualDisk FQDD > -new_rl <raid_level> -
pdkey:<pdisk_fqdd separated by commas>
```

```
racadm storage rebuild:<PD FQDD>
```

```
racadm storage cancelrebuild:<PD FQDD>
```

```
racadm storage cancelbgi:<VD FQDD>
```

- To generate and view information about the inventory of controllers, virtual disks, storage enclosures, and physical disk drives.
  - To generate and view information about the inventory of storage root node.

    This command retrieves the status of the inventory for storage root node.

    ```
    racadm storage get status
    raid Root Node Status : Ok
    ```

    - To generate and view information about the inventory of controllers connected to the server.

      NOTE: If you set the NVMe mode to Non-Raid, then S140/S150 RollupStatus is displayed as Unknown.

      ```
      racadm storage get controllers
      RAID.Integrated.1-1
      ```

      The following command is an optimized version and displays the full controller objects along with their keys:

      ```
      racadm storage get controllers -o
      RAID.Slot.4-1
         Status                          = Ok
         DeviceDescription               = RAID Controller in Slot 4
         RollupStatus                    = Ok
         Name                            = PERC H740P Adapter  (PCI Slot 4)
         PciSlot                         = 4
         FirmwareVersion                 = 50.5.1-1733
      ```

```
   RebuildRate                       = 30
   BgiRate                           = 30
   CheckConsistencyRate              = 30
   ReconstructRate                   = 30
   PatrolReadRate                    = 30
   PatrolReadMode                    = Automatic
   PatrolReadState                   = Stopped
   CheckConsistencyMode              = Normal
   LoadBalanceSetting                = Auto
   CopybackMode                      = ON
   PreservedCache                    = Not Present
   CacheMemorySize                   = 8192 MB
   PersistHotspare                   = Disabled
   KeyID                             = null
   SpindownUnconfiguredDrives        = Disabled
   SpindownHotspare                  = Disabled
   Timeintervalforspindown           = 30 (Minutes)
   SecurityStatus                    = Security Key Assigned
   EncryptionMode                    = Security Enterprise Key Manager
   SasAddress                        = 0x5D09466073045100
   PciDeviceId                       = 0x16
   PciSubdeviceId                    = 0x1fcb
   PciVendorId                       = 0x1000
   PciSubvendorId                    = 0x1028
   PciBus                            = 0x0
   PciDevice                         = 0x0
   PciFunction                       = 0x0
   BusWidth                          = Other
   SlotLength                        = Other
   SlotType                          = Other
   MaxCapableSpeed                   = 12.0 Gb/s
   LearnMode                         = Not supported
   T10PICapability                   = Not Capable
   SupportRAID10UnevenSpans          = Supported
   SupportEnhancedAutoForeignImport  = Supported
   EnhancedAutoImportForeignConfig   = Disabled
   SupportControllerBootMode         = Supported
   ControllerBootMode                = Continue Boot On Error
   RealtimeConfigurationCapability   = Capable
   RaidMode                          = None
   SharedSlotAssignmentAllowed       = Not Applicable
   bootVD                            = Disk.Virtual.0:RAID.Slot.4-1
   CurrentControllerMode             = RAID
   SupportEnhancedHBA                = Supported
```

The following command displays the filtered property values for all returned controller objects:

```
racadm storage get controllers -o -p Name
RAID.Integrated.1-1
Name = PERC H710P Adapter (Embedded)
```

The following examples show the pending operation when used with `storage get <object>` commands:

To list storage objects without displaying the properties:

- This operation displays `vdisk`, which has pending operation:

  ```
  racadm storage get vdisks -pending
  DISK.Virtual.267386880:RAID.Slot.5-1
  ```

- This operation displays controllers, which have pending operations:

  ```
  racadm storage get controllers -pending
  RAID.Integrated.1-1
  ```

- This operation displays `pdisk`, which has pending operation:

  ```
  racadm storage get pdisks -pending
  Disk.Bay.20:Enclosure.Internal.0-1:RAID.Integrated.1-1
  ```

- This operation displays enclosures, which have pending operations:

```
racadm storage get enclosures -pending
Enclosure.Internal.0-1:RAID.Integrated.1-1
```

  Changing the attribute by using `racadm set storage` or storage configuration command displays the storage object in the `-pending` command output. If there are no pending objects, the following error message is displayed:

```
racadm storage get pdisks -pending
ERROR: STOR0103 : No physical disks are displayed.
Check if the server has power, physical disks are available, and physical disks
are connected to the enclosure or backplane.
```

The following examples show the pending operation while listing the properties:

By default, if there is no change in properties, the `-pending` command displays the current value. If the property has any pending objects, the `-pending` command displays the pending value.

- This operation displays the current state of `pdisk`, which is in `Ready` state:

```
/admin1-> racadm storage get pdisks -o -p state
Disk.Bay.4:Enclosure.Internal.0-1:RAID.Integrated.1-1
   State                            = Ready
```

- This operation displays state of a `pdisk` on which `createvd` operation is pending:

```
/admin1-> racadm storage get pdisks -o -p state -pending
Disk.Bay.4:Enclosure.Internal.0-1:RAID.Integrated.1-1
```

The following command displays the output for H740P adapter controller objects along with their keys:

```
racadm storage get controllers -o
   RAID.Slot.3-1
   Status                           = Ok
   DeviceDescription                = RAID Controller in Slot 3
   RollupStatus                     = Ok
   Name                             = PERC H740P Adapter  (PCI Slot 3)
   PciSlot                          = 3
   FirmwareVersion                  = 50.5.1-2571
   DriverVersion                    = Information Not Available
   RebuildRate                      = 33
   BgiRate                          = 44
   CheckConsistencyRate             = 22
   ReconstructRate                  = 98
   PatrolReadRate                   = 30
   PatrolReadMode                   = Automatic
   PatrolReadState                  = Stopped
   CheckConsistencyMode             = Normal
   LoadBalanceSetting               = Auto
   CopybackMode                     = ON
   PreservedCache                   = Not Present
   CacheMemorySize                  = 8192 MB
   PersistHotspare                  = Disabled
   KeyID                            =
1D509463F308D96D00C4BB14B1C0F51F860176C1E275264C73B62D7E96DD3007
   SpindownUnconfiguredDrives       = Disabled
   SpindownHotspare                 = Disabled
   Timeintervalforspindown          = 30 (Minutes)
   SecurityStatus                   = Security Key Assigned
   EncryptionMode                   = Secure Enterprise Key Manager
   EncryptionCapability             = Local Key Management and Secure Enterprise Key
Manager Capable
   SasAddress                       = 0x5D0946600B5E9F00
   PciDeviceId                      = 0x16
   PciSubdeviceId                   = 0x1fcb
   PciVendorId                      = 0x1000
   PciSubvendorId                   = 0x1028
   PciBus                           = 0x33
   PciDevice                        = 0x0
   PciFunction                      = 0x0
   BusWidth                         = 16x or x16
```

```
SlotLength                          = Long Length
SlotType                            = PCI Express Gen3
MaxCapableSpeed                     = 12.0 Gb/s
LearnMode                           = Not supported
T10PICapability                     = Not Capable
SupportRAID10UnevenSpans            = Supported
SupportEnhancedAutoForeignImport    = Supported
EnhancedAutoImportForeignConfig     = Enabled
SupportControllerBootMode           = Not Supported
RealtimeConfigurationCapability     = Capable
RaidMode                            = None
SharedSlotAssignmentAllowed         = Not Applicable
bootVD                              = Disk.Virtual.0:RAID.Slot.3-1
CurrentControllerMode               = RAID
SupportEnhancedHBA                  = Supported
```

- To generate and view information about the inventory of batteries that are connected to the controller, run the following command:

```
racadm storage get batteries
```

The following command is an optimized version and displays the batteries along with their keys:

```
racadm storage get batteries -o
Battery.Integrated.1:RAID.Integrated.1-1
Name                              = Battery
DeviceDescription                 = Battery on Integrated raid Controller 1
Status                            = Ok
State                             = Ready
```

The following command displays the filtered property values for all battery objects:

```
racadm storage get batteries -o -p Name
Battery.Integrated.1:RAID.Integrated.1-1
Name  = Battery
```

The following command displays all battery keys that are connected to the controllers:

```
racadm storage get batteries --refkey RAID.Integrated.1-1
Battery.Integrated.1:RAID.Integrated.1-1
```

The following command is an optimized and filtered version:

```
racadm storage get batteries --refkey RAID.Integrated.1-1 -o -p Name
Battery.Integrated.1:RAID.Integrated.1-1
Name                              = Battery
```

- To generate and view information about the inventory of virtual disks that are connected to the controller, run the following command:

```
racadm storage get vdisks
Disk.Virtual.0:RAID.Integrated.1-1
```

The following command displays all virtual disk keys that are connected to the controllers:

```
racadm storage get vdisks --refkey RAID.Integrated.1-1
Disk.Virtual.0:RAID.Integrated.1-1
```

The following command is an optimized and filtered version:

```
racadm storage get vdisks -o -p DeviceDescription,OperationalState
Disk.Virtual.0:RAID.Integrated.1-1
DeviceDescription        = Virtual Disk 0 on Integrated raid Controller 1
OperationalState         = Not applicable
```

- To generate and view information about the inventory of virtual disks, run the following command:

```
racadm storage get vdisks -o
Disk.Virtual.2:RAID.Integrated.1-1
```

Table 95. Details of storage get vdisks

Status	Ok
DeviceDescription	Virtual Disk 2 on Integrated RAID Controller 1
Name	OS
RollupStatus	Ok
State	Online
OperationalState	Not applicable
Layout	Raid-0
Size	278.88 GB
SpanDepth	1
AvailableProtocols	SAS
MediaType	HDD
ReadPolicy	Read Ahead
WritePolicy	Write Back
StripeSize	64K
DiskCachePolicy	Default
BadBlocksFound	NO
Secured	NO
RemainingRedundancy	0
EnhancedCache	Not Applicable
T10PIStatus	Disabled
BlockSizeInBytes	512

- To generate and view information about the inventory of storage enclosures that are connected to the connector.

  This command displays all enclosure objects for the connector FQDD.

```
racadm storage get enclosures -o
Enclosure.Internal.0-1:RAID.Integrated.1-1
```

Table 96. Details of storage get enclosure

Status	Ok
State	Ready
DeviceDescription	Backplane 1 on Connector 0 of Integrated RAID Controller 1
RollupStatus	Ok
Name	BP13G+EXP 0:1
BayId	1
FirmwareVersion	0.23
SasAddress	0x500056B31234ABFD
SlotCount	24

The following command displays all enclosure keys that are connected to the connectors:

```
racadm storage get enclosures --refkey RAID.Integrated.1-1
Enclosure.Internal.0-1:RAID.Integrated.1-1
```

The following command is an optimized and filtered version:

```
racadm storage get enclosures --refkey RAID.Integrated.1-1 -o -p Name
Enclosure.Internal.0-1:RAID.Integrated.1-1
Name = BP12G+EXP 0:1
```

- To generate and view information about the inventory of physical disk drives connected to the enclosure or backplanes, run the following command:

```
racadm storage get pdisks
Disk.Bay.0:Enclosure.Internal.0-1:RAID.Integrated.1-1
```

The following command is an optimized version and displays the full controller objects along with their keys:

```
racadm storage get pdisks -o
Disk.Bay.0:Enclosure.Internal.0-1:RAID.Slot.4-1
   Status                          = Ok
   DeviceDescription               = Disk 0 in Backplane 1 of RAID Controller in Slot 4
   RollupStatus                    = Ok
   Name                            = Physical Disk 0:1:0
   State                           = Online
   OperationState                  = Not Applicable
   PowerStatus                     = Spun-Up
   Size                            = 1117.250 GB
   FailurePredicted                = NO
   RemainingRatedWriteEndurance    = Not Applicable
   SecurityStatus                  = Not Capable
   BusProtocol                     = SAS
   MediaType                       = HDD
   UsedRaidDiskSpace               = 200.001 GB
   AvailableRaidDiskSpace          = 917.250 GB
   Hotspare                        = NO
   Manufacturer                    = SEAGATE
   ProductId                       = ST1200MM0099
   Revision                        = ST31
   SerialNumber                    = WFK1BNX3
   PartNumber                      = CN0G2G54SGW0087A01RHA00
   NegotiatedSpeed                 = 12.0 Gb/s
   ManufacturedDay                 = 5
   ManufacturedWeek                = 28
   ManufacturedYear                = 2018
   ForeignKeyIdentifier            = null
   SasAddress                      = 0x5000C500B8ED7081
   FormFactor                      = 2.5 Inch
   RaidNominalMediumRotationRate   = 10000
   T10PICapability                 = Not Capable
   BlockSizeInBytes                = 512
   MaxCapableSpeed                 = 12 Gb/s
   RaidType                        = None
   SystemEraseCapability           = SecureErasePD
   SelfEncryptingDriveCapability   = Not Capable
   EncryptionCapability            = Not Capable
   CryptographicEraseCapability    = Capable
```

The following command displays the filtered property values for all returned controller objects:

```
racadm storage get pdisks -o -p State
Disk.Bay.0:Enclosure.Internal.0-1:RAID.Integrated.1-1
State = Online
```

The following command displays all physical disk drive keys that are connected to the enclosures:

```
racadm storage get pdisks --refkey RAID.Integrated.1-1
Disk.Bay.0:Enclosure.Internal.0-1:RAID.Integrated.1-1
```

The following command is an optimized version and displays all disk objects for the enclosure FQDD:

```
racadm storage get pdisks -o
Disk.Bay.0:Enclosure.Internal.0-1:RAID.Slot.4-1
   Status                          = Ok
   DeviceDescription               = Disk 0 in Backplane 1 of RAID Controller in Slot 4
   RollupStatus                    = Ok
   Name                            = Physical Disk 0:1:0
   State                           = Online
   OperationState                  = Not Applicable
   PowerStatus                     = Spun-Up
   Size                            = 1117.250 GB
   FailurePredicted                = NO
   RemainingRatedWriteEndurance    = Not Applicable
   SecurityStatus                  = Not Capable
   BusProtocol                     = SAS
   MediaType                       = HDD
   UsedRaidDiskSpace               = 200.001 GB
   AvailableRaidDiskSpace          = 917.250 GB
   Hotspare                        = NO
   Manufacturer                    = SEAGATE
   ProductId                       = ST1200MM0099
   Revision                        = ST31
   SerialNumber                    = WFK1BNX3
   PartNumber                      = CN0G2G54SGW0087A01RHA00
   NegotiatedSpeed                 = 12.0 Gb/s
   ManufacturedDay                 = 5
   ManufacturedWeek                = 28
   ManufacturedYear                = 2018
   ForeignKeyIdentifier            = null
   SasAddress                      = 0x5000C500B8ED7081
   FormFactor                      = 2.5 Inch
   RaidNominalMediumRotationRate   = 10000
   T10PICapability                 = Not Capable
   BlockSizeInBytes                = 512
   MaxCapableSpeed                 = 12 Gb/s
   RaidType                        = None
   SystemEraseCapability           = SecureErasePD
   SelfEncryptingDriveCapability   = Not Capable
   EncryptionCapability            = Not Capable
   CryptographicEraseCapability    = Capable
```

The following command is an optimized and filtered version:

```
racadm storage get pdisks --refkey Enclosure.Internal.0-1:RAID.Integrated.1-1 -o -p State
Disk.Bay.0:Enclosure.Internal.0-1:RAID.Integrated.1-1
State = Online
```

- To generate and view information about the inventory of fans that are connected to the enclosure.

  The following command displays all the fan keys that are connected to the enclosures:

  ```
  racadm storage get fans --refkey <enclosure FQDDs separated
  by comma>
  ```

  The following command displays all the fan objects for the enclosure FQDD:

  ```
  racadm storage get fans --refkey <enclosure FQDDs separated
  by comma > -o
  ```

  ```
  racadm storage get fans --refkey <enclosure FQDDs separated
  by comma> -o -p <property names separated by comma>
  ```

- To generate and view information about the inventory of EMMs connected to the enclosure.

  The following command returns all the EMM keys that are connected to the enclosures:

  ```
  racadm storage get emms -refkey <enclosure FQDDs separated
  by comma enclosure FQDDs separated
  by comma>
  ```

The following command is an optimized version and displays all the EMM objects for the enclosure FQDD:

```
racadm storage get emms --refkey <enclosure FQDDs separated
by comma> -o
```

The following command is an optimized and filtered version:

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

- To generate and view information about the inventory of PSU connected to the enclosure.

  The following command displays all the PSUs connected to the enclosures:

  ```
  racadm storage get psus --refkey <enclosure FQDDs separated
  by comma>
  ```

  The following command is an optimized version and displays all the PSUs objects for the enclosure FQDD:

  ```
  racadm storage get psus --refkey <enclosure FQDDs separated
  by comma > -o
  ```

  The following command is an optimized and filtered version:

  ```
  racadm storage get psus --refkey <enclosure FQDDs separated
  by comma> -o -p <property names separated by comma>
  ```

- To get the list of enclosures and properties of the PCIeSSD enclosure.
  - The following command provides the list of enclosures:

    ```
    racadm storage get enclosures
    Enclosure.Internal.0-1:RAID.Integrated.1-1\
    Enclosure.Internal.0-1:PCIeExtender.Slot.3
    ```

  - The following command provides the properties of the specified PCIeSSD enclosure:

    ```
    racadm storage get enclosures:Enclosure.Internal.0-1:PCIeExtender.Slot.3
    Enclosure.Internal.0-1:PCIeExtender.Slot.3
    RollupStatus = Ok
    DeviceDescription = Enclosure.Internal.0-1:PCIeExtender.Slot.3
    Name = PCIe SSD BP 1
    SlotCount = 4
    FirmwareVersion = 0.80
    PcieSSDBusId = 182
    PcieSSDDeviceId = 0
    PcieSSDFunctionId = 0
    ```

  - To get the list of physical disks and properties of the specified PCIeSSD physical disk.

    The following command provides the list of physical disks:

    ```
    racadm storage get pdisks
    Disk.Bay.0:Enclosure.Internal.0-1:RAID.Integrated.1-1
    Disk.Bay.1:Enclosure.Internal.0-1:RAID.Integrated.1-1
    Disk.Bay.2:Enclosure.Internal.0-1:RAID.Integrated.1-1
    Disk.Bay.3:Enclosure.Internal.0-1:RAID.Integrated.1-1
    Disk.Bay.4:Enclosure.Internal.0-1:RAID.Integrated.1-1
    Disk.Bay.5:Enclosure.Internal.0-1:RAID.Integrated.1-1
    Disk.Bay.8:Enclosure.Internal.0-1:PCIeExtender.Slot.3
    Disk.Bay.6:Enclosure.Internal.0-1:PCIeExtender.Slot.3
    Disk.Bay.7:Enclosure.Internal.0-1:PCIeExtender.Slot.3
    Disk.Bay.9:Enclosure.Internal.0-1:PCIeExtender.Slot.3
    ```

    The following command provides the properties of the specified PCIeSSD physical disk:

    ```
    racadm storage get pdisks:Disk.Bay.8:Enclosure.Internal.0-1:PCIeExtender.Slot.3
    Disk.Bay.8:Enclosure.Internal.0-1:PCIeExtender.Slot.3
    Status = Ok
    DeviceDescription = PCIe Solid-State Drive in Slot 8 in Bay 1
    Name = Physical Device 8
    ```

```
State = Ready
Size = 745.21 GB
BusProtocol = PCIe
MediaType = SSD
Model = SAMSUNG MZWEI800HAGM 000D3
ProductId = a820
SerialNumber = S1J1NYAD90019
DeviceProtocol = NVMe1.0
Manufacturer = SAMSUNG
PCIeNegotiatedLinkWidth = x4
PCIeCapableLinkWidth = x4
MaxCapableSpeed = 8 GT/s
NegotiatedSpeed = 8 GT/s
FormFactor = 2.5 Inch
Revision = IPM0ED35SAM SAMSUNG MZWEI800HAGM 000D3
RemainingRatedWriteEndurance = 100 %
FailurePredicted = NO
```

To get the list of controllers and properties of the PCIeSSD controller:

The following command provides the list of controllers:

```
racadm storage get controllers
RAID.Integrated.1-1
PCIeExtender.Slot.3
```

The following command provides the properties of the specified PCIeSSD controller:

```
racadm storage get controllers:PCIeExtender.Slot.3
PCIeExtender.Slot.3
RollupStatus = Ok
DeviceDescription = PCIe Extender in PCIe Slot 3
Status = Ok
Name = PCIeExtender 3 (PCI Slot 3)
```

Configuration

- To view the help details for a configuration command, run the following command:

```
admin1-> racadm storage help createvd
Storage configuration of hardware RAID connected to the system.

Usage:
racadm storage createvd:<Controller FQDD> -rl {r0|r1|r5|r6|r10|r50|r60}[-wp {wt|wb|wbf}] [-
rp {nra|ra|ara}]
[-ss {1k|2k|4k|8k|16k|32k|64k|128k|256k|512k|1M|2M|4M|8M|16M}]
-pdkey:<comma separated PD FQDD> [-dcp {enabled|disabled|default}]
[-name <VD name>] [-size <VD size>{b|k|m|g|t}] [-T10PIEnable]
--------------------------------------------------------------------------------

Options :
-rl                    : Set the RAID Level
 r0                  : RAID 0  - Striping
 r1                  : RAID 1  - Mirroring
 r5                  : RAID 5  - Striping with Parity
 r6                  : RAID 6  - Striping with Extra Parity
 r10                 : RAID 10 - Spanned Striping with Mirroring
 r50                 : RAID 50 - Spanned Striping with Parity
 r60                 : RAID 60 - Spanned Striping with Extra Parity
 -wp {wt | wb | wbf}    : Set the write policy to Write Through or Write Back or Write
Back Force
 -rp {nra|ra|ara}       : Set the read policy to No Read Ahead, Read Ahead, Adaptive Read
Ahead
 -ss                    : Specify the stripe size to use
 -pdkey:<PD FQDD list>  : The PDs to use in the VD.
 -dcp                   : Set the Disk Cache Policy in the VD
 enabled           : Enabled - Allow the disk to use it's cache
 disabled          : Disabled - Disallow the disk from using it's cache
 default           : Default - Use the default cache policy.
 SAS Drives  - Use Disabled by Default
 SATA Drives - Use Enabled by Default
 -name <VD name>        : The name to give the VD
 -size <VD size>        : The size of the VD
```

```
 b                : Specify the size in bytes
 k                : Specify the size in kilobytes
 m                : Specify the size in megabytes
 g                : Specify the size in gigabytes
 t                : Specify the size in terabytes
 -sc               : Spandepth: Number of spans in a virtual disk

Note:
 - This option is mandatory for hybrid raid level like RAID 10, RAID50 and RAID60.
 - The default value is one for basic RAID levels.
 - If RAID10 Uneven Span is Supported then for RAID10:
 -    -sc option will be optional.
 -    Will allow only 0 value for this option.
 -T10PIEnable                : To create a VD with PI
-------------------------------------------------------------------------------
Description :
Create a VD.
-------------------------------------------------------------------------------

Examples :
racadm storage createvd:RAID.Integrated.1-1 -rl r0 -
pdkey:Disk.Bay.0:Enclosure.Internal.0-0:RAID.Integrated.1-1
```

- To create, delete, and secure the virtual disks.
  - The following command creates a virtual disk:

    ```
    racadm storage createvd:RAID.Integrated.1-1 -rl r0 -
    pdkey:Disk.Bay.0:Enclosure.Internal.0-0:RAID.Integrated.1-1
    ```

  - The following command starts an initialization operation on a specified virtual disk:

    ```
    racadm storage init:Disk.Virtual.0:RAID.Integrated.1-1 -speed fast
    ```

  - The following command deletes the specified virtual disk:

    ```
    racadm storage deletevd:Disk.Virtual.0:RAID.Integrated.1-1
    ```

  - The following command encrypts the specified virtual disk:

    ```
    racadm storage encryptvd:Disk.Virtual.0:RAID.Integrated.1-1
    ```

    NOTE: Virtual disk must be created with SED:

  - The following command assigns Local Key Management (LKM) security key for controller:

    ```
    racadm storage createsecuritykey:RAID.Integrated.1-1 -key <Key id> -xxx <passphrase>
    ```

  - The following command modifies Local Key Management (LKM) security key for controller:

    ```
    racadm storage modifysecuritykey:RAID.Integrated.1-1 -key <Key id> -oldpasswd
    <oldpassphrase> -newpasswd <newpassphrase>
    ```

  - The following command deletes Local Key Management (LKM) security key for controller:

    ```
    racadm storage deletesecuritykey:RAID.Integrated.1-1
    ```

- To convert the physical disk drive and assign hotspare.
  - The following command converts the specified nonstorage physical disk drive to a storage capable physical disk drive:

    ```
    racadm storage converttoraid:Disk.Bay.0:Enclosure.Internal.0-0:RAID.Integrated.1-1
    ```

  - The following command converts the specified physical disk drive to a nonstorage physical disk drive:

    ```
    racadm storage converttononraid:Disk.Bay.0:Enclosure.Internal.0-0:RAID.Integrated.1-1
    ```

- The following command assigns or unassigns a global or dedicated Hot spare:

```
racadm storage hotspare:Disk.Bay.0:Enclosure.Internal.0-0:RAID.Integrated.1-1 -assign no
```

```
racadm storage hotspare:Disk.Bay.0:Enclosure.Internal.0-0:RAID.Integrated.1-1 -assign
yes -type ghs
```

```
racadm storage hotspare:Disk.Bay.0:Enclosure.Internal.0-0:RAID.Integrated.1-1 -assign
yes -type dhs -vdkey:Disk.Virtual.0:RAID.Integrated.1-1
```

- The following command converts the specified nonstorage physical disk to a storage capable physical disk with windows meta data

```
racadm storage converttoraid:Disk.Bay.0:Enclosure.Internal.0-0:RAID.Integrated.1-1 -
mdtype windows
```

- To reset, clear, and import the storage configuration to the controller.
  - The following command imports the current foreign configuration from the controller:

```
racadm storage importconfig:RAID.Integrated.1-1
```

  - The following command deletes all virtual disks and unassigns hot spare from the associated controller:

```
racadm storage resetconfig:RAID.Integrated.1-1
```

  - The following command clears the current foreign configuration from the controller:

```
racadm storage clearconfig:RAID.Integrated.1-1
```

NOTE: After a `resetconfig` or `clearconfig` operation, the data cannot be reversed.

- To blink or unblink the PCIeSSD device.
  - The following command blinks the specified PCIeSSD device:

```
racadm storage blink:Disk.Bay.8:Enclosure.Internal.0-1:PCIeExtender.Slot.3
STOR095 : Storage operation is successfully completed.
```

  - The following command unblinks the specified PCIeSSD device:

```
racadm storage unblink:Disk.Bay.8:Enclosure.Internal.0-1:PCIeExtender.Slot.3
STOR095 : Storage operation is successfully completed.
```

- To prepare the specified PCIeSSD device for removal, run the following command:

```
racadm storage preparetoremove: Disk.Bay.8:Enclosure.Internal.0-1:PCIeExtender.Slot.3
STOR089 : Successfully accepted the storage configuration operation.
To apply the configuration operation, create a configuration job with --realtime option.
To create the required commit jobs, run the jobqueue command.
For more information about the jobqueue command, enter the RACADM command "racadm help
jobqueue”
```

- To perform a cryptographic erase operation on the specified PCIeSSD device, run the following command:

```
racadm storage secureerase: Disk.Bay.8:Enclosure.Internal.0-1:PCIeExtender.Slot.3
RAC1040 : Successfully accepted the storage configuration operation.
To apply the configuration operation, create a configuration job, and then restart the
server.
To create the required commit and reboot jobs, run the jobqueue command.
For more information about the jobqueue command, enter the RACADM command "racadm help
jobqueue”
```

- To perform a cryptographic erase operation on SED (self-encrypting drive) device, run the following command:

```
racadm storage cryptographicerase:<SED FQDD>
```

- To request iDRAC to rekey only a specific storage controller

```
racadm storage rekey:RAID.Integrated.1-1
```

SupportAssist

Table 97. Details of SupportAssist

Description

Allows you to perform SupportAssist operations such as:

- `collect` : Collects the SupportAssist data and exports to local share, or remote share, or Dell site depending on the parameters given in the command. You can specify the type of the logs to be in the collect command. To run this command, user must accept the End User License Agreement (EULA).
- `register` : Allows registration of SupportAssist to enable related features.
- `exportlastcollection` : Exports the last collected SupportAssist data to the share which is mentioned in the command or to the default share. Default share can be configured using the SupportAssist attributes.
- `accepteula` : Accepts the End User License Agreement (EULA).
- `geteulastatus`: Provides the status of the End User License Agreement (EULA).
- `uploadlastcollection` : Upload last collection to Dell SupportAssist server.
- `exposeismminstallertohostos`: Exposes iSM installer to host OS, so that user can install the iSM from host side.
- `autocollectscheduler`: Provides options to create view, and clear the time-based automatic collections. User must perform registration for this feature.

  NOTE: All the commands except `accepteula`,`geteulastatus` , and `autocollectscheduler` will create job ID to track the progress of the operation.

Synopsis

- To perform SupportAssist operation by specifying the type of the operation.

```
racadm supportassist <support assist command type>
```

- To collect the data and store it in the iDRAC.

```
racadm supportassist collect -t <logtype>
```

- To collect the data and export to network share

```
racadm supportassist collect -t <logtype>  -l <CIFS/NFS/TFTP/FTP/HTTP/HTTPS
share> -u <username> -p <password>
```

- To collect the data and upload to Dell SupportAssist server.

```
racadm supportassist collect -t <logtype> -upload
```

- To collect the data and export to local share. This is only allowed from remote and local RACADM.

```
racadm supportassist collect -t <logtype>  -f <filename>
```

- To collect the data and export to remote share and to Dell SupportAssist server.

```
racadm supportassist collect -t <logtype>  -l <CIFS or NFS share location> -
u <username> -p <password> --upload
```

- To Export the last collected SupportAssist data to a remote share.

```
racadm supportassist exportlastcollection -l <<CIFS/NFS/TFTP/FTP/HTTP/HTTPS
share> -u myuser -p mypass
```

- To export the last collected SupportAssist data to the default network share.

```
racadm supportassist exportlastcollection
```

- To accept End User License Agreement (EULA)

```
racadm supportassist accepteula
```

- To check End User License Agreement (EULA) status

```
racadm supportassist geteulastatus
```

- To register iDRAC for SupportAssist features

```
racadm supportassist register -pfname <primary  first name> -plname
<primary last name> -pmnumber <primary number>
-panumber <primary alternate number> -pmailid <primary email id> -sfname
<secondary first name> -slname <secondary last name> -smnumber
<secondary number> -sanumber  <secondary alternate number>-smailid
<secondary email id> -company <company name> -street1 <street1 name>
-street2 <street2 name> -city <city name> -state <state name> -country
<country name> -zip <zip or postal code>
```

- To upload last collection to Dell SupportAssist server.

```
racadm supportassist uploadlastcollection
```

- To expose iSM installer to host operating system.

```
racadm supportassist exposeismsinstallertohostos
```

- To schedule auto collection of SupportAssist data weekly.

```
racadm supportassist autocollectscheduler create -time <time>  -dow
<DayofWeek> -rp <repeat>
```

- To schedule auto collection of SupportAssist data monthly.

```
racadm supportassist autocollectscheduler create -time <time> -dom
<DayOfMonth> -rp <repeat>
```

```
racadm supportassist autocollectscheduler create -time <time> -wom
<WeekOfMonth> -dow <DayofWeek> -rp <repeat>
```

- To schedule auto collection of SupportAssist data quarterly.

```
racadm supportassist autocollectscheduler create -time <time> -wom
<WeekOfMonth> -dow <DayofWeek> -rp <repeat>
```

- To view the auto collection data

```
racadm supportassist autocollectscheduler view
```

- To clear the auto collection data

```
racadm supportassist autocollectscheduler clear
```

Input

- `-t`—Specifies the types of logs to be included in the export data.
  - `-sysinfo`—System information
  - `-osAppAll`—OS and Application data
  - `-ttylog`—Storage log information
  - `-Debug`—iDRAC debug logs
- `-l`—Specifies the network share location.
- `-u`—Specifies the user name of the remote share.
- `-p`—Specifies the password of the remote share.
- `-f`—Specifies the target filename of the exported data.

  NOTE: The filename must have .zip as the extension.
- `-pfname`—Specifies the primary user's first name for the registration.
- `-plname`—Specifies the primary user's last name for the registration.
- `-pmnumber`—Specifies the primary user' s number.
- `-panumber`—Specifies the primary user' s alternative number.
- `-pmailid`—Specifies the primary user' s email address.
- `-sfname`—Specifies the secondary user' s first name.
- `-slname`—Specifies the secondary user' s last name.

- `-smnumber`—Specifies the secondary user' s number.
- `-sanumber`—Specifies the secondary user' s alternate number.
- `-smailid`—Specifies the secondary user' s email address.
- `-company`—Specifies the company name.
- `-street1`—Specifies the street address of the company.
- `-street2`—Specifies the secondary street address of the company.
- `-city`—Specifies the name of the city.
- `-state`—Specifies the name of the state.
- `-country`—Specifies the name of the country.
- `-zip`—Specifies the zip or postal code.
- `-time`—Specifies the time to schedule a SupportAssist collection in HH:MM 12-hour format.
- `-dom`—Specifies the day of the month to schedule a SupportAssist collection. Valid values are 1-28, L(Last day) or '*' (default - any day). If -dom option is included in the command, then -wom and -dow options should not be included.
- `-wom`—Specifies the week of the month to schedule a SupportAssist collection. Valid values are 1-4, L(Last week) or '*' (default - any week). If -wom option is included in the command, then only -dow option should be included. -dom should not be included.
- `-dow` — Specifies the day of the week to schedule a SupportAssist collection. Valid values sunday, monday,...saturday '*' (default - any day).
- `-rp` — Specifies the repeat parameter weekly, or monthly, or quarterly. Weekly is allowed only with dow parameter. Monthly/quarterly is allowed either with dom or dow and wom together.

Example

- To collect the system information data.

```
racadm supportassist collect
```

- To collect the filtered data.

```
racadm supportassist collect --filter
```

- To collect the data and export to an FTP share.

```
racadm supportassist collect -t Debug -l ftp://192.168.10.24/share -u myuser -p mypass
```

- To collect the data and export to a TFTP share.

```
racadm supportassist collect -t Debug -l tftp://192.168.10.24/share
```

- To collect the data and export to an CIFS share.

```
racadm supportassist collect -t sysinfo -l //192.168.10.24/share -u myuser -p mypasss
```

- To collect the data and export to a HTTP share.

```
racadm supportassist collect -t TTYLog -l http://192.168.10.24/share -u myuser -p mypass
```

- To collect the data and export to an HTTPS share.

```
racadm supportassist collect -t Debug -l https://192.168.10.24/share -u myuser -p mypass
```

- To export the last collected SupportAssist data to an FTP share

```
racadm supportassist exportlastcollection -l ftp://192.168.10.24/share -u myuser -p mypass
```

- To collect the data and export to an NFS network share:

```
racadm supportassist collect -l 10.94.161.103:/supportassist_share
```

- To collect the data and upload to the Dell SupportAssist server.

```
 racadm supportassist collect --upload
```

- To collect the data and export to a local share. This is allowed only from a remote or a local RACADM.

```
racadm supportassist collect -f tsr.zip
```

- To collect the data and export to a remote share and to the Dell SupportAssist server.

```
racadm supportassist collect -t Debug -l //192.168.10.24/share -u myuser -p mypass --
upload
```

- To export the last collected SupportAssist data to a CIFS share

```
racadm supportassist exportlastcollection -l //192.168.10.24/share -u myuser -p mypass
```

- To export the collected SupportAssist data to the default network share.

```
racadm supportassist exportlastcollection
```

- To accept the End User License Agreement (EULA).

```
racadm supportassist accepteula
```

- To check the End User License Agreement (EULA) status.

```
racadm supportassist geteulastatus
```

- To register the iDRAC for SupportAssist features.

```
racadm supportassist register -pfname abc -plname xyz -pmnumber 1234567890 -panumber
1234567899 -pmailid abc_xyz@Dell.com -sfname abc -slname xyz -smnumber 1234567890 -
sanumber 7777799999 -smailid abc_xyz@dell.com -company dell -street1
xyztechpark -street2 -city bangalore -state karnataka -country india -zip
123456
```

- To upload the last collection to the Dell SupportAssist server.

```
racadm supportassist uploadlastcollection
```

- To expose the iSM installer to the host operating system for the iSM installation.

```
racadm supportassist exposeismInstallertohostos
```

- To schedule auto collection of SupportAssist data weekly.

```
racadm supportassist autocollectscheduler create -time 4:05am -dow sunday -rp weekly
```

- To schedule auto collection of the SupportAssist data monthly.

```
racadm supportassist autocollectscheduler create -time 7:55pm -dom 20 -rp monthly
```

- To schedule auto collection of the SupportAssist data quarterly.

```
racadm supportassist autocollectscheduler create -time 7:55am -wom 2 -dow monday -rp
quarterly
```

- To view the auto collection schedule.

```
racadm supportassist autocollectscheduler view
```

- To clear the auto collection schedule.

```
racadm supportassist autocollectscheduler clear
```

swinventory

Table 98. Details of swinventory

Description	Displays the list of software objects and associated properties that are installed on a server.

NOTE: Lifecycle Controller and CSIOR should not be enabled to run this subcommand.

Synopsis

```
racadm swinventory
```

Input

```
racadm swinventory
```

Output

```
racadm swinventory

-------------------------SOFTWARE INVENTORY-----------------------
ComponentType = FIRMWARE
ElementName = Integrated Dell Remote Access Controller
FQDD = iDRAC.Embedded.1-1
InstallationDate = NA
Rollback Version = 3.30.30.30
HashValue = NA
----------------------------------------------------------------

ComponentType = FIRMWARE
ElementName = Integrated Dell Remote Access Controller
FQDD = iDRAC.Embedded.1-1
InstallationDate = 2019-01-07T03:20:46Z
Current Version = 3.30.30.30
HashValue = NA
----------------------------------------------------------------

ComponentType = FIRMWARE
ElementName = Broadcom Gigabit Ethernet BCM5720 - 00:0A:F7:E8:4A:C6
FQDD = NIC.Integrated.1-3-1
InstallationDate = NA
Available Version = 20.8.4
HashValue = e8abf74757e0d0e01ff5f483af68b3ae62c6908ea0f7443f685b01c7baa9a81b
----------------------------------------------------------------

ComponentType = FIRMWARE
ElementName = Broadcom Gigabit Ethernet BCM5720 - 00:0A:F7:E8:4A:C6
FQDD = NIC.Integrated.1-3-1
InstallationDate = 2018-08-25T14:22:29Z
Current Version = 20.8.4
HashValue = e8abf74757e0d0e01ff5f483af68b3ae62c6908ea0f7443f685b01c7baa9a81b
----------------------------------------------------------------

ComponentType = FIRMWARE
ElementName = Broadcom Gigabit Ethernet BCM5720 - 00:0A:F7:E8:4A:C7
FQDD = NIC.Integrated.1-4-1
InstallationDate = NA
Available Version = 20.8.4
HashValue = e8abf74757e0d0e01ff5f483af68b3ae62c6908ea0f7443f685b01c7baa9a81b
----------------------------------------------------------------

ComponentType = FIRMWARE
ElementName = Broadcom Gigabit Ethernet BCM5720 - 00:0A:F7:E8:4A:C7
FQDD = NIC.Integrated.1-4-1
InstallationDate = 2018-08-25T14:22:31Z
Current Version = 20.8.4
HashValue = e8abf74757e0d0e01ff5f483af68b3ae62c6908ea0f7443f685b01c7baa9a81b
----------------------------------------------------------------

ComponentType = FIRMWARE
ElementName = Broadcom Adv. Dual 10GBASE-T Ethernet - 00:0A:F7:E8:4A:C8
FQDD = NIC.Integrated.1-1-1
InstallationDate = NA
Available Version = 20.08.04.03
HashValue = f4d291569d9b81ccbf3f9b07e3abf5e6ac0d886ca88a9ada770c882114c0e820
----------------------------------------------------------------

ComponentType = FIRMWARE
ElementName = Broadcom Adv. Dual 10GBASE-T Ethernet - 00:0A:F7:E8:4A:C8
FQDD = NIC.Integrated.1-1-1
```

```
InstallationDate = 2018-08-25T14:27:34Z
Current Version = 20.08.04.03
HashValue = f4d291569d9b81ccbf3f9b07e3abf5e6ac0d886ca88a9ada770c882114c0e820
----------------------------------------------------------------------

ComponentType = FIRMWARE
ElementName = Broadcom Adv. Dual 10GBASE-T Ethernet - 00:0A:F7:E8:4A:C9
FQDD = NIC.Integrated.1-2-1
InstallationDate = NA
Available Version = 20.08.04.03
HashValue = f4d291569d9b81ccbf3f9b07e3abf5e6ac0d886ca88a9ada770c882114c0e820
----------------------------------------------------------------------
```

NOTE: Configuration changes and firmware updates that are made within the operating system may not reflect properly in the inventory until you perform a server restart.

switchconnection

Table 99. Details of switchconnection

Description

Provides the switch port details of iDRAC and server network ports. Refresh switch port details of all ports in the server. To run this command, you must have the `Login` privilege.

Synopsis

- `racadm switchconnection view`
- `racadm switchconnection view [iDRAC FQDD | NIC FQDD]`
- `racadm switchconnection refresh`

Input

- `<iDRAC FQDD | NIC FQDD>` — is the fully qualified device descriptor of iDRAC or NIC.

Examples

- To provide switch port details of all iDRAC and server network port

  ```
  racadm switchconnection view
  ```

- To provide switch port details of requested FQDD NIC.Integrated.1-1-1:BRCM

  ```
  racadm switchconnection view
  NIC.Integrated.1-1-1:BRCM
  ```

- To refresh switch port details of all ports in the server

  ```
  racadm switchconnection refresh
  ```

systemconfig

Table 100. Details of systemconfig

Description

Enables you to perform the following:

- Backup and restore for iDRAC and entire system configuration.
- Automatic scheduling of backup operation.
- View the auto backup feature settings.
- Clear the auto backup feature settings.

NOTE:

- **To run this subcommand, you require the Server Profile Export and Import license.**
- **Backup operation is licensed (Enterprise) but restore operation is not licensed.**
- **If the Lifecycle Controller is disabled, starting a restore operation is unsuccessful.**

- **You can reset iDRAC even when a server-profile backup or restore operation is in progress.**
- **If CSIOR is disabled, the system inventory can have old data during the backup operation. An appropriate warning message is displayed.**
- **The `autobackupscheduler` can be enabled or disabled.**
- **The minimum Lifecycle Controller version 1.3 is required.**

Synopsis

- ```
  racadm systemconfig backup -f <filename> <target> [-n passphrase] [-l
  <location> -u <user name> -p <password>] [--vFlash]
  ```
- ```
  racadm systemconfig restore -f <filename> <target> [-n passphrase ] [--
  nopreserve] [-l <location> -u <user name> -p <password>] [--vFlash]
  ```
- To create an AutoBackup Schedule.

  ```
  racadm systemconfig backup [-f <filename>] <target> [-n <passphrase>][-l
  <location> -u <user name> -p <password>] [--vFlash] -time <time> [-dom
  <DayOfMonth>] [-wom <WeekOfMonth>] [-dow <DayofWeek>] -rp <repeat> -mb
  <MaxBackup>
  ```
- To view an AutoBackup Schedule.

  ```
  racadm systemconfig getbackupscheduler
  ```
- To delete an AutoBackup Schedule.

  ```
  racadm systemconfig clearbackupscheduler
  ```

NOTE: After the parameters are cleared, the AutoBackupScheduler is disabled. To schedule the backup again, enable the AutoBackupScheduler.

This command does not support setting the proxy parameters if the share location (-l) is HTTP/HTTPS. For more information, see Proxy parameter section.

Input

- `-n`—Specifies a pass phrase that is used to encrypt or decrypt the configuration data. The pass phrase must have 8–32 characters, and one upper and lower case character.

  NOTE: This pass phrase is optional.
- `-l`—Specifies the network share location, can be either CIFS, NFS, HTTP, or HTTPS.
- `-f`—Specifies the image location and the file name.

  NOTE: If the file is in a subfolder within the share location, then specify the network share location in the `-l` option and specify the subfolder location and the filename in the `-f` option.
- `-u`—Specifies the user name for the remote share access.
- `-p`—Specifies the password for the remote share access.
- `--vFlash`—Selects vFlash SD as target location for back-up.
- `--nopreserve`—Deletes all the virtual disks and configurations.
- `-time`: Specifies the time to schedule an autobackup in HH:MM format. This parameter must be specified.
- `-dom`: Specifies the day of month to schedule an autobackup. Valid values are 1–28, L(Last day) or '*' (default —any day).
- `-wom`: Specifies the week of month to schedule an autobackup. Valid values are 1–4, L(Last week) or '*' (default—any week).
- `-dow`: Specifies the day of week to schedule an autobackup. Valid values are sun, mon, tue, which is wed, thu, fri, sat, or '*' (default—any day).

NOTE: The `-dom`, `-wom`, or `-dow` option must be in the command for the autoupdate schedule. The * value for the options must be included within ' ' (single quotation mark).

- **If the `-dom` option is specified, and then the `-wom` and `-dom` options are not required.**
- **If the`-wom` option is specified, then the`-dow` is required and `-dom` is not required.**
- **If the`-dom` option is non-'*', then the schedule repeats by month.**
- **If the`-wom` option is non-'*', then the schedule repeats by month.**
- **If the`-dom` and `-wom` options are '*' and the `-dow` option is non-'*', then the schedule repeats by week.**

- **If all the three `-dom`, `-wom` and `-dow` options are '*', then the schedule repeats by day.**

- `-rp`: Specifies the repeat parameter. This parameter must be specified.
  - If the `-dom` option is specified, then the valid values for `-rp` are 1–12.
  - If the `-wom` option is specified, then the valid values for `-rp` are 1–52
  - If the `-dow` option is specified, then the valid values for `-rp` are 1–366.
- `-mb`: Specifies the maximum backup parameter. For `--vflash` maximum backup is 1.

NOTE:

- **Avoid using the `-l`, `-u`, and `-p` options with `--vFlash` option.**
- **If a backup file is created in a subfolder within the CIFS shared folder, then the subfolder name must be mentioned in the filename option.**

Output

Job ID is displayed when the backup or restore operation is successful.

Example

- Back up system to CIFS share and encrypt the data.

```
racadm systemconfig backup -f image.img -l //192.168.0/share -u admin -p
xxx -n Encryptp@sswd123
```

- Back up system to NFS share and encrypt the data.

```
racadm systemconfig backup -f image.img -l 192.168.0 :/share -u admin -p
xxx -n Encryptp@sswd123
```

- Back up system to vFlash SD.

```
racadm systemconfig backup --vFlash
```

- Restore system from vFlash SD and clear the VD configurations.

```
racadm systemconfig restore -vFlash --nopreserve
```

- Restore system from NFS share without clearing the VD configurations.

```
racadm systemconfig restore -f image.img -l 192.168.0:/share -u admin -p xxx
```

- Restore system from HTTP share without clearing the VD configurations.

```
racadm systemconfig restore -f image.img -l http://test.com/share -u
httpuser -p httppswd
```

- Restore system from HTTPS share without clearing the VD configurations.

```
racadm systemconfig restore -f image.img -l https://test.com/share -u
httpsuser -p httpspswd
```

- Create a backup file in a subfolder within the CIFS shared folder.

```
racadm systemconfig backup -f rts/Backup.img -l //192.168.0/CIFSshare -u
username -p xxx
```

- To enable or disable AutoBackupScheduler.

```
racadm set lifecyclecontroller.lcattributes.autobackup 1
racadm set lifecyclecontroller.lcattributes.autobackup 0
```

- AutoBackup system to CIFS share and encrypt the data.

```
racadm systemconfig backup -f image.img -l //192.168.0/share -u admin -p
xxx -n encryptpasswd123 -time 14:30 -dom 1 -rp 6 -mb 10
```

- AutoBackup system to NFS share and encrypt the data.

```
racadm systemconfig backup -f image.img -l 192.168.0:/share -u admin -p xxx
-n encryptpasswd123 -time 14:30 -dom 1 -rp 6 -mb 20
```

- AutoBackup system to vFlash SD.

```
racadm systemconfig backup --vFlash -time 10:30 -wom 1 -dow mon -rp 6 -mb 1
```

- AutoBackup system to HTTP and encrypt the data.

```
racadm systemconfig backup -f image.img -l http://test.com -u admin -p
passwd -n Encryptp@sswd123 -time 14:30 -dom 1 -rp 6 -mb 20
```

- AutoBackup system to HTTPS and encrypt the data.

```
racadm systemconfig backup -f image.img -l https://test.com -u admin -p
passwd -n Encryptp@sswd123-time 14:30 -dom 1 -rp 6 -mb 20
```

systemerase

Table 101. systemerase

Description

Allows you to erase the components to remove the server from use.

Synopsis

- To erase a specific component.

```
racadm systemerase <component>
```

- To erase multiple components.

```
racadm systemerase <component>,<component>,<component>
```

Input

- `<component>`—the valid types of components are:
  - `bios`—To reset the BIOS to default.
  - `diag`—To erase embedded diagnostics.
  - `drvpack`—To erase embedded OS driver pack.
  - `idrac`—To reset the iDRAC to default.
  - `lcdata`—To erase Lifecycle Controller data.
  - `allaps`—To reset all apps.
  - `secureerasepd`—To erase the physical disk. This supports SED, NVMe drives, and PCIe cards
  - `overwritepd`—To overwrite physical disk. This supports SAS and SATA drives.
  - `percnvcache`—To erase NV cache.
  - `vflash`—To erase vFlash.
  - `nvdimm`—To erase all NonVolatileMemory.

NOTE: When BIOS is selected for System Erase, the server is turned off and the iDRAC is reset at the end of the Automated Task Application. To complete the process of BIOS reset, the server power must be restored. When the server is turned on, during POST, the BIOS completes the process of resetting to the default properties. At the completion of the reset process, the server is again turned off. Resetting the BIOS also includes the erasing of BIOS-related nonvolatile settings that are used by the OS and embedded in the UEFI applications.

NOTE: When the racadm systemerase command is executed, the iDRAC will take the following actions if the:

- **Server is powered off—it is powered on.**
- **Server is powered on—a graceful system reboot will be executed.**
- **ACPI is enabled on the server— a graceful shutdown occurs within a minute or two.**
- **ACPI is not enabled—a forced shutdown occurs and it may require up to ten minutes to complete.**

Following the server reboot, the Lifecycle Controller will execute the System Erase job to carry out the requested actions. All actions performed by the System Erase operations are recorded to the Lifecycle Log, including details of all devices erased. When these actions are completed, the server

will be powered off and remain in this state, allowing service personnel to perform any needed posterase actions such as drive removal or hardware reconfiguration. When the server is powered on to return to service, the Lifecycle Controller will collect the system inventory and reflect any hardware or firmware changes made after the System Erase.

Examples

- `racadm systemerase bios`
- `racadm systemerase diag`
- `racadm systemerase drvpack`
- `racadm systemerase idrac`
- `racadm systemerase lcdata`
- `racadm systemerase bios,diag,drvpack`
- `racadm systemerase bios,idrac,lcdata`
- `racadm systemerase allapps`
- `racadm systemerase secureerasepd`
- `racadm systemerase overwritepd`
- `racadm systemerase percnvcache`
- `racadm systemerase vflash`
- `racadm systemerase secureerasepd,vflash,percnvcache`
- `racadm systemerase nvdimm`

systemperfstatistics

Table 102. Details of systemperfstatistics

Description Allows you to view and manage the system performance monitoring operations.

Synopsis

- To view the FQDD's of system performance monitoring sensors

```
racadm systemperfstatistics view
```

- To list the usage statistics of a specific sensor

```
racadm systemperfstatistics <sensor_FQDD>
```

- To reset the utilization peaks of system performance monitoring sensors

```
racadm systemperfstatistics PeakReset <FQDD>
```

- To run the peakreset operation you must have configure iDRAC privilege.

Examples:

- To view the FQDD's of system performance monitoring sensors

```
racadm systemperfstatistics view
[key = iDRAC.Embedded.1#SystemBoardCPUUsageStat]
[key = iDRAC.Embedded.1#SystemBoardIOUsageStat]
```

```
[key = iDRAC.Embedded.1#SystemBoardMEMUsageStat]
[key = iDRAC.Embedded.1#SystemBoardSYSUsageStat]
```

- To list the usage statistics of a specific sensor

```
racadm systemperfstatistics iDRAC.Embedded.1#SystemBoardCPUUsageStat

Minimum Readings
Last Hour    = 0% [At Mon, 05 May 2017 17:13:04]
Last Day     = 0% [At Mon, 05 May 2017 15:59:53]
Last Week    = 0% [At Mon, 05 May 2017 15:59:53]

Maximum Readings
Last Hour    = 0% [At Thu, 01 Jan 1970 00:00:00]
Last Day     = 0% [At Thu, 01 Jan 1970 00:00:00]
Last Week    = 0% [At Thu, 01 Jan 1970 00:00:00]

Average Readings
Last Hour    = 0%
Last Day     = 0%
Last Week    = 0%

Peak Readings
Last Week    0% [At Mon, 05 May 2017 15:58:35]
```

- To reset the peak utilization of a specific sensor

```
racadm systemperfstatistics PeakReset iDRAC.Embedded.1#SystemBoardCPUUsageStat
RAC1163: The peak utilization value of Out-Of-Band performance monitoring sensor CPU Usage
is successfully reset.
```

techsupreport

Table 103. Details of techsupreport subcommand

Description

Allows you to perform the technical support report operations.

Tech Support Report (TSR) is now known as SupportAssist Collections and the new term is used in all documentation and GUI. To maintain compatibility across server generations, the RACADM command has been retained as techsupreport.

The types of operations are:

- `collect`—Collects the technical support report data to export. You can specify the various types of logs to be in the report.

  This operation generates a Job ID. Use this Job ID to check the status of the collect operation. To run this operation, you must have the Server Control Commands permission.
- `export`—Exports the collected Tech Support Report data. To run this subcommand, you must have the Execute Server Control Commands permission.
- `getupdatetime`—Gets the timestamp of the last operating system application data collection.
- `updateosapp`—Updates the operating system application data collection. To run this subcommand, you must have the Execute Server Control Commands permission.

Synopsis

- To perform the technical support report operation by specifying the type of operation.

  ```
  racadm techsupreport <tech support report command type>
  ```
- To collect the report data.

  ```
  racadm techsupreport collect [-t <type of logs>]
  ```
- To export the collected report data.

  ```
  racadm techsupreport export -l <CIFS,NFS,TFTP,FTP> -u <username> -p
  <password>
  ```

- To get the timestamp of the last operating system application data collection.

```
racadm techsupreport getupdatetime
```

- To update the operating system application data collection.

```
racadm techsupreport updateosapp -t <type of OS App logs>
```

- To export the collected report data to local share.

```
racadm techsupreport export -f <filename>
```

Input

- `-t`—type of logs. You can specify any of the following values that are separated by a ',' (comma)
  - `SysInfo`—System Information
  - `OSAppNoPII`—Filtered OS and Application data
  - `OSAppAll`—OS and Application data
  - `TTYLog`—TTYLog data

  NOTE:
  - **For updating the operating system application data collection, enter the value `OSAppNoPII` or `OSAppAll` to the `-t` option.**
  - **If no value is specified and system information data is collected.**
  - **To perform the OSLog collection, ensure that ISM is installed and running.**
  - **TTYLog includes PCIeSSD data.**
- `-l`—network share location to export the report
- `-u`—user name for the remote share to export the report
- `-p`—password for the remote share to export the report
- `-f`—target filename for the exported log.

  NOTE: The filename must have .zip as the extension.

Examples

- To collect the system information data.

```
racadm techsupreport collect –t <type of logs>
```

- To collect the system information and TTYLog data.

```
racadm techsupreport collect -t SysInfo,TTYLog
```

- To collect the operating system application data.

```
racadm techsupreport collect -t OSAppAll
```

- To export the collected Tech Support Report, to an FTP share

```
racadm techsupreport export -l ftp://192.168.0/share -u myuser -p xxx
```

- To export the collected Tech Support Report, to a TFTP share

```
racadm techsupreport export -l tftp://192.168.0/share
```

- To export the collected Tech Support Report, to a CIFS share.

```
racadm techsupreport export -l //192.168.0/share -u myuser -p xxx
```

- To export the collected Tech Support Report, to an NFS share.

```
racadm techsupreport export -l 192.168.0:/share
```

- To export the collected Tech Support Report to the local file system.

```
racadm techsupreport export -f tsr_report.zip
```

testemail

Table 104. Details of testemail

Description	Sends a test email from iDRAC to a specified destination. Prior to running the test email command, make sure that the SMTP server is configured. The specified index in the **idrac.EmailAlert** group must be enabled and configured properly. For more information, see *iDRAC RACADM CLI Guide* available at www.dell.com/idracmanuals.
Synopsis	`racadm testemail -i <index>`
Input	`-i <index>` — Specifies the index of the email alert to test.
Output	`Success: Test e-mail sent successfully Failure: Unable to send test e-mail`

Example	Commands for the **idrac.EmailAlert** group:
	• Enable the alert.
	`racadm set idrac.EmailAlert.1.Enable 1`
	• Set the destination email address.
	`racadm set idrac.EmailAlert.1.Address user1@mycompany.com`
	• Set the custom message that is sent to the destination email address.
	`racadm set idrac.emailalert.1.CustomMsg "This is a test!"`
	• Make sure that the SMTP IP address is configured properly.
	`racadm set idrac.remotehosts.SMTPServerIPAddress 192.168.0`
	• View the current email alert settings.
	`racadm get idrac.EmailAlert.<index>`
	where `<index>` is a number from 1 to 8.

testtrap

Table 105. Details of testtrap

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

Example

- Enable the alert.

```
racadm set idrac.emailalert.1.CustomMsg 1
racadm set iDRAC.SNMPAlert.1.Enable 1
```

- Set the destination email IP address.

```
racadm set iDRAC.SNMPAlert.1.Destination
192.168.0
```

- View the current test trap settings.

```
racadm get iDRAC.SNMPAlert.<index>
```

where `<index>` is a number from 1 to 8

testalert

Table 106. Details of testalert

Description

Tests FQDN supported SNMP trap notifications.

To run this subcommand, you must have the Test Alert User Access.

Synopsis

```
racadm testalert -i <index>
```

Input

`-i` — Specifies the index of the trap test. *index* must be an integer from 1 to 8 on iDRAC.

Output

```
Success: Test trap sent successfully
```

```
Failure: Unable to send test trap
```

Example

- Test a trap with index as 1.

```
 racadm testalert -i 1
```

```
Test trap sent successfully.
```

- Test a trap that has not been configured yet.

```
racadm testalert -i 2
```

```
ERROR: Trap at specified index is not currently enabled.
```

traceroute

Table 107. Details of traceroute

Description

Traces network path of the routers as the packets traverse from the system to a destination IPv4 address.

To run this subcommand, you must have the Execute Diagnostic Commands permission.

Synopsis

```
racadm traceroute <IPv4 address>
```

Input

`IPv4` — Specifies IPv4 address.

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 108. Details of traceroute6

Description

Traces the network path of routers as the packets traverse from the system to a destination IPv6 address.

To run this subcommand, you must have the Execute Diagnostic Commands permission.

Synopsis

```
racadm traceroute6 <IPv6address>
```

Input

<IPv6address> – Specifies IPv6 address.

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
```

update

Table 109. Details of update subcommand

Description

Allows you to update the firmware of devices on the server. The supported firmware image file types are:

- `.exe` — Windows-based Dell Update Package (DUP)
- `.d9`
- `.pm`
- `.sc`

The supported catalog files are:

- `.xml`
- `xml.gzip`

NOTE: Updating the platforms from the repository is not supported for IPv6.

NOTE: The firmware update through FTP has a limitation of file name up to 64 characters.

NOTE: Depending on the network traffic, the HTTP packet transfer may fail if you perform update operation from a remote RACADM through a local share. In such cases, retry the operation. If the issue persists, use remote RACADM with the CIFS or NFS share.

NOTE: The supported share types for single file or DUP updates are CIFS, NFS, HTTP, and HTTPS. For Repository updates, the supported share types are CIFS, NFS, FTP, TFTP, and HTTP.

Synopsis

For single file or DUP update:

```
racadm update -f <updatefile>
```

```
racadm update -f <updatefile> -l <location> -u <username for CIFS share> -p
<password for CIFS share>
```

```
racadm update -f <updatefile> -l <location>
```

For Repository updates

```
racadm update -f <catalog file> -t <Repository type> -l <location> \ -u
<username for CIFS share> -p <password for CIFS share> \ [-a <restart>] [--
verifycatalog]
```

```
racadm update -f <catalog file> -t <Repository type> \ -e <FTP server with
the path to the catalog file> [-a <restart>] \[--verifycatalog]
```

```
racadm update -f <catalog file> -t <Repository type> \ -e <FTP server with
the path to the catalog file> [-a <restart>] \ -ph <proxy ip> -pu <proxy
user> -pp <proxy pass> -po <proxy port> \
  -pt <proxy type>
```

```
racadm update viewreport
```

Input

For single file or DUP update:

- `-f: <updatefile>`—Update filename (Windows DUP, `.d9`,`.pm`, `.sc`) only.
- `-u: < username for CIFS share>`—Specifies username of the remote share that stores the update file. Specify username in a domain as domain/username.
- `-p: <password for CIFS share`—Specifies password of the remote share that stores the update file.
- `-l: <location>`—Specifies network share location that stores the update file. For more information on NFS or CIFS share, see section on Usage examples
- `–reboot`—Performs a graceful system reboot after the firmware update.

For Repository update:

- `-f: <updatefile>`—Update filename .

  For update from repository `.xml` files are allowed. If a file name is not specified for repository update, Catalog.xml is taken as default.

  If a file name is not specified for repository update, then the `Catalog.xml` is taken as default.
- `-u: < username for CIFS share>`—Username of the remote share that stores the update file. Specify username in a domain as domain/username.
- `-p: <password for CIFS share` — Specifies password of the remote share that stores the update file.
- `-l: <location>`—Specifies network share location (CIFS/NFS/HTTP/HTTPS/FTP), that stores the update file. For more information on network share, see section on Usage examples
- `-a: <restart>` — This option indicates if the server should be restarted after the update from repository operation completes. Must be one of the below:
  - TRUE : restart after update completes
  - FALSE : do not restart after update completes

  NOTE: These options are case insensitive.
- `-t:Repository type>`—Specifies the type of repository being used for the update.

  Must be one of the below:
  - FTP: Repository is FTP
  - TFTP: Repository is TFTP
  - HTTP: Repository is HTTP
  - HTTPS: Repository is HTTPS
  - CIFS: Repository is CIFS
  - NFS: Repository is NFS

  NOTE: These options are case insensitive. If the repository update functionality is to be invoked, this option is necessary.
- `-e:<FTP server with the path to the catalog file>`—Specifies the Server path for the FTP, TFTP, HTTP, and HTTPS.

- `-ph : <proxy ip>`—Specifies the IP address of the proxy server.
- `-pu : <proxy user>`—Specifies the user name for proxy credentials.
- `-pp : <proxy pass>`—Specifies the password for proxy credentials.
- `-po : <proxy port>`—Specifies the port for proxy server.
- `-pt : <proxy type>`—Specifies the proxy type.

  Must be one of the below:

  - HTTP: Proxy is HTTP
  - SOCKS4: Proxy is SOCKS4

  NOTE:

  - **If the repository has to be through a proxy, the proxy server address, proxy username and the proxy password are necessary. The Lifecycle Controller must be enabled for repository update.**
  - **This command supports both IPV4 and IPV6 formats. IPV6 is applicable only for CIFS and NFS remote share.**

Output

Firmware update job for `<filename>` is initiated.

This firmware update job may take several minutes to complete depending on the component or firmware being updated. To view the progress of the job, run the `racadm jobqueue view` command.

For repository update command, the output is:

```
Update from repository operation has been initiated. Check the progress of
the operation using "racadm jobqueue view -i JID_809364633532" command.
```

For devices that perform update process without rebooting the host, the update status changes from `Downloading` to `Completed`. For devices that require host reboot to perform update process, the update status changes from `Downloading` to `Scheduled`. When the status is displayed as `Scheduled`, reboot the host to start the update process.

The following devices require host reboot to perform the update process:

- Backplanes
- BIOS
- Complex programmable logic device (CPLD)
- Hard disk drives
  - Solid-state drives (SSD)
- Network interface cards (NIC) or Fibre Channel (FC) cards
- PCIe SSD devices
- Power supply unit (PSU)
- Storage controllers

Example

For single file or DUP updates:

- Upload the update file from a remote FTP share

  ```
  racadm update -f <updatefile> -u admin -p mypass -l ftp://1.2.3.4/share
  ```

- Upload the update file from a remote FTP share and to perform a graceful system reboot after update:

  ```
  racadm update -f <updatefile> -u admin -p mypass -l ftp://1.2.3.4/share --
  reboot
  ```

- Upload the update file from a remote CIFS share:

  ```
  racadm update -f <updatefile> -u admin -p mypass -l //1.2.3.4/share
  ```

- Upload the update file from a remote CIFS share and under a user domain "dom":

  ```
  racadm update -f <updatefile> -u dom/admin -p mypass -l //1.2.3.4/share
  ```

- Upload the update file from a remote NFS share:

```
racadm update -f <updatefile> -l 1.2.3.4:/share
```

- Upload the update file from a remote HTTP share:

```
 racadm update -f <updatefile> -u admin -p mypass -l http://1.2.3.4/share
```

- Upload the update file from a remote HTTPS share:

```
 racadm update -f <updatefile> -u admin -p mypass -l https://1.2.3.4/share
```

- Upload the update file from the local file system using Local RACADM.

```
racadm update -f <updatefile>
```

- Upload the Update file from a remote CIFS share and to perform a graceful system reboot after update:

```
racadm update -f <updatefile> -u admin -p mypass -l //1.2.3.4/share --reboot
```

- Upload the Update file from a remote NFS share and to perform a graceful system reboot after update:

```
racadm update -f <updatefile> -l 1.2.3.4:/share --reboot
```

- Upload the update file from a remote HTTP share and to perform a graceful system reboot after update:

```
racadm update -f <updatefile> -u admin -p mypass -l http://1.2.3.4/share --
reboot
```

- Upload the Update file from the local file system using local racadm and to perform a graceful system reboot after update:

```
racadm update -f <updatefile> --reboot
```

For Repository updates:

- Perform update from an FTP repository and to apply the updates, reboot the server:

```
  racadm update -f Catalog.xml -l //192.168.11.10/Repo -u test -p passwd -a
TRUE -t CIFS
```

- Generate a comparison report using about the available updates in the repository:

```
racadm update -f Catalog.xml -l 192.168.11.10:/Repo -t NFS -a FALSE --
verifycatalog
```

- Perform update from an FTP repository and reboot the server to apply the updates:

```
racadm update -f Catalog.xml -e 192.168.11.10/Repo/MyCatalog -a TRUE -t FTP
```

- Perform update from an FTP repository with authentication and reboot the server to apply the updates

```
racadm update -f Catalog.xml -e 192.168.11.10/Repo/MyCatalog -u user -p
mypass -a TRUE -t FTP
```

- Perform update from a HTTP repository and restart the server to apply the updates.

```
racadm update -f Catalog.xml -e 192.168.11.10/Repo/MyCatalog -a TRUE -t HTTP
```

- Perform update from a TFTP repository and restart the server to apply the updates.

```
  racadm update -f Catalog.xml -e 192.168.11.10/Repo/MyCatalog -a TRUE -t
TFTP
```

- Perform update from an FTP repository through a proxy server.

```
racadm update -f Catalog.xml -e 192.168.11.10/Repo/MyCatalog -a TRUE -ph
145.140.12.56 -pu prxyuser -pp prxypass -po 80 -pt http -t FTP
```

- Perform update from an downloads.dell.com

```
racadm update -f Catalog.xml.gz -e ftp.dell.com/Catalog -a TRUE -t FTP
```

- View the comparison report generated when --verifycatalog is used.

```
racadm update viewreport
```

usercertupload

Table 110. Details of usercertupload

Description	Uploads a user certificate or a user CA certificate from the client to iDRAC. To run this subcommand, you must have the Configure iDRAC permission.
Synopsis	`racadm usercertupload -t <type> [-f <filename>] -i <index>`

Input	• `-t` — Specifies the type of certificate to upload, either the CA certificate or server certificate.
	  • `1`=user certificate
	  • `2`=user CA certificate
	• `-f` — Specifies the filename of the certificate that must be uploaded. If the file is not specified, the `sslcert` file in the current directory is selected.
	• `-i` — Index number of the user. Valid values 2–16.

Output	If upload is successful, the message `User certificate successfully uploaded to the RAC`. If unsuccessful, appropriate error message is displayed.
Example	To upload user certificate for user 6. `racadm usercertupload -t 1 -f c:\cert\cert.txt -i 6`

usercertview

Table 111. Details of usercertview

Description	Displays the user certificate or user CA certificate that exists on iDRAC.
Synopsis	`racadm usercertview -t <type> [-A] -i <index>`

Input	• `-t` — Specifies the type of certificate to view, either the user certificate or the user CA certificate.
	  • 1=user certificate
	  • 2=user CA certificate
	• `-A` — Prevents printing headers or labels.
	• `-i` — Index number of the user. Valid values are 2–16.

Example	To view user certificate for user 6.
	`racadm usercertview -t 1 -i 6`
	`Serial Number : 01`
	`Subject Information:`
	`Country Code (CC) : US`
	`State (S) : Texas`
	`Locality (L) : Round Rock`
	`Organization (O) : Dell Inc.`

```
Common Name (CN)        : iDRAC default certificate

Issuer Information:
Country Code (CC)       : US
State (S)               : Texas
Locality (L)            : Round Rock
Organization (O)        : Dell Inc.
Organizational Unit (OU): Remote Access Group
Common Name (CN)        : iDRAC default certificate

Valid From              : May 7 23:54:19 2017 GMT
Valid To                : May 4 23:54:19 2027 GMT
```

vflashsd

Table 112. Details of vflashsd

Description

Allows you to initialize or get the status of the vFlash SD card. The initialize operation removes all the existing partitions and resets the card.

The status operation displays the status of the last operation performed on the card.

To run this subcommand, you must have the Access Virtual Media privilege.

NOTE: After you restart the iDRAC, the status of the previous initialize operation is erased.

Synopsis

- `racadm vflashsd initialize`
- `racadm vflashsd status`

Input

- `Initialize`— performs initialize operation on SD card.
- `Status` — indicates to view the progress or status report of the initialize operation.

Output

If initialization is in progress, the message `Initialization of the vFlash SD Card is now in progress` is displayed. If unsuccessful, appropriate error message is displayed.

If the status of the last operation performed is successful, the message `LastAction Progress Status==========Initialize SD Card 100 % Complete` is displayed. If unsuccessful, appropriate error message is displayed.

vflashpartition

Table 113. Details of vflashpartition subcommand

Description

Manages the partitions on the vFlash SD card.

NOTE:

- **To run this subcommand, you must have the iDRAC Enterprise license.**
- **After iDRAC restart, the status of the previous operation performed on the partition(s) is erased.**

Synopsis

```
racadm vflashpartition <create | delete | status | list> -i<index> -o<label> -
e<emulation type> -s<size> -f<format type> -t<partition type> -l<path> -
u<user> -p<password> -a
```

Input

- `-o` — Label that is displayed when the partition is mounted on the operating system. This option must be a string of up to six alphanumeric characters. VFLASH is the only accepted volume label for non-Dell SD card.
- `-e` — Emulation type must be either floppy, cddvd, or hdd.
  - `floppy` — emulates a floppy disk
  - `cddvd` — emulates a CD or DVD
  - `hdd` — emulates a hard disk

- `-s` — Partition size in MB.
- `-f` — Format type for the partition based on the type of the file system. Valid options are `raw`, `ext2`, `ext3`, `fat16`, and `fat32`.
- `-t` — Create a partition of the following type:
  - `empty` — Creates an empty partition
  - `image` — Creates a partition using an image relative to iDRAC.

  NOTE: Creating an empty partition with emulation type as floppy with ext2 format type by using the Telnet session might result in a state where the partition creation status is shown as zero. If this happens then it is recommended to remove the SD card and format it in order to reuse.

  Creation of a partition may be unsuccessful if:
  - The network share is not reachable.
  - The user name or password provided is not correct.
  - The file provided does not exist.
  - The memory available on the SD card is lesser than size of the image file.
- `-l` — Specifies the remote path relative to iDRAC.
- `-u` — User name for accessing the remote image.
- `-p` — Password for accessing the remote image.
- `-a` — Display the status of operations on all the existing partitions.
- `list` — Lists the existing partitions and its properties.

Example

- Create a 20MB empty partition.

```
racadm vflashpartition create -i 1 -o Drive1 -e hdd -t empty -f fat16 -s 20
```

- Create a partition from a remote image.

```
racadm vflashpartition create -i 1 -o Drive1 -e cddvd -t image -l
//ipaddress/sharefolder/isoimge.iso -u username -p xxx
```

A new partition is created. By default, the created partition is read-only. This command is case-sensitive for the image filename extension. If the filename extension is in uppercase, for example FOO.ISO instead of FOO.iso, then the command returns a syntax error.

NOTE:

- **This feature is not supported in Local RACADM.**
- **Creating vFlash partition from an image file on the CFS or NFS IPv6 enabled network share is not supported.**

- Delete a partition.

```
racadm vflashpartition delete -i 1
```

- Status of operation on partition 1.

```
racadm vflashpartition status -i 1
```

- Status of all the existing partitions.

```
racadm vflashpartition status -a
```

- List all the existing partitions and its properties.

```
racadm vflashpartition list
```

vmdisconnect

Table 114. Details of vmdisconnect

Description	Allows you to end another Virtual Media session. After the session ends, the web-based interface reflects the correct connection status. Enables an iDRAC user to disconnect all active Virtual Media sessions. The active Virtual Media sessions are displayed on iDRAC web-based interface or by running the RACADM subcommands `remoteimage` or `getssninfo`. To run this subcommand, you must have the Access Virtual Media permission.
Synopsis	`racadm vmdisconnect`

3

iDRAC Property Database Group and Object Descriptions

The iDRAC property database contains the configuration information for iDRAC. Associated object is organizing data, and object group is organizing object. The IDs for the groups and objects that the property database supports are listed in this section for iDRAC Enterprise on Blade Servers and iDRAC Enterprise or Express on Rack and Tower Servers.

To configure iDRAC, use the group and object IDs with the RACADM subcommands.

NOTE: You can configure a setting that does not have a hash symbol (#) as the prefix in its output name. To modify a configurable object, use the `-o` option.

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:

- cfgSensorRedundancy
- cfgVFlashSD
- cfgVFlashPartition
- cfgLogging
- cfgRacSecurity

Displayable Characters

Displayable characters include the following set:

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

Table 115. Object groups for iDRAC Enterprise

Subcommand	iDRAC on Blade Servers
cfgServerinfo	No
cfgServerPowerSupply	No
cfgIpmiSerial	No
cfgNetTuning	No
cfgSensorRedundancy	No

idRacInfo

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

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

idRacProductInfo (Read Only)

Table 116. Details of idRacProductInfo

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

idRacDescriptionInfo (Read Only)

Table 117. 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 **Dell PowerEdge** servers.

idRacVersionInfo (Read Only)

Table 118. 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 119. Details of idRacBuildInfo

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

idRacName (Read Only)

Table 120. Details of idRacName

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

cfgStaticLanNetworking

This group contains parameters to configure the device NIC for IPv4.

NOTE: A few objects in this group may require the device NIC to be reset, that may cause a brief loss in connectivity.

cfgNicStaticEnable (Read or Write)

Table 121. cfgNicStaticEnable

Description	Enables or disables the NIC.
Legal Values	• 0 — Disabled • 1 — Enabled
Default	1 — Enabled

NOTE: If this object is modified, then the object `cfgNicEnable` is also modified.

cfgNicStaticIPv4Enable (Read or Write)

Table 122. cfgNicStaticIPv4Enable

Description	Enables or disables the IPv4 stack.
Legal Values	• 0 — Disabled • 1 — Enabled
Default	1 — Enabled

NOTE: If this object is modified, then the object `cfgNicIPv4Enable` is also modified.

cfgNicStaticIpAddress (Read or Write)

Table 123. cfgNicStaticIpAddress

Description	Returns or sets the current IPv4 address. **NOTE: Only set the current IPv4 address if `cfgNicUseDhcp` is set to 0(false).**
Legal Values	Any Valid IPv4 address
Default	192.168.0

cfgNicStaticUseDhcp (Read or Write)

Table 124. cfgNicStaticUseDhcp

Description	Specifies whether DHCP is used to configure the IPv4 network.
Legal Values	• 0 — IP Address, subnet mask and gateway are configured on the device. • 1 — IP Address, subnet mask and gateway are assigned from the DHCP server.
Default	0 — Do not use DHCP

NOTE: If this object is modified, then the object `cfgNicUseDhcp` is also modified.

cfgNicStaticNetmask (Read or Write)

Table 125. cfgNicStaticNetmask

Description	Returns or sets the static IPv4 Netmask. **NOTE: Only set the current IPv4 netmask, if `cfgNicUseDhcp` is set to `0 (false).`**
Legal Values	Any Valid IPv4 Netmask
Default	255.255.255.0

cfgNicStaticGateway (Read or Write)

Table 126. cfgNicStaticGateway

Description	Returns or sets the static IPv4 address.
Legal Values	Any Valid IPv4 address
Default	`192.168.0.120`

cfgDNSStaticServersFromDHCP (Read or Write)

Table 127. cfgDNSStaticServersFromDHCP

Description	Specifies the DNS server static IP addresses.
Legal Values	• DNS Addresses are configured on the Device • DNS Addresses are assigned via DHCP
Default	0

cfgDNSStaticServer1 (Read or Write)

Table 128. cfgDNSStaticServer1

Description	Specifies the IP address for DNS server 1. **NOTE: This property is only valid if `cfgDNSServersFromDHCP` is set to `0` (FALSE).**
Legal Values	• `0` — IP Address, subnet mask and gateway are configured on the device. • `1` — IP Address, subnet mask and gateway are assigned from the DHCP server.
Default	`0` — Do not use DHCP

NOTE: If this object is modified, then the object `cfgNicUseDhcp` is also modified.

cfgDNSStaticServer2 (Read or Write)

Table 129. cfgDNSStaticServer2

Description	Specifies the static IP address for DNS server 2.
Legal Values	A Valid IPv4 Address
Default	`0.0.0.0`

cfgDNSStaticDomainName(Read or Write)

Table 130. cfgDNSStaticDomainName

Description	The DNS static domain name.
Legal Values	String of up to 254 ASCII characters. Characters are restricted to alphanumeric, hyphens and periods. At least one of the characters must be alphabetic.

NOTE: **Microsoft Active Directory only supports Fully Qualified Domain Names (FQDN) of 64 characters or fewer lengths.**

Default Null

cfgDNSStaticDomainNameFromDHCP (Read or Write)

Table 131. cfgDNSStaticDomainNameFromDHCP

Description	Specifies the device DNS static domain name.
Legal Values	• 0 — Do not use DHCP to get the Domain Name • 1 — Use DHCP to get the Domain Name
Default	0 — Disabled

cfgRemoteHosts

This group provides properties that allow configuration of the SMTP server for email alerts.

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

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

cfgRhostsFwUpdateTftpEnable (Read or Write)

Table 132. cfgRhostsFwUpdateTftpEnable

Description	Enables or disables firmware update from a network TFTP server. NOTE: **This object is read-only for iDRAC Modular servers.**
Legal Values	• 1 (TRUE) • 0 (FALSE)
Default	1

cfgRhostsFwUpdateIpAddr (Read or Write)

Table 133. Details of cfgRhostsFwUpdateIpAddr

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

cfgRhostsFwUpdatePath (Read or Write)

Table 134. cfgRhostsFwUpdatePath

Description	Specifies TFTP path where firmware image file exists on the TFTP server. The TFTP path is relative to the TFTP root path on the TFTP server. NOTE: **The server may still require you to specify the drive (for example, `C:`).**

Legal Values	A string with a maximum length of 255 ASCII characters.
Default	<blank>

cfgRhostsSmtpServerIpAddr (Read or Write)

Table 135. Details of cfgRhostsSmtpServerIpAddr

Description	The IPv4 or IPv6 address of the network SMTP server. The SMTP server transmits email alerts from iDRAC if the alerts are configured and enabled.
Legal Values	A string representing a valid SMTP server IPv4 or IPv6 address. For example: 192.168.0.2.
Default	For IPv4, it is 0.0.0.0

cfgRhostsSyslogEnable (Read or Write)

Table 136. Details of cfgRhostsSyslogEnable

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

cfgRhostsSyslogPort (Read or Write)

Table 137. Details of cfgRhostsSyslogPort

Description	Remote syslog port number to use for writing the RAC and SEL logs to a remote syslog server.
Legal Values	10–65535
Default	514

cfgRhostsSyslogServer1 (Read or Write)

Table 138. Details of cfgRhostsSyslogServer1

Description	To store the RAC and SEL logs specify the first of three possible remote syslog servers. This property is only valid if cfgRhostsSyslogEnable is set to 1 (enabled).
Legal Values	String from 0 to 63 characters.
Default	<blank>

cfgRhostsSyslogServer2 (Read or Write)

Table 139. Details of cfgRhostsSyslogServer2

Description	To store the RAC and SEL logs Specify the second of three possible remote syslog servers. This property is only valid if cfgRhostsSyslogEnable is set to 1 (enabled).

Legal Values	String from 0 to 63 characters.
Default	<blank>

cfgRhostsSyslogServer3 (Read or Write)

Table 140. Details of cfgRhostsSyslogServer3

Description	To store the RAC and SEL logs specify the third of three possible remote syslog servers. This property is only valid if cfgRhostsSyslogEnable is set to 1(enabled).
Legal Values	String from 0 to 63 characters.
Default	<blank>

cfgUserAdmin

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

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

Use this object with the config or getconfig subcommands. To use the command as follows: -i <index group>, supply an index group number

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

cfgUserAdminIndex (Read Only)

Table 141. Details of cfgUserAdminIndex

Description	The unique index of a user.
Legal Values	This parameter is populated based on the existing instances.
Default	<index of the instance>

cfgUserAdminIpmiLanPrivilege (Read or Write)

Table 142. Details of cfgUserAdminIpmiLanPrivilege

Description	The maximum privilege on the IPMI LAN channel.
Legal Values	• 2(User) • 3(Operator) • 4(Administrator) • 15(No access)
Default	• 4(User 2) • 15(All others)

cfgUserAdminIpmiSerialPrivilege (Read or Write)

Table 143. Details of cfgUserAdminIpmiSerialPrivilege

Description	The maximum privilege on the IPMI LAN channel. This object is applicable only for iDRAC on Rack and Tower Servers and not for iDRAC Enterprise on Blade Servers.

Legal Values	• 2 (User) • 3 (Operator) • 4 (Administrator) • 15 (No access)
Default	• 4 (User 2) • 15 (All others)

cfgUserAdminPrivilege (Read or Write)

Table 144. 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	0x00000000 to 0x000001ff, and 0x0
Default	0x00000000

Example

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

```
# cfgUserAdminIndex=1
cfgUserAdminEnable=1
cfgUserAdminUserName=root
# cfgUserAdminPassword=******** (Write-Only)
cfgUserAdminPrivilege=0x00000fff
```

Table 145. Bit masks for user privileges

iDRAC Specific User Privilege	Privilege Bit Mask
Log in 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

Table 146. Examples

User Privileges	Privilege Bit Mask

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

cfgUserAdminUserName (Read or Write)

Table 147. Details of cfgUserAdminUserName

Description

The name of the user for this index. Writing a string of double quotation mark (" ") disables the user. The string cannot contain / (forward slash), \ (backward slash), . (period), @ (at symbol), quotation marks, ; (semicolon), or ‘ (backward quotation mark).

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 148. 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 149. 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 1 (User 2), 0 (All others)

cfgUserAdminSolEnable (Read or Write)

Table 150. Details of cfgUserAdminSolEnable

Description	Enables or disables Serial Over LAN (SOL) user access for the user.
Legal Values	• 1 (TRUE) • 0(FALSE)
Default	0

cfgEmailAlert

This group contains parameters to configure iDRAC email alerting capabilities. Up to four instances of this group are allowed.

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

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

cfgEmailAlertAddress (Read or Write)

Table 151. Details of cfgEmailAlertAddress

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

cfgEmailAlertEnable (Read or Write)

Table 152. Details of cfgEmailAlertEnable

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

cfgEmailAlertIndex (Read Only)

Table 153. Details of cfgEmailAlertIndex

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

cfgEmailAlertCustomMsg (Read or Write)

Table 154. Details of cfgEmailAlertCustomMsg

Description	Specifies a custom message that forms the subject of the alert.
Legal Values	A string of up to 32 characters
Default	<blank>

cfgEmailAlertEmailName (Read Only)

Table 155. Details of cfgEmailAlertEmailName

Description	Specifies name or other identifier associated with the destination email address. The email 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 iDRAC. One instance of the group is allowed. Displays current settings for and configures the idle timeout properties for web server, Telnet, SSH and RACADM sessions. Changes to idle time out settings take effect at the next login. To disable the idle time out property for a connection, set this property to 0.

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

cfgSsnMgtRacadmTimeout (Read or Write)

Table 156. 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	10–1920
Default	60

Example

```
racadm getconfig -g cfgSessionManagement cfgSsnMgtWebserverTimeout=0
cfgSsnMgtTelnetIdleTimeout=0
cfgSsnMgtSshIdleTimeout=1800
cfgSsnMgtRacadmTimeout=0
```

cfgSsnMgtConsRedirMaxSessions (Read or Write)

Table 157. Details of cfgSsnMgtWebserverTimeout

Description	Specifies the maximum number of Virtual Console sessions allowed on iDRAC.
Legal Values	1–4
Default	4

cfgSsnMgtWebserverTimeout (Read or Write)

Table 158. 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 canceled if the time limit exceeds this property. Changes to this setting do not affect the current session. 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

cfgSsnMgtSshIdleTimeout (Read or Write)

Table 159. Details of cfgSsnMgtSshIdleTimeout

Description	Defines the secure shell idle 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 canceled if the time limit exceeds this property. Changes to this setting do not affect the current session; log out and log in again to make the new settings effective. An expired secure shell session displays the following error message: • For iDRAC on Rack and Tower Servers: Connection timed out • For iDRAC Enterprise on Blade Servers: `Session timed out. Closing the session.` After the message is displayed, the system returns to the shell that generated the Secure Shell session.
Legal Values	• `0` —(No timeout) • 60–10800 **NOTE: If 0 (no timeout), the network connection does not send alive packets to probe the client. Otherwise, keep alive packets are sent to guarantee that the client is responding.**
Default	• For iDRAC on Rack and Tower Servers: 300 • For iDRAC Enterprise on Blade Servers: 1800

cfgSsnMgtTelnetIdleTimeout (Read or Write)

Table 160. Details of cfgSsnMgtTelnetIdleTimeout

Description	Defines the Telnet idle timeout. 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 canceled if the time limit exceeds this property. 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 Telnet session displays the following error message: • For iDRAC on Rack and Tower Servers: `Connection timed out`

- For iDRAC Enterprise on Blade Servers: `Session timed out. Closing the session.`

After the message is displayed, the system returns you to the shell that generated the Telnet session.

Legal Values

- `0` (No timeout)
- 60–10800

NOTE: If 0 (no timeout is specified), the network connection does not send alive packets to probe the client. Otherwise, keep alive packets are sent to guarantee that the client is responding.

Default

- For iDRAC on Rack and Tower Servers: 300
- For iDRAC Enterprise on Blade Servers: 1800

cfgSerial

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

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

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

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

cfgSerialBaudRate (Read or Write)

Table 161. Details of cfgSerialBaudRate

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

cfgSerialConsoleEnable (Read or Write)

Table 162. Details of cfgSerialConsoleEnable

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

cfgSerialConsoleQuitKey (Read or Write)

Table 163. Details of cfgSerialConsoleQuitKey

Description	This key or key combination terminates Virtual Console text for iDRAC when using the `console com2` command.
Legal value:	^ follows any alphabet (a-z, A-Z) ^ follows the listed special characters: [ ] \ ^ _ **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: <Ctrl> \

cfgSerialConsoleIdleTimeout (Read or Write)

Table 164. Details of cfgSerialConsoleIdleTimeou

Description	The maximum number of seconds to wait before an idle serial session is disconnected.
Legal Values	• 0 = No timeout • 60–1920
Default	300

cfgSerialConsoleNoAuth (Read or Write)

Table 165. Details of cfgSerialConsoleNoAuth

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

cfgSerialConsoleCommand (Read or Write)

Table 166. Details of cfgSerialConsoleCommand

Description	Specifies a serial command that is executed after a user logs in to the serial console interface.
Legal Values	A string of up to 128 characters.
Default	<blank>

cfgSerialHistorySize (Read or Write)

Table 167. Details of cfgSerialHistorySize

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

cfgSerialCom2RedirEnable (Read or Write)

Table 168. Details of cfgSerialSshEnable

Description	Enables or disables the console for COM 2-port redirection. The `cfgSerialCom2RedirEnable` object property is applicable only for iDRAC on Rack and Tower Servers.
Legal Values	• `1` (TRUE) • `0` (FALSE)
Default	1

cfgSerialSshEnable (Read or Write)

Table 169. Details of cfgSerialSshEnable

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

Example

```
racadm getconfig -g cfgSerial
```

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

cfgSerialTelnetEnable (Read or Write)

Table 170. Details of cfgSerialTelnetEnable

Description	Enables or disables the Telnet console interface.
Legal Values	• `1` (TRUE) • `0` (FALSE)
Default	0

cfgOobSnmp

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

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

This group is not applicable for iDRAC on Rack and Tower Servers.

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

cfgOobSnmpAgentCommunity (Read or Write)

Table 171. Details of cfgOobSnmpAgentCommunity

Description	Specifies the SNMP Community Name 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 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 or Write)

Table 172. Details of cfgOobSnmpAgentEnable

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

cfgRacTuning

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

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

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

cfgRacTuneConRedirPort (Read or Write)

Table 173. Details of cfgRacTuneConRedirPort

Description	To use for keyboard, mouse, video and Virtual Media traffic to iDRAC, specify the port.
Legal Values	1024–65535
Default	5900

cfgRacTuneRemoteRacadmEnable (Read or Write)

Table 174. Details of cfgRacTuneRemoteRacadmEnable

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

Default	1

cfgRacTuneCtrlEConfigDisable

Table 175. Details of cfgRacTuneCtrlEConfigDisable

Description	To configure iDRAC from the BIOS POST option-ROM, enables or disables the ability of the local user. This object is applicable only for iDRAC on Rack and Tower Servers and not for iDRAC Enterprise on Blade Servers.
Legal Values	• 1 (TRUE) • 0 (FALSE)
Default	0

cfgRacTuneHttpPort (Read or Write)

Table 176. Details of cfgRacTuneHttpPort

Description	To use HTTP network communication, specify the port number.
Legal Values	10–65535
Default	80

cfgRacTuneHttpsPort (Read or Write)

Table 177. Details of cfgRacTuneHttpsPort

Description	To use HTTPS network communication, specify the port number.
Legal Values	10–65535
Default	443

cfgRacTuneIpRangeEnable (Read or Write)

Table 178. Details of cfgRacTuneIpRangeEnable

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

cfgRacTuneIpRangeAddr (Read or Write)

Table 179. Details of cfgRacTuneIpRangeAddr

Description	Specifies the acceptable IPv4 address bit pattern in the positions of the "1"s in the range mask property (`cfgRacTuneIpRangeMask`).
Legal Values	An IPv4 address formatted string, for example, `192.168.0`.

Default	192.168.0

cfgRacTuneIpRangeMask (Read or Write)

Table 180. Details of cfgRacTuneIpRangeMask

Description	Standard IP mask values with left-justified bits. For example, `255.255.255.0`.
Legal Values	An IPv4 address formatted string, for example, `255.255.255.0`.
Default	255.255.255.0

cfgRacTuneSshPort (Read or Write)

Table 181. Details of cfgRacTuneSshPort

Description	Specifies the port number used for the SSH interface.
Legal Values	1–65535
Default	22

cfgRacTuneTelnetPort (Read or Write)

Table 182. Details of cfgRacTuneTelnetPort

Description	Specifies the port number used for the Telnet interface.
Legal Values	1–65535
Default	23

cfgRacTuneConRedirEnable (Read or Write)

Table 183. Details of cfgRacTuneConRedirEnable

Description	Enables or disables Virtual Console.
Legal Values	• 1 (TRUE) • 0 (FALSE)
Default	1

cfgRacTuneConRedirEncryptEnable (Read or Write)

Table 184. Details of cfgRacTuneConRedirEncryptEnable

Description	Encrypts the video in a Virtual Console session.
Legal Values	• 1 (TRUE) • 0 (FALSE)
Default	1

cfgRacTuneAsrEnable (Read or Write)

Table 185. Details of cfgRacTuneAsrEnable

Description	Enables or disables iDRAC last crash screen capture feature. This object property requires an iDRAC reset before it becomes active.
Legal Values	• 1 (TRUE) • 0 (FALSE)
Default	0

cfgRacTuneDaylightOffset (Read Only)

Table 186. 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 -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
# cfgRacTuneTimezoneOffset=-18000
# cfgRacTuneDaylightOffset=3600
```

cfgRacTuneTimezoneOffset (Read Only)

Table 187. Details of cfgRacTuneTimezoneOffset

Description	Specifies the time zone offset (in minutes) from Greenwich Mean Time (GMT) / Coordinated Universal Time (UTC) to use for the RAC Time. Some common time zone offsets for time zones in the United States are: • –480 (PST — Pacific Standard Time) • –420 (MST — Mountain Standard Time) • –360 (CST — Central Standard Time) • –300 (EST — Eastern Standard Time)
Legal Values	–720–7800
Default	0

Example

```
racadm getconfig -g cfgRacTuning
```

```
cfgRacTuneRemoteRacadmEnable=1
cfgRacTuneWebserverEnable=1
cfgRacTuneHttpPort=80
cfgRacTuneHttpsPort=443
cfgRacTuneTelnetPort=23
cfgRacTuneSshPort=22
cfgRacTuneIpRangeEnable=0
cfgRacTuneIpRangeAddr=192.168.1.1
cfgRacTuneIpRangeMask=255.255.255.0
# cfgRacTuneTimezoneOffset=-18000
# cfgRacTuneDaylightOffset=3600
```

cfgRacTuneLocalServerVideo (Read or Write)

Table 188. Details of cfgRacTuneLocalServerVideo

Description	Enables or disables the local server video.
Legal Values	• 1 (TRUE — Enables) • 0 (FALSE— Disables)
Default	1

cfgRacTuneLocalConfigDisable (Read or Write)

Table 189. Details of cfgRacTuneLocalConfigDisable

Description	Disables write access to iDRAC configuration data. **NOTE: Access can be disabled using the local RACADM or iDRAC web interface; however, once disabled, access can be re-enabled only through iDRAC web interface.**
Legal Values	• 0 (TRUE-Enables) • 1 (FALSE-Disables)
Default	0

cfgRacTuneWebserverEnable (Read or Write)

Table 190. Details of cfgRacTuneWebserverEnable

Description	Enables or disables the web server. If this property is disabled then it 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

cfgRacTuneVirtualConsoleAuthorizeMultipleSessions (Read or Write)

Table 191. Details of cfgRacTuneVirtualConsoleAuthorizeMultipleSessions

Description	If a first user is already using the Virtual Console, the value of this object affects the privileges granted to the subsequent user's shared request after the timeout of 30 seconds. This object is applicable only for iDRAC on Rack and Tower Servers and not for iDRAC Enterprise on Blade Servers. **NOTE: To modify this property, you must have Configure iDRAC permission. This object can be used only with remote or firmware (SSH or Telnet) RACADM and not with local RACADM or with earlier DRAC products.**
Legal Values	0 — (If the user of the first session has not responded for session sharing request by subsequent user. The next session user gets an access denied error after the default timeout value of 30 seconds.) 1 — (If the user of the first session has not responded for session sharing request by subsequent user. The next session user gets a read-only access after the default timeout value of 30 seconds.) 2 — (If the user of the first session has not responded for session sharing request by subsequent user. The next session user gets administrator access after default timeout value of 30 seconds.)
Default	0

cfgRacTunePluginType (Read or Write)

Table 192. Details of cfgRacTunePluginType

Description	To virtual console from browser, specifies the plug-in type.
Legal Values	• 0 = Use Active X /Native Plugin • 1 = Use Java Plugin
Default	0 = Active X /Native Plugin

ifcRacManagedNodeOs

This group contains properties that describe the managed server operating system. One instance of the group is allowed.

The following sections provide information about the objects in the ifcRacManagedNodeOs.

ifcRacMnOsHostname (Read Only)

Table 193. Details of ifcRacMnOsHostname

Description	The host name of the managed server.
Legal Values	A string of up to 255 characters.
Default	<blank>

ifcRacMnOsOsName (Read Only)

Table 194. Details of ifcRacMnOsOsName

Description	The operating system name of the managed server.

Legal Values	A string of up to 255 characters.
Default	<blank>

cfgRacVirtual

This group contains parameters to configure the iDRAC Virtual Media feature. One instance of the group is allowed.

The following sections provide information about the objects in the cfgRacVirtual.

cfgVirMediaAttached (Read or Write)

Table 195. Details of cfgVirMediaAttached

Description	This object is used to attach virtual devices to the system via the USB bus. When the devices are attached, the server recognizes valid USB mass storage devices attached to the system. Which is equivalent to attaching a local USB CDROM/floppy drive to a USB port on the system. When the devices are attached, they can be connected to the virtual devices remotely using iDRAC web interface or the CLI. Setting this object to 0 causes the devices to detach from the USB bus. **NOTE: Modifying this property does not impact the remote file sharing operation.**
Legal Values	• 0 = Detach • 1 = Attach • 2 = AutoAttach
Default	0

cfgVirtualBootOnce (Read or Write)

Table 196. Details of cfgVirtualBootOnce

Description	Enables or disables the Virtual Media Boot Once feature of iDRAC. If this property is enabled when the host server is rebooted, this feature attempts to start from the virtual media devices — if the appropriate media is installed in the device.
Legal Values	• 1 (TRUE) • 0 (FALSE)
Default	0

cfgVirMediaFloppyEmulation (Read or Write)

Table 197. Details of cfgVirMediaFloppyEmulation

Description	When set to 0, the virtual floppy drive is recognized as a removable disk by Windows operating systems. Windows operating systems assigns a drive letter that is C: or higher during enumeration. When set to 1, the Virtual Floppy drive is seen as a floppy drive by Windows operating systems. Windows operating systems assigns a drive letter of A: or B:. **NOTE: Virtual Media has to be reattached (using cfgVirMediaAttached) for this change to take effect.**
Legal Values	• 1 (TRUE) • 0(FALSE)

Default	0

cfgSDWriteProtect (Read Only)

Table 198. Details of cfgSDWriteProtect

Description	Displays if the physical write protect latch on the SD card is enabled or disabled. **NOTE: This command is deprecated from 12G iDRAC 1.0 release onwards. The functionality of this command is covered by `cfgVFlashSDWriteProtect`. While execution of the `cfgSDWriteProtect` command is successful, use the `cfgVFlashSDWriteProtect` command. For more information, see cfgVFlashwriteProtect (Read Only).**
Legal Values	• 1 (TRUE) • 0(FALSE)
Default	0

cfgServerInfo

This group allows you to select the BIOS first boot device and provides the option to start the selected device only once.

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

The following sections provide information about the objects in the `cfgServerInfo`.

cfgServerName (Read Or Write)

Table 199. Details of cfgServerName

Description	Displays the name of the specified server.
Legal Values	Maximum of 15 non-extended (ASCII characters (ASCII codes 32 through 126). For more information, see Guidelines to quote strings containing special character.
Default	SLOT — `<slot number>`

cfgServerNic3MacAddress (Read Only)

Table 200. Details of cfgServerNic3MacAddress

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

cfgServerNic4MacAddress (Read Only)

Table 201. Details of cfgServerNic4MacAddress

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

cfgServerDNSIMCName (Read or Write)

Table 202. Details of cfgServerDNSIMCName

Description	Displays the DNS domain name for iDRAC or IMC.
Legal Values	A valid string values
Default	None

cfgServerFirstBootDevice (Read or Write)

Table 203. Details of cfgServerFirstBootDevice

Description	Sets or displays the first boot device. You can also set a vFlash partition that is attached as a bootable device. For more information, see cfgVFlashPartitionOSVolLabel. **NOTE: If RFS is configured as the next boot device, during restart, the system starts normally and not from RFS.** **NOTE: First attach, to configure vFlash as First Boot Device. When a detached / non-existent vFlash partition or a nonstandard boot device is configured as first boot device, the following error message is displayed:** `Invalid object value`
Legal Values	• Normal • PXE • HDD • DIAG • CD-DVD • BIOS • vFDD • VCD-DVD • FDD • SD • F10 • F11 • UEFIDevicePath • UEFIHttp
Default	No-Override

cfgServerBootOnce (Read or Write)

Table 204. Details of cfgServerBootOnce

Description	Enables or disables the server start once feature.
Legal Values	• 1(True) • 0 (False)
Default	1(True)

cfgActiveDirectory

This group contains parameters to configure iDRAC Active Directory feature.

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

The following sections provide information about the objects in the `cfgActiveDirectory`.

cfgADSSOEnable (Read or Write)

Table 205. Details of cfgADSSOEnable

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

cfgADDomainController1 (Read or Write)

Table 206. Details of cfgADDomainController1

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

cfgADDomainController2 (Read or Write)

Table 207. Details of cfgADDomainController2

Description	To obtain user names, specify the LDAP server from which you want the iDRAC. This object is applicable only to iDRAC.
Legal Values	A string of up to 254 ASCII characters representing a valid IP address or a fully qualified domain name (FQDN).
Default	None

cfgADDomainController3 (Read or Write)

Table 208. Details of cfgADDomainController3

Description	To obtain user names, specify the LDAP server from which you want the iDRAC. This object is applicable only to iDRAC.
Legal Values	A string of up to 254 ASCII characters representing a valid IP address or a fully qualified domain name (FQDN).
Default	None

cfgADRacName (Read or Write)

Table 209. Details of cfgADRacName

Description	Name of iDRAC as recorded in the Active Directory forest.

Legal Values	Any printable text string of up to 254 characters, with no white space.
Default	<blank>

cfgADRacDomain (Read or Write)

Table 210. Details of cfgADRacDomain

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

cfgADAuthTimeout (Read or Write)

Table 211. Details of cfgADAuthTimeout

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

cfgADEnable (Read or Write)

Table 212. Details of cfgADEnable

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

cfgADType (Read or Write)

Table 213. Details of cfgADType

Description	To use the Active Directory, determine the schema type.
Legal Values	• 1— (Enables Active Directory with the extended schema) • 2— (Enables Active Directory with the standard schema)
Default	1

cfgADGlobalCatalog1 (Read or Write)

Table 214. Details of cfgADGlobalCatalog1

Description	To obtain user names, specify the Global Catalog server from which you want the iDRAC.

This object is applicable only to iDRAC.

Legal Values	A string of up to 254 ASCII characters representing a valid IP address or a fully qualified domain name (FQDN).
Default	None

cfgADGlobalCatalog2 (Read or Write)

Table 215. Details of cfgADGlobalCatalog2

Description	To obtain user names, specify the Global Catalog server from which you want the iDRAC. This object is applicable only to iDRAC.
Legal Values	A string of up to 254 ASCII characters representing a valid IP address or a fully qualified domain name (FQDN).
Default	None

cfgADGlobalCatalog3 (Read or Write)

Table 216. Details of cfgADGlobalCatalog3

Description	To obtain user names, specify the Global Catalog server from which you want the iDRAC. This object is applicable only to iDRAC.
Legal Values	A string of up to 254 ASCII characters representing a valid IP address or a fully qualified domain name (FQDN).
Default	None

cfgADCertValidationEnable (Read or Write)

Table 217. 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

cfgADDcSRVLookupEnable (Read or Write)

Table 218. Details of cfgADDcSRVLookupEnable

Description	Configures iDRAC 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`. iDRAC does not failover to the specified domain controllers when DNS lookup is unsuccessful or none of the servers returns to the DNS lookup works. This object is applicable only to iDRAC.
Legal Values	• 1 (TRUE) — use DNS to look up domain controllers • 0 (FALSE) — use pre-configured domain controllers
Default	0

cfgADDcSRVLookupbyUserdomain (Read or Write)

Table 219. Details of cfgADDcSRVLookupbyUserdomain

Description	Chooses the way the user domain is looked up for Active Directory. This object is applicable only to iDRAC.
Legal Values	• 1 (TRUE) — use user domain as the search domain to look up DCs. The user domain is chosen from either the user domain list or by entering into the user login. • 0 (FALSE) — use the configured search domain cfgADDcSrvLookupDomainName to look up DCs.
Default	1

cfgADDcSRVLookupDomainName (Read or Write)

Table 220. Details of cfgADDcSRVLookupDomainName

Description	Use the Active Directory Domain when cfgAddcSrvLookupbyUserDomain is set to 0. This object is applicable only to iDRAC.
Legal Values	String. Maximum length = 254
Default	Null

cfgADGcSRVLookupEnable (Read or Write)

Table 221. Details of cfgADGcSRVLookupEnable

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

cfgADGcRootDomain (Read or Write)

Table 222. Details of cfgADGcRootDomain

Description	The names of the Active Directory root domain used for DNS look up, to locate Global Catalog servers. This object is applicable only to iDRAC.
Legal Values	String. Maximum length = 254
Default	Null

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.

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

cfgLDAPBaseDN (Read or Write)

Table 223. Details of cfgLDAPBaseDN

Description	The domain name of the branch of the directory where all searches must start.
Legal Values	String. Maximum length = 254
Default	Null

cfgLDAPBindPassword (Write Only)

Table 224. Details of cfgLDAPBindPassword

Description	A bind password is used with the bindDN. The bind password is a sensitive data, and must be protected. It is optional to support anonymous bind.
Legal Values	String maximum length = 254
Default	Null

cfgLDAPCertValidationEnable (Read or Write)

Table 225. Details of cfgLDAPCertValidationEnable

Description	Controls certificate validation during SSL handshake.
Legal Values	• 1 (TRUE) — Uses the CA certificate to validate the LDAP server certificate during SSL handshake. • 0 (FALSE) —Skips the certificate validation step of SSL handshake.
Default	1

cfgLDAPBindDN (Read or Write)

Table 226. 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. If necessary It is optional to support anonymous bind. **NOTE: If `cfgLDAPBindDN` is [null] and `cfgLDAPBindPassword` is [null], then the iDRAC attempts an anonymous bind.**
Legal Values	String maximum length = 254
Default	Null

cfgLDAPEnable (Read or Write)

Table 227. Details of cfgLDAPEnable

Description	Enables or disables LDAP service. If this property is disabled, local iDRAC authentication is used for user logins.
Legal Values	• 1 — Enable • 0 — Disable

Default	0

cfgLDAPGroupAttribute (Read or Write)

Table 228. Details of cfgLDAPGroupAttribute

Description	Specifies which LDAP attribute is used to check for group membership. It must be an attribute of the group class. If not specified then the member and unique member attributes are used.
Legal Values	String maximum length = 254
Default	Null

cfgLDAPGroupAttributeIsDN (Read or Write)

Table 229. Details of cfgLDAPGroupAttributeIsDN attribute

Description	When it is set to `1`, iDRAC compares the `userDN` retrieved from the directory to compare to the members of the group. If it is set to `0`, the user name provides the login user to compare to the members of the group. It does not affect the search algorithm for the bind. iDRAC always searches the `userDN` and uses the `userDN` to bind.
Legal Values	• `1`(TRUE) — Use the `userDN` from the LDAP Server • `0`(FALSE) — Use the `userDN` to provide the login user
Default	1

cfgLDAPPort (Read or Write)

Table 230. Details of cfgLDAPPort

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

cfgLDAPSearchFilter (Read or Write)

Table 231. Details of cfgLDAPSearchFilter

Description	To validate LDAP search filter, use the user attribute that 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 = 254 characters
Default	(objectless=*) Searches for all objects in tree.

cfgLDAPServer (Read or Write)

Table 232. 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 = 1024
Default	Null

cfgLDAPUserAttribute (Read or Write)

Table 233. Details of cfgLDAPUserAttribute

Description	To search for, specify the user attribute. 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 is unsuccessful with error.
Legal Values	String. Maximum length = 254
Default	Null

cfgLdapRoleGroup

This group allows the user to configure role groups for LDAP.

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

`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 iDRAC privilege map

Each LDAP-authenticated user assumes the total set of iDRAC 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 that DNs.

The following sections provide information about the objects in the `cfgLdapRoleGroup`.

cfgLdapRoleGroupDN (Read or Write)

Table 234. Details of cfgLdapRoleGroupDN

Description	It is the Domain Name of the group in this index.
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 or Write)

Table 235. 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
```

cfgStandardSchema

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

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

The following sections provide information about the objects in the `cfgStandardSchema`.

cfgSSADRoleGroupDomain (Read or Write)

Table 236. 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>`

cfgSSADRoleGroupIndex (Read Only)

Table 237. Details of cfgSSADRoleGroupIndex

Description	Index of the Role Group as recorded in the Active Directory.
Legal Values	An integer from 1 to 5
Default	`<instance>`

cfgSSADRoleGroupName (Read or Write)

Table 238. 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>`

cfgSSADRoleGroupPrivilege (Read or Write)

Table 239. 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 to 0x000001ff
Default	`<blank>`

- **Example**

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

```
# cfgSSADRoleGroupIndex=1
cfgSSADRoleGroupName=blsys-1
cfgSSADRoleGroupDomain=
cfgSSADRolGroupPrivilege=3081
```

Table 240. Bit masks for Role Group privileges

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

cfgThermal

This group displays and configures the thermal settings. Use this object with the `config` or `getconfig` subcommands.

To set the configurations, you must have the **Chassis Configuration Administrator** privileges.

cfgThermalEnhancedCoolingMode (Read or Write)

Table 241. Details of cfgThermalEnhancedCoolingMode

Description	Configures the enhanced cooling mode.
Legal Values	• `1` — Enabled • `0` — Disabled
Default	0 — Disabled

cfgIpmiSol

This group is used to configure the Serial Over LAN (SOL) capabilities of the system.

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

cfgIpmiSolEnable (Read or Write)

Table 242. Details of cfgIpmiSolEnable

Description	Enables or disables SOL.

Legal Values	• 1(TRUE) • 0(FALSE)
Default	1

cfgIpmiSolBaudRate (Read or Write)

Table 243. Details of cfgIpmiSolBaudRate

Description	Specifies baud rate for serial communication over LAN.
Legal Values	9600, 19200, 57600, 115200
Default	115200

cfgIpmiSolMinPrivilege (Read or Write)

Table 244. Details of cfgIpmiSolMinPrivilege

Description	Specifies the minimum privilege level required for SOL access.
Legal Values	• 2(User) • 3(Operator) • 4(Administrator)
Default	4

cfgIpmiSolAccumulateInterval (Read or Write)

Table 245. Details of cfgIpmiSolAccumulateInterval

Description	Specifies the typical amount of time that iDRAC waits before transmitting a partial SOL character data packet. This value is *1-based 5ms* increments.
Legal Values	1–255
Default	10

cfgIpmiSolSendThreshold (Read or Write)

Table 246. Details of cfgIpmiSolSendThreshold

Description	To buffer before sending an SOL data packet, specify the SOL threshold limit value and the maximum number of bytes.
Legal Values	1–255
Default	255

cfgIpmiLan

This group is used to configure the IPMI over LAN capabilities of the system.

The following sections provide information about the objects in the `cfgIpmiLan` group.

cfgIpmiLanEnable (Read or Write)

Table 247. Details of cfgIpmiLanEnable

Description	Enables or disables the IPMI over LAN interface.
Legal Values	• 1(TRUE) • 0(FALSE)
Default	0

cfgIpmiLanPrivLimit (Read or Write)

Table 248. Details of cfgIpmiLanPrivLimit

Description	Specifies the maximum privilege level allowed for IPMI over LAN access.
Legal Values	• 2(User) • 3(Operator) • 4(Administrator)
\Default	4

cfgIpmiLanAlertEnable (Read or Write)

Table 249. Details of cfgIpmiLanAlertEnable

Description	Enables or disables global email alerting. This property overrides all individual email alerting enable or disable properties.
Legal Values	• 1(TRUE) • 0(FALSE)
Default	0

cfgIpmiLanEncryptionKey (Read or Write)

Table 250. Details of cfgIpmiLanEncryptionKey

Description	Specifies the IPMI encryption key.
Legal Values	A string of hexadecimal digits from 0 to 40 characters with no spaces. Only an even number of digits is allowed.
Default	0000000000000000000000000000000000000000

cfgIpmiLanPetCommunityName (Read or Write)

Table 251. Details of cfgIpmiLanPetCommunityName

Description	Specifies the SNMP community name for traps.
Legal Values	A string of up to 18 characters.
Default	public

cfgIpmiPetIpv6

This group is used to configure IPv6 platform event traps on the managed server.

The following sections provide information about the objects in the `cfgIpmiPetIpv6` group.

cfgIpmiPetIPv6Index (Read Only)

Table 252. Details of cfgIpmiPetIPv6Index

Description	Unique identifier for the index corresponding to the trap.
Legal Values	1–4
Default	`<index Values>`

cfgIpmiPetIPv6AlertDestIpAddr

Table 253. Details of cfgIpmiPetIPv6AlertDestIpAddr

Description	Configures the IPv6 alert destination IP address for the trap.
Legal Values	IPv6 address
Default	`<blank>`

cfgIpmiPetIPv6AlertEnable (Read or Write)

Table 254. Details of cfgIpmiPetIPv6AlertEnable

Description	Enables or disables the IPv6 alert destination for the trap.
Legal Values	• `1` (TRUE) • `0` (FALSE)
Default	0

cfgIpmiPef

This group is used to configure the platform event filters available on the managed server.

The event filters can be used to control policy related to actions that are triggered when critical events occur on the managed server.

The following sections provide information about the objects in the `cfgIpmiPef` group.

cfgIpmiPefName (Read Only)

Table 255. Details of cfgIpmiPefName

Description	Specifies the name of the platform event filter.
Legal Values	A string of up to 255 characters.
Default	The name of the index filter.

cfgIpmiPefIndex (Read or Write)

Table 256. Details of cfgIpmiPefIndex

Description	Specifies the index of a specific platform event filter.
Legal Values	• For iDRAC on Rack and Tower Servers: 1–22 • For iDRAC Enterprise on Blade Servers: 1–9
Default	The index value of a platform event filter object.

cfgIpmiPefAction (Read or Write)

Table 257. Details of cfgIpmiPefAction

Description	Specifies the action that is performed on the managed server when the alert is triggered. **NOTE: For iDRAC on Rack and Tower servers, this object is read-only for indexes 20, 21, and 22.**
Legal Values	• 0 (None) • 1 (Power Down) • 2(Reset) • 3(Power Cycle)
Default	0

cfgIpmiPefEnable (Read or Write)

Table 258. Details of cfgIpmiPefEnable

Description	Enables or disables a specific platform event filter.
Legal Values	• 1(TRUE) • 0(FALSE)
Default	1

cfgIpmiPet

This group is used to configure platform event traps on the managed server.

The following sections provide information about the objects in the `cfgIpmiPet` group.

cfgIpmiPetIndex (Read Only)

Table 259. Details of cfgIpmiPetIndex

Description	Unique identifier for the index corresponding to the trap.
Legal Values	1–4
Default	The index value of a specific platform event trap.

cfgIpmiPetAlertDestIpAddr (Read/Write)

Table 260. Details of cfgIpmiPetAlertDestIpAddr

Description	Specifies the destination IPv4 address for the trap receiver on the network. The trap receiver receives an SNMP trap when an event is triggered on the managed server.
Legal Values	A string representing a valid IPv4 address. For example, `192.168.0.67`.
Default	0.0.0.0

cfgIpmiPetAlertEnable (Read or Write)

Table 261. Details of cfgIpmiPetAlertEnable

Description	Enables or disables a specific trap.
Legal Values	• `1` (TRUE) • `0` (FALSE)
Default	0

cfgUserDomain

This group is used to configure the Active Directory user domain names. A maximum of 40 domain names can be configured at any given time.

The following sections provide information about the objects in the `cfgUserDomain` group.

cfgUserDomainIndex (Read Only)

Table 262. Details of cfgUserDomainIndex

Description	Represents a specific domain.
Legal Values	1–40
Default	The index value.

cfguserdomainname (Read Only)

Table 263. Details of cfguserdomainname

Description	Specifies the Active Directory user domain name.
Legal Values	A string of up to 254 ASCII characters
Default	`<blank>`

cfgServerPower

This group provides several power management features.

The following sections provide information about the objects in the `cfgServerPower` group.

cfgServerPowerStatus (Read Only)

Table 264. Details of cfgServerPowerStatus

Description	Represents the server power state, either ON or OFF.
Legal Values	• 1 (ON) • 0 (OFF)
Default	0

cfgServerPowerAllocation (Read Only)

Table 265. Details of cfgServerPowerAllocation

Description	Represents the available allocated power supply for server usage. **NOTE: If there is more than one power supply, this object represents the minimum capacity power supply.** **NOTE: This object is applicable only for iDRAC Enterprise on Rack and Tower Servers and not for iDRAC on Blade Servers.**
Legal Values	A string of up to 32 characters
Default	<blank>

cfgServerActualPowerConsumption (Read Only)

Table 266. Details of cfgServerActualPowerConsumption

Description	Represents the power consumption by the server at the current time.
Legal Values	Not applicable
Default	<blank>

cfgServerPowerCapEnable (Read or Write)

Table 267. Details of cfgServerPowerCapEnable

Description	Enables or disables the user specified power budget threshold. This object is Read only for iDRAC Enterprise on Blade Servers.
Legal Values	• 0 — Disables the user specified power budget threshold • 1 — Enables the user specified power budget threshold
Default	1

cfgServerMinPowerCapacity (Read Only)

Table 268. Details of cfgServerMinPowerCapacity

Description	Represents the minimum server power capacity on a blade based on the current component inventory.

Legal Values	Not applicable
Default	<blank>

cfgServerMaxPowerCapacity (Read Only)

Table 269. Details of cfgServerMaxPowerCapacity

Description	Represents the maximum server power capacity based on the current component consumption.
Legal Values	Not applicable
Default	<blank>

cfgServerPeakPowerConsumption (Read Only)

Table 270. Details of cfgServerPeakPowerConsumption

Description	Represents the server's maximum power consumption until the current time.
Legal Values	Not applicable
Default	Peak power consumption of the server

cfgServerPeakPowerConsumptionTimestamp (Read Only)

Table 271. Details of cfgServerPeakPowerConsumptionTimestamp

Description	Specifies time when the maximum power consumption was recorded.
Legal Values	A string of up to 32 characters.
Default	Timestamp of the peak power consumption of the server.

cfgServerPowerConsumptionClear (Write Only)

Table 272. Details of cfgServerPowerConsumptionClear

Description	Clears the current recorded power statistics.
Legal Values	1 — Clears the Power Consumption Statistics
Default	None

cfgServerPowerCapWatts (Read or Write)

Table 273. Details of cfgServerPowerCapWatts

Description	Represents the server power threshold in Watts. **NOTE: This value is applicable only if the `cfgServerPowerCapEnable` is set to `1`.**
Legal Values	None

Default	Server power threshold in Watts.

cfgServerPowerCapBtuhr (Read or Write)

Table 274. Details of cfgServerPowerCapBtuhr

Description	Represents the server power threshold in BTU/hr. **NOTE: This value is applicable only if `cfgServerPowerCapEnable` is set to `1`.**
Legal Values	None
Default	Server power threshold in BTU/hr.

cfgServerPowerCapPercent (Read or Write)

Table 275. Details of cfgServerPowerCapPercent

Description	Represents the server power threshold in percentage. **NOTE: This value is applicable only if `cfgServerPowerCapEnable` is set to `1`.**
Legal Values	None
Default	Server power threshold in percentage.

cfgServerPowerLastHourAvg (Read Only)

Table 276. Details of cfgServerPowerLastHourAvg

Description	Displays the average power value during the last hour.
Legal Values	None
Default	Average power value during the last hour.

cfgServerPowerLastDayAvg (Read Only)

Table 277. Details of cfgServerPowerLastDayAvg

Description	Displays the average power value during the last day.
Legal Values	None
Default	Average power value during the last day.

cfgServerPowerLastWeekAvg (Read Only)

Table 278. Details of cfgServerPowerLastWeekAvg

Description	Displays the average power value during the last week.
Legal Values	None

Default	Average power value during the last week.

cfgServerPowerLastHourMinPower (Read Only)

Table 279. Details of cfgServerPowerLastHourMinPower

Description	Displays the minimum power value during the last hour.
Legal Values	Not applicable
Default	Minimum power value during the last hour.

cfgServerPowerLastHourMinTime (Read Only)

Table 280. Details of cfgServerPowerLastHourMinTime

Description	Displays the timestamp of minimum power value during the last minute.
Legal Values	Time in the format: DD MM Date HH:MM:SS YYYY cfgServerPowerLastHourMinTime=Mon Sep 26 19:10:56 2011 where, • DD= Day of the week • MM= Month • Date=Date • YYYY = Year • HH = hour • MM=Minutes • SS = Seconds
Default	Minimum power value during the last minute.

cfgServerPowerLastHourMaxPower (Read Only)

Table 281. Details of cfgServerPowerLastHourMaxPower

Description	Displays the maximum power value during the last hour.
Legal Values	Not applicable
Default	Maximum power value during the last hour.

cfgServerPowerLastHourMaxTime (Read Only)

Table 282. Details of cfgServerPowerLastHourMaxTime

Description	Displays the timestamp of maximum power value during the last hour.
Legal Values	Time in the format: DD MM Date HH:MM:SS YYYY where, • DD= Day of the week • MM= Month • Date=Date

- YYYY = Year
- HH = hour
- MM=Minutes
- SS = Seconds

Default Maximum power value during the last hour.

cfgServerPowerLastDayMinPower (Read Only)

Table 283. Details of cfgServerPowerLastDayMinPower

Description Displays the minimum power value during the last day.

Legal Values Not applicable

Default Minimum power value during the last day.

cfgServerPowerLastDayMinTime (Read Only)

Table 284. Details of cfgServerPowerLastDayMinTime

Description Displays the timestamp of minimum power value during the last day.

Legal Values Time in the format: DD MM Date HH:MM:SS YYYY

where,

- DD = Day of the week
- MM = Month
- Date = Date
- YYYY = Year
- HH = hour
- MM = Minutes
- SS = Seconds

Default Timestamp of the minimum power value during the last day.

cfgServerPowerLastDayMaxPower (Read Only)

Table 285. Details of cfgServerPowerLastDayMaxPower

Description Displays the maximum power value during the last day.

Legal Values Not applicable

Default Maximum power value during the last day.

cfgServerPowerLastDayMaxTime (Read Only)

Table 286. Details of cfgServerPowerLastDayMaxTime

Description Displays the timestamp of maximum power value during the last day.

Legal Values Time in the format: DD MM Date HH:MM:SS YYYY

where,

- DD = Day of the week
- MM = Month
- Date = Date
- YYYY = Year
- HH = hour
- MM = Minutes
- SS = Seconds

Default Timestamp of the maximum power value during the last day.

cfgServerPowerLastWeekMinPower (Read Only)

Table 287. Details of cfgServerPowerLastWeekMinPower

Description Displays the minimum power value during the last week.

Legal Values Not applicable

Default Minimum power value during the last week.

cfgServerPowerLastWeekMinTime (Read Only)

Table 288. Details of cfgServerPowerLastWeekMinTime

Description Displays the timestamp of minimum power value during the last week.

Legal Values A string of up to 32 characters.

Time in the format: DD MM Date HH:MM:SS YYYY

where,

- DD = Day of the week
- MM = Month
- Date = Date
- YYYY = Year
- HH = hour
- MM = Minutes
- SS = Seconds

Default Timestamp of the minimum power value during the last week.

cfgServerPowerLastWeekMaxPower (Read Only)

Table 289. Details of cfgServerPowerLastWeekMaxPower

Description Displays the maximum power value during the last week.

Legal Values None

Default Maximum power value during the last week.

cfgServerPowerLastWeekMaxTime (Read Only)

Table 290. Details of cfgServerPowerLastWeekMaxTime

Description	Displays the timestamp of maximum power value during the last week.
Legal Values	A string of up to 32 characters. Time in the format: DD MM Date HH:MM:SS YYYY where, • DD = Day of the week • MM= Month • Date = Date • YYYY = Year • HH = hour • MM = Minutes • SS = Seconds
Default	Timestamp of the maximum power value during the last week.

cfgServerPowerInstHeadroom (Read Only)

Table 291. Details of cfgServerPowerInstHeadroom

Description	Displays the difference between the available power and the current power consumption. This object is applicable only for iDRAC on Rack and Tower Servers and not for iDRAC Enterprise on Blade Servers.
Legal Values	Not applicable
Default	Difference between the available power and the current power consumption.

cfgServerPowerPeakHeadroom (Read Only)

Table 292. Details of cfgServerPowerInstHeadroom

Description	Displays the difference between the available power and the peak power consumption. This object is applicable only for iDRAC on Rack and Tower Servers and not for iDRAC Enterprise on Blade Servers.
Legal Values	None
Default	Difference between the available power and the peak power consumption.

cfgServerActualAmperageConsumption (Read Only)

Table 293. Details of cfgServerActualAmperageConsumption

Description	Displays the current power consumption.
Legal Values	Not applicable
Default	Current power consumption.

cfgServerPeakAmperage (Read Only)

Table 294. Details of cfgServerPeakAmperage

Description	Displays the current peak power consumption.
Legal Values	Not applicable
Default	Current peak power consumption.

cfgServerPeakAmperageTimeStamp (Read Only)

Table 295. Details of cfgServerPeakAmperageTimeStamp

Description	Displays the timestamp of the current peak power consumption.
Legal Values	A string of up to 32 characters. Time in the format: DD MM Date HH:MM:SS YYYY where, • DD = Day of the week • MM = Month • Date = Date • YYYY = Year • HH = hour • MM = Minutes • SS = Seconds
Default	Timestamp of the current peak power consumption.

cfgServerCumulativePowerConsumption (Read Only)

Table 296. Details of cfgServerCumulativePowerConsumption

Description	Displays the cumulative power consumption.
Legal Values	Not applicable
Default	Cumulative power consumption.

cfgServerCumulativePowerConsumptionTimeStamp (Read Only)

Table 297. Details of cfgServerCumulativePowerConsumptionTimeStamp

Description	Displays the timestamp of the cumulative power consumption.
Legal Values	A string of up to 32 characters. Time in the format: DD MM Date HH:MM:SS YYYY where, • DD = Day of the week • MM= Month • Date=Date

- YYYY = Year
- HH = hour
- MM=Minutes
- SS = Seconds

Default Timestamp of the cumulative power consumption.

cfgServerCumulativePowerClear (Write Only)

Table 298. Details of cfgServerCumulativePowerClear

Description	Clears the `cfgServerCumulativePowerConsumption` and `cfgServerCumulativePowerConsumptionTimeStamp` values.
Legal Values	1
Default	None

cfgServerPowerPCIeAllocation (Read or Write)

Table 299. Details of cfgServerPowerPCIeAllocation

Description	Amount of power allocated to the PCIe cards. This object is applicable for iDRAC Enterprise only for specific Blade Servers and not for iDRAC on Rack and Tower Servers. You must have the Administrator privileges to modify the value for this object.
Legal Values	0 W: For platforms that do not support PCIe cards. 100 W — 500 W: For platforms that support PCIe cards.
Default	0: For platforms that do not support PCIe cards. 500 W: For platforms that support PCIe cards.

cfgServerPowerSupply

This group contains information related to the power supplies.

The `cfgServerPowerSupply` object group is applicable only for iDRAC on Rack and Tower Servers and not for iDRAC Enterprise on Blade Servers.

NOTE: The `getconfig` subcommand always shows eight `cfgServerPowerSupply` indexes, even if two power supplies are installed in the system or the system supports a maximum of two PSUs. For the uninstalled and unsupported units, all the objects in the `cfgServerPowerSupply` group displays a value of `0`.

The following sections provide information about the objects in the `cfgServerPowerSupply` group.

cfgServerPowerSupplyCurrentDraw (Read Only)

Table 300. Details of cfgServerPowerSupplyCurrentDraw

Description	Displays the instantaneous current consumption in 0.1 amps.
Legal Values	A string of up to 32 characters.
Default	0

cfgServerPowerSupplyFwVer (Read Only)

Table 301. Details of cfgServerPowerSupplyFwVer

Description	Displays the firmware version of the PSU, in the format x.xx.xxx.
Legal Values	A string up to 8 characters.
Default	Null

cfgServerPowerSupplyIndex

Table 302. Details of cfgServerPowerSupplyIndex

Description	Specifies index of the PSU. **NOTE: Indexes 1–8 are supported to support up to 8 PSUs. If any PSU is not present then `cfgServerPowerSupplyOnlineStatus` does not exist and for all the other properties, it is 0.**
Legal Values	Integer 1–8
Default	None

cfgServerPowerSupplyMaxInputPower (Read Only)

Table 303. Details of cfgServerPowerSupplyMaxInputPower

Description	Displays the AC input rated power in Watts.
Legal Values	A string of up to 32 characters.
Default	0

cfgServerPowerSupplyMaxOutputPower (Read Only)

Table 304. Details of cfgServerPowerSupplyMaxOutputPower

Description	Displays the AC output rated power in Watts.
Legal Values	A string of up to 32 characters.
Default	0

cfgServerPowerSupplyOnlineStatus (Read Only)

Table 305. Details of cfgServerPowerSupplyOnlineStatus

Description	Displays the status of the PSU.
Legal Values	• 0 — Present • 1 — Absent • 2 — Failure • 3 — Predictive failure
Default	0 — Present

cfgServerPowerSupplyType

Table 306. Details of cfgServerPowerSupplyType

Description	Displays whether the power supply is AC or DC.
Legal Values	A string of up to 32 characters.
Default	0

cfgIPv6LanNetworking

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

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

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

cfgIPv6Enable (Read or Write)

Table 307. Details of cfgIPv6Enable

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

cfgIPv6Address1 (Read or Write)

Table 308. Details of cfgIPv6Address1

Description	Specifies iDRAC IPv6 address.
Legal Values	String representing a valid IPv6 entry.
Default	::

cfgIPv6Gateway (Read or Write)

Table 309. Details of cfgIPv6Gateway

Description	iDRAC gateway IPv6 address.
Legal Values	Specifies string representing a valid IPv6 entry.
Default	" :: "

cfgIPv6AutoConfig (Read or Write)

Table 310. Details of cfgIPv6AutoConfig

Description	Enables or disables the `IPv6 Auto Configuration` option.

NOTE: If this value is set to `0`, the iDRAC disables auto configuration and statically assigns IPv6 addresses. If this value is set to `1`, the iDRAC obtains address and route information using stateless `auto configuration` and `DHCPv6`.

NOTE: The iDRAC uses its MAC address for its DUID (DUID-LL) when communicating with a DHCPv6 server.

Legal Values	• 1 (TRUE) • 0 (FALSE)
Default	0

cfgIPv6PrefixLength (Read or Write)

Table 311. Details of cfgIPv6PrefixLength

Description	Specifies the prefix length for IPv6 address. **NOTE:** • **This property can be configured even when `cfgIPv6AutoConfig` is enabled.**
Legal Values	1–128
Default	64

cfgIPv6LinkLocalAddress (Read Only)

Table 312. Details of cfgIPv6LinkLocalAddress

Description	The iDRAC IPv6 link local address.
Legal Values	Specifies a string representing a valid IPv6 entry.
Default	:

cfgIPv6Address2 (Read Only)

Table 313. Details of cfgIPv6Address2

Description	The iDRAC IPv6-second address.
Legal Values	A string representing a valid IPv6 entry.
Default	:

cfgIPv6Address3 (Read Only)

Table 314. Details of cfgIPv6Address3

Description	The iDRAC IPv6 third address.
Legal Values	String representing a valid IPv6 entry.
Default	:

cfgIPv6Address4 (Read Only)

Table 315. Details of cfgIPv6Address4

Description	The iDRAC IPv6 fourth address.
Legal Values	String representing a valid IPv6 entry.
Default	:

cfgIPv6Address5 (Read Only)

Table 316. Details of cfgIPv6Address5

Description	The iDRAC IPv6 fifth address.
Legal Values	String representing a valid IPv6 entry.
Default	:

cfgIPv6Address6 (Read Only)

Table 317. Details of cfgIPv6Address6

Description	The iDRAC IPv6 sixth address.
Legal Values	String representing a valid IPv6 entry.
Default	:

cfgIPv6Address7 (Read Only)

Table 318. Details of cfgIPv6Address7

Description	The iDRAC IPv6 seventh address.
Legal Values	String representing a valid IPv6 entry.
Default	:

cfgIPv6Address8 (Read Only)

Table 319. Details of cfgIPv6Address8

Description	The iDRAC IPv6 eighth address.
Legal Values	String representing a valid IPv6 entry.
Default	:

cfgIPv6Address9 (Read Only)

Table 320. Details of cfgIPv6Address9

Description	The iDRAC IPv6 ninth address.
Legal Values	String representing a valid IPv6 entry.
Default	:

cfgIPv6Address10 (Read Only)

Table 321. Details of cfgIPv6Address10

Description	The iDRAC IPv6 tenth address.
Legal Values	String representing a valid IPv6 entry.
Default	:

cfgIPv6Address11 (Read Only)

Table 322. Details of cfgIPv6Address11

Description	The iDRAC IPv6 eleventh address.
Legal Values	String representing a valid IPv6 entry.
Default	:

cfgIPv6Address12 (Read Only)

Table 323. Details of cfgIPv6Address12

Description	The iDRAC IPv6 twelfth address.
Legal Values	String representing a valid IPv6 entry.
Default	:

cfgIPv6Address13 (Read Only)

Table 324. Details of cfgIPv6Address13

Description	The iDRAC IPv6 thirteenth address.
Legal Values	String representing a valid IPv6 entry.
Default	:

cfgIPv6Address14 (Read Only)

Table 325. Details of cfgIPv6Address14

Description	The iDRAC IPv6 fourteenth address.
Legal Values	String representing a valid IPv6 entry.
Default	:

cfgIPv6Address15 (Read Only)

Table 326. Details of cfgIPv6Address15

Description	The iDRAC IPv6 fifteenth address.
Legal Values	String representing a valid IPv6 entry.
Default	:

cfgIPv6DNSServer1 (Read or Write)

Table 327. 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	" :: "

cfgIPv6DNSServersFromDHCP6 (Read or Write)

Table 328. Details of cfgIPv6DNSServersFromDHCP6

Description	Specifies whether `cfgIPv6DNSServer1` and `cfgIPv6DNSServer2` are `static` or `DHCP IPv6 addresses`. **NOTE: This property is used only if `cfgIPv6AutoConfig` is set to `1`(true).**
Legal Values	`1` (TRUE) `0` (FALSE)
Default	`0`

cfgIpv6StaticLanNetworking

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

cfgIPv6StaticEnable (Read or Write)

Table 329. Details of cfgIPv6StaticEnable

Description	Enables or disables the static IPv6 stack.
Legal Values	• 0 — Disabled • 1 — Enabled
Default	0 — Disabled

NOTE: If this object is modified, then the object `cfgIPv6Enable` is also modified.

cfgIPv6StaticAddress1 (Read or Write)

Table 330. Details of cfgIPv6StaticAddress1

Description	Returns or sets the static IPv6 address1. **NOTE: Only set the current IPv4 address if `cfgNicUseDhcp` is set to 0 (false).**
Legal Values	Any IPv6 address
Default	

cfgIPv6StaticGateway (Read or Write)

Table 331. Details of cfgIPv6StaticGateway

Description	Returns or sets gateway static IPv6 address.
Legal Values	Any IPv6 address
Default	

cfgIPv6StaticPrefixLength (Read or Write)

Table 332. Details of cfgIPv6StaticPrefixLength

Description	The prefix length for static IPv6 address 1.
Legal Values	0–128
Default	64

cfgIPv6StaticAutoConfig (Read/Write)

Table 333. Details of cfgIPv6StaticAutoConfig

Description	Enables or disables the static IPv6 AutoConfig option.
Legal Values	• 0 — Disabled • 1 — Enabled
Default	1 — Enabled

NOTE: If this object is modified, then the object `cfgIPv6Autoconfig` is also modified.

cfgIPv6StaticDNSServersFromDHCP6 (Read or Write)

Table 334. Details of cfgIPv6StaticDNSServersFromDHCP6

Description	Specifies the DNS server static IP addresses.
Legal Values	• 0 — DNS Server must be configured as static. • 1 — The device will get the DNS servers from DHCPv6.
Default	0 — Disabled

cfgIPv6StaticDNSServer1 (Read or Write)

Table 335. Details of cfgIPv6StaticDNSServer1

Description	Specifies the DNS server 1 static IPv6 address.
Legal Values	Any IPv6 Address
Default	

cfgIPv6StaticDNSServer2 (Read or Write)

Table 336. Details of cfgIPv6StaticDNSServer2

Description	Specifies the DNS server 2 static IPv6 address.
Legal Values	Any IPv6 address
Default	

cfgIPv6DNSServer2 (Read or Write)

Table 337. Details of cfgIPv6DNSServer2

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

Example

```
$ racadm getconfig -g cfgIPv6LanNetworking

cfgIPv6Enable=1

cfgIPv6AutoConfig=1

cfgIPv6Address=::

cfgIPv6PrefixLength=64

cfgIPv6Gateway=::

cfgIPv6DNSServersFromDHCP6=1

cfgIPv6DNSServer1=::

cfgIPv6DNSServer2=::
```

If both IPv4 and IPv6 are enabled on the iDRAC, IPv6 DNS servers take priority. The order of preference for DNS servers is:

- `cfgIPv6DNSServer1`
- `cfgIPv6DNSServer2`
- `cfgDNSServer1`
- `cfgDNSServer2`

cfgIPv6URL

This group specifies properties used to configure iDRAC IPv6 URL.

The following sections provide information about the objects in the `cfgIPv6URL` group.

cfgIPv6URLstring (Read Only)

Table 338. Details of cfgIPv6URLstring

Description	The iDRAC IPv6 URL.
Legal Values	A string of up to 80 characters.
Default	`<blank>`

cfgIpmiSerial

This group specifies properties used to configure the IPMI serial interface of the BMC.

It is applicable only for iDRAC on Rack and Tower Servers and not for iDRAC Enterprise on Blade Servers.

cfgIpmiSerialBaudRate (Read or Write)

Table 339. Details of cfgIpmiSerialBaudRate

Description	Specifies the baud rate for a serial connection over IPMI.
Legal Values	9600, 19200, 57600, 115200

Default	57600

cfgIpmiSerialChanPrivLimit (Read or Write)

Table 340. Details of cfgIpmiSerialChanPrivLimit

Description	Specifies the maximum privilege level allowed on the IPMI serial channel.
Legal Values	• 2 (User) • 3 (Operator) • 4 (Administrator)
Default	4

cfgIpmiSerialConnectionMode (Read or Write)

Table 341. Details of cfgIpmiSerialConnectionMode

Description	When the iDRAC `cfgSerialConsoleEnable` property is set to 0(disabled), the iDRAC serial port becomes the IPMI serial port. This property determines the IPMI defined mode of the serial port. In Basic mode, the port uses binary data with the intent of communicating with an application program on the serial client. In Terminal mode, the port assumes that a dumb ASCII terminal is connected and allows simple commands to be entered.
Legal Values	• 0(Terminal) • 1(Basic)
Default	1

cfgIpmiSerialDeleteControl (Read or Write)

Table 342. Details of cfgIpmiSerialDeleteControl

Description	Enables or disables delete control on the IPMI serial interface.
Legal Values	• 0 (FALSE) • 1 (TRUE)
Default	0

cfgIpmiSerialEchoControl (Read or Write)

Table 343. Details of cfgIpmiSerialEchoControl

Description	Enables or disables echo control on the IPMI serial interface.
Legal Values	• 0(FALSE) • 1 (TRUE)
Default	1

cfgIpmiSerialFlowControl (Read or Write)

Table 344. Details of cfgIpmiSerialFlowControl

Description	Specifies the flow control setting for the IPMI serial port.
Legal Values	• 0 (None) • 1 (CTS or RTS)
Default	1

cfgIpmiSerialHandshakeControl (Read or Write)

Table 345. Details of cfgIpmiSerialHandshakeControl

Description	Enables or disables the IPMI terminal mode handshake control.
Legal Values	• 0(FALSE) • 1 (TRUE)
Default	1

cfgIpmiSerialInputNewLineSequence (Read or Write)

Table 346. Details of cfgIpmiSerialInputNewLineSequence

Description	Specifies the input new line sequence specification for the IPMI serial interface.
Legal Values	• 1 — ENTER • 2 — NULL
Default	1

cfgIpmiSerialLineEdit (Read or Write)

Table 347. Details of cfgIpmiSerialLineEdit

Description	Enables or disables line editing on the IPMI serial interface.
Legal Values	• 0(FALSE) • 1(TRUE)
Default	1

cfgIpmiSerialNewLineSequence (Read or Write)

Table 348. Details of cfgIpmiSerialNewLineSequence

Description	Specifies the new line sequence specification for the IPMI serial interface.
Legal Values	• 0 — None • 1 — CR-LF • 2 — NULL • 3 — CR

- 4 — LF-CR
- 5 — LF

Default 1

cfgSmartCard

This group specifies properties used to support access to iDRAC using a smart card.

The following sections provide information about the objects in the `cfgSmartCard` group.

cfgSmartCardLogonEnable (Read or Write)

Table 349. Details of cfgSmartCardLogonEnable

Description To iDRAC using a smart card, enable or disable with Remote RACADM support for access.

NOTE: Enabling with remote RACADM is only applicable for iDRAC on Rack and Tower Servers.

Legal Values
- 0 (Disabled)
- 1 (Enabled)
- 2 (Enabled with Remote RACADM) — It is not applicable for iDRAC Enterprise on Blade Servers.

Default 0

cfgSmartCardCRLEnable (Read or Write)

Table 350. Details of cfgSmartCardCRLEnable

Description Enables or disables the Certificate Revocation List (CRL).

This object is applicable only for iDRAC on Rack and Tower Servers and not for iDRAC Enterprise on Blade Servers.

Legal Values
- 1 (TRUE)
- 0 (FALSE)

Default 0

cfgNetTuning

This group enables users to configure the advanced network interface parameters for the RAC NIC. When configured, the updated settings may take up to a minute to become active.

NOTE: This group is applicable only for iDRAC on Rack and Tower Servers and not for iDRAC Enterprise on Blade Servers.

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.

The following sections provide information about the objects in the `cfgNetTuning` group.

cfgNetTuningNicAutoneg (Read or Write)

Table 351. Details of cfgNetTuningNicAutoneg

Description	Enables auto negotiation of physical link speed and duplex. If enabled, auto negotiation 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
```

cfgNetTuningNic100MB (Read or Write)

Table 352. Details of cfgNetTuningNic100MB

Description	Specifies the speed for iDRAC NIC. **NOTE: To set this property:** • **iDRAC NIC selection must be set to `Dedicated` mode.** • **iDRAC NIC Auto negotiation must be disabled.** • **iDRAC IPv4 must be enabled.** • **iDRAC IPv4 DHCP must be enabled.** • **iDRAC IPv6 must be enabled.** • **iDRAC IPv6 auto configuration must be enabled.**
Legal Values	• 0 (10 MBit) • 1 (100 MBit) • 2 (1000 MBit) **NOTE: You cannot manually set the Network Speed to 1000 MBit. This option is available only if `cfgNetTuningNicAutoNeg` is set to 1 (Enabled).**
Default	1

cfgNetTuningNicFullDuplex (Read or Write)

Table 353. Details of cfgNetTuningNicFullDuplex

Description	Specifies the duplex setting for the NIC.
Legal Values	• 0 (Half Duplex) • 1 (Full Duplex)
Default	1
Dependency	None

cfgNetTuningNicMtu (Read or Write)

Table 354. Details of cfgNetTuningNicMtu

Description	Indicated the maximum size of units in bytes transmitted by NIC.
Legal Values	576–1500
Default	1500

cfgSensorRedundancy

This group is used to set the power supply redundancy.

The following sections provide information about the objects in the `cfgSensorRedundancy` group.

This group is applicable only for iDRAC on Rack and Tower Servers and not for iDRAC Enterprise on Blade Servers.

cfgSensorRedundancyCapabilities (Read Only)

Table 355. Details of cfgSensorRedundancyCapabilities

Description	Returns the redundancy capabilities in the form of a bitmask. This bitmask allows the user to know which values can be set for `cfgSensorRedundancyPolicy`.
Legal Values	A bit mask. More than 1 bit can be set at a time to indicate multiple redundancy support. • 0- N/A, for systems that are not supported • 1- Non-Redundant • 2- 1+1 — Redundant • 4- 2+1 — Redundant • 8- 2+2 — Redundant
Default	0

cfgSensorRedundancyIndex (Read Only)

Table 356. Details of cfgSensorRedundancyIndex

Description	Specifies index for the sensor redundancy group being read. Only power supply redundancy is supported.
Legal Values	1
Default	None

cfgSensorRedundancyPolicy (Read or Write)

Table 357. Details of cfgSensorRedundancyPolicy

Description	Sets the power supply redundancy policy.
Legal Values	• `2` — N/A, for systems that are not supported • `3` — Non Redundant • `4`–1+1 Redundant • `4`–2+1 Redundant • `16`–2+2 Redundant

Default	Any legal value at that particular execution instance.

cfgSensorRedundancyStatus (Read Only)

Table 358. Details of cfgSensorRedundancyStatus

Description	Indicates the redundancy status. The status is N/A on platforms that do not support the power supply sensor redundancy.
Legal Values	String: • N/A • Full • Lost • Degraded
Default	None

cfgVFlashSD

This group is used to configure the properties for the Virtual Flash SD card.

NOTE: If the vFlash card is present but is not enabled, the query for any property under this group displays:

```
ERROR: vFlash is not enabled.
```

To view the properties of this group, enable the vFlash using the command:

```
racadm config -g cfgvFlashSD -o cfgvFlashSDEnable 1
```

The following sections provide information about the objects in the `cfgVFlashSD` group.

cfgVFlashSDInitialized (Read Only)

Table 359. Details of cfgVFlashSDInitialized

Description	Displays whether an SD card is initialized.
Legal Values	• 0 • 1
Default	None

cfgVFlashSDEnable (Read or Write)

Table 360. Details of cfgVFlashSDEnable

Description	Enables or disables the vFlash SD card. **NOTE: Disabling `vFlashPartition` by setting `cfgVFlashSDEnable` to `0` does not require a license.**
Legal Values	• 0 (Disable) • 1 (Enable)
Default	1

cfgVFlashSDSize (Read Only)

Table 361. Details of cfgVFlashSDSize

Description	Displays the size of the vFlash SD card in megabytes (MB).
Legal Values	A string of up to 64 characters.
Default	`<card size>`

cfgVFlashSDLicensed (Read Only)

Table 362. Details of cfgVFlashSDLicensed

Description	Displays whether an SD card or vFlash SD card is inserted. The vFlash SD card supports the new enhanced vFlash features and the SD card supports only the limited vFlash features.
Legal Values	• 0(SD card is inserted) • 1(vFlash SD card is inserted)
Default	None

cfgVFlashSDAvailableSize (Read Only)

Table 363. Details of cfgVFlashSDAvailableSize

Description	Displays the available memory (in MB) on the vFlash SD card that can be used to create new partitions.
Legal Values	A string of up to 64 characters.
Default	If the card is not initialized, default is 0. If initialized, displays the unused memory on the card.

cfgVFlashSDHealth (Read Only)

Table 364. Details of cfgVFlashSDHealth

Description	Displays the current health status of the vFlash SD card.
Legal Values	String: • OK • Warning • Critical • Unknown
Default	OK

cfgVFlashSDWriteProtect (Read Only)

Table 365. Details of cfgVFlashSDWriteProtect

Description	Displays whether the physical WriteProtect latch on the vFlash SD card is enabled or disabled.
Legal Values	• 0 (vFlash is not write-protected) • 1 (vFlash is write-protected)

Default	None

cfgVFlashPartition

This group is used to configure properties for individual partitions on the vFlash SD Card. Up to 16 partitions are supported, indexed from 1 to 16.

NOTE: For SD cards, the index value is limited to 1 because only a single partition of size 256MB is allowed.

The following sections provide information about the objects in the `cfgVFlashPartition` group.

cfgVFlashPartitionIndex (Read Only)

Table 366. Details of cfgVFlashPartitionIndex

Description	The index value of the partition.
Legal Values	Integer 1–16
Default	None

cfgVFlashPartitionSize (Read Only)

Table 367. Details of cfgVFlashPartitionSize

Description	Displays the size of the partition.
Legal Values	1 MB to 4 GB
Default	None

cfgVFlashPartitionEmulationType (Read or Write)

Table 368. Details of cfgVFlashPartitionEmulationType

Description	View or modify the emulation type for the partition.
Legal Values	String: • HDD • Floppy • CD-DVD
Default	None

cfgVFlashPartitionFlashOSVolLabel (Read Only)

Table 369. Details of cfgVFlashPartitionFlashOSVolLabel

Description	Displays the label for the partition that is visible to the operating system.
Legal Values	An alphanumeric string of up to six characters.
Default	None

cfgVFlashPartitionFormatType (Read Only)

Table 370. Details of cfgVFlashPartitionFormatType

Description	Displays the format type of the partition.
Legal Values	String: • FAT16 • FAT32 • EXT2 • EXT3 • CD • RAW
Default	None

cfgVFlashPartitionAccessType (Read or Write)

Table 371. Details of cfgVFlashPartitionAccessType

Description	Indicates the partition access permissions. It configures the access type to read-write.
Legal Values	• 0 (Read Only) • 1 (Read-Write)
Default	0

cfgVFlashPartitionAttachState (Read or Write)

Table 372. Details of cfgVFlashPartitionAttachState

Description	View or modify the partition to attached or detached. **NOTE: Detaching the vFlashPartition by setting the `cfgVFlashPartitionAttachState` to `0` does not require a license.**
Legal Values	• 1 — Attached • 0 — Detached
Default	0 — Detached

cfgLogging

This group contains parameters to enable or disable the OEM event log filtering.

The following section provide information about the objects in the `cfgLogging` group:

cfgLoggingSELOEMEventFilterEnable (Read or Write)

Table 373. Details of cfgLoggingSELOEMEventFilterEnable

Description	Enables or disables the SEL Log filtering.
Legal Values	• 0 (Disable) • 1(Enable)

Default	0

cfgRacSecurity

For more information about generating certificate signing requests, see the subcommand `sslcsrgen`.

For the country code, go to the link **http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm**

The following sections provide information about the objects in the `cfgRacSecurity` group.

cfgRacSecCsrCommonName (Read or Write)

Table 374. Details of cfgRacSecCsrCommonName

Description	Specifies the CSR Common Name (CN) that must be an IP or iDRAC name as given in the certificate.
Legal Values	A string of up to 64 characters.
Default	`<blank>`

cfgRacSecCsrOrganizationName (Read or Write)

Table 375. Details of cfgRacSecCsrOrganizationName

Description	Specifies the CSR Organization Name (O).
Legal Values	A string of up to 64 characters.
Default	`<blank>`

cfgRacSecCsrOrganizationUnit (Read or Write)

Table 376. Details of cfgRacSecCsrOrganizationUnit

Description	Specifies the CSR Organization Unit (OU).
Legal Values	A string of up to 64 characters.
Default	`<blank>`

cfgRacSecCsrLocalityName (Read or Write)

Table 377. Details of cfgRacSecCsrLocalityName

Description	Specifies the CSR Locality (L).
Legal Values	A string of up to 128 characters.
Default	`<blank>`

cfgRacSecCsrStateName (Read or Write)

Table 378. Details of cfgRacSecCsrStateName

Description	Specifies the CSR State Name (S).
Legal Values	A string of up to 128 characters.
Default	<blank>

cfgRacSecCsrCountryCode (Read/Write)

Table 379. Details of cfgRacSecCsrCountryCode

Description	Specifies the CSR Country Code (CC).
Legal Values	A string of 2 alphabet country code.
Default	US

cfgRacSecCsrEmailAddr (Read or Write)

Table 380. Details of cfgRacSecCsrEmailAddr

Description	Specifies the CSR email address.
Legal Values	A string of up to 64 characters.
Default	<blank>

Example

```
racadm config -g cfgRacSecurity
```

```
cfgRacSecCsrKeySize=1024
cfgRacSecCommonName=
cfgRacSecOrganizationName=
cfgRacSecOrganizationUnit=
cfgRacSecLocalityName=
cfgRacSecStateName=
cfgRacSecCountryCode=
cfgRacSecEmailAddr=
```

4

Database Objects With Get and Set Commands

This chapter provides the database groups and objects that must be used with the `get` or `set` subcommands. When using the objects, they must begin with FQDD or FQDD alias.

The set operations for iDRAC, Lifecycle Controller, and system objects do not require server restart. However, the set operations for NIC and BIOS objects are staged to apply and commit the pending values.

NOTE: The attributes with License—Not applicable can be used with iDRAC Basic, iDRAC Express, and iDRAC Enterprise license types.

NOTE: The iDRAC9 with Lifecycle Controller Attribute Registry provides information about all attributes to perform get and set operations using RACADM interface. For more information, see *iDRAC9 with Lifecycle Controller Attribute Registry* available at https://www.dell.com/idracmanuals.

- While entering an attribute value that is more than one word, ensure that you enclose the attribute value within single quotation marks in the set command.

  Example:

```
racadm>>set system.thermalsettings.ThermalProfile 'Maximum performance'
racadm set system.thermalsettings.ThermalProfile 'Maximum performance'
[Key=system.Embedded.1#ThermalSettings.1]
Object value modified successfully
```

- The staged configuration has the associated pending value in the output of the get operation, after it is configured successfully.
- The object values in the BIOS and NIC groups are case-sensitive.
- For NIC objects, the definition of the key format is: `Key = <Device Class>.<Locator>.<Device Number>–<Port Number>[-<Partition Number>]#GroupName"` where,
  - Device Class: NIC
  - Locator: Integrated, Slot, Mezzanine or Embedded

    Example:

```
$racadm get NIC.NICConfig
NIC.NICConfig.1 [Key=NIC.Integrated.1-1#NICConfig]
NIC.NICConfig.2 [Key=NIC.Integrated.1-2#NICConfig]
NIC.NICConfig.3 [Key=NIC.Integrated.1-3#NICConfig]
NIC.NICConfig.4 [Key=NIC.Integrated.1-4#NICConfig]
```

- The link between the NIC instance and the corresponding key varies from system to system depending on the system configuration.
- The command `racadm help` provides a list of all the attributes along with the description.
- To view the help details of group level, enter the following command: `racadm help <group name>`

  Example:

```
$racadm help NIC.NICConfig
NICConfig       -- (null)
These are the objects supported by the group
------------------------------------------------------------------------------
BannerMessageTimeout      -- Specify the number of seconds that the OptionROM banner is
displayed during POST.
Usage                     -- Values from 0 - 14
Required License          -- RACADM
Dependency                -- None

BootOptionROM             -- Controls the enablement of legacy Boot Protocols in the
Option ROM.
Usage                     -- Enabled; Disabled
Required License          -- RACADM
```

```
Dependency                -- None

BootRetryCnt              -- Specify the number of retries to attempt in case of boot
failure.
Usage                     -- NoRetry - 0;1Retry - 1; 2Retries - 2;3Retries - 3;4Retries -
4; 5Retries - 5;6Retries- 6; IndefiniteRetries, Default - NoRetry
Required License          -- RACADM
Dependency                -- None
```

```
BootStrapType             -- Specify the boot strap method used to boot to the operating
system.
Usage                     -- AutoDetect - 0;BBS - 1; Int18h - 2; Int19h- 3; Default -
AutoDetect
Required License          -- RACADM
Dependency                -- None

HideSetupPrompt           -- Specifies whether to display or hide the legacy Option ROM
setup prompt during system Power On Self Test (POST).
Usage                     -- Enabled; Disabled; Default - Disabled
Required License          -- RACADM
Dependency                -- None

LegacyBootProto           -- Select a non-UEFI network boot protocol
Usage                     -- PXE; iSCSI; FCoE; NONE; iSCSIPrimary; iSCSISecondary
Required License          -- RACADM
Dependency                -- None
```

```
LnkSpeed                  -- Specifies the port speed used for the selected boot protocol
Usage                     -- AutoNeg; 10Mbps Half; 10Mbps Full; 100Mbps Half; 100Mbps Full
Required License          -- RACADM
Dependency                -- None

NumberVFAdvertised        -- The number of PCI Virtual Functions (VFs) to be advertised on
this port in non-NPAR mode.
Usage                     -- Values from 0 - 256, Default - 0
Required License          -- RACADM
Dependency                -- VLanMode has to be Enabled

VLanId                    -- Specifies the ID (tag) for the VLAN Mode. VLAN ID must be in
the range from 0 to 4095
Usage                     -- Values from 1 - 4095
Required License          -- RACADM
Dependency                -- VLanMode has to be Enabled
```

```
VLanMode                  -- Virtual LAN mode enables use of a VLAN tag to be used by
[vendor defined boot protocols]
Usage                     -- Enabled; Disabled
Required License          -- RACADM
Dependency                -- None

WakeOnLan                 -- Enables the server to be powered on using an in-band magic
packet
Usage                     -- Enabled; Disabled
Required License          -- RACADM
Dependency                -- None

WakeOnLanLnkSpeed         -- Select the port speed used for Wake on LAN mode
Usage                     -- AutoNeg; 10Mbps Half; 10Mbps Full; 100Mbps Half; 100Mbps Full
Required License          -- RACADM
Dependency                -- None
```

- To view the help details of attribute level, enter the following command: `racadm help <attribute name>`

  Example:

```
/tmp # racadm help NIC.NICConfig.WakeOnLanLnkSpeed
WakeOnLanLnkSpeed -- Select the port speed used for Wake on LAN mode
Usage -- AutoNeg; 10Mbps Half; 10Mbps Full; 100Mbps Half; 100Mbps Full
Required License -- RACADM
Dependency -- None/tmp #
```

- The get and set commands for BIOS and NIC provide the list of attributes on the basis of the system configuration, BIOS version used, hardware, and so on.

5

New Groups and Objects for iDRAC9

Table 381. New groups and new objects added for iDRAC9

Groups	Objects
iDRAC.GroupManager	iDRAC.GroupManager.GlobalState(Read or Write)
	iDRAC.GroupManager.GroupName(Read)
	iDRAC.GroupManager.GroupUID(Read)
iDRAC.GUI	iDRAC.GUI.SecurityPolicyMessage
iDRAC.Security	iDRAC.Security.FIPSMode (Read or Write)
iDRAC.SerialRedirection	iDRAC.SerialRedirection.QuitKey (Read or Write)
iDRAC.ServerBoot	iDRAC.ServerBoot.FirstBootDevice (Read or Write)
iDRAC.ServiceModule.	iDRAC.ServiceModule. HostSNMPAlert (Read or Write)
iDRAC.SupportAssist	iDRAC.SupportAssist.DefaultIPAddress
	iDRAC.SupportAssist.DefaultWorkgroupName
	iDRAC.SupportAssist.DefaultPassword
	iDRAC.SupportAssist.DefaultProtocol
	iDRAC.SupportAssist.DefaultShareName
	iDRAC.SupportAssist.DefaultUserName
	iDRAC.SupportAssist.EmailOptIn
	iDRAC.SupportAssist.EventBasedAutoCollection
iDRAC.Webserver	iDRAC.Webserver.TLSProtocol (Read or Write)
LifecycleController.LCAttributes	LifecycleController.LCAttributes.IgnoreCertWarning(Read and Write)
	LifecycleController.LCAttributes.UserProxyPassword (Read and Write)
	LifecycleController.LCAttributes. UserProxyPort (Read and Write)
	LifecycleController.LCAttributes. UserProxyServer (Read and Write)
	LifecycleController.LCAttributes. UserProxyType (Read and Write)
	LifecycleController.LCAttributes. UserProxyUserName (Read and Write)
System.Chassis	System.Chassis.ChassisInfraPower(Read)
	System.Chassis.ChassisPowerCap(Read)
Storage.enclosure	Storage.Enclosure.SupportedSplitModes(Read Only)
	Storage.Enclosure.Assetname
	Storage.Enclosure.Assettag
System.pcieSlotLFM	System. pcieSlotLFM.3rdPartyCard(Read)
	System.pcieSlotLFM. CardType (Read)

Groups	Objects
	System.pcieSlotLFM. CustomLFM (Read or Write)
	System.pcieSlotLFM .LFMMode(Read or Write)
	System.pcieSlotLFM.MaxLFM (Read)
	System.pcieSlotLFM.Slot (Read)
	System.pcieSlotLFM.SlotState (Read)
	System.pcieSlotLFM.TargetLFM
	System.pcieSlotLFM. CardType (Read)
	System.pcieSlotLFM. CustomLFM (Read or Write)
	System.pcieSlotLFM .LFMMode(Read or Write)
	System.pcieSlotLFM.MaxLFM (Read)
	System.pcieSlotLFM.Slot (Read)
	System.pcieSlotLFM.SlotState (Read)
	System.pcieSlotLFM.TargetLFM
Storage.PhysicalDisk	Storage.PhysicalDisk.Raidtype
System.QuickSync	System.QuickSync. ReadAuthentication (Read or Write)
	System.QuickSync.WiFi (Read or Write)
System.Storage	System.Storage.AvailableSpareAlertThreshold (Read or Write)
	System.Storage.RemainingRatedWriteEnduranceAlertThreshold (Read or Write)
System.pcieSlotLFM	System. pcieSlotLFM.3rdPartyCard(Read)
	System.pcieSlotLFM. CardType (Read)
	System.pcieSlotLFM. CustomLFM (Read or Write)
	System.pcieSlotLFM .LFMMode(Read or Write)
	System.pcieSlotLFM.MaxLFM (Read)
	System.pcieSlotLFM.Slot (Read)
	System.pcieSlotLFM.SlotState (Read)
	System.pcieSlotLFM.TargetLFM
	System.pcieSlotLFM. CardType (Read)
	System.pcieSlotLFM. CustomLFM (Read or Write)
	System.pcieSlotLFM .LFMMode(Read or Write)
	System.pcieSlotLFM.MaxLFM (Read)
	System.pcieSlotLFM.Slot (Read)
	System.pcieSlotLFM.SlotState (Read)
	System.pcieSlotLFM.TargetLFM

6

Legacy and New Groups and Objects

Table 382. Legacy and New Groups and Objects

Legacy Groups and Objects	New Groups and Objects
idRacInfo	**iDRAC.Info**
idRacType	Type
idRacProductInfo	Product
idRacDescriptionInfo	Description
idRacVersionInfo	Version
idRacBuildInfo	Build
idRacName	Name
cfgActiveDirectory	**iDRAC.ActiveDirectory**
cfgADEnable	Enable
cfgADRacDomain	RacDomain
cfgADRacName	RacName
cfgADAuthTimeout	AuthTimeout
cfgADType	Schema
cfgADDomainController1	DomainController1
cfgADDomainController2	DomainController2
cfgADDomainController3	DomainController3
cfgADGlobalCatalog1	GlobalCatalog1
cfgADGlobalCatalog2	GlobalCatalog2
cfgADGlobalCatalog3	GlobalCatalog3
cfgADCertValidationEnable	CertValidationEnable
cfgADSSOEnable	SSOEnable
cfgADDcSRVLookupEnable	DCLookupEnable
cfgADDcSRVLookupbyUserdomain	DCLookupByUserDomain
cfgADDcSRVLookupDomainName	DCLookupDomainName
cfgADGcSRVLookupEnable	GCLookupEnable
cfgADGcRootDomain	GCRootDomain

Legacy Groups and Objects	New Groups and Objects
cfgLanNetworking	**iDRAC.Nic**
cfgNicEnable	Enable
cfgNicMacAddress	MACAddress
cfgDNSRacName	DNSRacName
cfgNicSelection	Selection
cfgNicFailoverNetwork	Failover
cfgDNSDomainName	DNSDomainName
cfgDNSDomainNameFromDHCP	DNSRacName
cfgDNSRegisterRac	DNSRegister
cfgNicVLanEnable	VLanEnable
cfgNicVLanID	VLanID
cfgNicVLanPriority	VLanPriority
	iDRAC.IPv4
cfgNicIPv4Enable	Enable
cfgNicIpAddress	Address
cfgNicNetmask	NetMask
cfgNicGateway	Gateway
cfgNicUseDhcp	DHCPEnable
cfgDNSServersFromDHCP	DNSFromDHCP
cfgDNSServer1	DNS1
cfgDNSServer2	DNS2
cfgIpv6LanNetworking	**iDRAC.IPv6**
cfgIPv6Enable	Enable
cfgIPv6Address1	Address1
cfgIPv6Gateway	Gateway
cfgIPv6PrefixLength	PrefixLength
cfgIPv6AutoConfig	AutoConfig
cfgIPv6LinkLocalAddress	LinkLocalAddress
cfgIPv6Address2	Address2
cfgIPv6Address3	Address3
cfgIPv6Address4	Address4

Legacy Groups and Objects	New Groups and Objects
cfgIPv6Address5	Address5
cfgIPv6Address6	Address6
cfgIPv6Address7	Address7
cfgIPv6Address8	Address8
cfgIPv6Address9	Address9
cfgIPv6Address10	Address10
cfgIPv6Address11	Address11
cfgIPv6Address12	Address12
cfgIPv6Address13	Address13
cfgIPv6Address14	Address14
cfgIPv6Address15	Address15
cfgIPv6DNSServersFromDHCP6	DNSFromDHCP6
cfgIPv6DNSServer1	DNS1
cfgIPv6DNSServer2	DNS2
cfgServerPower	**System.Power**
cfgServerPowerStatus	Status
cfgServerActualPowerConsumption	Realtime.Power
cfgServerMinPowerCapacity	Cap.MinThreshold
cfgServerMaxPowerCapacity	Cap.MaxThreshold
cfgServerPeakPowerConsumption	Max.Power
cfgServerPeakPowerConsumptionTimestamp	Max.Power.Timestamp
cfgServerPowerConsumptionClear	Max.PowerClear
cfgServerPowerCapWatts	Cap.Watts
cfgServerPowerCapBtuhr	Cap.BtuHr
cfgServerPowerCapPercent	Cap.Percent
cfgServerPowerCapEnable	Cap.Enable
cfgServerPowerLastHourAvg	Avg.LastHour
cfgServerPowerLastDayAvg	Avg.LastDay
cfgServerPowerLastWeekAvg	Avg.LastWeek
cfgServerPowerLastHourMinPower	Min.LastHour
cfgServerPowerLastHourMinTime	Min.LastHour.Timestamp

Legacy Groups and Objects	New Groups and Objects
cfgServerPowerLastHourMaxPower	Max.LastHour
cfgServerPowerLastHourMaxTime	Max.LastHour.Timestamp
cfgServerPowerLastDayMinPower	Min.LastDay
cfgServerPowerLastDayMinTime	Min.LastDay.Timestamp
cfgServerPowerLastDayMaxPower	Max.LastDay
cfgServerPowerLastDayMaxTime	Max.LastDay.Timestamp
cfgServerPowerLastWeekMinPower	Min.LastWeek
cfgServerPowerLastWeekMinTime	Min.LastWeek.Timestamp
cfgServerPowerLastWeekMaxPower	Max.LastWeek
cfgServerPowerLastWeekMaxTime	Max.LastWeek.Timestamp
cfgServerPowerInstHeadroom	Realtime.Headroom
cfgServerPowerPeakHeadroom	Max.Headroom
cfgServerActualAmperageConsumption	Realtime.Amps
cfgServerPeakAmperage	Max.Amps
cfgServerPeakAmperageTimeStamp	Max.Amps.Timestamp
cfgServerCumulativePowerConsumption	EnergyConsumption
cfgServerCumulativePowerConsumptionTimeStamp	EnergyConsumption.StarttimeStamp
cfgServerCumulativePowerClear	EnergyConsumption.Clear
cfgServerPowerPicEAllocation	PCIePowerAllocation
cfgServerPowerSupply	**System.Power.Supply**
cfgServerPowerSupplyIndex	Index
cfgServerPowerSupplyInputStatus	LineStatus
cfgServerPowerSupplyMaxInputPower	MaxInputPower
cfgServerPowerSupplyMaxOutputPower	MaxOutputPower
cfgServerPowerSupplyOnlineStatus	Status
cfgServerPowerSupplyFwVer	FwVer
cfgServerPowerSupplyCurrentDraw	CurrentDraw
cfgServerPowerSupplyType	Type
cfgServerPowerBusMonitoring	PMBusMonitoring
cfgUserAdmin	**iDRAC.Users**
cfgUserAdminIndex	NA

Legacy Groups and Objects	New Groups and Objects
cfgUserAdminUserName	UserName
cfgUserAdminPassword	Password
cfgUserAdminEnable	Enable
cfgUserAdminPrivilege	Privilege
cfgUserAdminIpmiLanPrivilege	IpmiLanPrivilege
cfgUserAdminIpmiSerialPrivilege	IpmiSerialPrivilege
cfgUserAdminSolEnable	SolEnable
cfgRemoteHosts	**iDRAC.SysLog**
cfgRhostsSyslogEnable	SysLogEnable
cfgRhostsSyslogServer1	Server1
cfgRhostsSyslogServer2	Server2
cfgRhostsSyslogServer3	Server3
cfgRhostsSyslogPort	Port
	iDRAC.Update
cfgRhostsFwUpdateTftpEnable	FwUpdateTFTPEnable
cfgRhostsFwUpdateIpAddr	FwUpdateIPAddr
cfgRhostsFwUpdatePath	FwUpdatePath
	[iDRAC.RemoteHosts]
cfgRhostsSmtpServerIpAddr	SMTPServerIPAddress
cfgEmailAlert	**iDRAC.EmailAlert**
cfgEmailAlertIndex	NA
cfgEmailAlertEnable	Enable
cfgEmailAlertAddress	Address
cfgEmailAlertCustomMsg	CustomMsg
cfgSessionManagement	
cfgSsnMgtTelnetIdleTimeout	**iDRAC.Telnet**
	Enable
	Port
	Timeout
cfgSsnMgtSshIdleTimeout	**iDRAC.SSH**
	Enable

Legacy Groups and Objects	New Groups and Objects
	Port
	Timeout
cfgSsnMgtRacadmTimeout	**iDRAC.Racadm**
	Enable
	Timeout
cfgSsnMgtConsRedirMaxSessions	**iDRAC.VirtualConsole**
	EncryptEnable
	Enable
	PluginType
	LocalVideo
	Port
	MaxSessions
	Timeout
	AccessPrivilege
cfgSsnMgtWebserverTimeout	**iDRAC.Webserver**
	Enable
	HttpPort
	Timeout
	HttpsPort
	LowerEncryptionBitLength
[cfgSerial]	**iDRAC.Serial**
cfgSerialBaudRate	BaudRate
cfgSerialConsoleEnable	Enable
cfgSerialConsoleIdleTimeout	IdleTimeout
cfgSerialConsoleNoAuth	NoAuth
cfgSerialConsoleCommand	Command
cfgSerialHistorySize	HistorySize
	iDRAC.SerialRedirection
cfgSerialConsoleQuitKey	QuitKey
cfgSerialCom2RedirEnable	Enable

Legacy Groups and Objects	New Groups and Objects
cfgSerialTelnetEnable	**iDRAC.Telnet**
cfgSerialSshEnable	**iDRAC.SSH**
[cfgOobSnmp]	**iDRAC.SNMP**
cfgOobSnmpAgentEnable	AgentEnable
cfgOobSnmpAgentCommunity	AgentCommunity
[cfgNetTuning]	
cfgNetTuningNic100MB	**iDRAC.Nic**
cfgNetTuningNicFullDuplex	**iDRAC.Nic**
cfgNetTuningNicMtu	**iDRAC.Nic**
cfgNetTuningNicAutoneg	**iDRAC.Nic**
[cfgRacTuning]	
cfgRacTuneRemoteRacadmEnable=1	**iDRAC.Racadm**
cfgRacTuneWebserverEnable=1	**iDRAC.Webserver**
cfgRacTuneHttpPort=80	**iDRAC.Webserver**
cfgRacTuneHttpsPort=443	**iDRAC.Webserver**
cfgRacTuneTelnetPort=23	**iDRAC.Telnet**
cfgRacTuneSshPort=22	**iDRAC.SSH**
cfgRacTuneConRedirEnable=1	**iDRAC.VirtualConsole**
cfgRacTuneConRedirPort=5900	**iDRAC.VirtualConsole**
cfgRacTuneConRedirEncryptEnable=1	**iDRAC.VirtualConsole**
cfgRacTuneLocalServerVideo=1	**iDRAC.VirtualConsole**
	iDRAC.IPBlocking
cfgRacTuneIpRangeEnable=0	RangeEnable
cfgRacTuneIpRangeAddr=192.168.1.1	RangeAddr
cfgRacTuneIpRangeMask=255.255.255.0	RangeMask
	iDRAC.Time
cfgRacTuneTimezoneOffset=0	TimeZoneOffset
cfgRacTuneDaylightOffset=0	DaylightOffset
cfgRacTuneAsrEnable=1	TBD
cfgRacTunePlugintype=0	**iDRAC.VirtualConsole**
	iDRAC.LocalSecurity

Legacy Groups and Objects	New Groups and Objects
cfgRacTuneCtrlEConfigDisable=0	PrebootConfig
cfgRacTuneLocalConfigDisable=0	LocalConfig
cfgRacTuneVirtualConsoleAuthorizeMultipleSessions=0	**iDRAC.VirtualConsole**
ifcRacManagedNodeOs	**System.ServerOS**
ifcRacMnOsHostname	HostName
ifcRacMnOsOsName	OSName
cfgRacSecurity	**iDRAC.Security**
cfgRacSecCsrKeySize	CsrKeySize
cfgRacSecCsrCommonName	CsrCommonName
cfgRacSecCsrOrganizationName	CsrOrganizationName
cfgRacSecCsrOrganizationUnit	CsrOrganizationUnit
cfgRacSecCsrLocalityName	CsrLocalityName
cfgRacSecCsrStateName	CsrStateName
cfgRacSecCsrCountryCode	CsrCountryCode
cfgRacSecCsrEmailAddr	CsrEmailAddr
cfgRacVirtual	**iDRAC.VirtualMedia**
cfgVirMediaAttached	Attached
cfgVirtualBootOnce	BootOnce
cfgVirMediaFloppyEmulation	FloppyEmulation
cfgLDAP	**iDRAC.LDAP**
cfgLdapEnable	Enable
cfgLdapServer	Server
cfgLdapPort	Port
cfgLdapBaseDN	BaseDN
cfgLdapUserAttribute	UserAttribute
cfgLdapGroupAttribute	GroupAttribute
cfgLdapGroupAttributeIsDN	GroupAttributeIsDN
cfgLdapBindDN	BindDN
# cfgLdapBindPassword	BindPassword
cfgLdapSearchFilter	SearchFilter
cfgLdapCertValidationEnable	CertValidationEnable

Legacy Groups and Objects	New Groups and Objects
cfgLdapRoleGroup	**iDRAC.LDApRole**
cfgLdapRoleGroupIndex	NA
cfgLdapRoleGroupDN	DN
cfgLdapRoleGroupPrivilege	Privilege
cfgStandardSchema	**iDRAC.ADGroup**
cfgSSADRoleGroupIndex	NA
cfgSSADRoleGroupName	Name
cfgSSADRoleGroupDomain	Domain
cfgSSADRoleGroupPrivilege	Privilege
cfgIpmiSerial	**iDRAC.IPMISerial**
cfgIpmiSerialConnectionMode	ConnectionMode
cfgIpmiSerialBaudRate	BaudRate
cfgIpmiSerialFlowControl	FlowControl
cfgIpmiSerialChanPrivLimit	ChanPrivLimit
cfgIpmiSerialLineEdit	LineEdit
cfgIpmiSerialDeleteControl	DeleteControl
cfgIpmiSerialEchoControl	EchoControl
cfgIpmiSerialHandshakeControl	HandshakeControl
cfgIpmiSerialNewLineSequence	NewLineSeq
cfgIpmiSerialInputNewLineSequence	InputNewLineSeq
cfgIpmiSol	**iDRAC.IPMISol**
cfgIpmiSolEnable	Enable
cfgIpmiSolBaudRate	BaudRate
cfgIpmiSolMinPrivilege	MinPrivilege
cfgIpmiSolAccumulateInterval	AccumulateInterval
cfgIpmiSolSendThreshold	SendThreshold
cfgIpmiLan	**iDRAC.IPMILan**
cfgIpmiLanEnable	Enable
cfgIpmiLanPrivilegeLimit	PrivLimit
cfgIpmiLanAlertEnable	AlertEnable
cfgIpmiEncryptionKey	EncryptionKey

Legacy Groups and Objects	New Groups and Objects
cfgIpmiPetCommunityName	CommunityName
cfgUserDomain	**iDRAC.UserDomain**
cfgUserDomainIndex	NA
cfgUserDomainName	Name
cfgSmartCard	**iDRAC.SmartCard**
cfgSmartCardLogonEnable	SmartCardLogonEnable
cfgSmartCardCRLEnable	SmartCardCRLEnable
[cfgIPv6URL]	
cfgIPv6URLString	NA
cfgVFlashSD	**iDRAC.vFlashSD**
cfgVFlashSDSize	Size
cfgVFlashSDLicensed	Licensed
cfgVFlashSDAvailableSize	AvailableSize
cfgVFlashSDHealth	Health
cfgVFlashSDEnable	Enable
cfgVFlashSDWriteProtect	WriteProtect
cfgVFlashSDInitialized	Initialized
cfgVFlashPartition	**iDRAC.vFlashPartition**
cfgVFlashPartitionIndex	NA
cfgVFlashPartitionSize	Size
cfgVFlashPartitionEmulationType	EmulationType
cfgVFlashPartitionFlashOSVolLabel	VolumeLabel
cfgVFlashPartitionFormatType	FormatType
cfgVFlashPartitionAccessType	AccessType
cfgVFlashPartitionAttachState	AttachState
cfgServerInfo	**iDRAC.ServerBoot**
cfgServerBootOnce	BootOnce
cfgServerFirstBootDevice	FirstBootDevice
cfgLogging	**iDRAC.Logging**
cfgLoggingSELOEMEventFilterEnable	SELOEMEventFilterEnable

Legacy Groups and Objects	New Groups and Objects
	iDRAC.SNMPAlert
cfgIpmiPetAlertEnable	Enable
cfgIpmiPetAlertDestIpAddr	DestAddr

7

Deprecated and New Subcommands

Table 383. Details of Deprecated and New Subcommands

Deprecated Subcommands	New Subcommands
getconfig	get
config	set
getuscversion	getversion
raid	storage

NOTE: The following attributes are obsoleted and these attributes do not support the ipBlocking feature:

- **ipBlockingEnabled**
- **ipBlockingFailCount**
- **ipBlockingFailWindow**
- **ipBlockingPenaltyTime**