

**Dell OpenManage
SNMP Reference Guide for iDRAC and Chassis
Management Controller**



Notes, cautions, and warnings

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

 **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.

Copyright © 2015 Dell Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Dell™ and the Dell logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

2015 - 09

Rev. A00

Contents

1 Introduction.....	5
Supported SNMP Versions.....	5
Managed Object Used in This Document.....	5
Server Administrator Remote Access MIB.....	6
Dell Remote Access Controller Out-of-Band MIB.....	7
Basic Terminology.....	7
Frequently Used Terms in Variable Names.....	7
Tables.....	8
SNMP Tables.....	8
Other Documents You May Need.....	10
2 Chassis Management Controller Group.....	11
Product Information.....	11
Chassis Status.....	16
Chassis Power.....	22
CMC Power Information.....	23
CMC PSU Information.....	25
Chassis Servers.....	27
CMC Server Information.....	27
Chassis Alert.....	30
Chassis Alert 2.....	31
Legacy Alerting.....	32
3 SNMP Traps.....	34
Understanding Trap Severity.....	34
RAC Traps.....	35
BMC Traps.....	36
PowerEdge M1000e CMC Traps.....	39
PowerEdge VRTX CMC Traps and PowerEdge FX2 CMC Traps.....	40
System Trap Group.....	40
Storage Trap Group.....	45
Audit Traps.....	49
Configuration Traps.....	50
Updates Traps.....	51
4 iDRAC MIB.....	52
Supported Systems.....	52
Blade Servers.....	52

Rack and Tower Servers.....	52
iDRAC Supported SNMP Versions.....	52
iDRAC SNMP Data Security Features.....	53
iDRAC Out-of-Band Group.....	53
RAC Information Group.....	53
Chassis Information Group.....	55
System Information Group.....	56
Status Group.....	59
Systems Details Group.....	60
Storage Details Group.....	60
iDRAC Traps.....	61
Trap Variables.....	61
System Trap Group.....	63
Storage Trap Group.....	73
Updates Trap Group.....	76
Audit Trap Group.....	76
Configuration Trap Group.....	78


Introduction

This reference guide provides information about Simple Network Management Protocol (SNMP) Management Information Base (MIB) which are released with the current version of Dell iDRAC and Chassis Management Controller.

Sections in this guide follow MIB groups and provide explanations and definitions for the terms used to define MIB objects. All essential Simple Network Management Protocol (SNMP) terms are defined in this guide. Some of the vocabulary may seem complex and unfamiliar to system administrators who are using SNMP for the first time.

Supported SNMP Versions

iDRAC version	SNMP Alerts / Traps	SNMP Gets
iDRAC7	SNMP v1 ,v2, v3	v1,v2,v3
iDRAC8	SNMP v1,v2,v3	v1,v2,v3

 **NOTE:** SNMP alerts and traps v3 is supported on iDRAC7 for firmware version 2.10.10.10 and later systems.

Managed Object Used in This Document


The MIB is divided into several major groups. The following table provides information about the MIB names, name of the agent that uses each MIB and the purpose:

MIB Name	Agent / Hardware Supported	Purpose of the MIB
10892.mib	Server Administrator	Provides the information about the systems monitored by Server Administrator instrumentation software. This is the primary MIB for PowerEdge systems.
dcs3fru.mib	Server Administrator	Provides the information about the system Field Replaceable Unit (FRU) to SNMP management applications.
dcstorag.mib	Server Administrator Storage Management	Provides the information about the storage hardware components and RAID configurations monitored by Server Administrator.
iDRAC-SMlv1.mib	iDRAC7 and iDRAC 8	Provides information about the SNMP data and traps supported by iDRAC7 and iDRAC8. This is the SMLv1 version of the iDRAC MIB.

MIB Name	Agent / Hardware Supported	Purpose of the MIB
iDRAC-SMIv2.mib	iDRAC7 and iDRAC 8	Provides information about the SNMP data and traps supported by iDRAC7 and iDRAC8. This is the SMIv2 version of the iDRAC MIB.
dcs3rmt.mib	Dell Remote Access controller 5 (DRAC 5)	Provides information about remote access components monitored by the Server Administrator Remote Access Service.
rac_host.mib	Remote access out-of-band agent	Provides information about the components monitored by the remote access out-of-band software agent.
DELL-RAC-MIB.txt	Chassis Management Controller (CMC)	Provides information about components monitored by the Chassis Management Controller for modular chassis. This MIB is the legacy iDRAC MIB. Changes made in this MIB are not for iDRAC. iDRAC does not support all the objects and traps defined in this MIB. The new and more extensive iDRAC MIB is available for iDRAC7 and later versions.
DcAsfSrv.mib	Baseboard Management Controller (BMC)	Provides information about Dell server Platform Event Traps generated by the Baseboard Management Controller.

For further details see Release Notes for *Management Information Base* [readme_mibs.txt](#).

Server Administrator Remote Access MIB

 **NOTE:** This section contains information that is applicable only if the Server Administrator is installed in the system.

The Server Administrator Remote Access MIB (filename **dcs3rmt.mib**) provides in-band information about remote access hardware that may be present in your system.

The Server Administrator Remote Access MIB structures its MIB objects into groups of scalar objects or MIB tables that provide related information. Table below describes each Server Administrator Remote Access MIB group and lists the MIB group number assigned to the MIB group. The Server Administrator Remote Access MIB groups are identified by the SNMP OID 1.3.6.1.4.1.674.10892.1.<MIB group number> where <MIB group number> is the MIB group number assigned to the MIB group. See the relevant section for more information about the MIB objects defined in a MIB group.

Table 1. Server Administrator Remote Access MIB Sections in This Guide

Topic	MIB Group Numbers
Remote Access Group – provides information about remote access hardware that may be present in your system and defines variables for	1700

Topic	MIB Group Numbers
administrative users, SNMP trap destinations, modem configuration for dial-up networking, dial-in configuration, and dial-out destinations	

Dell Remote Access Controller Out-of-Band MIB

The Dell Remote Access Controller Out-of-Band MIB (filename **DELL-RAC-MIB.txt**) provides management data that allows you to monitor the Chassis Management Controller. This MIB also contains information on RAC legacy alerting. The following table describes each Dell RAC Out-of-Band group and lists the MIB group number assigned to the MIB group. See the relevant section for more information about the MIB objects defined in a MIB group.

Table 2. Dell RAC Out-of-Band MIB

Topics	MIB Group Number
The Dell RAC Out-of-Band MIB consists of information for the following groups:	2
<ul style="list-style-type: none"> • Product Information • Chassis Status • Chassis Power • CMC Power Information • CMC PSU Information • Chassis Alerts • Legacy Alerting 	

Basic Terminology

It is important to have a good understanding of the key technical terms used in this guide. This guide provides definitions for all essential terms used in describing the Server Administrator MIBs. For definitions on all essential terms and acronyms, see the *Glossary* available on the Dell Support website at dell.com/support/manuals.

Frequently Used Terms in Variable Names

The following terms are frequently used in the name of a MIB variable:

Capability refers to the actions an object can perform, or to actions that can be taken by the object. Hot-pluggable is an example of a capability. If a card is hot-pluggable, it can be replaced while a system is

running. Capability settings refer to the capabilities of the object that the user can select from and activate if desired. Capability settings allow users of the server administrator to predetermine how an object behaves under specific conditions.

Settings are the conditions of a manageable object that determine what happens when a certain value is detected in a component. For example, a user can set the upper critical threshold of a temperature probe to 75 degrees Celsius. If the probe reaches that temperature, the setting causes an alert to be sent to the management console. Some settings, when reached, can trigger a system shutdown or other response to prevent damage to the system.

State refers to the condition of an object that has more than one condition. For example, an object may be in a *not ready* or in an *enabled* state.

Status refers to the health of an object or how the object is functioning. For example, the status of a temperature probe that is measuring acceptable temperatures would be reported as normal. When the probe begins reading temperatures that exceed limits set by the user, it reports a critical status.

Tables

This reference guide contains two types of tables: tables that are used to organize and define variable values and tables that define MIB objects. Readers must understand the difference between these two types of tables.

SNMP Tables

Most of the MIB objects defined in this reference guide are organized into SNMP tables. SNMP tables organize data into two-dimensional structural arrays. In SNMP, objects that have a relationship to other objects are called columnar objects. Columnar objects are objects used to form lists and tables. When a MIB group is divided into one or more discrete tables, the word *table* has a technical meaning. An example is the section of this reference guide entitled Universal Unique Identifier (UUID). The UUID object has a type and a value that uniquely identifies an object such as a chassis. The table defines all of the variables that comprise the managed object UUID.

The following table is an example of an SNMP table. The table contains variables that must occur in a definite sequence. In the example table the defined variables are UUID Chassis Index, UUID Index, UUID Type, and UUID Value.

These objects comprise the Server Administrator definitions for the UUID.

Table 3. UUID Table

Name	uUIDTable
Object ID	1.3.6.1.4.1.674.10892.1.300.20
Description	Defines the UUID table.
Syntax	SEQUENCE OF UUIDTableEntry
Access	Not accessible

Table 4. UUID Table Entry

Name	<code>uUIDTableEntry</code>
Object ID	1.3.6.1.4.1.674.10892.1.300.20.1
Description	Defines the UUID table entry.
Syntax	<code>UUIDTableEntry</code>
Access	Not accessible
Index	<code>uUIDIndex</code> , <code>uUIDchassisIndex</code>

Table 5. UUID Chassis Index

Name	<code>uUIDchassisIndex</code>
Object ID	1.3.6.1.4.1.674.10892.1.300.20.1.1
Description	Defines the index (one-based) of this chassis.
Syntax	<code>DellObjectRange</code>
Access	Read-only

Table 6. UUID Index

Name	<code>uUIDIndex</code>
Object ID	1.3.6.1.4.1.674.10892.1.300.20.1.2
Description	Defines the index of the UUID in a specified chassis.
Syntax	<code>DellObjectRange</code>
Access	Read-only

Table 7. UUID Type

Name	<code>uUIDType</code>
Object ID	1.3.6.1.4.1.674.10892.1.300.20.1.3
Description	Defines the type of the UUID for this chassis.
Syntax	<code>DellUUIDType</code>
Access	Read-only

Table 8. UUID Value

Name	<code>uUIDValue</code>
Object ID	1.3.6.1.4.1.674.10892.1.300.20.1.4
Description	Defines the value of the UUID for this chassis.
Syntax	Octet String (SIZE[16])

Other Documents You May Need

In addition to this guide, you can access the following guides available on the Dell Support website at dell.com/support/manuals. On the **Manuals** page, click **Software Systems Management**. Click the appropriate product link on the right-side to access the documents.

- The *Server Administrator Messages Reference Guide* lists the messages that you can receive on your systems management console or on your operating system's event viewer. This guide explains the text, severity, and cause of each message that the server administrator issues.
- The *Server Administrator CIM Reference Guide* documents the Common Information Model (CIM) provider, an extension of the standard management object format (MOF) file. The Server-Administrator CIM provider documents supported classes of management objects.
- The *Glossary* provides information on the terms used in this document.

Chassis Management Controller Group

Dell Remote Access Controller Out-of-Band Group

The Dell Remote Access Controller Out-of-Band MIB contains information for both Chassis Management Controller (CMC) and RAC Legacy Alerting. This MIB consists of information for the following groups:

Product Information

The following MIB attributes provide product information for the chassis management controller:

Table 9. DRsProductName

Name	drsProductName
Object ID	1.3.6.1.4.1.674.10892.2.1.1.1
Description	Defines the product name of a chassis management controller.
Syntax	DellString
Access	Read-only

Table 10. DRsProductShortName

Name	drsProductShortName
Object ID	1.3.6.1.4.1.674.10892.2.1.1.2
Description	Defines the short product name of a chassis management controller.
Syntax	DellString
Access	Read-only

Table 11. DRsProductDescription

Name	drsProductDescription
Object ID	1.3.6.1.4.1.674.10892.2.1.1.3
Description	Defines the product description of a chassis management controller.
Syntax	DellString
Access	Read-only

Table 12. DRsProductManufacturer

Name	drsProductManufacturer
Object ID	1.3.6.1.4.1.674.10892.2.1.1.4

Description	Defines the product manufacturer of a chassis management controller.
Syntax	DellString
Access	Read-only

Table 13. DRsProductVersion

Name	drsProductVersion
Object ID	1.3.6.1.4.1.674.10892.2.1.1.5
Description	Defines the product version of a chassis management controller.
Syntax	DellString
Access	Read-only

Table 14. DRsChassisServiceTag

Name	drsChassisServiceTag
Object ID	1.3.6.1.4.1.674.10892.2.1.1.6
Description	Defines the Service Tag of the chassis.
Syntax	DellString
Access	Read-only

Table 15. DRsProductURL

Name	drsProductURL
Object ID	1.3.6.1.4.1.674.10892.2.1.1.7
Description	Defines the out-of-band UI URL of a chassis management controller.
Syntax	DellString
Access	Read-only

Table 16. DRsProductChassisAssetTag

Name	drsProductChassisAssetTag
Object ID	1.3.6.1.4.1.674.10892.2.1.1.8
Description	Defines the Asset Tag of the chassis.
Syntax	DellString
Access	Read-only

Table 17. DRsProductChassisLocation

Name	drsProductChassisLocation
Object ID	1.3.6.1.4.1.674.10892.2.1.1.9
Description	Defines the location of the chassis.
Syntax	DellString
Access	Read-only

Table 18. DRsProductChassisName

Name	drsProductChassisName
Object ID	1.3.6.1.4.1.674.10892.2.1.1.10
Description	Defines the name of the chassis.
Syntax	DellString
Access	Read-only

Table 19. DRsSystemServiceTag

Name	drsSystemServiceTag
Object ID	1.3.6.1.4.1.674.10892.2.1.1.11
Description	Defines the service tag of a system.
Syntax	DellString
Access	Read-only

Table 20. DRsProductSystemAssetTag

Name	drsProductSystemAssetTag
Object ID	1.3.6.1.4.1.674.10892.2.1.1.12
Description	Defines the asset tag of a system.
Syntax	DellString
Access	Read-only

Table 21. DRsProductSystemSlot

Name	drsProductSystemSlot
Object ID	1.3.6.1.4.1.674.10892.2.1.1.13
Description	Defines the slot number of a CMC.
Syntax	DellString
Access	Read-only

Table 22. DRsProductType

Name	drsProductType
Object ID	1.3.6.1.4.1.674.10892.2.1.1.14
Description	Defines type of a remote access card.
Syntax	DellRacType
Access	Read-only

Table 23. DRsProductChassisDataCenter

Name	drsProductChassisDataCenter
Object ID	1.3.6.1.4.1.674.10892.2.1.1.15

Description	Defines the data center locator of the chassis.
Syntax	DellString
Access	Read-only

Table 24. DRsProductChassisAisle

Name	drsProductChassisAisle
Object ID	1.3.6.1.4.1.674.10892.2.1.1.16
Description	Defines the aisle locator of the chassis.
Syntax	DellString
Access	Read-only

Table 25. DRsProductChassisRack

Name	drsProductChassisRack
Object ID	1.3.6.1.4.1.674.10892.2.1.1.17
Description	Defines the rack locator of the chassis.
Syntax	DellString
Access	Read-only

Table 26. DRsProductChassisRackSlot

Name	drsProductChassisRackSlot
Object ID	1.3.6.1.4.1.674.10892.2.1.1.18
Description	Defines the rack slot locator of the chassis.
Syntax	DellString
Access	Read-only

Table 27. DRsProductChassisModel

Name	drsProductChassisModel
Object ID	1.3.6.1.4.1.674.10892.2.1.1.19
Description	Defines the model of the chassis.
Syntax	DellString
Access	Read-only

Table 28. DRsProductChassisExpressServiceCode

Name	drsProductChassisExpressServiceCode
Object ID	1.3.6.1.4.1.674.10892.2.1.1.20
Description	Defines the express service code of the chassis.
Syntax	DellString
Access	Read-only

Table 29. DRsProductChassisSystemID

Name	drsProductChassisSystemID
Object ID	1.3.6.1.4.1.674.10892.2.1.1.21
Description	Defines the system ID of the chassis.
Syntax	INTEGER
Access	Read-only

Table 30. DRsProductChassisSize

Name	drsProductChassisSize
Object ID	1.3.6.1.4.1.674.10892.2.1.1.22
Description	Defines the size of the chassis in rack units (U). A U is a standard unit of measure for the height of a rack or rack-mountable component.
Syntax	INTEGER
Access	Read-only

Table 31. DRsFirmwareVersion

Name	drsFirmwareVersion
Object ID	1.3.6.1.4.1.674.10892.2.1.2.1
Description	Defines the firmware version of a chassis management controller 1.
Syntax	DellString
Access	Read-only

Table 32. DRsiKVMFirmwareVersion

Name	drsiKVMFirmwareVersion
Object ID	1.3.6.1.4.1.674.10892.2.1.2.2
Description	Defines the firmware version of the iKVM.
Syntax	DellString
Access	Read-only

Table 33. DRsFirmwareVersion2

Name	drsFirmwareVersion2
Object ID	1.3.6.1.4.1.674.10892.2.1.2.3
Description	Defines the firmware version of chassis management controller 2.
Syntax	DellString
Access	Read-only

Chassis Status

The following MIB attributes provide status information on the chassis being monitored by the chassis management controller.

Table 34. DRSGlobalSystemStatus

Name	drsGlobalSystemStatus
Object ID	1.3.6.1.4.1.674.10892.2.2.1
Description	Defines the overall chassis status being monitored by the chassis management card.
Syntax	DellStatus
Access	Read-only

Table 35. DRSGlobalCurrStatus

Name	drsGlobalCurrStatus
Object ID	1.3.6.1.4.1.674.10892.2.3.1.1
Description	Defines the overall chassis status being monitored by the chassis management card.
Syntax	DellStatus
Access	Read-only

Table 36. DRsIOMCurrStatus

Name	drsIOMCurrStatus
Object ID	1.3.6.1.4.1.674.10892.2.3.1.2
Description	Defines the IOM subsystem status being monitored by the chassis management card.
Syntax	DellStatus
Access	Read-only

Table 37. DRsKVMCurrStatus

Name	drsKVMCurrStatus
Object ID	1.3.6.1.4.1.674.10892.2.3.1.3
Description	Defines the iKVM subsystem health status being monitored by the chassis management card.
Syntax	DellStatus
Access	Read-only

Table 38. DRsRedCurrStatus

Name	drsRedCurrStatus
Object ID	1.3.6.1.4.1.674.10892.2.3.1.4

Description	Defines the redundancy status being monitored by the chassis management card.
Syntax	DellStatus
Access	Read-only

Table 39. DRsPowerCurrStatus

Name	drsPowerCurrStatus
Object ID	1.3.6.1.4.1.674.10892.2.3.1.5
Description	Defines the power subsystem health status being monitored by the chassis management card.
Syntax	DellStatus
Access	Read-only

Table 40. DRsFanCurrStatus

Name	drsFanCurrStatus
Object ID	1.3.6.1.4.1.674.10892.2.3.1.6
Description	Defines the fan subsystem health status being monitored by the chassis management card.
Syntax	DellStatus
Access	Read-only

Table 41. DRsBladeCurrStatus

Name	drsBladeCurrStatus
Object ID	1.3.6.1.4.1.674.10892.2.3.1.7
Description	Defines the blade subsystem health status being monitored by the chassis management card.
Syntax	DellStatus
Access	Read-only

Table 42. DRsTempCurrStatus

Name	drsTempCurrStatus
Object ID	1.3.6.1.4.1.674.10892.2.3.1.8
Description	Defines the temperature sensor subsystem health status being monitored by the chassis management card.
Syntax	DellStatus
Access	Read-only

Table 43. DRsCMCCurrStatus

Name	drsCMCCurrStatus
Object ID	1.3.6.1.4.1.674.10892.2.3.1.9

Description	Defines the CMC health status being monitored by the chassis management card.
Syntax	DellStatus
Access	Read-only

Table 44. DRsChassisFrontPanelAmbientTemperature

Name	drsChassisFrontPanelAmbientTemperature
Object ID	1.3.6.1.4.1.674.10892.2.3.1.10
Description	Defines the ambient temperature reading (in degrees Celsius) for the chassis front panel controller.
Syntax	DellTemperatureReading
Access	Read-only

Table 45. DRsCMCAmbientTemperature

Name	drsCMCAmbientTemperature
Object ID	1.3.6.1.4.1.674.10892.2.3.1.11
Description	Defines the ambient temperature reading (in degrees Celsius) for the chassis management card.
Syntax	DellTemperatureReading
Access	Read-only

Table 46. DRsCMCProcessorTemperature

Name	drsCMCProcessorTemperature
Object ID	1.3.6.1.4.1.674.10892.2.3.1.12
Description	Defines the temperature reading (in degrees Celsius) for the chassis management card processor.
Syntax	DellTemperatureReading
Access	Read-only

Table 47. DRsGlobalPrevStatus

Name	drsGlobalPrevStatus
Object ID	1.3.6.1.4.1.674.10892.2.3.2.1
Description	Defines the previous chassis status recorded by the chassis management card.
Syntax	DellStatus
Access	Read-only

Table 48. DRsIOMPprevStatus

Name	drsIOMPprevStatus
Object ID	1.3.6.1.4.1.674.10892.2.3.2.2

Description	Defines the previous IOM subsystem status recorded by the chassis management card.
Syntax	DellStatus
Access	Read-only

Table 49. DRsKVMPrevStatus

Name	drsKVMPrevStatus
Object ID	1.3.6.1.4.1.674.10892.2.3.2.3
Description	Defines the previous iKVM subsystem health status recorded by the chassis management card.
Syntax	DellStatus
Access	Read-only

Table 50. DRsRedPrevStatus

Name	drsRedPrevStatus
Object ID	1.3.6.1.4.1.674.10892.2.3.2.4
Description	Defines the previous redundancy status recorded by the chassis management card.
Syntax	DellStatus
Access	Read-only

Table 51. DRsPowerPrevStatus

Name	drsPowerPrevStatus
Object ID	1.3.6.1.4.1.674.10892.2.3.2.5
Description	Defines the previous power subsystem health status recorded by the chassis management card.
Syntax	DellStatus
Access	Read-only

Table 52. DRsFanPrevStatus

Name	drsFanPrevStatus
Object ID	1.3.6.1.4.1.674.10892.2.3.2.6
Description	Defines the previous fan health status being monitored by the chassis management card.
Syntax	DellStatus
Access	Read-only

Table 53. DRsBladePrevStatus

Name	drsBladePrevStatus
Object ID	1.3.6.1.4.1.674.10892.2.3.2.7

Description	Defines the previous blade subsystem health status recorded by the chassis management card.
Syntax	DellStatus
Access	Read-only

Table 54. DRSTempPrevStatus

Name	drsTempPrevStatus
Object ID	1.3.6.1.4.1.674.10892.2.3.2.8
Description	Defines the temperature sensor health status being monitored by the chassis management card.
Syntax	DellStatus
Access	Read-only

Table 55. DRSCMCPrevStatus

Name	drsCMCPrevStatus
Object ID	1.3.6.1.4.1.674.10892.2.3.2.9
Description	Defines the CMC health status being monitored by the chassis management card.
Syntax	DellStatus
Access	Read-only

Table 56. DRSGlobalChangeTime

Name	drsGlobalChangeTime
Object ID	1.3.6.1.4.1.674.10892.2.3.3.1
Description	Defines the timestamp of the most recent global status change.
Syntax	TimeTicks
Access	Read-only

Table 57. DRsIOMChangeTime

Name	drsIOMChangeTime
Object ID	1.3.6.1.4.1.674.10892.2.3.3.2
Description	Defines the timestamp of the most recent IOM status change.
Syntax	TimeTicks
Access	Read-only

Table 58. DRsKVMChangeTime

Name	drsKVMChangeTime
Object ID	1.3.6.1.4.1.674.10892.2.3.3.3
Description	Defines the timestamp of the most recent iKVM status change.

Syntax	TimeTicks
Access	Read-only

Table 59. DRsRedChangeTime

Name	drsRedChangeTime
Object ID	1.3.6.1.4.1.674.10892.2.3.3.4
Description	Defines the timestamp of the most recent Redundancy status change.
Syntax	TimeTicks
Access	Read-only

Table 60. DRsPowerChangeTime

Name	drsPowerChangeTime
Object ID	1.3.6.1.4.1.674.10892.2.3.3.5
Description	Defines the timestamp of the most recent power health status change.
Syntax	TimeTicks
Access	Read-only

Table 61. DRsFanChangeTime

Name	drsFanChangeTime
Object ID	1.3.6.1.4.1.674.10892.2.3.3.6
Description	Defines the timestamp of the most recent fan health status change.
Syntax	TimeTicks
Access	Read-only

Table 62. DRsBladeChangeTime

Name	drsBladeChangeTime
Object ID	1.3.6.1.4.1.674.10892.2.3.3.7
Description	Defines the timestamp of the most recent blade health status change.
Syntax	TimeTicks
Access	Read-only

Table 63. DRsTempChangeTime

Name	drsTempChangeTime
Object ID	1.3.6.1.4.1.674.10892.2.3.3.8
Description	Defines the timestamp of the most recent temperature sensor health status change.
Syntax	TimeTicks
Access	Read-only

Table 64. DRsCMCChangeTime

Name	drsCMCChangeTime
Object ID	1.3.6.1.4.1.674.10892.2.3.3.9
Description	Defines the timestamp of the most recent CMC health status change.
Syntax	TimeTicks
Access	Read-only

Chassis Power

The following MIB tables provide power information for the chassis being monitored by the chassis management controller.

Table 65. DRsCMC Power Table

Name	drsCMCPowerTable
Object ID	1.3.6.1.4.1.674.10892.2.4.1
Description	Defines the CMC power table.
Syntax	SEQUENCE OF DrsCMCPowerTableEntry
Access	Not-accessible

Table 66. DRsCMC Power Table Entry

Name	drsCMCPowerTableEntry
Object ID	1.3.6.1.4.1.674.10892.2.4.1.1
Description	Defines the CMC power table entry.
Syntax	DrsCMCPowerTableEntry
Access	Not-accessible

Table 67. DRsCMC PSU Table

Name	drsCMCPSU Table
Object ID	1.3.6.1.4.1.674.10892.2.4.2
Description	Defines the CMC PSU table.
Syntax	SEQUENCE OF DrsCMCPSU TableEntry
Access	Not-accessible

Table 68. DRsCMC PSU Table Entry

Name	drsCMCPSU TableEntry
Object ID	1.3.6.1.4.1.674.10892.2.4.2.1
Description	Defines the CMC PSU table entry.
Syntax	DrsCMCPSU TableEntry
Access	Not-accessible

CMC Power Information

The following MIB tables provide information on the chassis power.

Table 69. DRsChassisIndex

Name	drsChassisIndex
Object ID	1.3.6.1.4.1.674.10892.2.4.1.1.1
Description	Defines the index (one-based) of the associated chassis.
Syntax	DellCMCPowerIndexRange
Access	Read-only

Table 70. DRsPotentialPower

Name	drsPotentialPower
Object ID	1.3.6.1.4.1.674.10892.2.4.1.1.2
Description	Defines the power (in watts) required by the chassis infrastructure, along with the maximum power requirements for all systems currently turned on.
Syntax	DellPowerReading
Access	Read-only

Table 71. DRsIdlePower

Name	drsIdlePower
Object ID	1.3.6.1.4.1.674.10892.2.4.1.1.3
Description	Defines the power (in watts) required by the chassis infrastructure, along with the minimum power requirements for all systems currently turned on.
Syntax	DellPowerReading
Access	Read-only

Table 72. DRsMaxPowerSpecification

Name	drsMaxPowerSpecification
Object ID	1.3.6.1.4.1.674.10892.2.4.1.1.4
Description	Defines the power limit (in watts) at which server throttling takes place.
Syntax	DellPowerReading
Access	Read-only

Table 73. DRsPowerSurplus

Name	drsPowerSurplus
Object ID	1.3.6.1.4.1.674.10892.2.4.1.1.5
Description	Defines the power surplus (in watts) remaining above the drsPotentialPower reading.

Syntax	DellPowerReading
Access	Read-only

Table 74. DRsKWhCumulative

Name	drsKWhCumulative
Object ID	1.3.6.1.4.1.674.10892.2.4.1.1.6
Description	Defines the cumulative chassis power usage (in KWh) since last reset.
Syntax	DellPowerReading
Access	Read-only

Table 75. DRsKWhCumulativeTime

Name	drsKWhCumulativeTime
Object ID	1.3.6.1.4.1.674.10892.2.4.1.1.7
Description	Defines the timestamp of the most recent chassis power accumulator reset.
Syntax	DellTimestamp
Access	Read-only

Table 76. DRsWattsPeakUsage

Name	drsWattsPeakUsage
Object ID	1.3.6.1.4.1.674.10892.2.4.1.1.8
Description	Defines the chassis peak power usage (in watts) since last reset.
Syntax	DellPowerReading
Access	Read-only

Table 77. DRsWattsPeakTime

Name	drsWattsPeakTime
Object ID	1.3.6.1.4.1.674.10892.2.4.1.1.9
Description	Defines the timestamp of the most recent chassis peak power usage.
Syntax	DellTimestamp
Access	Read-only

Table 78. DRsWattsMinUsage

Name	drsWattsMinUsage
Object ID	1.3.6.1.4.1.674.10892.2.4.1.1.10
Description	Defines the chassis minimum power usage (in watts) since last reset.
Syntax	DellPowerReading
Access	Read-only

Table 79. DRsWattsMinTime

Name	drsWattsMinTime
Object ID	1.3.6.1.4.1.674.10892.2.4.1.1.11
Description	Defines the time stamp of the most recent chassis minimum power usage.
Syntax	DellPowerReading
Access	Read-only

Table 80. DRsWattsResetTime

Name	drsWattsResetTime
Object ID	1.3.6.1.4.1.674.10892.2.4.1.1.12
Description	Defines the time stamp of the most recent reset of the chassis minimum/maximum watts readings.
Syntax	DellTimestamp
Access	Read-only

Table 81. DRsWattsReading

Name	drsWattsReading
Object ID	1.3.6.1.4.1.674.10892.2.4.1.1.13
Description	Defines the instantaneous chassis power usage (in watts).
Syntax	DellPowerReading
Access	Read-only

Table 82. DRsAmpsReading

Name	drsAmpsReading
Object ID	1.3.6.1.4.1.674.10892.2.4.1.1.14
Description	Defines the instantaneous chassis current usage (in watts).
Syntax	DellPowerReading
Access	Read-only

CMC PSU Information

The following MIB tables provide information on the chassis power supply units.

Table 83. DRsPSUChassisIndex

Name	drsPSUChassisIndex
Object ID	1.3.6.1.4.1.674.10892.2.4.2.1.1
Description	Defines the index (one-based) of the associated chassis.
Syntax	DellCMCPowerIndexRange

Access Read-only

Table 84. DRsPSUIndex

Name drsPSUIndex
Object ID 1.3.6.1.4.1.674.10892.2.4.2.1.2
Description Defines the index (one-based) of the associated CMC PSU.
Syntax DellCMCPSUIndexRange
Access Read-only

Table 85. DRsPSULocation

Name drsPSULocation
Object ID 1.3.6.1.4.1.674.10892.2.4.2.1.3
Description Defines the location of the CMC PSU.
Syntax DellString
Access Read-only

Table 86. DRsPSUMonitoringCapable

Name drsPSUMonitoringCapable
Object ID 1.3.6.1.4.1.674.10892.2.4.2.1.4
Description Defines the monitoring capabilities or the absence of a PSU in this location.
Syntax DellCMCPSUCapable
Access Read-only

Table 87. DRsPSUVoltsReading

Name drsPSUVoltsReading
Object ID 1.3.6.1.4.1.674.10892.2.4.2.1.5
Description Defines the instantaneous PSU voltage reading.
Syntax DellPowerReading
Access Read-only

Table 88. DRsPSUAmpsReading

Name drsPSUAmpsReading
Object ID 1.3.6.1.4.1.674.10892.2.4.2.1.6
Description Defines the instantaneous PSU current reading.
Syntax DellPowerReading
Access Read-only

Table 89. DRsPSUWattsReading

Name	drsPSUWattsReading
Object ID	1.3.6.1.4.1.674.10892.2.4.2.1.7
Description	Defines the instantaneous PSU wattage reading.
Syntax	DellPowerReading
Access	Read-only

Chassis Servers

The following MIB tables provide server information for the chassis being monitored by the chassis management controller.

Table 90. DRsCMCServerTable

Name	drsCMCServerTable
Object ID	1.3.6.1.4.1.674.10892.2.5.1
Description	Defines the CMC server table.
Syntax	SEQUENCE OF DrsCMCServerTableEntry
Access	Not-Accessible

Table 91. DRsCMCServerTableEntry

Name	drsCMCServerTableEntry
Object ID	1.3.6.1.4.1.674.10892.2.5.1.1
Description	Defines the CMC server table entry.
Syntax	DrsCMCServerTableEntry
Access	Not-Accessible

CMC Server Information

The following MIB tables provide CMC server information being monitored by the chassis management controller.

Table 92. DRsServerIndex

Name	drsServerIndex
Object ID	1.3.6.1.4.1.674.10892.2.5.1.1.1
Description	Defines the index (one-based) of the associated CMC server.
Syntax	DellCMCServerIndexRange
Access	Read-only

Table 93. DRsServerMonitoringCapable

Name	drsServerMonitoringCapable
Object ID	1.3.6.1.4.1.674.10892.2.5.1.1.2
Description	Defines the monitoring capabilities, or the absence of a server in this location.
Syntax	DellCMCServerCapable
Access	Read-only

Table 94. DRsServerServiceTag

Name	drsServerServiceTag
Object ID	1.3.6.1.4.1.674.10892.2.5.1.1.3
Description	Defines the Service Tag of the CMC server.
Syntax	DellString
Access	Read-only

Table 95. DRsServerSlotName

Name	drsServerSlotName
Object ID	1.3.6.1.4.1.674.10892.2.5.1.1.4
Description	Defines the slot name of the CMC server.
Syntax	DellString
Access	Read-only

Table 96. DRsServerSlotNumber

Name	drsServerSlotNumber
Object ID	1.3.6.1.4.1.674.10892.2.5.1.1.5
Description	Defines the chassis slot number of the CMC server.
Syntax	DellString
Access	Read-only

Table 97. DRsServerNodeID

Name	drsServerNodeID
Object ID	1.3.6.1.4.1.674.10892.2.5.1.1.6
Description	Defines the Node ID of the CMC server. The Node ID provides a unique identifier for the server.
Syntax	DellString
Access	Read-only

Table 98. DRsServerModel

Name	drsServerModel
Object ID	1.3.6.1.4.1.674.10892.2.5.1.1.7
Description	This attribute defines the Model of the CMC server.
Syntax	DellString
Access	Read-only

Table 99. DRsServerAssetTag

Name	drsServerAssetTag
Object ID	1.3.6.1.4.1.674.10892.2.5.1.1.8
Description	This attribute defines the Asset Tag of the CMC server.
Syntax	DellString
Access	Read-only

Table 100. DRsServerNumStorageControllers

Name	drsServerNumStorageControllers
Object ID	1.3.6.1.4.1.674.10892.2.5.1.1.9
Description	This attribute defines the number of storage controllers on the storage sled. The value will be zero if this is not a storage sled.
Syntax	INTEGER
Access	Read-only

Table 101. DRsServerStorageMode

Name	drsServerStorageMode
Object ID	1.3.6.1.4.1.674.10892.2.5.1.1.10
Description	This attribute defines the Storage Mode of the storage sled.
Syntax	DellCMCServerStorageMode
Access	Read-only

Table 102. DRsServerIntrusionState

Name	drsServerIntrusionState
Object ID	1.3.6.1.4.1.674.10892.2.5.1.1.11
Description	This attribute defines the Intrusion State of the CMC server if supported by the server.
Syntax	DellCMCServerIntrusionState
Access	Read-only

Table 103. DRsServerAssignedServerSlots

Name	drsServerAssignedServerSlots
Object ID	1.3.6.1.4.1.674.10892.2.5.1.1.12
Description	This attribute defines the server slots to which a storage sled is assigned. If this is a storage sled that is assigned to one more or more server slots, the value will be a comma-separated list of one or more server slot names. If the storage sled is not assigned to a server slot, the value will be an empty string. If this is not a storage sled, the value will be N/A.
Syntax	DellString
Access	Read-only

Chassis Alert

The following MIB tables provide information on the chassis management controller alerts.

Table 104. DRsCASubSystem

Name	drsCASubSystem
Object ID	1.3.6.1.4.1.674.10892.2.20.10.1
Description	Defines the subsystem name of the CMC Alert.
Syntax	DellString
Access	Read-only

Table 105. DrsCASSCurrStatus

Name	drsCASSCurrStatus
Object ID	1.3.6.1.4.1.674.10892.2.20.10.2
Description	Defines the current status of the alerting subsystem.
Syntax	DellStatus
Access	Read-only

Table 106. DrsCASSPrevStatus

Name	drsCASSPrevStatus
Object ID	1.3.6.1.4.1.674.10892.2.20.10.3
Description	Defines the previous status of the alerting subsystem.
Syntax	DellStatus
Access	Read-only

Table 107. DrsCASSChangeTime

Name	drsCASSChangeTime
Object ID	1.3.6.1.4.1.674.10892.2.20.10.4

Description	Defines the time stamp of the most recent change of the alerting subsystem.
Syntax	TimeTicks
Access	Read-only

Table 108. DrsCAMessage

Name	drsCAMessage
Object ID	1.3.6.1.4.1.674.10892.2.20.10.5
Description	Defines the CSSD message of the CMC alert.
Syntax	DellString
Access	Read-only

Chassis Alert 2

Table 109. DRsCA2MessageID

Name	drsCA2MessageID
Object ID	1.3.6.1.4.1.674.10892.2.21.10.1
Description	Defines the message ID of the alert.
Syntax	DisplayString
Access	Read-only

Table 110. DrsCA2Message

Name	drsCA2Message
Object ID	1.3.6.1.4.1.674.10892.2.21.10.2
Description	Defines the message describing the alert.
Syntax	DellString
Access	Read-only

Table 111. DrsCA2MessageArgs

Name	drsCA2MessageArgs
Object ID	1.3.6.1.4.1.674.10892.2.21.10.3
Description	Defines the concatenated set of strings that represent the message arguments that are used to construct the alert message. The message argument strings are enclosed within double quotes and are separated with a comma. Double quotes used within the message argument strings are preprocessed and changed to single quotes.
Syntax	DellString
Access	Read-only

Table 112. DrsCA2AlertStatus

Name	drsCA2AlertStatus
Object ID	1.3.6.1.4.1.674.10892.2.21.10.4
Description	Defines the status of the alert.
Syntax	DellStatus
Access	Read-only

Table 113. DrsCA2FQDD

Name	drsCA2FQDD
Object ID	1.3.6.1.4.1.674.10892.2.21.10.5
Description	Defines the fully qualified device descriptor of device causing the alert.
Syntax	DisplayString
Access	Read-only

Legacy Alerting

The following MIB tables provide information on the RAC legacy alerting.

Table 114. DRsAlertSystem

Name	drsAlertSystem
Object ID	1.3.6.1.4.1.674.10892.2.5000.10.1
Description	Name of the system generating the alert.
Syntax	Octet String
Access	Read-only

Table 115. DRsAlertTableIndexOID

Name	drsAlertTableIndexOID
Object ID	1.3.6.1.4.1.674.10892.2.5000.10.2
Description	Alert Index Object Identifier.
Syntax	OBJECT IDENTIFIER
Access	Read-only

Table 116. DRsAlertMessage

Name	drsAlertMessage
Object ID	1.3.6.1.4.1.674.10892.2.5000.10.3
Description	Message describing the alert.
Syntax	Octet String
Access	Read-only

Table 117. DRsAlertCurrentStatus

Name	drsAlertCurrentStatus
Object ID	1.3.6.1.4.1.674.10892.2.5000.10.4
Description	Current status of object causing the alert.
Syntax	DellStatus
Access	Read-only

Table 118. DRsAlertPreviousStatus

Name	drsAlertPreviousStatus
Object ID	1.3.6.1.4.1.674.10892.2.5000.10.5
Description	Previous status of object causing the alert.
Syntax	DellStatus
Access	Read-only

Table 119. DRsAlertData

Name	drsAlertData
Object ID	1.3.6.1.4.1.674.10892.2.5000.10.6
Description	Alert data
Syntax	Octet String
Access	Read-only

SNMP Traps

SNMP is frequently used to monitor systems for fault conditions such as temperature violations, hard drive failures, and so on. Management applications can monitor for these conditions by polling the appropriate OIDs with the Get command and analyzing the returned data. This method has its drawbacks. If it is done frequently, significant amounts of network bandwidth can be consumed. If it is done infrequently, the response to the fault condition may not occur in a timely fashion. SNMP traps avoid these limitations of the polling method.

An SNMP trap is an asynchronous event indicating that something significant has occurred. This is analogous to a pager receiving an important message, except that the SNMP trap frequently contains all the information needed to diagnose a fault.

Two drawbacks to SNMP traps are that they are sent using UDP, which is not a guaranteed delivery mechanism, and that they are not acknowledged by the receiver.

An SNMP trap message contains the trap's enterprise OID, the agent IP address, a generic trap ID, the specific trap ID, a time stamp, and zero or more variable bindings (varbinds). The combination of an enterprise OID and a specific trap ID uniquely identifies each Server Administrator-defined trap. A varbind consists of an OID and its value and provides additional information about the trap.

In order for a management system to receive SNMP traps from a managed system, the node must be configured to send traps to the management system. Trap destination configuration is dependent on the operating system. When this configuration is done, a management application on the management system can wait for traps and act on them when received.

For a list of traps supported by the Remote Access Controller, see RAC Traps, BMC Traps ,iDRAC7 and iDRAC8 Traps.

Understanding Trap Severity

Traps often contain information about values recorded by probes or sensors. Probes and sensors monitor critical components for values such as amperage, voltage, and temperature. When an event occurs on your system, the Server Administrator sends information about one of the following event types to the system management console:

- **Information/Informational**—An event that describes the successful operation of a unit, such as a power supply turning on or a sensor reading returning to normal.
- **Warning** — An event that is not necessarily significant, but may indicate a possible future problem, such as crossing a warning threshold.
- **Critical/Error** — A significant event that indicates actual or imminent loss of data or loss of function, such as crossing a failure threshold or a hardware failure.

RAC Traps

This section describes the traps that are generated by the SNMP agent of the Remote Access Controller (RAC). All of the enterprise-specific traps documented in this section belong to the MIB enterprise identified by OID 1.3.6.1.4.1.674.10892.2 and are sent with all of the trap variables documented in the section. The trap variables are sent in the order in which they are listed.


 **NOTE:** The PowerEdge M1000e CMC, PowerEdge VRTX CMC and PowerEdge FX2 CMC do not generate the traps in this section. They generate the traps documented in the CMC Traps.

Table 120. RAC Traps

TrapID	Name	Description	Severity	Category	Cause	Support ed by RAC Platform
0	CodeStart	SNMP agent is initializing itself	Information	Status	RAC power on or reset.	All
1	Authentication	Failure Request received with an invalid community name	Critical	Error	SNMP request with an invalid community name.	All
1001	alertDrscTest TrapEvent	The RAC generated a test trap event in response to a user request	Information	Status	A test SNMP trap generated by a RAC.	All
1002	alertDrscAuth Error	RAC Authentication failures during a time period have exceeded a threshold	Minor	Error	RAC login failure caused by authentication failure, number of concurrent logins exceed limit, or permission denied.	All
1015	alertDrscSE L	Warning The RAC has detected a new event in the System Event Log with Severity: Warning	Major	Error	RAC detected a new system event log with warning severity (detailed log info is in drsAlert Message varbind).	All
1016	alertDrscSE L	Critical The RAC has	Critical	Error	RAC detected a new system event log with	All

TrapID	Name	Description	Severity	Category	Cause	Support ed by RAC Platfor m
		detected a new event in the System Event Log with Severity: Critical			critical severity (detailed log info is in drsAlert Message varbind).	
1017	alertDrscSEL 80 percentFull	The RAC system event log is 80% full	Major	Status	RAC detected system event log is 80% full.	All
1018	alertDrscSEL 90 percentFull	The RAC system event log is 90% full	Major	Status	RAC detected system event log is 90% full.	All
1018	alertDrscSEL 90 percentFull	The RAC system event log is 90% full	Major	Status	RAC detected system event log is 90% full.	All
1020	alertDrscSEL Normal	The RAC has detected a new event in the System Event Log with Severity: Normal	Information	Error	RAC detected a new system event log with normal severity (detailed log info is in drsAlert Message varbind).	All

BMC Traps

The BMC monitors the system for critical events by communicating with various sensors on the system board and by sending alerts and log events when certain parameters exceed their preset thresholds. All of the traps documented in this section belong to the MIB enterprise identified by OID 1.3.6.1.4.1.3183.1.1.1.

TrapID	Description	Severity
262402	Generic Critical Fan Failure	Critical
262530	Generic Critical Fan Failure Cleared	Information
131330	Under-Voltage Problem (Lower Critical - going low)	Critical
131458	Under-Voltage Problem Cleared	Information
131841	Generic Critical Voltage Problem	Critical
131840	Generic Critical Voltage Problem Cleared	Information

TrapID	Description	Severity
65792	Under-Temperature Warning (Lower non-critical, going low)	Warning
65920	Under-Temperature Warning Cleared	Information
65794	Under-Temperature Problem (Lower Critical - going low)	Critical
65922	Under-Temperature Problem Cleared	Information
65799	Over-Temperature warning (Upper non-critical, going high)	Minor
65927	Over-Temperature warning Cleared	Information
65801	Over-Temperature Problem (Upper Critical - going high)	Critical
65929	Over-Temperature Problem Cleared	Information
131328	Under-Voltage Warning (Lower Non Critical - going low)	Warning
131456	Under-Voltage Warning Cleared	Information
131330	Under-Voltage Problem (Lower Critical - going low)	Critical
131458	Under-Voltage Problem Cleared	Information
131335	Over-Voltage Warning (Upper Non Critical - going high)	Warning
131463	Over-Voltage Warning Cleared	Information
131337	Over-Voltage Problem (Upper Critical - going high)	Critical
131465	Over-Voltage Problem Cleared	Information
131841	Generic Critical Voltage Problem	Critical
131840	Generic Critical Voltage Problem Cleared	Information
356096	Chassis Intrusion - Physical Security Violation	Critical
356224	Chassis Intrusion (Physical Security Violation) Event Cleared	Information
262400	Generic Predictive Fan Failure (predictive failure asserted)	Minor

TrapID	Description	Severity
262528	Generic Predictive Fan Failure Cleared	Information
262402	Generic Critical Fan Failure	Critical
262530	Generic Critical Fan Failure Cleared	Information
264962	Fan redundancy has been degraded	Warning
264961	Fan Redundancy Lost	Critical
264960	Fan redundancy has returned to Normal	Information
2715392	Battery Low (Predictive Failure)	Warning
2715520	Battery Low (Predictive Failure) Cleared	Information
2715393	Battery Failure	Critical
2715521	Battery Failure Cleared	Information
487169	CPU Thermal Trip (Over Temperature Shutdown)	Critical
487297	CPU Thermal Trip (Over Temperature Shutdown) Cleared	Information
487168	CPU Internal Error Critical 487296 CPU Internal Error Cleared	Information
487173	CPU Configuration Error	Critical
487301	CPU Configuration Error Cleared	Information
487175	CPU Presence (Processor Presence detected)	Information
487303	CPU Not Present (Processor Not Present)	Critical
487170	CPU BIST (Built In Self Test) Failure	Critical
487298	CPU BIST (Built In Self Test) Failure Cleared	Information
487176	CPU Disabled (Processor Disabled)	Critical
487304	CPU Enabled (Processor Enabled)	Information
487178	CPU Throttle (Processor Speed Reduced)	Warning

TrapID	Description	Severity
487306	CPU Throttle Cleared (Normal Processor Speed)	Information
527106	Power Supply Redundancy Degraded	Warning
527105	Power Supply Redundancy Lost	Critical
527104	Power Supply Redundancy has returned to Normal	Information
552704	Power Supply Inserted	Information
552832	Power Supply Removed	Warning
552705	Power Supply Failure	Critical
552833	Power Supply Failure Cleared	Information
552706	Power Supply Warning	Warning
552834	Power Supply Warning Cleared	Information
552707	Power Supply AC Lost	Critical
552835	Power Supply AC Restored	Information
789249	Memory Redundancy has been Lost	Critical
789248	Memory redundancy has returned to Normal	Information
1076994	System Event Log (SEL) Cleared	Information
1076996	System Event Log (SEL) Full (Logging Disabled)	Critical
2322176	ASR (Automatic System Recovery) Timer Expired	Critical
2322177	ASR (Automatic System Recovery) Reset Occurred	Critical
2322178	ASR (Automatic System Recovery) Power Down Occurred	Critical
2322179	ASR (Automatic System Recovery) Power Cycle Occurred	Critical

PowerEdge M1000e CMC Traps

This section describes the traps that are generated by the SNMP agent of the PowerEdge M1000e CMC. All of the enterprise-specific traps documented in this section belong to the MIB enterprise identified by OID 1.3.6.1.4.1.674.10892.2 and are sent with the following trap variables: drsProductChassisName,

drsProductChassisLocation, drsGlobalCurrStatus, drsCASubSystem, drsCASSCurrStatus, drsCASSPrevStatus, drsCASSChangeTime and drsCAMessage.

PowerEdge M1000e CMC version 5.0 and later supports a setting to generate the traps listed in the section "PowerEdge VRTX CMC Traps and PowerEdge FX2 CMC Traps". The setting is named "Enable Enhanced Chassis Logging and Events" in the PowerEdge M1000e CMC GUI and is located in the General Chassis Settings page which can be found by navigating to Chassis Overview -> Setup -> General in the CMC GUI. When the setting is disabled, the traps listed in this section are generated by the CMC. When the setting is enabled, the traps listed in the section "PowerEdge VRTX CMC Traps and PowerEdge FX2 CMC Traps" are generated by the CMC instead of the traps listed in this section. The setting is disabled by default. The trap variables are defined in the [Dell Remote Access Controller Out-of-Band Group](#) section.

Table 121. PowerEdge M1000e CMC traps

TrapID	Name	Description	Severity	Category
2000	alertCMCTestTrap	CMC has generated a test trap.	Informational	Error Events
2002	alertCMCNormalTrap	CMC reported a return-to-normal or informational event.	Normal	Error Events
2003	alertCMCWarningTrap	CMC reported a warning event.	Warning	Error Events
2004	alertCMCCriticalTrap	CMC reported a critical event.	Critical	Error Events
2005	alertCMCNonRecoverableTrap	CMC reported a catastrophic event.	Non-Recoverable	Error Events

PowerEdge VRTX CMC Traps and PowerEdge FX2 CMC Traps

This section defines the traps that are generated by the SNMP agent of the PowerEdge VRTX CMC and PowerEdge FX2 CMC. All of the enterprise-specific traps documented in this section belong to the MIB enterprise identified by OID 1.3.6.1.4.1.674.10892.2.21 and are sent with the following trap variables: drsCA2MessageID, drsCA2Message, drsCA2MessageArgs, drsCA2AlertStatus, drsCA2FQDD, drsProductChassisName, drsProductChassisLocation, drsChassisServiceTag and drsGlobalCurrStatus. The trap variables are defined in the [Dell Remote Access Controller Out-of-Band Group](#) section.

System Trap Group

The System Trap Group contains traps that fall under the System event category.

Table 122. Amperage Probe Traps

TrapID	Description	Category	SubCategory	Severity
alert2AmperageProbeNormal				
2179	Current sensor reading is within range.	Status Events	Amperage	Informational
alert2AmperageProbeWarning				

TrapID	Description	Category	SubCategory	Severity
2178	Current sensor has detected a warning value.	Status Events	Amperage	Minor
alert2AmperageProbeFailure				
2177	Current sensor has detected a failure value.	Error Events	Amperage	Critical

Table 123. Battery Traps

TrapID	Description	Category	SubCategory	Severity
alert2BatteryNormal				
2227	Battery state has returned to normal; or battery presence had been detected.	Status Events	Battery	Informational
alert2BatteryWarning				
2226	Battery is low.	Status Events	Battery	Minor
alert2BatteryFailure				
2225	Battery has failed or battery is absent.	Error Events	Battery	Critical

Table 124. Cable Traps

TrapID	Description	Category	SubCategory	Severity
alert2CableFailure				
2393	Cable failure.	Error Events	Cable	Critical

Table 125. CMC Traps

TrapID	Description	Category	SubCategory	Severity
alert2CMCWarning				
2546	Chassis Management Controller detected a warning.	Status Events	CMC	Minor
alert2CMCFailure				
2545	Chassis Management Controller detected an error.	Error Events	CMC	Critical

Table 126. Fan Traps

TrapID	Description	Category	SubCategory	Severity
alert2FanInformation				
2155	Fan information.	Status Events	Fan	Informational

TrapID	Description	Category	SubCategory	Severity
alert2FanWarning				
2154	Fan warning.	Status Events	Fan	Minor
alert2FanFailure				
2153	Fan failure.	Error Events	Fan	Critical

Table 127. Hardware Configuration Traps

TrapID	Description	Category	SubCategory	Severity
alert2HardwareConfigurationInformation				
2331	Hardware configuration information.	Status Events	Hardware Configuration	Informational
alert2HardwareConfigurationWarning				
2330	Hardware configuration warning.	Status Events	Hardware Configuration	Minor
alert2HardwareConfigurationFailure				
2329	Hardware configuration failure or critical event.	Error Events	Hardware Configuration	Critical

Table 128. IO Virtualization Traps

TrapID	Description	Category	SubCategory	Severity
alert2IOVirtualizationInformation				
2555	IO Virtualization information.	Status Events	IO Virtualization	Informational
alert2IOVirtualizationWarning				
2554	IO Virtualization warning.	Status Events	IO Virtualization	Minor
alert2IOVirtualizationFailure				
2553	IO Virtualization failure or critical event.	Error Events	IO Virtualization	Critical

Table 129. Link Status Traps

TrapID	Description	Category	SubCategory	Severity
alert2LinkStatusInformation				
2251	Link status information.	Status Events	Link Status	Informational
alert2LinkStatusWarning				
2250	Link status warning.	Status Events	Link Status	Minor
alert2LinkStatusFailure				

TrapID	Description	Category	SubCategory	Severity
2249	Link status failure or critical event.	Error Events	Link Status	Critical

Table 130. PCI Device Traps

TrapID	Description	Category	SubCategory	Severity
alert2PCIDeviceInformation				
2419	PCI device information.	Status Events	PCI Device	Informational
alert2PCIDeviceWarning				
2418	PCI device warning.	Status Events	PCI Device	Minor
alert2PCIDeviceFailure				
2417	PCI device failure or critical event.	Error Events	PCI Device	Critical

Table 131. Power Supply Traps

TrapID	Description	Category	SubCategory	Severity
alert2PowerSupplyNormal				
2187	Power supply has returned to normal.	Status Events	Power Supply	Informational
alert2PowerSupplyWarning				
2186	Power supply has detected a warning.	Status Events	Power Supply	Minor
alert2PowerSupplyFailure				
2185	Power supply has detected a failure.	Error Events	Power Supply	Critical

Table 132. Power Supply Absent Trap

TrapID	Description	Category	SubCategory	Severity
alert2PowerSupplyAbsent				
2465	Power supply is absent.	Error Events	Power Supply	Critical

Table 133. Power Usage Traps

TrapID	Description	Category	SubCategory	Severity
alert2PowerUsageInformation				
2275	Power usage information.	Status Events	Power Usage	Informational
alert2PowerUsageWarning				

TrapID	Description	Category	SubCategory	Severity
2274	Power usage warning.	Status Events	Power Usage	Minor
alert2PowerUsageFailure				
2273	Power usage failure.	Error Events	Power Usage	Critical

Table 134. Redundancy Traps

TrapID	Description	Category	SubCategory	Severity
alert2RedundancyInformation				
2475	Redundancy information.	Status Events	Redundancy	Informational
alert2RedundancyDegraded				
2474	Redundancy is degraded.	Status Events	Redundancy	Minor
alert2RedundancyLost				
2473	Redundancy is lost.	Error Events	Redundancy	Critical

Table 135. Security Event Traps

TrapID	Description	Category	SubCategory	Severity
alert2SecurityInformation				
2387	Security information.	Status Events	Security	Informational
alert2SecurityWarning				
2386	Security warning.	Status Events	Security	Minor
alert2SecurityFailure				
2385	Security failure or critical event.	Error Events	Security	Critical

Table 136. System Event Log Traps

TrapID	Description	Category	SubCategory	Severity
alert2SystemEventLogInformation				
2379	System Event Log information.	Status Events	System Event Log	Informational
alert2SystemEventLogWarning				
2378	System Event Log warning.	Status Events	System Event Log	Minor
alert2SystemEventLogFailure				
2377	System Event Log failure or critical event.	Error Events	System Event Log	Critical

Table 137. Software Configuration Traps

TrapID	Description	Category	SubCategory	Severity
alert2SoftwareConfigurationInformation				
2339	Software configuration information.	Status Events	Software Configuration	Informational
alert2SoftwareConfigurationWarning				
2338	Software configuration warning.	Status Events	Software Configuration	Minor
alert2SoftwareConfigurationFailure				
2337	Software configuration failure.	Error Events	Software Configuration	Critical

Table 138. Temperature Probe Traps

TrapID	Description	Category	SubCategory	Severity
alert2TemperatureProbeNormal				
2163	Temperature sensor value is within range.	Status Events	Temperature	Informational
alert2TemperatureProbeWarning				
2162	Temperature sensor has detected a warning value.	Status Events	Temperature	Minor
alert2TemperatureProbeFailure				
2161	Temperature sensor has detected a failure value.	Error Events	Temperature	Critical

Table 139. Voltage Probe Traps

TrapID	Description	Category	SubCategory	Severity
alert2VoltageProbeNormal				
2171	Voltage sensor reading is within range.	Status Events	Voltage	Informational
alert2VoltageProbeWarning				
2170	Voltage sensor has detected a warning value.	Status Events	Voltage	Minor
alert2VoltageProbeFailure				
2169	Voltage sensor has detected a failure value.	Error Events	Voltage	Critical

Storage Trap Group

The Storage Trap Group contains traps that fall under the Storage event category.

Table 140. Storage Battery Traps

TrapID	Description	Category	Subcategory	Severity
alert2StorageBatteryInformation				
4275	Storage battery information.	Error Events	Battery	Informational
alert2StorageBatteryWarning				
4274	Storage battery warning.	Error Events	Battery	Minor
alert2StorageBatteryFailure				
4273	Storage battery failure.	Error Events	Battery	Critical

Table 141. Storage Controller Traps

TrapID	Description	Category	Subcategory	Severity
alert2StorageControllerInformation				
4331	Storage controller information.	Error Events	Controller	Informational
alert2StorageControllerWarning				
4330	Storage controller warning.	Error Events	Controller	Minor
alert2StorageControllerFailure				
4329	Storage controller failure.	Error Events	Controller	Critical

Table 142. Storage Enclosure Traps

TrapID	Description	Category	Subcategory	Severity
alert2StorageEnclosureInformation				
4339	Storage enclosure information.	Error Events	Enclosure	Informational
alert2StorageEnclosureWarning				
4338	Storage enclosure warning.	Error Events	Enclosure	Minor
alert2StorageEnclosureFailure				
4337	Storage enclosure failure.	Error Events	Enclosure	Critical

Table 143. Storage Fan Traps

TrapID	Description	Category	Subcategory	Severity
alert2StorageFanInformation				
4203	Storage fan information.	Error Events	Fan	Informational
alert2StorageFanWarning				
4202	Storage fan warning.	Status Events	Fan	Minor

TrapID	Description	Category	Subcategory	Severity
alert2StorageFanFailure				
4201	Storage fan failure.	Error Events	Fan	Critical

Table 144. Storage Physical Disk Traps

TrapID	Description	Category	Subcategory	Severity
alert2StoragePhysicalDiskInformation				
4347	Storage physical disk information.	Error Events	Physical Disk	Informational
alert2StoragePhysicalDiskWarning				
4346	Storage physical disk warning.	Error Events	Physical Disk	Minor
alert2StoragePhysicalDiskFailure				
4345	Storage physical disk failure.	Error Events	Physical Disk	Critical

Table 145. Storage Power Supply Traps

TrapID	Description	Category	Subcategory	Severity
alert2StoragePowerSupplyInformation				
4235	Storage power supply information.	Error Events	Power Supply	Informational
alert2StoragePowerSupplyWarning				
4234	Storage power supply warning.	Error Events	Power Supply	Minor
alert2StoragePowerSupplyFailure				
4233	Storage power supply failure.	Error Events	Power Supply	Critical

Table 146. Security Event Traps

TrapID	Description	Category	Subcategory	Severity
alert2StorageSecurityInformation				
4435	Storage Security information.	Status Events	Security Event	Informational
alert2StorageSecurityWarning				
4434	Storage Security warning.	Status Events	Security Event	Minor
alert2StorageSecurityFailure				
4433	Storage Security failure or critical event	Error Events	Security Event	Critical

Table 147. Storage Management Status Traps

TrapID	Description	Category	Subcategory	Severity
alert2StorageManagementInformation				
4179	Storage Management information. There is no global status change associated with this trap.	Error Events	Storage Management	Informational
alert2StorageManagementWarning				
4178	Storage Management has detected a device independent warning condition. There is no global status change associated with this trap.	Error Events	Storage Management	Minor
alert2StorageManagementFailure				
4177	Storage Management has detected a device independent error condition. There is no global status change associated with this trap.	Error Events	Storage Management	Critical

Table 148. Storage Temperature Probe Traps

TrapID	Description	Category	Subcategory	Severity
alert2StorageTemperatureProbeInformation				
4211	Storage temperature probe information.	Error Events	Temperature Probe	Informational
alert2StorageTemperatureProbeWarning				
4210	Storage temperature probe warning.	Error Events	Temperature Probe	Minor
alert2StorageTemperatureProbeFailure				
4209	Storage temperature probe failure.	Error Events	Temperature Probe	Critical

Table 149. Storage Virtual Disk Traps

TrapID	Description	Category	Subcategory	Severity
alert2StorageVirtualDiskInformation				
4355	Storage virtual disk information.	Error Events	Virtual Disk	Informational
alert2StorageVirtualDiskWarning				

TrapID	Description	Category	Subcategory	Severity
4354	Storage virtual disk warning.	Error Events	Virtual Disk	Minor
alert2StorageVirtualDiskFailure				
4353	Storage Virtual disk failure.	Error Events	Virtual Disk	Critical

Audit Traps

The Audit Trap group contains traps that fall under the Audit event category.

Table 150. Audit CMC Traps

TrapID	Description	Category	SubCategory	Severity
alert2CMCAuditInformation				
8691	Chassis Management Controller audit information.	Status Events	CMC	Informational
alert2CMCAuditWarning				
8690	Chassis Management Controller audit warning.	Status Events	CMC	Minor
alert2CMCAuditFailure				
8689	Chassis Management Controller audit failure or critical event.	Error Events	CMC	Critical

Table 151. Audit IO Virtualization Traps

TrapID	Description	Category	SubCategory	Severity
alert2IOVirtualizationAuditWarning				
8698	IO Virtualization audit warning.	Status Events	IO Virtualization	Minor

Table 152. Audit License Traps

TrapID	Description	Category	SubCategory	Severity
alert2LicenseInformation				
8515	License information.	Status Events	License	Informational
alert2LicenseWarning				
8514	License warning.	Status Events	License	Minor
alert2LicenseFailure				
8513	License failure.	Error Events	License	Critical

Table 153. Audit PCI Device Traps

TrapID	Description	Category	SubCategory	Severity
alert2PCIDeviceAuditWarning				
8562	PCI device audit warning.	Status Events	PCI Device	Minor

Table 154. Audit Power Supply Traps

TrapID	Description	Category	SubCategory	Severity
alert2PowerSupplyAuditWarning				
8330	Power supply audit warning.	Status Events	Power Supply	Minor
alert2PowerSupplyAuditFailure				
8329	Power supply audit failure or critical event.	Error Events	Power Supply	Critical

Table 155. Audit Power Usage Traps

TrapID	Description	Category	SubCategory	Severity
alert2PowerUsageAuditInformation				
8419	Power usage audit information.	Status Events	Power Usage	Informational
alert2PowerUsageAuditWarning				
8418	Power usage audit warning.	Status Events	Power Usage	Minor
alert2PowerUsageAuditFailure				
8417	Power usage audit failure or critical event.	Error Events	Power Usage	Critical

Table 156. Audit Software Change Traps

TrapID	Description	Category	SubCategory	Severity
alert2SoftwareChangeAuditFailure				
8361	Software change audit failure or critical event.	Error Events	Software Change	Critical

Configuration Traps

The Configuration Trap group contains traps that fall under the Configuration event category.

Table 157. Configuration IO Virtualization Traps

TrapID	Description	Category	SubCategory	Severity
alert2IOVConfigurationInformation				
10747	IO virtualization configuration information.	Status Events	IO Virtualization	Informational
alert2IOVConfigurationWarning				

TrapID	Description	Category	SubCategory	Severity
10746	IO Virtualization configuration warning.	Status Events	IO Virtualization	Minor

Table 158. Configuration PCI Device Traps

TrapID	Description	Category	SubCategory	Severity
alert2PCIDeviceConfigurationInformation				
10611	PCI device configuration information.	Status Events	PCI Device	Informational

Table 159. Software Configuration Traps

TrapID	Description	Category	SubCategory	Severity
alert2SWCCConfigurationWarning				
10530	Software configuration warning.	Status Events	Software Config	Minor
alert2SWCCConfigurationFailure				
10529	Software configuration failure.	Error Events	Software Config	Critical

Table 160. Configuration Test Traps

TrapID	Description	Category	SubCategory	Severity
alert2CMCTestTrap				
10395	Test trap generated by CMC in response to a user request.	Status Events	Test	Informational

Updates Traps


The Updates Trap group contains traps that fall under the Updates event category.

Table 161. Software Change Traps

TrapID	Description	Category	Subcategory	Severity
alert2SoftwareChangeUpdateWarning				
6314	Software change update warning.	Status Events	Software Change	Minor

iDRAC MIB

The Integrated Dell Remote Access Controller (iDRAC) MIB (filename **iDRAC-SMlv1.mib/ iDRAC-SMlv2.mib**) is the MIB supported by the Integrated Dell Remote Access Controller 7 and 8 (iDRAC7 and iDRAC8). This MIB provides management data that allows you to monitor devices and software on a system via an out-of-band connection to the iDRAC7 and iDRAC8 of a system.

 **NOTE:** From iDRAC7 firmware release r1.30.30 or later and iDRAC8, the iDRAC7 or iDRAC8 MIB file is published in both types of SMI (Structure of Managed Information) notations: SMIv1 and SMIv2. The SMIv1 copy of the iDRAC7 or iDRAC8 MIB file is named iDRAC-SMlv1.mib. And the SMIv2 copy is named iDRAC-SMlv2.mib. Prior to iDRAC7 firmware release r1.30.30, only a SMIv1 copy was published. And the file name of the SMIv1 copy was **iDRAC-MIB.txt**.

Supported Systems

The iDRAC MIB supported on the following systems for this release:

Blade Servers

The Blade servers for this release:

- PowerEdge M830
- PowerEdge FC430

Rack and Tower Servers

The Rack and Tower servers for this release:

- PowerEdge R930
- PowerEdge R530xd
- C6320
- PowerEdge FX2/FX2s 1.2
- PowerEdge FD332
- DSS 2500
- DSS 1500

iDRAC Supported SNMP Versions

The following table identifies the SNMP versions that support iDRAC for the given SNMP operations.

SNMP Operations

Supported SNMP version

GET, GETNEXT, GETBULK

SNMP v1, v2c and v3

TRAP

SNMP v1, SNMP v2c and SNMP v3



NOTE: iDRAC does not support the SNMP SET operation for any data.



NOTE: iDRAC7 firmware release r1.30.30 or later and iDRAC8 supports SNMP query operations (GET, GETNEXT, GETBULK) via the SNMPv3 protocol. In addition to supporting query operations via the SNMP v1 and SNMP v2c protocols, SNMP User Security Model (USM) is supported.

iDRAC SNMP Data Security Features

iDRAC firmware supports the following data security features:

- SNMP security lockout feature
 - iDRAC supports a simply, non-configurable SNMP security lockout feature. If more than six SNMPv3 USM authentication failures occur within a 2-minute window, then the iDRAC SNMP Agent blocks all subsequent SNMPv3 requests/queries for 10 minutes.
- Restriction of access to **sensitive** data
 - Some of the MIB data that iDRAC supports can only be accessed via SNMPv3 queries. Access to such data is blocked for SNMPv1 and SNMPv2c queries.
 - Currently, the following one attribute, and one table, are considered to be “sensitive” data and have this restriction:
 - * numLCLogEntries (which has an SNMP OID of: 1.3.6.1.4.1.674.10892.5.4.300.2.0)
 - * lcLogTable (which has an SNMP OID of: 1.3.6.1.4.1.674.10892.5.4.300.90)

iDRAC Out-of-Band Group

The objects of the Integrated Dell Remote Access Controller (iDRAC) MIB (**iDRAC-SMlv1.mib** and **iDRAC-SMlv2.mib**) are organized into subgroups of the iDRAC Out-of-Band Group. The subgroups are:

- RAC Information Group
- Chassis Information Group
- System Information Group
- Status Group
- System Details Group
- Storage Details Group

The following sections document the subgroups and the objects within each subgroup.

RAC Information Group

The RAC Information Group objects provide information about the iDRAC.

Table 162. RAC Name

Name	racName
Object ID	1.3.6.1.4.1.674.10892.5.1.1.1.0

Description	This attribute defines the product name of a remote access card.
Syntax	StringType
Access	Read-only

Table 163. RAC Short Name

Name	racShortName
Object ID	1.3.6.1.4.1.674.10892.5.1.1.2.0
Description	This attribute defines the short product name of a remote access card.
Syntax	StringType
Access	Read-only

Table 164. RAC Description

Name	racDescription
Object ID	1.3.6.1.4.1.674.10892.5.1.1.3.0
Description	This attribute defines the product description of a remote access card.
Syntax	StringType
Access	Read-only

Table 165. RAC Manufacturer

Name	racManufacturer
Object ID	1.3.6.1.4.1.674.10892.5.1.1.4.0
Description	This attribute defines the product manufacturer of a remote access card.
Syntax	StringType
Access	Read-only

Table 166. RAC Version

Name	racVersion
Object ID	1.3.6.1.4.1.674.10892.5.1.1.5.0
Description	This attribute defines the product version of a remote access card.
Syntax	StringType
Access	Read-only

Table 167. RAC URL

Name	racURL
Object ID	1.3.6.1.4.1.674.10892.5.1.1.6.0
Description	This attribute defines the out-of-band UI URL of a remote access card.
Syntax	StringType

Access Read-only

Table 168. RAC Type

Name	racType
Object ID	1.3.6.1.4.1.674.10892.5.1.1.7.0
Description	This attribute defines the type of a remote access card.
Syntax	RacTypeEnum
Access	Read-only

Table 169. RAC Firmware Version

Name	racFirmwareVersion
Object ID	1.3.6.1.4.1.674.10892.5.1.1.8.0
Description	This attribute defines the firmware version of a remote access card.
Syntax	StringType
Access	Read-only

Chassis Information Group

The Chassis Information Group objects provide information about the modular chassis in which a blade system resides.


 **NOTE:** This Chassis information is only available for modular/blade systems. For Rack and Tower systems, the information is empty. Currently there is just one object under the Chassis Information Group.

Table 170. Chassis Service Tag

Name	chassisServiceTag
Object ID	1.3.6.1.4.1.674.10892.5.1.2.1.0
Description	This attribute defines the service tag of the enclosing chassis.
Syntax	StringType
Access	Read-only

Table 171. Chassis Name Modular

Name	chassisNameModular
Object ID	1.3.6.1.4.1.674.10892.5.1.2.2.0
Description	This attribute defines the chassis name of the modular chassis. The value is zero length if not a modular system.
Syntax	StringType
Access	Read-only

Table 172. Chassis Model Modular

Name	chassisModelModular
Object ID	1.3.6.1.4.1.674.10892.5.1.2.3.0
Description	This attribute defines the model of the modular chassis. The value is zero length if not a modular system.
Syntax	StringType
Access	Read-only

System Information Group

The System Information Group objects provide information about the system in which the iDRAC resides.

Table 173. System Fully Qualified Domain Name

Name	systemFQDN
Object ID	1.3.6.1.4.1.674.10892.5.1.3.1.0
Description	This attribute defines the fully qualified domain name of the system.
Syntax	StringType
Access	Read-only

Table 174. System Service Tag

Name	systemServiceTag
Object ID	1.3.6.1.4.1.674.10892.5.1.3.2.0
Description	This attribute defines the service tag of the system.
Syntax	StringType
Access	Read-only

Table 175. System Express Service Code

Name	systemExpressServiceCode
Object ID	1.3.6.1.4.1.674.10892.5.1.3.3.0
Description	This attribute defines the express service code of the system.
Syntax	StringType
Access	Read-only

Table 176. System Asset Tag

Name	systemAssetTag
Object ID	1.3.6.1.4.1.674.10892.5.1.3.4.0
Description.	This attribute defines the asset tag of the system.
Syntax	StringType
Access	Read-only

Table 177. System Blade Slot Number

Name	systemBladeSlotNumber
Object ID	1.3.6.1.4.1.674.10892.5.1.3.5.0
Description	This attribute defines the slot number of the blade in the chassis.
Syntax	StringType
Access	Read-only

Table 178. System Operating System Name

Name	systemOSName
Object ID	1.3.6.1.4.1.674.10892.5.1.3.6.0
Description	This attribute defines the name of the operating system that the host is running.
Syntax	StringType
Access	Read-only

Table 179. System Form Factor

Name	systemFormFactor
Object ID	1.3.6.1.4.1.674.10892.5.1.3.7.0
Description	This attribute defines the form factor of the system.
Syntax	SystemFormFactorEnum
Access	Read-only

Table 180. System Data Center Name

Name	systemDataCenterName
Object ID	1.3.6.1.4.1.674.10892.5.1.3.8.0
Description	This attribute defines the Data Center locator of the system.
Syntax	StringType
Access	Read-only

Table 181. System Aisle Name

Name	systemAisleName
Object ID	1.3.6.1.4.1.674.10892.5.1.3.9.0
Description	This attribute defines the Aisle locator of the system.
Syntax	StringType
Access	Read-only

Table 182. System Rack Name

Name	systemRackName
Object ID	1.3.6.1.4.1.674.10892.5.1.3.10.0

Description	This attribute defines the Rack locator of the system.
Syntax	StringType
Access	Read-only

Table 183. System Rack Slot

Name	systemRackSlot
Object ID	1.3.6.1.4.1.674.10892.5.1.3.11.0
Description	This attribute defines the Rack Slot locator of the system.
Syntax	StringType
Access	Read-only

Table 184. System Model Name

Name	systemModelName
Object ID	1.3.6.1.4.1.674.10892.5.1.3.12.0
Description	This attribute defines the model name of the system.
Syntax	StringType
Access	Read-only

Table 185. System System ID

Name	systemSystemID
Object ID	1.3.6.1.4.1.674.10892.5.1.3.13.0
Description	This attribute defines the system ID of the system.
Syntax	Unsigned16BitRange
Access	Read-only

Table 186. System OS Version

Name	systemOSVersion
Object ID	1.3.6.1.4.1.674.10892.5.1.3.14.0
Description	This attribute defines the version of the operating system that the host is running.
Syntax	StringType
Access	Read-only

Table 187. System Room Name

Name	systemRoomName
Object ID	1.3.6.1.4.1.674.10892.5.1.3.15.0
Description	This attribute defines the Room locator of the system.
Syntax	StringType

Access Read-only

Table 188. System Chassis System Height

Name systemChassisSystemHeight
Object ID 1.3.6.1.4.1.674.10892.5.1.3.16.0
Description This attribute defines the height of the system, in 'U's. A U is a standard unit of measure for the height of a rack or rack-mountable component.
Syntax INTEGER
Access Read-only

Table 189. System Blade Geometry

Name systemBladeGeometry
Object ID 1.3.6.1.4.1.674.10892.5.1.3.17.0
Description This attribute defines the blade geometry for a blade system. (If not applicable, a 'no such name' error is returned.)
Syntax BladeGeometryEnum
Access Read-only

Table 190. System Node ID

Name systemNodeID
Object ID 1.3.6.1.4.1.674.10892.5.1.3.18.0
Description This attribute defines the node ID of the system. The node ID provides a unique identifier for the system.
Syntax StringType
Access Read-only

Status Group

The Status Group objects provide status information about the system and storage.

Table 191. Global System Status

Name globalSystemStatus
Object ID 1.3.6.1.4.1.674.10892.5.2.1.0
Description This attribute defines the overall rollup status of all components in the system being monitored by the remote access card.
Syntax ObjectStatusEnum
Access Read-only

Table 192. System LCD Status

Name systemLCDStatus
Object ID 1.3.6.1.4.1.674.10892.5.2.2.0

Description	This attribute defines the system status as it is reflected by the LCD front panel. Not all system components may be included.
Syntax	ObjectStatusEnum
Access	Read-only

Table 193. Global Storage Status

Name	globalStorageStatus
Object ID	1.3.6.1.4.1.674.10892.5.2.3.0
Description	This attribute defines the overall storage status being monitored by the remote access card.
Syntax	ObjectStatusEnum
Access	Read-only

Table 194. System Power State


Name	systemPowerState
Object ID	1.3.6.1.4.1.674.10892.5.2.4.0
Description	This attribute defines the power state of the system.
Syntax	PowerStateStatusEnum
Access	Read-only

Table 195. System Power Up Time

Name	systemPowerUpTime
Object ID	1.3.6.1.4.1.674.10892.5.2.5.0
Description	This attribute defines the power-up time of the system in seconds.
Syntax	Unsigned32BitRange
Access	Read-only


Systems Details Group

The Systems Details Group contains objects and tables that provide detailed information about the system in which the iDRAC resides.

 **NOTE:** See the iDRAC MIB file for details of the objects and tables supported under the Systems Details Group.

Storage Details Group

The Storage Details Group contains tables that provide detailed information about the external storage subsystem of the system in which iDRAC resides.

 **NOTE:** See the iDRAC MIB file for details of the tables supported under the Storage Details Group.

iDRAC Traps

The iDRAC generates events that result in Simple Network Management Protocol (SNMP) traps and/or entries in the iDRAC Lifecycle Log. This section describes the traps, also known as alerts, generated by the iDRAC.


The iDRAC generates events in response to changes in the status of sensors and other monitored parameters. When an event with predefined characteristics occurs on your system, the SNMP subagent sends information about the event, along with trap variables, to the management console.

Each event generates an identifier called the trap ID and a list of trap variables that provide additional details about the event. The trap variables are listed in the following on [Trap Variables](#).

The traps of the iDRAC MIB are organized into five subgroups of traps. Each subgroup corresponds to one of the five categories of events that iDRAC supports (the **System Health**, **Storage Health**, **Updates**, **Audit**, and **Configuration** categories). Here is a list of the trap subgroups are:

- System Trap Group
- Storage Trap Group
- Updates Trap Group
- Audit Trap Group
- Configuration Trap Group

The trap subgroups, and all the traps within each trap subgroup, are described and listed in sections following the [Trap Variables](#) section.

 **NOTE:** The traps listed in this document can be correlated to specific events that are documented in the *Dell Event Message Reference* guide. There is 1-to-many relationship between SNMP traps and events in iDRAC. To correlate a trap to a specific event or set of events, you can match the **Trap ID** value of a trap in this document to the **Trap/Event ID** value of events in the *Dell Event Message Reference* guide.

Trap Variables

This section lists the six variables that are sent with iDRAC traps to provide additional information about a trap or alert generated by some event on the system. The trap variables presented here apply to all iDRAC7 and iDRAC8 traps. The trap variables are sent in the order listed and are reserved for use only in traps.

Table 196. Alert Message ID

Variable Name	alertMessageID
Object ID	1.3.6.1.4.1.674.10892.5.3.1.1.0
Description	Message ID of the event.
Syntax	DisplayString
Access	Read-only

Table 197. Alert Message

Variable Name	alertMessage
Object ID	1.3.6.1.4.1.674.10892.5.3.1.2.0
Description	Message describing the alert.
Syntax	StringType

Table 198. Alert Current Status

Variable Name	alertCurrentStatus
Object ID	1.3.6.1.4.1.674.10892.5.3.1.3.0
Description	Current status of object causing the alert, if applicable.
Syntax	ObjectStatusEnum
Access	Read-only

Table 199. Alert System Service Tag

Variable Name	alertSystemServiceTag
Object ID	1.3.6.1.4.1.674.10892.5.3.1.4.0
Description	Service tag of the system.
Syntax	DisplayString

Table 200. Alert System FQDN

Variable Name	alertSystemFQDN
Object ID	1.3.6.1.4.1.674.10892.5.3.1.5.0
Description	Fully qualified domain name of the system.
Syntax	StringType

Table 201. Alert FQDD

Variable Name	alertFQDD
Object ID	1.3.6.1.4.1.674.10892.5.3.1.6.0
Description	Fully qualified device descriptor of the device.
Syntax	DisplayString

Table 202. Alert Device Display Name

Variable Name	alertDeviceDisplayName
Object ID	1.3.6.1.4.1.674.10892.5.3.1.7.0
Description	Display name of the device/FQDD
Syntax	DisplayString

Table 203. Alert Message Arguments

Variable Name	alertMessageArguments
Object ID	1.3.6.1.4.1.674.10892.5.3.1.8.0
Description	Concatenated set of strings representing the message arguments of the event. Each message argument string is enclosed in double quotes, and there is a comma after the ending double quote of each message argument string, except the last one. Any double quotes found within a message argument string are preprocessed and changed to single quotes.
Syntax	StringType

Table 204. Alert Chassis Service Tag

Variable Name	alertChassisServiceTag
Object ID	1.3.6.1.4.1.674.10892.5.3.1.9.0
Description	For modular systems, the service tag of the enclosing chassis. For rack and tower systems, this varbind will be empty (zero length).
Syntax	DisplayString

Table 205. Alert Chassis Name

Variable Name	alertChassisName
Object ID	1.3.6.1.4.1.674.10892.5.3.1.10.0
Description	For modular systems, the chassis name of the enclosing chassis. For rack and tower systems, this varbind will be empty (zero length).
Syntax	DisplayString

Table 206. Alert Rac FQDN

Variable Name	alertRacFQDN
Object ID	1.3.6.1.4.1.674.10892.5.3.1.11.0
Description	Fully qualified domain name of the remote access card.
Syntax	StringType

System Trap Group

The System Trap Group contains traps that fall under the *System Health* event category of the iDRAC. System Health traps are traps those are generally generated in response to events related to the hardware of the system in which an iDRAC resides.

Table 207. Amperage Probe Traps

TrapID	Description	Category	SubCategory	Severity
Amperage Probe Normal				
2179	Current sensor reading is within range.	System Health	Amperage	Informational
Amperage Probe Warning				

TrapID	Description	Category	SubCategory	Severity
2178	Current sensor has detected a warning value.	System Health	Amperage	Minor
Amperage Probe Failure				
2177	Current sensor has detected a failure value.	System Health	Amperage	Critical

Table 208. Automatic System Recovery Trap

TrapID	Description	Category	SubCategory	Severity
Automatic System Recovery				
2233	Automatic system recovery (ASR) was performed.	System Health	Auto Sys Reset	Critical

Table 209. Battery Traps

TrapID	Description	Category	SubCategory	Severity
Battery Normal				
2227	Battery state has returned to normal; or battery presence had been detected.	System Health	Battery Event	Informational
Battery Warning				
2226	Battery is low.	System Health	Battery Event	Minor
Battery Failure				
2225	Battery has failed or battery is absent.	System Health	Battery Event	Critical

Table 210. Cable Traps

TrapID	Description	Category	SubCategory	Severity
Cable Failure				
2393	Cable failure or critical event.	System Health	Cable	Critical

Table 211. CMC Traps

TrapID	Description	Category	SubCategory	Severity
CMC Warning				
2546	Chassis Management Controller detected a warning.	System Health	CMC	Minor
CMC Failure				

TrapID	Description	Category	SubCategory	Severity
2545	Chassis Management Controller detected an error.	System Health	CMC	Critical

Table 212. Processor Device Status Traps

TrapID	Description	Category	SubCategory	Severity
Processor DeviceStatus Normal				
2243	Processor device status has returned to normal.	System Health	Processor	Informational
ProcessorDeviceStatusWarning				
2242	Processor device status has detected a warning.	System Health	Processor	Minor
ProcessorDeviceStatusFailure				
2241	Processor device status has detected a failure.	System Health	Processor	Critical

Table 213. Processor Device Absent Trap

TrapID	Description	Category	SubCategory	Severity
Processor Device Absent				
2457	Processor device is absent.	System Health	Proc Absent	Critical

Table 214. Fan Traps

TrapID	Description	Category	SubCategory	Severity
Fan Information				
2155	Fan information.	System Health	Fan Event	Informational
Fan Warning				
2154	Fan warning.	System Health	Fan Event	Minor
Fan Failure				
2153	Fan failure.	System Health	Fan Event	Critical

Table 215. Fiber Channel Traps

TrapID	Description	Category	SubCategory	Severity
Fiber Channel Information				
2539	Fiber Channel information.	System Health	Fiber Channel	Informational
Fiber Channel Warning				

TrapID	Description	Category	SubCategory	Severity
2538	Fiber Channel warning.	System Health	Fiber Channel	Minor
Fiber Channel Failure				
2537	Fiber Channel failure or critical event.	System Health	Fiber Channel	Critical

Table 216. Hardware Configuration Traps

TrapID	Description	Category	SubCategory	Severity
Hardware Configuration Information				
2331	Hardware configuration information.	System Health	Hardware Config	Informational
Hardware Configuration Warning				
2330	Hardware configuration warning.	System Health	Hardware Config	Minor
Hardware Configuration Failure				
2329	Hardware configuration failure or critical event.	System Health	Hardware Config	Critical

Table 217. IO Virtualization Traps

TrapID	Description	Category	SubCategory	Severity
IO Virtualization Failure				
2553	IO Virtualization failure or critical event.	System Health	IO Virtualization	Critical

Table 218. Link StatusTraps

TrapID	Description	Category	SubCategory	Severity
Link Status Information				
2251	Link status information.	System Health	Link Status	Informational
Link Status Warning				
2250	Link status warning.	System Health	Link Status	Minor
Link Status Failure				
2249	Link status failure or critical event.	System Health	Link Status	Critical

Table 219. Memory Device Traps

TrapID	Description	Category	SubCategory	Severity
Memory Device Information				
2267	Memory device informational event.	System Health	Memory	Informational
Memory Device Warning				
2266	Memory device status is noncritical.	System Health	Memory	Minor
Memory Device Failure				
2265	Memory device status is critical.	System Health	Memory	Critical

Table 220. NIC Traps

TrapID	Description	Category	SubCategory	Severity
Network Information				
2091	Network information.	System Health	NIC Config	Informational
Network Warning				
2090	Network warning.	System Health	NIC Config	Minor
Network Failure				
2089	Network failure or critical event.	System Health	NIC Config	Critical

Table 221. Operation System ("OS") Event Traps

TrapID	Description	Category	SubCategory	Severity
OS Information				
2411	An OS graceful stop occurred; or an OS graceful shut-down occurred.	System Health	OS Event	Informational
OS Failure				
2409	A critical stop occurred during OS load; or a runtime critical stop occurred.	System Health	OS Event	Critical

Table 222. PCI Device Traps

TrapID	Description	Category	SubCategory	Severity
PCI Device Information				
2419	An informational event was detected for a PCI device.	System Health	PCI Device	Informational

TrapID	Description	Category	SubCategory	Severity
PCI Device Warning				
2418	A warning event was detected for a PCI device.	System Health	PCI Device	Minor
PCI Device Failure				
2417	An error was detected for a PCI device.	System Health	PCI Device	Critical

Table 223. Physical Disk Traps

TrapID	Description	Category	SubCategory	Severity
Physical Disk Information				
2299	Physical disk information.	System Health	Physical Disk	Informational
Physical Disk Warning				
2298	Physical disk warning.	System Health	Physical Disk	Minor
Physical Disk Failure				
2297	Physical disk failure.	System Health	Physical Disk	Critical

Table 224. BIOS POST Trap

TrapID	Description	Category	SubCategory	Severity
Bios Post Failure				
2425	System BIOS detected a failure.	System Health	BIOS POST	Critical

Table 225. Power Supply Traps

TrapID	Description	Category	SubCategory	Severity
Power Supply Normal				
2187	Power supply has returned to normal.	System Health	Power Supply	Informational
Power Supply Warning				
2186	Power supply has detected a warning.	System Health	Power Supply	Minor
Power Supply Failure				
2185	Power supply has detected a failure.	System Health	Power Supply	Critical

Table 226. Power Supply Absent Trap

TrapID	Description	Category	SubCategory	Severity
Power Supply Absent				
2465	Power supply is absent.	System Health	PSU Absent	Critical

Table 227. Power Usage Traps

TrapID	Description	Category	SubCategory	Severity
Power Usage Information				
2275	System performance restored.	System Health	Power Usage	Informational
Power Usage Warning				
2274	System performance degraded.	System Health	Power Usage	Minor
Power Usage Failure				
2273	The system halted because system power exceeds capacity; or the system performance degraded because power draw exceeds the power threshold.	System Health	Power Usage	Critical

Table 228. Redundancy Traps

TrapID	Description	Category	SubCategory	Severity
Redundancy Information				
2475	Redundancy information.	System Health	Redundancy	Informational
Redundancy Degraded				
2474	Redundancy is degraded.	System Health	Redundancy	Minor
Redundancy Lost				
2473	Redundancy is lost.	System Health	Redundancy	Critical

Table 229. Integrated Dual SD Module Traps

TrapID	Description	Category	SubCategory	Severity
Integrated Dual SD ModuleInformation				
2211	Integrated Dual SD Module information.	System Health	IDSMD Media	Informational
Integrated Dual SD ModuleWarning				

TrapID	Description	Category	SubCategory	Severity
2210	Integrated Dual SD Module warning.	System Health	IDSDM Media	Minor
Integrated Dual SD ModuleFailure				
2297	Integrated Dual SD Module failure.	System Health	IDSDM Media	Critical

Table 230. Integrated Dual SD Module Absent Trap

TrapID	Description	Category	SubCategory	Severity
Integrated Dual SD ModuleAbsent				
2481	Integrated Dual SD Module is absent.	System Health	IDSDM Absent	Critical

Table 231. Integrated Dual SD Module Redundancy Traps

TrapID	Description	Category	SubCategory	Severity
Integrated Dual SD Module Redundancy Information				
2491	Integrated Dual SD Module redundancy information.	System Health	IDSDM Redundancy	Informational
Integrated Dual SD Module Redundancy Degraded				
2490	Integrated Dual SD Module redundancy is degraded.	System Health	IDSDM Redundancy	Minor
Integrated Dual SD Module Redundancy Lost				
2489	Integrated Dual SD Module redundancy is lost.	System Health	IDSDM Redundancy	Critical

Table 232. Security Event Traps

TrapID	Description	Category	SubCategory	Severity
Security Information				
2387	Security information.	System Health	Security Event	Informational
Security Warning				
2386	Security warning.	System Health	Security Event	Minor
Security Failure				
2385	Security failure or critical event.	System Health	Security Event	Critical

Table 233. System Event Log Traps

TrapID	Description	Category	SubCategory	Severity
System Event Log Information				
2379	System Event Log information.	System Health	Sys Event Log	Informational
System Event Log Warning				
2378	System Event Log warning.	System Health	Sys Event Log	Minor
System Event Log Failure				
2377	System Event Log failure or critical event.	System Health	Sys Event Log	Critical

Table 234. Software Configuration Traps

TrapID	Description	Category	SubCategory	Severity
Software Configuration Information				
2339	Software Configuration information.	System Health	Software Config	Informational
Software Configuration Warning				
2338	Software Configuration warning.	System Health	Software Config	Minor
Software Configuration Failure				
2337	Software Configuration failure or critical event.	System Health	Software Config	Critical

Table 235. Temperature Probe Traps

TrapID	Description	Category	SubCategory	Severity
Temperature Probe Normal				
2163	Temperature sensor value is within range.	System Health	Temperature	Informational
Temperature Probe Warning				
2162	Temperature sensor has detected a warning value.	System Health	Temperature	Minor
Temperature Probe Failure				
2161	Temperature sensor has detected a failure value.	System Health	Temperature	Critical

Table 236. Temperature Statistics Traps

TrapID	Description	Category	SubCategory	Severity
Temperature Statistics Warning				
2522	Temperature has been above the warning or critical threshold level for a long enough period of time to be considered in a warning state.	System Health	Temperature Statistics	Minor
Temperature Statistics Failure				
2521	Temperature has been above the warning or critical threshold level for a long enough period of time to be considered in a critical state.	System Health	Temperature Statistics	Critical

Table 237. vFlash Media Device Traps

TrapID	Description	Category	SubCategory	Severity
vFlash Media Device Information				
2507	vFlash Media device information.	System Health	vFlash Event	Informational
vFlash Media Device Warning				
2506	vFlash Media device warning.	System Health	vFlash Event	Minor
vFlash Media Device Failure				
2505	vFlash Media device failure.	System Health	vFlash Event	Critical

Table 238. vFlash Media Device Absent Trap

TrapID	Description	Category	SubCategory	Severity
vFlash Media Device Absent				
2515	vFlash Media device is absent.	System Health	vFlash Absent	Informational

Table 239. RAC Trap

TrapID	Description	Category	SubCategory	Severity
RAC Information				
2531	RAC information.	System Health	RAC	Informational

Table 240. Voltage Probe Traps

TrapID	Description	Category	SubCategory	Severity
Voltage Probe Normal				
2171	Voltage sensor reading is within range.	System Health	Voltage	Informational
Voltage Probe Warning				
2170	Voltage sensor has detected a warning value.	System Health	Voltage	Minor
Voltage Probe Failure				
2169	Voltage sensor has detected a failure value.	System Health	Voltage	Critical

Table 241. System Performance Trap

TrapID	Description	Category	SubCategory	Severity
System Performance Warning				
2650	System performance warning.	System Health	Performance	Minor

Storage Trap Group

The Storage Trap Group contains traps that fall under the Storage event category of iDRAC. Storage traps are traps generated in response to events related to the external storage subsystem of the system in which iDRAC resides.

Table 242. Battery Traps

TrapID	Description	Category	SubCategory	Severity
Battery Normal				
4275	Battery state has returned to normal; or battery presence has been detected.	Storage	Battery Event	Informational
Battery Warning				
4274	Battery is low.	Storage	Battery Event	Minor
Battery Failure				
4273	Battery has failed or battery is absent.	Storage	Battery Event	Critical

Table 243. Controller Traps

TrapID	Description	Category	SubCategory	Severity
Storage Controller Information				
4331	Controller information.	Storage	Storage Contr	Informational
Storage Controller Warning				

TrapID	Description	Category	SubCategory	Severity
4330	Controller warning.	Storage	Storage Contr	Minor
Storage Controller Failure				
4329	Controller failure.	Storage	Storage Contr	Critical

Table 244. Enclosure Traps

TrapID	Description	Category	SubCategory	Severity
Storage Enclosure Information				
4339	Enclosure information.	Storage	Storage Enclosur	Informational
Storage Enclosure Warning				
4338	Enclosure warning.	Storage	Storage Enclosur	Minor
Storage Enclosure Failure				
4337	Enclosure failure.	Storage	Storage Enclosur	Critical

Table 245. Fan Traps

TrapID	Description	Category	SubCategory	Severity
Storage Fan Information				
4203	Fan information.	Storage	Fan Event	Informational
Storage Fan Warning				
4202	Fan warning.	Storage	Fan Event	Minor
Storage Fan Failure				
4201	Fan failure.	Storage	Fan Event	Critical

Table 246. Physical Disk Traps

TrapID	Description	Category	SubCategory	Severity
Storage Physical Disk Information				
4347	Physical disk information.	Storage	Physical Disk	Informational
Storage Physical Disk Warning				
4346	Physical disk warning.	Storage	Physical Disk	Minor
Storage Physical Disk Failure				
4345	Physical disk failure.	Storage	Physical Disk	Critical

Table 247. Power Supply Traps

TrapID	Description	Category	SubCategory	Severity
Storage Power Supply Information				
4235	Power supply information.	Storage	Power Supply	Informational
Storage Power Supply Warning				
4234	Power supply warning.	Storage	Power Supply	Minor
Storage Power Supply Failure				
4233	Power supply failure.	Storage	Power Supply	Critical

Table 248. Security Event Traps

TrapID	Description	Category	SubCategory	Severity
Security Event Information				
4435	Security event information.	Storage	Security Event	Informational
Security Event Warning				
4434	Security event warning.	Storage	Security Event	Minor
Security Event Failure				
4433	Security event failure or critical event.	Storage	Security Event	Critical

Table 249. Storage Management Status Traps

TrapID	Description	Category	SubCategory	Severity
Storage Management Information				
4179	Storage Management information. There is no global status change associated with this trap.	Storage	Storage	Informational
Storage Management Warning				
4178	Storage Management has detected a device independent warning condition. There is no global status change associated with this trap.	Storage	Storage	Minor
Storage Management Failure				
4177	Storage Management has detected a device independent error condition. There is no global status change associated with this trap.	Storage	Storage	Critical

Table 250. Temperature Probe Traps

TrapID	Description	Category	SubCategory	Severity
Storage Temperature Probe Information				
4211	Temperature probe information.	Storage	Temperature	Informational
Storage Temperature Probe Warning				
4210	Temperature probe warning.	Storage	Temperature	Minor
Storage Temperature Probe Failure				
4209	Temperature probe failure.	Storage	Temperature	Critical

Table 251. Virtual Disk Trap

TrapID	Description	Category	SubCategory	Severity
Storage VirtualDisk Information				
4355	Virtual disk information.	Storage	Virtual Disk	Informational
Storage Virtual Disk Warning				
4354	Virtual disk warning.	Storage	Virtual Disk	Minor
Storage Virtual Disk Failure				
4353	Virtual disk failure.	Storage	Virtual Disk	Critical

Updates Trap Group

The Updates Trap Group contains traps that fall under the **Updates** event category of iDRAC. Updates traps are traps generated in response to events related to firmware/driver upgrades/downgrades.

Table 252. Update Traps

TrapID	Description	Category	SubCategory	Severity
Updates Trap Information				
6211	Update job information.	Updates	Updates	Informational

Table 253. Software Change Traps

TrapID	Description	Category	SubCategory	Severity
Software Change Update Warning				
6314	Software change update warning.	Updates	Software Change	Minor

Audit Trap Group

The Audit Trap Group contains traps that fall under the **Audit** event category of iDRAC8. Audit traps are traps generated in response to audit-type events of iDRAC8, such as authorizing of debugging, changes to iDRAC8 license state, power state changes, etc.

Table 254. CMC Traps

TrapID	Description	Category	SubCategory	Severity
CMC Audit Information				
8691	Chassis Management Controller audit information.	Audit	CMC	Informational
CMC Audit Warning				
8690	Chassis Management Controller audit warning.	Audit	CMC	Minor
CMC Audit Failure				
8689	Chassis Management Controller audit failure or critical event.	Audit	CMC	Critical

Table 255. Debug Traps

TrapID	Description	Category	SubCategory	Severity
Debug Information				
8595	Debug authorized.	Audit	Debug	Informational
DebugWarning				
8594	Debug authorization failed.	Audit	Debug	Minor

Table 256. User Tracking Traps

TrapID	Description	Category	SubCategory	Severity
User Tracking Warning				
8490	User tracking warning.	Audit	User Tracking	Minor

Table 257. iDRAC IP Address Change Trap

TrapID	Description	Category	SubCategory	Severity
iDRAC IP Address Change				
8499	iDRAC IP address has changed.	Audit	DRAC IP Address	Informational

Table 258. License Traps

TrapID	Description	Category	SubCategory	Severity
License Information				
8515	License information.	Audit	Licensing	Informational
License Warning				
8514	License warning.	Audit	Licensing	Minor
License Failure				
8513	License failure.	Audit	Licensing	Critical

Table 259. PCI DeviceTraps

TrapID	Description	Category	SubCategory	Severity
PCI Device Audit Warning				
8562	PCI device audit warning.	Audit	PCI Device	Minor

Table 260. Power SupplyTraps

TrapID	Description	Category	SubCategory	Severity
Power Supply Audit Warning				
8330	Power supply audit warning.	Audit	Power Supply	Minor
Power Supply Audit Failure				
8329	Power supply audit failure or critical event.	Audit	Power Supply	Critical

Table 261. Power Usage Traps

TrapID	Description	Category	SubCategory	Severity
Power Usage Audit Information				
8419	Power usage audit information.	Audit	Power Usage	Informational
Power Usage Audit Warning				
8418	Power usage audit warning.	Audit	Power Usage	Minor
Power Usage Audit Failure				
8417	Power usage audit failure or critical event.	Audit	Power Usage	Critical

Table 262. System Power State Change Trap

TrapID	Description	Category	SubCategory	Severity
System Power State Change Information				
8579	Host is going through a power state change (powering on or powering off).	Audit	System Info	Informational

Configuration Trap Group

The Configuration Trap Group contains traps that fall under the **Configuration** event category of the iDRAC8. Configuration traps are traps generated in response to events related to hardware configuration changes and software configuration changes.

Table 263. Auto Discovery Traps

TrapID	Description	Category	SubCategory	Severity
Auto Discovery Information				
10635	Auto discovery information.	Configuration	Auto Discovery	Informational

Table 264. NIC Configuration Traps

TrapID	Description	Category	SubCategory	Severity
Network Configuration Information				
10771	Network configuration information.	Configuration	IOID	Informational
Network Configuration Warning				
10770	Network configuration warning.	Configuration	IOID	Minor

Table 265. IP Address Traps

TrapID	Description	Category	SubCategory	Severity
IP Address Configuration Information				
10547	IP Address configuration information.	Configuration	IP Address	Informational

Table 266. Job Control Traps

TrapID	Description	Category	SubCategory	Severity
Job Control Configuration Information				
10267	Job control configuration information.	Configuration	Job Control	Informational

Table 267. PCI Device Traps

TrapID	Description	Category	SubCategory	Severity
PCI Device Configuration Information				
10611	PCI device configuration information.	Configuration	PCI Device	Informational

Table 268. Security Event Traps

TrapID	Description	Category	SubCategory	Severity
Security Event Configuration Warning				
10578	Security configuration warning.	Configuration	Security Event	Minor

Table 269. Software Configuration Traps

TrapID	Description	Category	SubCategory	Severity
SWC Configuration Warning				
10530	Software configuration warning.	Configuration	Software Config	Minor
SWC Configuration Failure				
10529	Software configuration failure.	Configuration	Software Config	Critical

Table 270. Test Trap

TrapID	Description	Category	SubCategory	Severity
Test Trap Event				
10395	The iDRAC generated a test trap event in response to a user request.	Configuration	Test Alert	Informational