Dell OpenManage
SNMP Reference Guide for iDRAC8

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.

2014 - 09

Rev. A00

Contents

1

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 iDRAC8.

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

What's New in This Release

This release of Dell iDRAC8 SNMP introduces the following new features:

New enhancement in iDRAC8 with SNMP v3 traps supported.

- Added new trap objects under **iDRAC8**
  - Changes in sub group are:

    System Trap Group

    * Added new Traps for
      RAC Trap

      and
      System Performance Trap

    Updated Trap Group

    * Added new Trap for :
      Update Trap

    Audit Trap Group

    * Added new Trap for :
      User Tracking Traps

Supported SNMP Versions

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

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-SMIv1.mib	iDRAC7 and iDRAC 8	Provides information about the SNMP data, and traps, supported by the iDRAC7. This is for SMv1.
iDRAC-SMIv2.mib	iDRAC7 and iDRAC 8	Provides information about the SNMP data, and traps, supported by the iDRAC7. This is for SMv2.
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.
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

Section	Topic	MIB Group Numbers
19	Remote Access Group — provides information about remote access hardware that may be present in your system and defines variables for administrative users, SNMP trap destinations, modem configuration for dial-up networking, dial-in configuration, and dial-out destinations	1700

Dell Remote Access Controller Out-of-Band MIB

The Dell Remote Access Controller Out-of-Band MIB (filename **dellRAC.mib**) 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

Section	Topics	MIB Group Number
25	The Dell RAC Out-of-Band MIB consists of information for the following groups: • Product Information • Chassis Status • Chassis Power • CMC Power Information • CMC PSU Information • Chassis Alerts • Legacy Alerting	2

How This Guide Defines Technical Terms

The following table provides information about where to find definitions for technical terms in this reference guide.

Table 3. Where to Find Definitions for Technical Terms

Type of Definition	See
Basic SNMP vocabulary.	Introduction
MIB-group-specific variable values. MIB-group-specific MIB variables contain links to the tables that define these values in the last section of the section in which these variables are used.	Sections 3, 5, 7, 8, 9, and 11 through 18.

Type of Definition	See
Systems management terms, acronyms, and commonly managed components referred to in this reference guide.	*Glossary* available on the Dell Support web site at **dell.com/support/manuals**.
Server Administrator-standard data types that specify variable values in this reference guide.	Appendix A, Standard Data Type Definitions.

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 4. 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 5. UUID Table Entry

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

Table 6. UUID Chassis Index

Name	`uUIDchassisIndex`
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	DellObjectRange
Access	Read-only

Table 7. UUID Index

Name	`uUIDIndex`
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	DellObjectRange

Access	Read-only

Table 8. UUID Type

Name	`uUIDType`
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	DellUUIDType
Access	Read-only

Table 9. UUID Value

Name	`uUIDValue`
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])
Access Read-only	Read-only

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.

2

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 Server Administrator Instrumentation Service, see Instrumentation Traps. For information on Server Administrator Storage Management traps, see Storage Management Alert Reference.

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

Trap Variables

This section describes the variables both on Traditional and Enhanced varbinds that are sent to the management console to provide additional information about a trap or alert generated by some event on your system. The trap variables presented here apply to all Instrumentation and RAC traps. Trap variables are sent in the order listed and are reserved for use only in traps. When a varbind is created for a trap variable, a zero is appended to the object ID (OID) to create the OID for the varbind.

The messages associated with each alertMessage varbind are available in the *Message Reference Guide* and can be found by matching the alert ID in the MIB to the event ID in the *Message Reference Guide*.

Table 10. Trap Variables

Variable Name	`alertSystem`
Object ID	1.3.6.1.4.1.674.10892.1.5000.10.1
Description	Identifies the system generating the alert.
Syntax	DisplayString

Table 11. Table Index OID

Variable Name	`alertTableIndexOID`
Object ID	1.3.6.1.4.1.674.10892.1.5000.10.2
Description	Specifies the object identifier for the index attribute in the table that contains the object causing the alert. Uniquely identifies the object causing the alert and can be used to correlate different alerts caused by the same object.
Syntax	`OBJECT IDENTIFIER`

Table 12. Message

Variable Name	`alertMessage`
Object ID	1.3.6.1.4.1.674.10892.1.5000.10.3
Description	Describes the alert.
Syntax	DisplayString

Table 13. Current Status

Variable Name	`alertCurrentStatus`
Object ID	1.3.6.1.4.1.674.10892.1.5000.10.4
Description	Specifies the current status of the object causing the alert.
Syntax	DellStatus

Table 14. Previous Status

Variable Name	`alertPreviousStatus`
Object ID	1.3.6.1.4.1.674.10892.1.5000.10.5
Description	Specifies the previous status of the object causing the alert.
Syntax	DellStatus

Table 15. Data

Variable Name	`alertData`
Object ID	1.3.6.1.4.1.674.10892.1.5000.10.6
Description	Provides Server Administrator-defined data related to the alert.

Syntax	Octet String

The following variables show the Enhanced varbinds:

Table 16. Message ID

Variable Name	`alertMsgID`
Object ID	1.3.6.1.4.1.674.10892.4.5000.10.7
Description	Specifies the enhanced message ID for the object generating the alert.
Syntax	DisplayString

Table 17. System FQDN

Variable Name	`alertSystemFQDN`
Object ID	1.3.6.1.4.1.674.10892.4.5000.10.8
Description	Specifies fully qualified domain name of the system generating the alert.
Syntax	DisplayString

Table 18. Service Tag

Variable Name	`alertServiceTag`
Object ID	1.3.6.1.4.1.674.10892.4.5000.10.9
Description	Specifies the system service tag of the system generating the alert.
Syntax	DisplayString

Table 19. Chassis Service Tag

Variable Name	`alertChassisServiceTag`
Object ID	1.3.6.1.4.1.674.10892.4.5000.10.10
Description	Specifies the chassis service tag of the system generating the alert.
Syntax	DisplayString

Understanding The Trap Description

The below table lists in alphabetical order each line item that may appear in the trap description.

Table 20. Trap Description

Description Line Item	Explanation
`Action performed was: <Action>`	Specifies the automatic server recovery action that was performed, for example: `Action performed was: Power cycle`
`Action requested was: <Action>`	Specifies the user initiated host control action that was requested, for example:

Description Line Item	Explanation
	Action requested was: Reboot, shutdown OS first
Additional details: <Additional details for the events>	Specifies possible additional details about the specified device, for example: Additional details: Memory device: DIMM_1A Serial number: 11111111 Memory device: DIMM_1B Serial number: 22222222
<Additional power supply status information>	Specifies any additional power supply information pertaining to the event, for example: Power supply input AC is off, Power supply POK (power OK) signal is not normal, Power supply is turned off
Battery sensor status: <status>	Specifies the status reported by the battery sensor, for example: Battery sensor status: Predictive failure
Chassis intrusion state: <Intrusion state>	Specifies the chassis intrusion state (open or closed), for example: Chassis intrusion state: Open
Chassis location: <Name of chassis>	Specifies the name of the chassis that generated the message, for example: Chassis location: Main System Chassis
Configuration error type: <type of configuration error>	Specifies the type of configuration error that occurred, for example: Configuration error type: Revision mismatch
Current sensor value (in Amps): <Reading>	Specifies the current sensor value in amps, for example: Current sensor value: 7.853
Date and time of action: <Date and time>	Specifies the date and time that an automatic server recovery action was performed, for example: Date and time of action: Fri May 30 23:55:44 2003.
Description: <Description of event>	Specifies the description of the event that occurred, for example: Description: Chipset Err: Critical Event sensor, front panel NMI / diagnostic interrupt was asserted.
Device location: <Location in chassis>	Specifies the location of the device in the specified chassis, for example: Device location: Mem Card A
Discrete current state: <State>	Specifies the state of the current sensor, for example: Discrete current state: Good
Discrete temperature state: <State>	Specifies the state of the temperature sensor, for example: Discrete temperature state: Good

Description Line Item	Explanation
`Discrete voltage state: <State>`	Specifies the state of the voltage sensor, for example: `Discrete voltage state: Good`

`Fan sensor value: <Reading>`	Specifies the fan speed in revolutions per minute (RPMs) or On/Off, for example:
	`Fan sensor value (in RPM): 2600`
	`Fan sensor value: Off`

`Log type: <Log type>`	Specifies the type of hardware log, for example: `Log type: Embedded Server Management (ESM)`
`Memory device bank location: <Bank name in chassis>`	Specifies the name of the memory bank in the system that generated the message, for example: `Memory device bank location: Bank_1`
`Memory device location: <Device name in chassis>`	Specifies the location of the memory module in the chassis, for example: `Memory device location: DIMM_A`
`Number of devices required for full redundancy: <Number>`	Specifies the number of power supply or cooling devices required to achieve full redundancy, for example: `Number of devices required for full redundancy: 4`
`Peak value (in Watts): <Reading>`	Specifies the peak value in Watts, for example: `Peak value (in Watts): 125`

`Possible memory module event cause: <list of causes>`	Specifies a list of possible causes for the memory module event, for example:
	`Possible memory module event cause: Single bit warning error rate exceeded`
	`Single bit error logging disabled`

`Power Supply type: <type of power supply>`	Specifies the type of power supply, for example: `Power Supply type: VRM`
`Pre-failure state was: <State>`	Specifies the status of the previous memory message, for example: `Pre-failure state was: Failed`
`Previous redundancy state was: <State>`	Specifies the status of the previous redundancy message, for example: `Previous redundancy state was: Lost`
`Previous state was: <State>`	Specifies the previous state of the sensor, for example: `Previous state was: OK (Normal)`
`Processor sensor status: <status>`	Specifies the status of the processor sensor, for example:

Description Line Item	Explanation
	`Processor sensor status: Configuration error`
`Redundancy unit: <Redundancy location in chassis>`	Specifies the location of the redundant power supply or cooling unit in the chassis, for example: `Redundancy unit: Fan Enclosure`
`SD card device type: <Type of SD card device>`	Specifies the type of SD card device, for example: `SD card device type: Hypervisor`
`SD card state: <State of SD card>`	Specifies the state of the SD card, for example: `SD card state: Present, Failed`
`Sensor location: <Location in chassis>`	Specifies the location of the sensor in the specified chassis, for example: `Sensor location: CPU1`
`Temperature sensor value (in degrees Celsius): <Reading>`	Specifies the temperature in degrees Celsius, for example: `Temperature sensor value (in degrees Celsius): 30`
`Voltage sensor value (in Volts): <Reading>`	Specifies the voltage sensor value in volts, for example: `Voltage sensor value: 1.693`

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 Traps . The trap variables are sent in the order in which they are listed.

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

Table 21. RAC Traps

TrapID	Name	Description	Severity	Category	Cause	Supported 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	alertDrscSEL	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	alertDrscSEL	Critical The RAC has detected a new event in the System Event Log with Severity: Critical	Critical	Error	RAC detected a new system event log with critical severity (detailed log info is in drsAlert Message varbind).	All
1017	alertDrscSEL 80 percentFull	The RAC system event log is 80% full	Major	Status	RAC detected system event log is 80% full.	All

TrapID	Name	Description	Severity	Category	Cause	Supported by RAC Platform
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
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

TrapID	Description	Severity
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
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

TrapID	Description	Severity
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
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

TrapID	Description	Severity
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

3

iDRAC8 MIB

The Integrated Dell Remote Access Controller (iDRAC) MIB (filename **iDRAC-SMIv1.mib/ iDRAC-SMIv2.mib**) is the MIB supported by the Integrated Dell Remote Access Controller 8 (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 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-SMIv1.mib. And the SMIv2 copy is named iDRAC-SMIv2.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 iDRAC8 MIB is supported on the following systems:

Rack and Tower Servers

The Rack and Tower servers for this release:

- PowerEdge R730
- PowerEdge R730xd
- PowerEdge R630
- PowerEdge T630
- PR7910
- C4130

iDRAC8 Supported SNMP Versions

The following table identifies the SNMP versions that support iDRAC8 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: iDRAC8 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.

iDRAC8 SNMP Data Security Features

iDRAC8 firmware supports the following data security features:

- SNMP security lockout feature
  - iDRAC8 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 iDRAC8 SNMP Agent blocks all subsequent SNMPv3 requests/queries for 10 minutes.
- Restriction of access to **sensitive** data
  - Some of the MIB data that iDRAC8 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)

iDRAC8 Out-of-Band Group

The objects of the Integrated Dell Remote Access Controller (iDRAC) MIB (**iDRAC-MIB.txt**) are organized into subgroups of the iDRAC8 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 22. 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 23. RAC 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 24. 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 25. 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 26. 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 27. 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 28. 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 29. 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 30. Chassis Service Tag

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

System Information Group

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

Table 31. 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 32. 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 33. 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 34. 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 35. 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 36. 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 37. 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 38. 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 39. 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 40. 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 41. 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 42. 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 43. 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 44. 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 45. 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 46. 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 47. 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

Status Group

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

Table 48. 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 49. 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 50. 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 51. 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

Systems Details Group

The Systems Details Group contains objects and tables that provide detailed information about the system in which the iDRAC8 resides.

NOTE: See the iDRAC8 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 iDRAC8 resides.

NOTE: See the iDRAC8 MIB file for details of the tables supported under the Storage Details Group.

iDRAC8 Traps

The iDRAC8 generates events that result in Simple Network Management Protocol (SNMP) traps and/or entries in the iDRAC8 Lifecycle Log. This section describes the traps, also known as alerts, generated by the iDRAC8.

The iDRAC8 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 iDRAC8 MIB are organized into five subgroups of traps. Each subgroup corresponds to one of the five categories of events that iDRAC8 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 iDRAC8. 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 iDRAC7 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 traps. The trap variables are sent in the order listed and are reserved for use only in traps.

Table 52. 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 53. 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 54. 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 55. 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 56. 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 57. 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 58. 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 59. 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 60. Alert Chassis Service Tag

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

System Trap Group

The System Trap Group contains traps that fall under the *System Health* event category of the iDRAC8. System Health traps are traps those are generally generated in response to events related to the hardware of the system in which an iDRAC8 resides.

Table 61. 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				
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 62. 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 63. 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

TrapID	Description	Category	SubCategory	Severity
Battery Failure				
2225	Battery has failed or battery is absent.	System Health	Battery Event	Critical

Table 64. 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 65. Processor Device Absent Trap

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

Table 66. 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 67. 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 68. 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 69. 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 70. 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				

TrapID	Description	Category	SubCategory	Severity
2089	Network failure or critical event.	System Health	NIC Config	Critical

Table 71. 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 72. 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
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 73. 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 74. BIOS POST Trap

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

Table 75. 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 76. Power Supply Absent Trap

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

Table 77. 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 78. 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 79. Integrated Dual SD Module Traps

TrapID	Description	Category	SubCategory	Severity
Integrated Dual SD ModuleInformation				
2211	Integrated Dual SD Module information.	System Health	IDSDM Media	Informational
Integrated Dual SD ModuleWarning				
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 80. 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 81. 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				

TrapID	Description	Category	SubCategory	Severity
2489	Integrated Dual SD Module redundancy is lost.	System Health	IDSDM Redundancy	Critical

Table 82. Security Event Traps

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

Table 83. 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 84. 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 85. 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 86. 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 87. 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 88. RAC Trap

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

Table 89. 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 90. 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 iDRAC7. Storage traps are traps generated in response to events related to the external storage subsystem of the system in which iDRAC7 resides.

Table 91. 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 92. 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 93. Enclosure Traps

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

Table 94. 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 95. 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 96. 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 97. 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 98. 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 99. 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 iDRAC8. Updates traps are traps generated in response to events related to firmware/driver upgrades/downgrades.

Table 100. Update Trap

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

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 101. Debug Traps

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

Table 102. User Tracking Traps

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

Table 103. 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 104. 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 105. 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 iDRAC7. Configuration traps are traps generated in response to events related to hardware configuration changes and software configuration changes.

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

4

Standard Data Type Definitions

This appendix contains definitions for data types that are standard in most contexts across the information technology industry. These are the most common data types for describing variable values defined in the **10892.mib** , **dcs3rmt.mib** and **dcs3fru.mib** files. Server Administrator-specific variable values are defined in the last section of the section in which they are introduced.

Common Data Types

Common data types include several types of strings, the object range, signed and unsigned bit ranges, and the familiar Boolean (true or false) data type.

Table 106. Common Data Types

Variable Name:	Definition
DellString	DisplayString (SIZE (0..64))
DellSecurityString	DisplayString (SIZE (0..255))
DellCostofOwnershipString	DisplayString (SIZE (0..64))
DellObjectRange	INTEGER (1..128)
DellUnsigned8BitRange	INTEGER (1..256)
DellUnsigned16BitRange	INTEGER (1..65535)
DellUnsigned32BitRange	INTEGER (1..2147483647)
DellSigned32BitRange	INTEGER (-2147483647..2147483647)
DellBoolean	INTEGER (0..1 (FALSE = 0, TRUE = 1))

Variables with Data Types of State Capabilities and State Capabilities Unique

Variables with definitions of `<variable name>StateCapabilities` or `<variable name>StateCapabilitiesUnique` are integers representing a series of bit definitions. They are NOT enumerations and should be treated as bit fields. The value is passed as a decimal value. The decimal value should be converted to hex and the appropriate bits should be parsed from hex. Some of the more common bit combinations are defined in some variables, but not all combinations are or will be defined.

Table 107. Dell State Capabilities

Variable Name: `DellStateCapabilities`

Data Type: `Integer`

Possible Data Values	Meaning of Data Value
`if set to zero(0)`	The object has no capabilities.

unknownCapabilities(1)	The object's capabilities are unknown.
enableCapable(2)	The object can be disabled (offline, a binary 0 value) or enabled (online, a binary 1 value).
notReadyCapable(4)	The object is not ready.
enableAndNotReadyCapable (6)	Enable and not ready capable.

Table 108. Dell State Settings

Variable Name: DellStateSettings

Data Type: Integer

Possible Data Values	Meaning of Data Value
if set to zero(0)	The object has no settings capabilities and its state is disabled.
unknown(1)	The object's state is unknown.
enabled(2)	The object's state is disabled (offline, a binary 0 value) or enabled (online, a binary 1 value).
notReady(4)	The object is not ready.
enableAndNotReady(6)	The object is enabled and not ready.

Table 109. Dell Probe Capabilities

Variable Name: DellProbeCapabilities

Data Type: Integer

Possible Data Values	Meaning of Data Value
if set to zero(0)	The object has no capabilities.
upperNonCriticalThresholdSetCapable(1)	The upper noncritical threshold can be set.
lowerNonCriticalThresholdSetCapable(2)	The lower noncritical threshold can be set.
upperNonCriticalThresholdDefaultCapable(4)	The upper noncritical threshold can be set to default.
lowerNonCriticalThresholdDefaultCapable(8)	The lower noncritical threshold can be set to default.

Dell Status Data Types

Status data types include DellStatus, DellStatusRedundancy, and DellStatusProbe.

Table 110. Dell Status

Variable Name: DellStatus

Data Type: Integer

Possible Data Values	Meaning of Data Value
other(1)	The object's status is not one of the following:
unknown(2)	The object's status is unknown.

ok(3)	The object's status is OK.
nonCritical(4)	The object's status is warning, noncritical.
critical(5)	The object's status is critical (failure).
nonRecoverable(6)	The object's status is nonrecoverable (dead).

Table 111. Dell Status Redundancy

Variable Name: DellStatusRedundancy

Data Type: Integer

Possible Data Values	Meaning of Data Value
other(1)	The object's status is not one of the following:
unknown(2)	The object's redundancy status is unknown.
full(3)	The object is fully redundant.
degraded(4)	The object's redundancy has been degraded.
lost(5)	The object's redundancy has been lost.
notRedundant(6)	Redundancy does not apply or it is not redundant.

Table 112. Dell Status Probe

Variable Name: DellStatusProbe

Data Type: Integer

Possible Data Values	Meaning of Data Value
other(1)	The object's status is not one of the following:
unknown(2)	The status of the object is unknown.
ok(3)	The status of the object is OK.
nonCriticalUpper(4)	The object is at the noncritical upper limit.
CriticalUpper(5)	The object is at the critical upper limit.
nonRecoverableUpper(6)	The object is at the nonrecoverable upper limit.
nonCriticalLower(7)	The object is at the noncritical lower limit.
criticalLower(8)	The object is at the critical lower limit.
nonRecoverableLower(9)	The object is at the nonrecoverable lower limit.
failed(10)	The status of the object is failed.

Dell Date

Variable Name: DellDate

Data Type: DellUnsigned64BitRange Octet String (SIZE(8))

The DellDate definition is required because SNMP V1 does not support 64-bit ranges. The information sent back by this subagent has the most significant byte of the information as the first byte. For example,

the hex address 0x1029384754657687 is sent as hex: 0001 0000 0010 1001 0011 1000 0100 0111 ... Byte 1 Byte 2 Byte 3 Byte 4.

Full Dates

Variable Name: `DellDateName`

Data Type: `DisplayString` DisplayString (SIZE (25))

Full dates are defined in the ASCII format: *yyyyMMddhhmmss.uuuuuu+fff or yyyyMMddhhmmss.uuuuuu-fff*

where *yyyy* is the year, MM is the month, *dd* is the day, *hh* are the hours, *mm* are the minutes, and ss are the seconds. uuuuuu is the number of microseconds, and *+fff* or *-fff* is the offset from UTC in minutes. For example, Friday, October 31, 2001, at 6:05:19 PM CST would be represented as 20011031180519.000000-360.

The values are zero-padded, and if a valid value for a field is not deliverable, each character in the field is replaced with an asterisk (*) character.