DELL Technologies

White Paper

iDRAC Service Module - In-Band iDRAC SNMP Alerts

Abstract

This White Paper provides information about the usage, configuration and troubleshooting of In-Band iDRAC SNMP Alerts in iDRAC Service Module v2.3 or later.

February 2023

Revisions

Date	Description
April 2016	Initial release
December 2016	Revised for iDRAC Service Module release 2.4.0
February 2023	Revised for iDRAC Service Module release 5.1.0.0

Acknowledgments

Author: Rose Verma, Faizal SN

Support: Navya V

Other:

Table of contents

Executive summary

This new feature of iDRAC Service Module 2.3 will act as an SNMP sub-agent to forward SNMP alerts. This feature is dependent on the Lifecycle Logs Replication in the OS Logs feature. This is because there is no separate interface in iDRAC to configure this feature for iSM. Hence, whatever logs are replicated as part of Lifecycle Logs replication feature in iSM shall be converted into SNMP traps by iSM. The administrator will have to configure the SNMP master agent on the host OS for trap destinations, community, SNMP version, etc.

The Dell Integrated Remote Access Controller (iDRAC) Service Module is a lightweight systems management application installed on a physical Host operating system (OS) of a managed server. iDRAC Service Module works as a system management application for Dell's Out of Band (OOB) system management processor which is the Integrated Dell Remote Access Controller (iDRAC). Installing iDRAC Service Module v or later allows the administrator to monitor the iDRAC SNMP alerts without configuring iDRAC. Administrators can manage the server remotely by configuring the SNMP traps and destinations on the Host OS.

Pre-requisites

- OpenManage Server Administrator is not running on the Host OS.
- Lifecycle Log Replication feature of iDRAC Service Module is enabled.
- Administrator must enable In-band iDRAC SNMP feature or this feature is enabled
- The SNMP configurations are met. For example: SNMP Traps should be enabled in VMware ESXi.
- The iDRAC Service Module should be installed and must be active and running (communicating with iDRAC.)

Dependencies

1. This feature in iDRAC Service Module 2.3 is dependent on the LifeCycleLog Replication. However, this feature can be independently turned off using the interfaces provided by iDRAC Service Module which are explained in subsequent sections of this document.
2. In-Band SNMP Alert feature will be a conflicting feature with OpenManage Server Administrator (OMSA). This feature will be automatically turned off when iDRAC Service Module detects OMSA is active.
3. This feature is dependent on the Windows SNMP Service on Windows OS-es and requires NET-SNMP to be configured on Linux OS-es with SMUX protocol enabled. The AGENTX method of configuring SNMP is not supported in iDRAC Service Module 2.3.0 version.
4. On VMWare ESXi, the sfcbd-watchdog should be running. Also, the SNMP traps should be enabled.

Supported Dell Servers or Platforms

- The In-band iDRAC SNMP Alerts feature is supported on all Dell PowerEdge yx4x and newer generation of servers.

Supported Operating Systems

- The In-band iDRAC SNMP Alerts feature is supported on all OS-es which iDRAC Service Module 2.3 supports.

1 Configuration on Windows Operating Systems

1.1 Enable In-Band iDRAC SNMP Alerts Feature

You can enable or disable the In-band iDRAC SNMP alerts feature by following the steps mentioned here. These steps are applicable, only if you have not enabled the feature during iDRAC Service Module installation. Enabling or disabling the feature creates an audit log in the host OS logs.

1.1.1 WMI extrinsic method

iDRAC Service Module provides a WMI method called `EnableInBandSNMPTraps` against the `root\cimv2\dcim` namespace. The method accepts an integer parameter – either a zero (0) to disable the feature or a one (1) to enable the feature. This WMI method requires iDRAC Service Module service to be active to take effect. Any subsequent alert generated from iDRAC and targeted for Lifecycle replication shall be converted into SNMP traps. The Windows SNMP service shall forward the trap to the respective configured trap destinations.

This can be invoked either on a local command prompt session by logging into the OS using a remote desktop session or remotely using the WinRM remote commands. Using the WinRM commands remotely requires WinRM to be configured as a listener on the Host OS. For more information on how to configure a WinRM listenerhttps://msdn.microsoft.com/en-us/library/windows/desktop/aa384372(v=vs.85).aspx

Example on a local command prompt session: `winrm i EnableInBandSNMPTraps wmi/root/cimv2/dcim/DCIM_iSMService?InstanceID=”iSMExportedFunctions” @{state=”1”}`

```
C:\Users\Administrator>winrm i EnableInBandSNMPTraps
wmi/root/cimv2/dcim/dcim_ismservice?instanceid="ismexportedfunctions"
@{state="1"}

      EnableInBandSNMPTraps_OUTPUT
      ReturnValue = 0
```

Example from a remote client: `winrm i EnableInBandSNMPTraps wmi/root/cimv2/dcim/DCIM_iSMService?InstanceID=”iSMExportedFunctions” @{state=”1”} -u:<admin username> -p:<admin password> -r:http://<remote hostname OR IP>/wsman -a:Basic -encoding:utf-8 -skipCACheck -skipCNCheck`

```
C:\Users\Administrator>winrm i EnableInBandSNMPTraps
wmi/root/cimv2/dcim/dcim_ismservice?instanceid="ismexportedfunctions"
@{state="1"} -u:<username> -p:<password> -r:http://<IP Address>/wsman -
a:Basic -encoding:utf-8 -skipCACheck -skipCNCheck

         EnableInBandSNMPTraps_OUTPUT
         ReturnValue = 0
```

Enable/Disable Using Remote WinRM Command

iDRAC Service Module is agnostic of SNMP versions since iDRAC Service Module functions as a sub-agent to the OS SNMP agent. Any mismatch in the SNMP versions between the Host OS and the trap destination shall be resolved by the SNMP master agent. However, any SNMP v3 related settings needs to be done by the administrator. For other content topics that are not listed in this template, use a heading of level two or lower.

1.2 Configuring Windows SNMP for Trap Forwarding

You can configure Windows SNMP service for forwarding traps to the destination using the following steps:

Ensure SNMP service is installed on the Host OS. If not, install SNMP service. For more information on how to configure SNMP, refer https://technet.microsoft.com/en-us/library/bb726987.aspx or related searches for configuring SNMP trap destinations on the Host OS.

2 Configuration on Linux Operating Systems

A default installation of iDRAC Service Module using the setup.sh shell script shall install this feature. By default, the feature is not enabled. The administrator can enable or disable the feature during run time by using the following script which gets installed as part of iDRAC Service Module.

`Enable-iDRACSNMPTrap.sh`

Executing the above script without any options will provide the command usage information to the user.

A snapshot of the same is shown below:

Usage: Ensure Net-SNMP package is installed with SMUX protocol enabled. The command usage is as follows-
`root@XXXXXX:/opt/dell/srvadmin/iSM/bin# ./Enable-iDRACSNMPTrap.sh`
`Enable-iDRACSNMPTrap.sh 1/enable` => Enable SNMP trap feature in iDRAC Service Module; Net-SNMP trap configuration should be done by Server Administrator.
`Enable-iDRACSNMPTrap.sh 1/enable --force` => Enable SNMP trap feature in iDRAC Service Module; Net-SNMP re-configuration is attempted; Trap Destinations need to be configured by Server Administrator.
`Enable-iDRACSNMPTrap.sh 0/disable` => Disable SNMP trap feature in iDRAC Service Module; Net-SNMP configuration should be done by Server Administrator.
`Enable-iDRACSNMPTrap.sh 0/disable --force` => Disable SNMP trap feature in iDRAC Service Module; Net-SNMP re-configuration is attempted.
`Enable-iDRACSNMPTrap.sh status` => Check if the feature is currently enabled.
`Enable-iDRACSNMPTrap.sh changesmuxpasswd <password>` => change the smux password. Use enable/force option for the new password to take effect.
`Enable-iDRACSNMPTrap.sh 0/disable --force` => Disable SNMP trap feature in iDRAC Service Module; Net-SNMP re-configuration is attempted.
`Enable-iDRACSNMPTrap.sh status` => Check if the feature is currently enabled.
`Enable-iDRACSNMPTrap.sh changesmuxpasswd <password>` => change the smux password. Use enable/force option for the new password to take effect.

To enable the feature, use:

```
Enable-iDRACSNMPTrap.sh 1 (OR)
Enable-iDRACSNMPTrap.sh enable
```

To disable the feature, use:

```
Enable-iDRACSNMPTrap.sh 0 (OR)
Enable-iDRACSNMPTrap.sh disable
```

To see the current status, use:

```
Enable-iDRACSNMPTrap.sh status
```

To change password for smux, use:

```
Enable-iDRACSNMPTrap.sh changemuxpasswd <password>
```

`--force` option configures the Net-SNMP and forwards the traps to the trap destination. However, the trap destination has to be configured by the administrator.

```
root@ubuntu: /opt/dell/srvadmin/iSM/bin# ./Enable-iDRACSNMPTrap.sh 1
SNMP Trap feature is enabled in iDRAC Service Module.
Please configure the Net-SNMP master agent to send traps and ensure smux is enabled. For iDRAC
Service Module smux peer configuration, please consult
/opt/dell/srvadmin/iSM/etc/ism_snmpd.conf and then restart the snmpd service.
```

Without the force option, you can also configure smux peer. For more information on configuring smux peer, refer `/opt/dell/srvadmin/iSM/etc/ism_snmpd.conf`.

2.1 Configuring the Net-SNMP for SNMPv3 informs

SNMPv3 User based Security Model (USM) user can be used in a number of ways depending on the `"securityLevel"` configuration parameter. For more information on configuring for SNMPv3, refer: http://www.net-snmp.org/wiki/index.php/TUT:Configuring_snmptrapd_to_receive_SNMPv3_notifications and http://www.net-snmp.org/wiki/index.php/TUT:snmpd_notification_filtering

2.2 Configuring the Net-SNMP for Trap/Informs Forwarding

2.2.1 Master Agent

Use below settings in `snmptrapd.conf` for enabling the forward for SNMPv1 and SNMPv2 traps:

```
disableAuthorization yes
authCommunity log public
```

2.2.2 SNMPv3 informs

Use below settings in `snmptrapd.conf` for enabling the forward for SNMPv1 and SNMPv2 traps:

```
authCommunity log,execute,net public
createUser informtest SHA mypassword AES mypassword
authUser log,execute,net informtest
```

In the above example, `informtest` is the USM user. This user needs to be configured in `snmpd.conf`.

2.2.3 Firewall access

To provide firewall access for SNMP port for the remote servers, execute the following command on the host operating system:

```
firewall-cmd --add-port=161/udp
```

2.3 Configuring the Trap Destination

2.3.1 Configuring the Trap Destination for SNMPv1

You can send SNMPv2 traps using the trapsink token by adding the following entry to `snmpd.conf`:

```
rocommunity public
trapsink <TRAP DESTINATION IP> public
```

Below is one example of traps forwarded by iDRAC Service Module and captured by `snmptrapd`.

```
2016-04-05 11:40:03 <IP Address>(via UDP: [127.0.0.1]:36452->[127.0.0.1]:162)TRAP,SNMPv1,communitypublic
SNMPv2-SMI::enterprises.674.10892.5.3.2.1 Enterprise Specific Trap (2153) Uptime:0:00:16.84
SNMPv2-SMI::enterprises.674.10892.5.3.1.1.0=STRING:"FAN0003"
SNMPv2-SMI::enterprises.674.10892.5.3.1.2.0=STRING:"Fan 1 RPM is greater than the upper critical threshold."
SNMPv2-SMI::enterprises.674.10892.5.3.1.3.0=INTEGER:5
SNMPv2-SMI::enterprises.674.10892.5.3.1.4.0=STRING:"DGCF862"
SNMPv2-SMI::enterprises.674.10892.5.3.1.5.0=STRING:"ubuntu"
SNMPv2-SMI::enterprises.674.10892.5.3.1.6.0=STRING:"System.Embedded.1"
SNMPv2-SMI::enterprises.674.10892.5.3.1.7.0=STRING:"iDRAC"
SNMPv2-SMI::enterprises.674.10892.5.3.1.8.0=STRING:"\"1\""
SNMPv2-SMI::enterprises.674.10892.5.3.1.9.0=STRING:"BGCF862"
SNMPv2-SMI::enterprises.674.10892.5.3.1.10.0=STRING:"CMC-BGCF862"
SNMPv2-SMI::enterprises.674.10892.5.3.1.11.0 = STRING: "idrac-DGCF862"
```

2.3.2 Configuring the Trap Destination for SNMPv2

You can send SNMPv2 traps using the trap2sink token. A non-standard port can be specified by adding the port after the host name or IP address. Update the `snmpd.conf` with below trap2sink token:

```
trap2sink <TRAP DESTINATION IP> public
```

Below is one example of traps forwarded by iDRAC Service Module and captured by `snmptrapd`.

```
2016-01-20 14:30:33 localhost [UDP: [127.0.0.1]:33619->[127.0.0.1]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (5390) 0:00:53.90
SNMPv2-MIB::snmpTrapOID.0 = OID:
SNMPv2-SMI::enterprises.674.10892.5.3.2.1.0.2153
SNMPv2-SMI::enterprises.674.10892.5.3.1.1.0 = STRING: "FAN0001"
SNMPv2-SMI::enterprises.674.10892.5.3.1.2.0 = STRING: "Fan 1 RPM is less than the lower critical threshold."
SNMPv2-SMI::enterprises.674.10892.5.3.1.3.0 = INTEGER: 5
SNMPv2-SMI::enterprises.674.10892.5.3.1.4.0 = STRING: "DGCF862"
SNMPv2-SMI::enterprises.674.10892.5.3.1.5.0 = STRING: "ubuntu"
SNMPv2-SMI::enterprises.674.10892.5.3.1.6.0 = STRING: "System.Embedded.1"
SNMPv2-SMI::enterprises.674.10892.5.3.1.7.0 = STRING: "iDRAC"
SNMPv2-SMI::enterprises.674.10892.5.3.1.8.0 = STRING: "\"1\""
SNMPv2-SMI::enterprises.674.10892.5.3.1.9.0 = STRING: "BGCF862"
SNMPv2-SMI::enterprises.674.10892.5.3.1.10.0 = STRING: "CMC-BGCF862"
SNMPv2-SMI::enterprises.674.10892.5.3.1.11.0 = STRING: "idrac-DGCF862"
SNMPv2-MIB::snmpTrapEnterprise.0 = OID:
SNMPv2-SMI::enterprises.674.10892.5.3.2.1
```

2.3.3 Configuring the Trap Destination for SNMPv3

You can send SNMPv3 informs with full SNMPv3 security using the trapsess token. As a first step configure a SNMPv3 INFORM User. Use the information for configuring trapsess token. Update the snmpd.conf with below trapsess token.

```
trapsess -Ci -v 3 -u informtest -l authPriv -a SHA -A mypassword -x AES -X
mypassword <TRAP DESTINATION IP>
```

Below is one example of informs forwarded by iDRAC Service Module and captured by `snmptrapd`.

```
2016-01-20 15:42:06 localhost [UDP: [127.0.0.1]:35185->[127.0.0.1]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (10107) 0:01:41.07
SNMPv2-MIB::snmpTrapOID.0 = OID:
SNMPv2-SMI::enterprises.674.10892.5.3.2.1.0.2153
SNMPv2-SMI::enterprises.674.10892.5.3.1.1.0 = STRING: "FAN0003"
SNMPv2-SMI::enterprises.674.10892.5.3.1.2.0 = STRING: "Fan 1 RPM is greater
than the upper critical threshold."
SNMPv2-SMI::enterprises.674.10892.5.3.1.3.0 = INTEGER: 5
SNMPv2-SMI::enterprises.674.10892.5.3.1.4.0 = STRING: "DGCF862"
SNMPv2-SMI::enterprises.674.10892.5.3.1.5.0 = STRING: "ubuntu"
SNMPv2-SMI::enterprises.674.10892.5.3.1.6.0 = STRING: "System.Embedded.1"
SNMPv2-SMI::enterprises.674.10892.5.3.1.7.0 = STRING: "iDRAC" SNMPv2-
SMI::enterprises.674.10892.5.3.1.8.0 = STRING: "\"1\""
SNMPv2-SMI::enterprises.674.10892.5.3.1.9.0 = STRING: "BGCF862"
SNMPv2-SMI::enterprises.674.10892.5.3.1.10.0 = STRING: "CMC-BGCF862"
SNMPv2-SMI::enterprises.674.10892.5.3.1.11.0 = STRING: "idrac-DGCF862"
SNMPv2-MIB::snmpTrapEnterprise.0 = OID:
SNMPv2-SMI::enterprises.674.10892.5.3.2.1
```

2.4 Configuring the SMUX peer password

Below output is for setting SMUX agent with password using Enable-iDRACSNMPTrap.sh.

```
root@XXXXX: /opt/dell/srvadmin/iSM/bin# ./Enable-iDRACSNMPTrap.sh
changesmuxpasswd test123
root@XXXXXX: /opt/dell/srvadmin/iSM/bin# ./Enable-iDRACSNMPTrap.sh 1 –force
* Restarting network management services:
* Restarting network management services:
* Stopping network management services:
* Starting network management services:
iDRAC Service Module smux peer is configured, please ensure smux is enabled for
master snmp agent.
SNMP Trap feature is enabled in iDRAC Service Module.
```

Below output is for setting SMUX agent without password using Enable-iDRACSNMPTrap.sh

```
root@ubuntu:/opt/dell/srvadmin/iSM/bin# ./Enable-iDRACSNMPTrap.sh
changesmuxpasswd ""
root@ubuntu:/opt/dell/srvadmin/iSM/bin# ./Enable-iDRACSNMPTrap.sh 1 –force
* Restarting network management services:
* Restarting network management services:
* Stopping network management services:
* Starting network management services:
iDRAC Service Module smux peer is configured, please ensure smux is enabled for
master snmp agent.
SNMP Trap feature is enabled in iDRAC Service Module.
```

2.5 Configuring the feature to use AgentX protocol

Beginning with iSM 2.4.0, you can configure Agent-x as the default protocol for In-band iDRAC SNMP alerts using the following command:

`./Enable-iDRACSNMPTrap.sh 1/agentx--force`

If `--force` is not specified, ensure that the Net-SNMP is configured and restart the snmpd service.

To enable this feature: `Enable-iDRACSNMPTrap.sh 1` (OR) `Enable-iDRACSNMPTrap.sh enable` –
To disable this feature: Enable-iDRACSNMPTrap.sh 0 (OR) Enable-iDRACSNMPTrap.sh disable

NOTE: The --force option configures the Net-SNMP to forward the traps. However, you must configure the trap destination

You can also switch between SMUX and AgentX protocol by using the relevant options.

Example: ./Enable-iDRACSNMPTrap.sh 1 protocol smux/agentx

3 Configuration on VMware ESXi 7.x Operating Systems

This feature shall be disabled and installed on the Host OS since there is no option to enable at the time of VIB installation. The only way you can enable or disable the feature is during run-time. iDRAC Service Module exposes a CIM extrinsic method called `EnableInBandSNMPTraps` which can be invoked remotely using wsman clients. The permissible values will be zero (0) and one (1) which corresponds to disabling and enabling the feature respectively.

The command syntax: `winrm i EnableInBandSNMPTraps http://schemas.dell.com/wbem/wscim/1/cim-schema/2/root/cimv2/dcim/DCIM_iSMService?__cimnamespace=root/cimv2/dcim+InstanceID=iSMExportedFunctions -u:<username> -p:<password> -r:https://<remote hostname OR IP Address>:443/wsman -a:basic -encoding:utf-8 -skipCNCheck -skipCACheck -skipRevocationcheck` **`@{state="1"}`**

In addition to enabling this feature in iDRAC Service Module; VMware ESXi has few settings for SNMP that should be reviewed and configured appropriately. Below are some of the frequently used commands in ESXi.

The command syntax: `winrm i EnableInBandSNMPTraps http://schemas.dell.com/wbem/wscim/1/cim-schema/2/root/cimv2/dcim/DCIM_iSMService?__cimnamespace=root/cimv2/dcim+InstanceID=iSMExportedFunctions -u:<username> -p:<password> -r:https://<remote hostname OR IP Address>:443/wsman -a:basic -encoding:utf-8 -skipCNCheck -skipCACheck -skipRevocationcheck` **`@{state="0"}`**

```
EnableInBandSNMPTraps_OUTPUT
ReturnValue = 0
```

Note: On Vmware ESXi 8.x operating system, remote enablement of the SNMP Trap feature is not supported

3.1 To view the current OS SNMP settings

```
# esxcli system snmp get
```

```
root@localhost: /opt/dell/srvadmin/iSM/bin] esxcli system snmp get
Authentication: none
Communities: public
Enable: true
Engineid: 00000063000000a100000000
Hwsrc: indications
Largestorage: true
Loglevel: info
Notraps:
Port: 161
Privacy: none
Remoteusers:
Syscontact:
Syslocation:
Targets: <IP Address>@162 public
Users:
V3targets:
```

3.2 To enable the SNMP traps in ESXi OS

```
# esxcli system snmp set --enable=TRUE
```

3.3 To set trap destinations

```
# esxcli system snmp set –targets=<IP Address>@162/public
```

where
162: UDP port number for SNMP
Public: community name string

4 Handling past SNMP Alerts

There could be scenarios where the In-band SNMP Alerts feature is enabled in iDRAC Service Module and the Host OS undergoes a reboot. During this down time, the administrator might miss few alerts since iDRAC Service Module and iDRAC are not connected. In such scenarios, after the reboot, all the traps shall be sent out as soon as the communication between iDRAC Service Module and iDRAC is restarted.

5 MIB description

Here is one of the MIB example:

```
SNMPv2-MIB::snmpTrapOID.0 = OID:
SNMPv2-SMI::enterprises.64.10892.5.3.2.1.0.2153
SNMPv2-SMI::enterprises.674.10892.5.3.1.1.0 = STRING: "FAN0003"
SNMPv2-SMI::enterprises.674.10892.5.3.1.2.0 = STRING: "Fan 1 RPM is greater than
the upper critical threshold."
SNMPv2-SMI::enterprises.674.10892.5.3.1.3.0 = INTEGER: 5
SNMPv2-SMI::enterprises.674.10892.5.3.1.4.0 = STRING: "DGCF862"
SNMPv2-SMI::enterprises.674.10892.5.3.1.5.0 = STRING: "ubuntu"
SNMPv2-SMI::enterprises.674.10892.5.3.1.6.0 = STRING: "System.Embedded.1"
SNMPv2-SMI::enterprises.674.10892.5.3.1.7.0 = STRING: "iDRAC"
SNMPv2-SMI::enterprises.674.10892.5.3.1.8.0 = STRING: "\"1\""
SNMPv2-SMI::enterprises.674.10892.5.3.1.9.0 = STRING: "BGCF862"
SNMPv2-SMI::enterprises.674.10892.5.3.1.10.0 = STRING: "CMC-BGCF862"
SNMPv2-SMI::enterprises.674.10892.5.3.1.11.0 = STRING: "idrac-DGCF862"
```

This MIB has information about message ID, message, current status, system service tag, system FQDD and alert FQDD.

6 Error Handling

6.1 SMUX Fails on Linux and Debian OS-es

If snmpd daemon is reporting the below warning about smuxpeer,

```
Warning: Unknown token: smuxpeer.
```

Then it means that, SMUX subsystem is disabled at daemon startup by an option set in `/etc/default/snmpd`.

Using the `-I` option will turn on (or off) a particular module used by snmpd.

In this case, the line looks like this:

```
14 No Restrictions | In-Band iDRAC SNMP Alerts
```

```
SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -g snmp -I -smux,mteTrigger,mteTriggerConf
-p /var/run/snmpd.pid'
```

With this configuration, the SMUX module is disabled.

For snmpd to support SMUX, the line should look like this instead (removing the -I option and its argument):

```
SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -g snmp -p /var/run/snmpd.pid'
```

After making the change, restart the daemon:

```
service snmpd restart
```

7 Mapping iDRAC to OMSA and OMSS SNMP Alerts

This feature enables to convert iDRAC SNMP alerts to OpenManage Server Administrator (OMSA) and OpenManage Storage Services (OMSS) alerts. Once iDRAC Service Module (iSM) receives the SNMP alert from iDRAC, iSM creates the SNMP varbinds payload applicable to OMSA and OMSS alerts and sends the payload to the SNMP agent. This mapping is designed and implemented as an enhancement to the existing iSM SNMP Feature Plug-in (FPI) feature.

When the Host SNMP OMSA Alerts feature is disabled, the existing feature of forwarding iDRAC LifeCycle Logs as SNMP traps is active. The following table indicates the various feature states:

Table 1. OMSA and OMSS SNMP alert feature states

iDRAC.ServiceModule.HostSNMPAlert	**iDRAC.ServiceModule.HostSNMPOMSAAlert**	**Remarks**
Yes	Yes	iDRAC to OMSA SNMP map is trapped and sent to destination.
Yes	No	Only iDRAC alerts are sent to destination (default condition).
No	Yes	NA
No	No	No alert is mapped and sent to any destination.

Based on the above feature configuration, iSM forwards the received iDRAC alert to the trap destination having any of the following Object Identifiers:

- iDRAC Enterprise Object Identifier (existing feature)
- OMSA and OMSS Enterprise Object Identifier (introduced from iSM 4.1.0.0 onwards)

The feature behavior is defined using `iDRAC.ServiceModule.HostSNMPOMSAAlert` attribute on iDRAC.

7.1 OMSA and OMSS SNMP OID description

Below is the list of OMSA and OMSS SNMP OIDs which are sent to the alert destinations.

Table 2. OMSA and OMSS SNMP alert OID

SNMP OID	Description
1.3.6.1.4.1.674.10892.1.5000.10.1.0	System host generating alert
1.3.6.1.4.1.674.10892.1.5000.10.2.0	Specifies the object identifier for the index attribute in the table that contains the object causing the alert.
1.3.6.1.4.1.674.10892.1.5000.10.3.0	Alert message
1.3.6.1.4.1.674.10892.1.5000.10.4.0	Current status (Alert category)
1.3.6.1.4.1.674.10892.1.5000.10.5.0	Previous status
1.3.6.1.4.1.674.10892.1.5000.10.6.0	Alert FQDD
1.3.6.1.4.1.674.10892.1.5000.10.7.0	Alert Message ID
1.3.6.1.4.1.674.10892.1.5000.10.8.0	System FQDN generating alert
1.3.6.1.4.1.674.10892.1.5000.10.9.0	System Service Tag
1.3.6.1.4.1.674.10892.1.5000.10.10.0	Chassis Service Tag

7.2 OMSA and OMSS SNMP Alerts Group OID

Below is the list of alerts specific OID. iSM reports the alert specific OID at the group level.

Table 3. OMSA SNMP alert OID at group level

OMSA	Group	OID
	AMP	1.3.6.1.4.1.674.10892.1.200.10.1
	ASR	1.3.6.1.4.1.674.10892.1.300.10.1
	BAT	1.3.6.1.4.1.674.10892.1.600.50.1
	FAN	1.3.6.1.4.1.674.10892.1.700.12.1
	HWC	1.3.6.1.4.1.674.10892.1.1200.10.1
	MEM	1.3.6.1.4.1.674.10892.1.1300
	PSU	1.3.6.1.4.1.674.10892.1.600.10
	PWR	1.3.6.1.4.1.674.10892.1.600.12
	RDU	1.3.6.1.4.1.674.10892.1.200.10.1
	RRDU	1.3.6.1.4.1.674.10892.1.1100.110.1

	SEC	1.3.6.1.4.1.674.10892.1.300.10.1
	SYS	1.3.6.1.4.1.674.10892.1.400.20
	TMP	1.3.6.1.4.1.674.10892.1.700.20.1.2
	VLT	1.3.6.1.4.1.674.10892.1.600.20.1.2
	CPU	1.3.6.1.4.1.674.10892.1.1100.30.1.2

Table 4. OMSS SNMP alert OID at group level

OMSS	Group	OID
	BAT	1.3.6.1.4.1.674.10893.1.20.130.15.1.1
	CTL	1.3.6.1.4.1.674.10893.1.20.130.1.1.1
	ENC	1.3.6.1.4.1.674.10893.1.20.130.3.1.1
	PDR	1.3.6.1.4.1.674.10893.1.20.130.4.1.1
	PSU	1.3.6.1.4.1.674.10893.1.20.130.9.1.1
	SSD	0.0
	STOR	0.0
	VDR	1.3.6.1.4.1.674.10893.1.20.140.1.1.1
	TMP	1.3.6.1.4.1.674.10893.1.20.130.11.1.1