iDRAC Service Module-In-Band iDRAC SNMP Alerts

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

Dell Engineering
July 2016

Rajib Saha

Bharath Koushik

Ranjit Ranjan

A Dell Technical White Paper

Revisions

Date	Description
July 2016	Initial release

Table of Contents

Revisions 2

Executive summary 4

1 Configuration on Windows Operating Systems 5

1.1 Enable In-Band iDRAC SNMP Alerts Feature 5

1.2 Configuring Windows SNMP for Trap Forwarding 6

2 Configuration on Linux Operating Systems 7

1.1 Configuring the Net-SNMP for SNMPv3 informs 8

1.2 Configuring the Net-SNMP for Trap/Informs Forwarding 8

1.2.1 SNMPv1 and SNMPv2 8

1.2.2 SNMPv3 informs 8

1.3 Configuring the Trap Destination 9

1.3.1 Configuring the Trap Destination for SNMPv1 9

1.3.2 Configuring the Trap Destination for SNMPv2 10

1.3.3 Configuring the Informs Destination for SNMPv3 10

1.4 Configuring the SMUX peer password 11

3 Configuration on VMware ESXi Operating Systems 11

4 Handling Past SNMP Alerts 12

5 MIB description 13

6 Error Handling 13

6.1 SMUX Fails on Linux and Debian OS-es 13

Executive summary

This new feature of iDRAC Service Module 2.3 acts as an SNMP sub-agent to forward SNMP alerts. This feature is dependent on the Lifecycle Logs Replication in the OS Logs feature. However, the administrator has to configure the SNMP master agent on the host OS for trap destinations, community, SNMP version, and so on.

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 v2.3 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.

Following are pre-requisites of for in-band SNMP Alert feature

- OpenManage Server Administrator is not running on the Host OS.
- Lifecycle Log Replication feature of iDRAC Service Module is enabled.
- Administrator has to 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 Lifecycle Log Replication feature which is already part of iDRAC Service Module since v1.0. 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 can co-exist with OpenManage Server Administrator (OMSA). This feature is automatically turned off when iDRAC Service Module detects OMSA is active.
3. This feature is dependent on the Windows SNMP Service on supported Microsoft Windows OSes and requires NET-SNMP to be configured on Linux OSes 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.

Limitations

1. This feature in iDRAC Service Module 2.3 has no iDRAC supported interface to enable or disable the feature as in other features such as WMI Information, OS Information, and so on. However, iDRAC Service Module provides its own way to configure this feature.

Supported Dell Servers or Platforms

- The In-band iDRAC SNMP Alerts feature is supported on all Dell 12th generation servers and above.

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. 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-passwd> -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:administrator -p:Dell_123$ -r:http://10.94.146.18/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.

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.aspxor 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 provides the command usage information to the user.

A snapshot of the same is shown here:

```
root@XXXXXX:/opt/dell/srvadmin/iSM/bin# ./Enable-iDRACSNMPTrap.sh
Usage: Ensure Net-SNMP package is installed with SMUX protocol enabled. the command usage is as follows -
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 <passowrd> => change the smux password. Use enble/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 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.

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

```
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.
```

1.1 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

1.2 Configuring the Net-SNMP for Trap/Informs Forwarding

1.2.1 SNMPv1 and SNMPv2

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

```
disableAuthorization yes
authCommunity log public
```

1.2.2 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 also.

1.3 Configuring the Trap Destination

1.3.1 Configuring the Trap Destination for SNMPv1

You can send SNMPv2 traps using the trapsink token.

```
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 10.94.146.63(via UDP: [127.0.0.1]:36452->[127.0.0.1]:162) TRAP, SNMP v1,
community public
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"
```

1.3.2 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
```

1.3.3 Configuring the Informs 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
```

1.4 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 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.
```

3 Configuration on VMware ESXi Operating Systems

This feature is 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:<user-name> -p:<passwd> -r:https://<remote-host-name 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.

C:\Users\Administrator>**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:rajib -p:Dell_123$ism -r:https://10.94.146.73:443/wsman -a:basic -encoding:utf-8 -skipCNCheck -skipCACheck -skipRevocationcheck @{state="0"}**

```
EnableInBandSNMPTraps_OUTPUT
 ReturnValue = 0
```

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: 10.94.146.4@162 public
   Users:
   V3targets:
```

2. To enable the SNMP traps in ESXi OS

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

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.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"
```

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:
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
```