Configure and Understand SNMP Traps to Monitor Cisco ISE

Contents

Introduction

This document describes how to configure and understand Simple Network Management Protocol (SNMP) traps in order to monitor the Cisco ISE.

Prerequisites

Requirements

Cisco recommends that you have the knowledge of these topics:

- Basic Linux
- SNMP
- Identity Services Engine (ISE)

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ISE, Release 3.1
- RHEL 7 server

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

SNMP traps are UDP messages sent from an SNMP-enabled device to a remote MIB Server. ISE can be configured to send traps to an SNMP server in order to monitor and troubleshoot. This document aims to familiarize some of the basic checks to isolate issues and understand the limitations of ISE traps.

Configuration

ISE supports SNMP v1, v2, and v3. Check if SNMP is enabled on the ISE CLI and the rest of the

configuration.

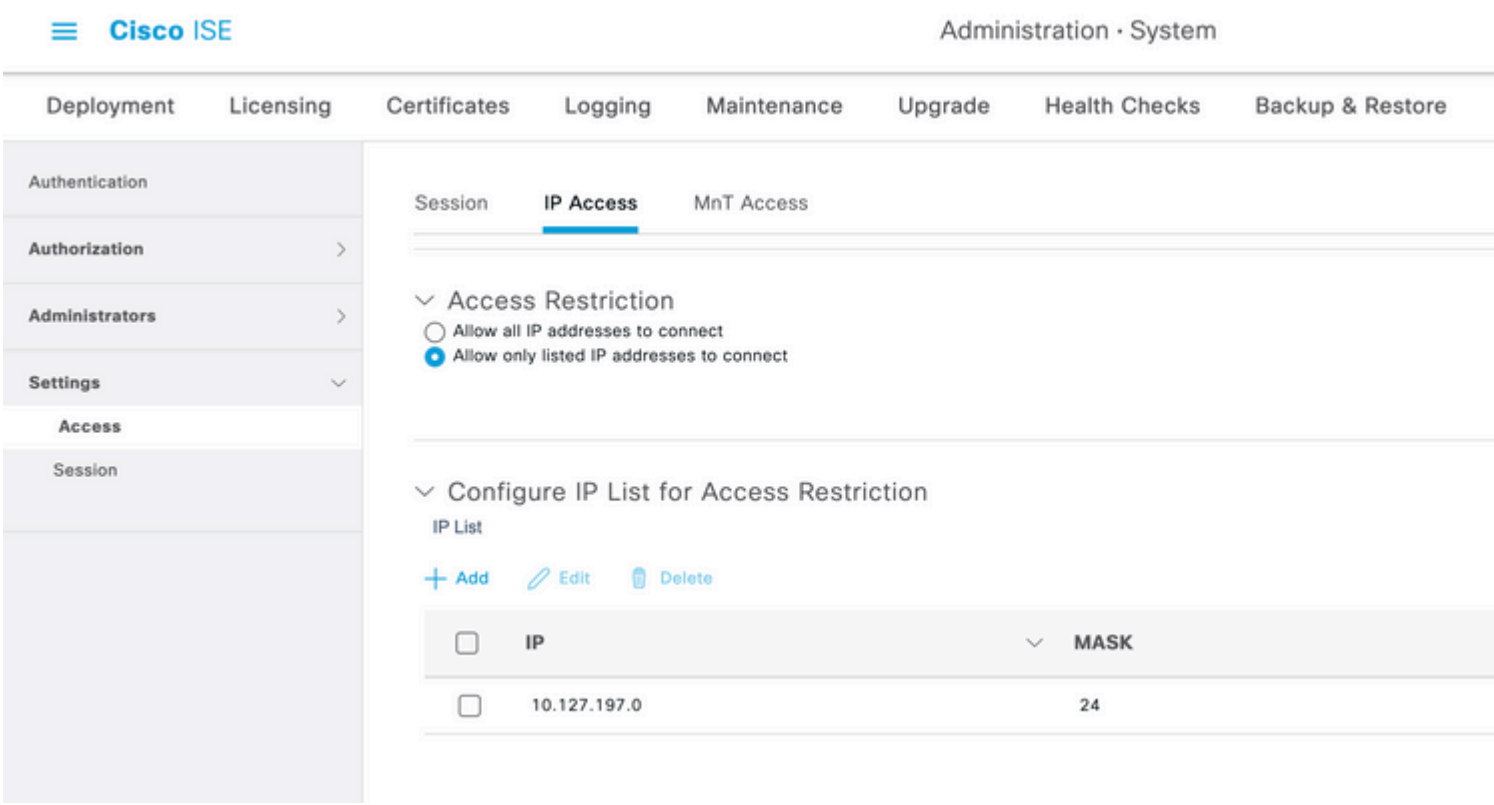
For example, SNMP v3:

<#root>

```
sotumu24/admin# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
sotumu24/admin(config)# snmp-server enable
sotumu24/admin(config)# snmp-server trap dskThresholdLimit "75"
sotumu24/admin(config)# snmp-server community SNMP$tring ro
sotumu24/admin(config)# snmp-server user SNMPUSER v3 plain authpasswd privpasswd


sotumu24/admin(config)# snmp-server host 10.127.197.81 version 3 SNMPUSER 0x474b49494c49464e474943 plain


>> The SNMP server might require the engineID if version 3 is being used and it can be dervied from the



sotumu24/admin# show snmp-server engineID
Local SNMP EngineID: GKIILIFNGIC


>> This is the same as ISE Serial number, need not be configured.



sotumu24/admin# sh udi

SPID: ISE-VM-K9
VPID: V01
Serial: GKIILIFNGIC
```

Ports and Reachability

The remote server must be able to reach the ISE in order to query traps if required. Ensure that ISE allows the SNMP server in IP access (if configured).



Check if port 161 is open on ISE CLI:

```
sotumu24/admin# sh ports | in 161
     udp: 0.0.0.0:25087, 0.0.0.0:161
--
     tcp: 169.254.0.228:49, 10.127.197.81:49, 169.254.0.228:50, 10.127.197.81:50
, 169.254.0.228:51, 10.127.197.81:51, 169.254.0.228:52, 10.127.197.81:52, 127.0.
0.1:8888, 10.127.197.81:8443, :::443, 10.127.197.81:8444, 10.127.197.81:8445, ::
:9085, 10.127.197.81:8446, :::19231, :::9090, 127.0.0.1:2020, :::9060, :::9061,
:::8905, :::8009, :::5514, :::9002, :::1099, :::8910, :::61616, :::80, :::9080
```

Logs

If the SNMP service daemon is stuck or unable to restart, the errors are seen in the messages log file.

```
2020-04-27T12:28:45.326652+05:30 sotumu24 su: (to oracle) root on none
2020-04-27T12:29:48.391712+05:30 sotumu24 snmpd[81079]: Received TERM or STOP signal...  shutting down..
2020-04-27T12:29:48.590240+05:30 sotumu24 snmpd[47597]: NET-SNMP version 5.7.2
2020-04-27T12:30:29.319929+05:30 sotumu24 rsyslogd: [origin software="rsyslogd" swVersion="7.4.7" x-pid=
```

Traps and Queries

Generic SNMP traps generated by default in Cisco ISE:

OID	Description	Trap Example
.1.3.6.1.4.1.8072.4.0.3 NET-SNMP-AGENT-MIB::nsNotifyRestart	An indication that the agent has been restarted.	DISMAN-EVENT-MIB:: 0:00:04.78 SNMPv SNMP-AGENT-MIB::ns MIB::snmpTrapEnterpr MIB::netSnmpNotificat
.1.3.6.1.4.1.8072.4.0.2 NET-SNMP-AGENT-MIB::nsNotifyShutdown	An indication that the agent is in the process of being shut down.	DISMAN-EVENT-MIB:: 0:00:04.79 SNMPv2-M SNMP-AGENT-MIB::ns MIB::snmpTrapEnterpr MIB::netSnmpNotificat
.1.3.6.1.6.3.1.1.5.4 IF-MIB::linkUp	A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the Down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.	DISMAN-EVENT-MIB:: 0:00:04.78 SNMPv2-M MIB::linkUp IF-MIB::ifIn MIB::ifAdminStatus.12 MIB::ifOperStatus.12 = MIB::snmpTrapEnterpr MIB::netSnmpAgentOI
.1.3.6.1.6.3.1.1.5.3 IF-MIB::linkDown	A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the Down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.	DISMAN-EVENT-MIB:: 0:00:04.79 SNMPv2-M MIB::linkDown IF-MIB:: MIB::ifAdminStatus.5 = MIB::ifOperStatus.5 = I MIB::snmpTrapEnterpr MIB::netSnmpAgentOI
.1.3.6.1.6.3.1.1.5.1 SNMPv2-MIB::coldStart	A coldStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered.	DISMAN-EVENT-MIB:: 0:00:00.08 SNMPv2-M MIB::coldStart SNMPv NET-SNMP-MIB::netSn

ISE does not have any MIB for process status or disk utilization. Cisco ISE uses OID HOST-RESOURCES-MIB::hrSWRunName for SNMP traps. snmp walk or snmp get command, in order to query the process status or disk utilization, cannot be used in ISE.

Source: Admin Guide

In the lab, SNMP Trap was set to trigger when the disk utilization crosses the threshold limit 75:
sotumu24/admin(config)# snmp-server trap dskThresholdLimit "75".

The data for this trap is collected from the outputs shown.

Run these commands on an external LINUX box or SNMP Server console:

```
Linux/admin# snmpwalk -v 3 -l authPriv -u SNMPUSER -a sha -x AES -A "authpasswd" -X "privpasswd" 10.127.

UCD-SNMP-MIB::dskPercent.1 = INTEGER: 11
UCD-SNMP-MIB::dskPercent.6 = INTEGER: 0
UCD-SNMP-MIB::dskPercent.8 = INTEGER: 0
UCD-SNMP-MIB::dskPercent.9 = INTEGER: 0
UCD-SNMP-MIB::dskPercent.29 = INTEGER: 0
UCD-SNMP-MIB::dskPercent.30 = INTEGER: 23
UCD-SNMP-MIB::dskPercent.31 = INTEGER: 2
UCD-SNMP-MIB::dskPercent.32 = INTEGER: 5
```

```
UCD-SNMP-MIB::dskPercent.33 = INTEGER: 0
UCD-SNMP-MIB::dskPercent.34 = INTEGER: 0
UCD-SNMP-MIB::dskPercent.35 = INTEGER: 0
UCD-SNMP-MIB::dskPercent.36 = INTEGER: 0
UCD-SNMP-MIB::dskPercent.37 = INTEGER: 5
UCD-SNMP-MIB::dskPercent.39 = INTEGER: 0
UCD-SNMP-MIB::dskPercent.41 = INTEGER: 0
UCD-SNMP-MIB::dskPercent.42 = INTEGER: 0
UCD-SNMP-MIB::dskPercent.43 = INTEGER: 0
UCD-SNMP-MIB::dskPercent.44 = INTEGER: 0

Linux/admin# snmpwalk -v 3 -l authPriv -u SNMPUSER -a sha -x AES -A "authpasswd" -X "privpasswd" 10.127.

UCD-SNMP-MIB::dskPath.1 = STRING: /
UCD-SNMP-MIB::dskPath.6 = STRING: /dev/shm
UCD-SNMP-MIB::dskPath.8 = STRING: /run
UCD-SNMP-MIB::dskPath.9 = STRING: /sys/fs/cgroup
UCD-SNMP-MIB::dskPath.29 = STRING: /tmp
UCD-SNMP-MIB::dskPath.30 = STRING: /boot
UCD-SNMP-MIB::dskPath.31 = STRING: /storedconfig
UCD-SNMP-MIB::dskPath.32 = STRING: /opt
UCD-SNMP-MIB::dskPath.33 = STRING: /localdisk
UCD-SNMP-MIB::dskPath.34 = STRING: /run/user/440
UCD-SNMP-MIB::dskPath.35 = STRING: /run/user/301
UCD-SNMP-MIB::dskPath.36 = STRING: /run/user/321
UCD-SNMP-MIB::dskPath.37 = STRING: /opt/docker/runtime/overlay
UCD-SNMP-MIB::dskPath.39 = STRING: /opt/docker/runtime/containers/ae1cef55c92ba90ae6c848bd74c9277c2fb52a
UCD-SNMP-MIB::dskPath.41 = STRING: /run/user/0
UCD-SNMP-MIB::dskPath.42 = STRING: /run/user/304
UCD-SNMP-MIB::dskPath.43 = STRING: /run/user/303
UCD-SNMP-MIB::dskPath.44 = STRING: /run/user/322
```

From these outputs, the disk utilization is calculated and when the value reaches 75, an SNMP Trap is sent to the configured SNMP-Sever HOST. There is no MIB Resource in order to calculate and display the disk utilization directly.

Further, the MIB process hrSWRunName is used to collect this information (as per the ISE Admin Guide).

A textual description of this running piece of software, that includes the manufacturer, revision, and the name by which it is commonly known. If this software was installed locally, this must be the same string as that used in the hrSWInstalledName that corresponds. The services taken into consideration are app-server, rsyslog, redis-server, ad-connector, mnt-collector , mnt-processor , ca-server est-server , and elasticsearch.

MIB Resources

ISE application is hosted on RHEL OS(Linux). However, as mentioned in the ISE admin guide, ISE uses Host Resources MIB to gather SNMP Trap information. This document has the list of Host Resources MIB that can be queried:

SNMP HOST MIB.

From the document, it can be inferred that there are no direct queries that can calculate and display the values of CPU, Memory, or Disk utilization. However, the data that is used to calculate the outputs are present in these tables:

- hrSWRunPerf Table
- hrDiskStorage

Table
- Scalars Table

Additional Pointers on Memory and Disk Utilization

Used Memory

In order to calculate the used memory, use:

mem_used = kb_main_total - kb_main_free - kb_main_cached - kb_main_buffers;

kb_main_cached = kb_page_cache + kb_slab_reclaimable;

Free Memory

There is a slight difference between the values collected in the SNMP Server and the ISE CLI root-bash. Memory utilization also has a difference in the values due to slab, which is not accounted for in the SNMP, and it shows the total value.

Free memory is a small amount of memory that is not currently used and causes this difference. This is the wasted part of the memory that the system is unable to utilize. ISE is hosted on a Linux OS and uses all physical memory that is not needed by current programs as a file cache, for efficiency. However, if programs need this physical memory, the kernel reallocates the file cache memory to the former. Hence, the memory used by the file cache is free but unutilized until it is needed by a program.

Refer to this link:

Free memory explanation.

Disk Utilization

Similarly, up to 5% of the filesystem is reserved for the root user in order to reduce file fragmentation. This output is not seen in 'df'.

Hence, it is expected to see a small difference in the percentage calculated in the root bash and subsequently the CLI output.

SNMP query does not consider this reserved disk space and calculates the output based on the values displayed in the table.

For more information, refer to the Difference in df output and df output reserved disk space.