Configuración y comprensión de trampas SNMP para supervisar Cisco ISE

Contenido

Introducción

Este documento describe cómo configurar y entender las trampas del Protocolo simple de administración de red (SNMP) para monitorear Cisco ISE.

Prerequisites

Requirements

Cisco recomienda que conozca estos temas:

- Linux básico
- SNMP (Protocolo de administración de red simple)
- Identity Services Engine (ISE)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco ISE, versión 3.1
- servidor RHEL 7

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Las trampas SNMP son mensajes UDP enviados desde un dispositivo habilitado para SNMP a un servidor MIB remoto. ISE se puede configurar para enviar capturas a un servidor SNMP con el fin de supervisar y solucionar problemas. Este documento tiene como objetivo familiarizar algunas de las comprobaciones básicas para aislar problemas y comprender las limitaciones de las trampas ISE.

Configuración

ISE admite SNMP v1, v2 y v3. Compruebe si SNMP está habilitado en la CLI de ISE y en el resto de la configuración.

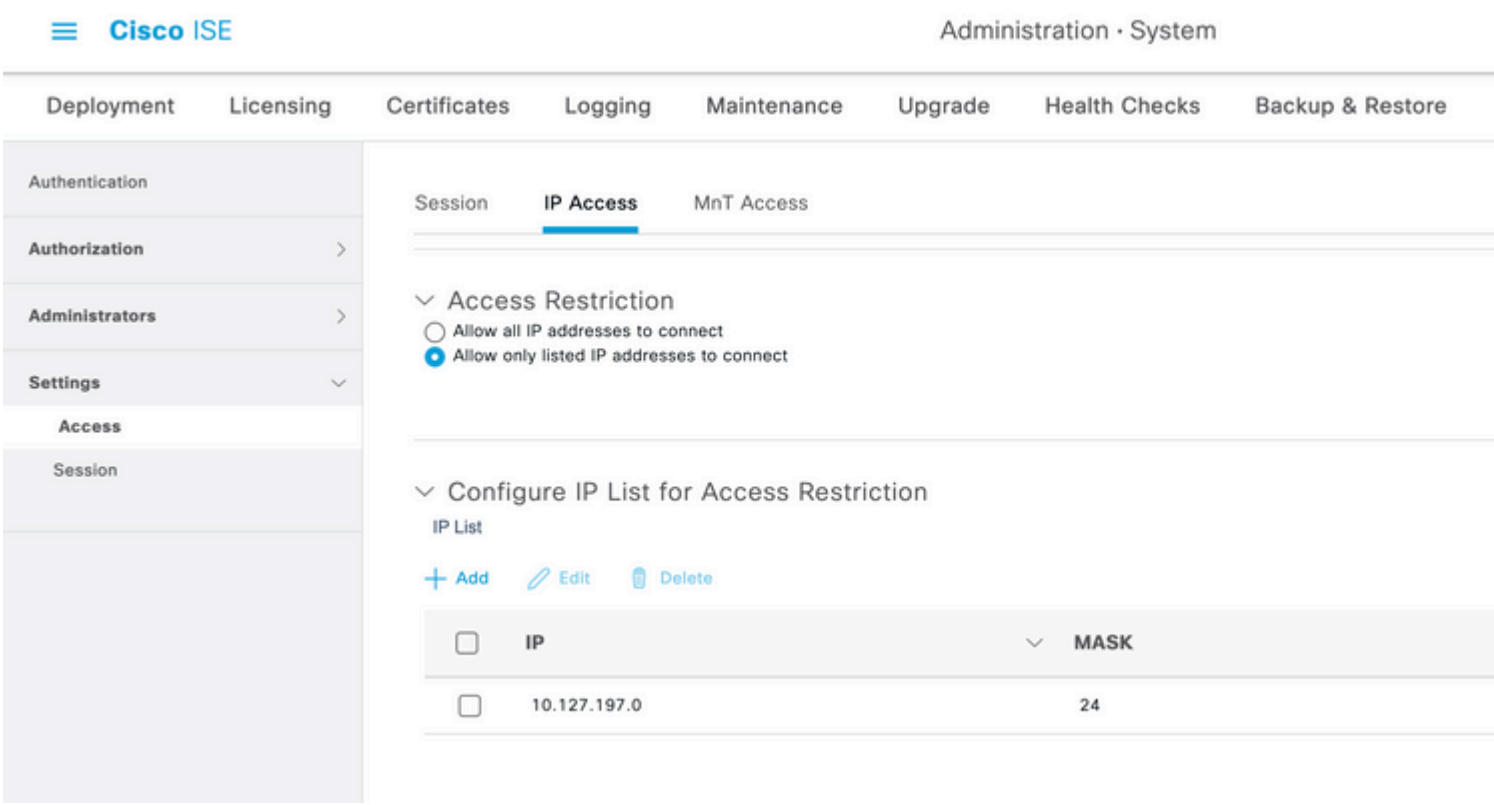
Por ejemplo, SNMP v3:

<#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
```

Puertos y disponibilidad

El servidor remoto debe ser capaz de alcanzar el ISE para consultar trampas si es necesario. Asegúrese de que ISE permite el servidor SNMP en el acceso IP (si está configurado).



Compruebe si el puerto 161 está abierto en la CLI de ISE:

```
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
```

Registros

Si el daemon del servicio SNMP está atascado o no puede reiniciarse, los errores se ven en el archivo de registro de mensajes.

```
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=
```

Trampas y consultas

Trampas SNMP genéricas generadas de forma predeterminada en 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::ifI 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::netS

ISE no tiene ningún MIB para el estado del proceso o la utilización del disco. Cisco ISE utiliza OID HOST-RESOURCES-MIB::hrSWRunName para las trampas SNMP. snmp walk or snmp get , para consultar el estado del proceso o la utilización del disco, no se puede utilizar en ISE.

Fuente: Admin Guide

En el laboratorio, la trampa SNMP se configuró para que se activara cuando el uso del disco cruzara el límite de umbral 75: sotumu24/admin(config)# snmp-server trap dskThresholdLimit "75".

Los datos para esta trampa se recopilan de las salidas mostradas.

Ejecute estos comandos en un cuadro LINUX externo o en la consola del servidor SNMP:

```
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
```

A partir de estas salidas, se calcula la utilización del disco y cuando el valor alcanza 75, se envía una trampa SNMP al HOST SNMP-Server configurado. No hay ningún recurso MIB para calcular y mostrar el uso del disco directamente.

Además, el proceso MIB hrSWRunName se utiliza para recopilar esta información (según la Guía de administración de ISE).

Una descripción textual de este software en ejecución, que incluye el fabricante, la revisión y el nombre por el que se conoce comúnmente. Si este software se instaló localmente, debe ser la misma cadena que la utilizada en el hrSWInstalledName que corresponde. Los servicios que se tienen en cuenta son app-server, rsyslog, redis-server, ad-connector, mnt-collector , mnt-processor , ca-server est-server ,y elasticsearch.

Recursos de MIB

La aplicación ISE está alojada en RHEL OS (Linux). Sin embargo, como se menciona en la guía de administración de ISE, ISE utiliza la MIB de recursos de host para recopilar información de trampas SNMP. Este documento tiene la lista de MIB de Recursos de Host que se pueden consultar:

MIB DE HOST SNMP.

A partir del documento, se puede inferir que no hay consultas directas que puedan calcular y mostrar los valores de uso de CPU, Memoria o Disco. Sin embargo, los datos que se utilizan para calcular las salidas

están presentes en estas tablas:

- hrSWRunPerf Tabla
- hrDiskStorage Tabla
- Tabla de escalares

Punteros adicionales sobre la utilización de memoria y disco

Memoria usada

Para calcular la memoria utilizada, utilice:

mem_used = kb_main_total - kb_main_free - kb_main_cached - kb_main_buffers;

kb_main_cached = kb_page_cache + kb_slab_reclaimable;

Memoria libre

Existe una pequeña diferencia entre los valores recopilados en el servidor SNMP y la base raíz de ISE CLI. La utilización de memoria también tiene una diferencia en los valores debido a la losa, que no se tiene en cuenta en el SNMP, y muestra el valor total.

La memoria libre es una pequeña cantidad de memoria que no se utiliza actualmente y causa esta diferencia. Esta es la parte desperdiciada de la memoria que el sistema no puede utilizar. ISE se aloja en un sistema operativo Linux y utiliza toda la memoria física que los programas actuales no necesitan como caché de archivos para lograr mayor eficacia. Sin embargo, si los programas necesitan esta memoria física, el núcleo reasigna la memoria caché de archivos a la anterior. Por lo tanto, la memoria utilizada por la memoria caché de archivos es libre pero no se utiliza hasta que un programa la necesita.

Consulte este enlace:

Explicación de memoria libre.

Utilización del disco

De manera similar, hasta el 5% del sistema de archivos se reserva para el usuario raíz con el fin de reducir la fragmentación de archivos. Este resultado no se ve en 'df'.

Por lo tanto, se espera ver una pequeña diferencia en el porcentaje calculado en la base raíz y, posteriormente, en el resultado de CLI.

La consulta SNMP no tiene en cuenta este espacio de disco reservado y calcula el resultado basándose en los valores mostrados en la tabla.

Para obtener más información, consulte Diferencia en la salida df y espacio en disco reservado de salida df.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).