Configurar e entender interceptações SNMP para monitorar o Cisco ISE

Contents

Introdução

Este documento descreve como configurar e entender traps do protocolo de gerenciamento de rede simples (SNMP - Simple Network Management Protocol) para monitorar o Cisco ISE.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha o conhecimento destes tópicos:

- Linux básico
- SNMP
- Identity services engine (ISE)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco ISE, versão 3.1
- servidor RHEL 7

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

As interceptações SNMP são mensagens UDP enviadas de um dispositivo ativado por SNMP para um servidor MIB remoto. O ISE pode ser configurado para enviar interceptações a um servidor SNMP para monitorar e solucionar problemas. Este documento tem como objetivo familiarizar algumas das verificações básicas para isolar problemas e entender as limitações de armadilhas do ISE.

Configuração

O ISE suporta SNMP v1, v2 e v3. Verifique se o SNMP está habilitado na CLI do ISE e no restante da configuração.

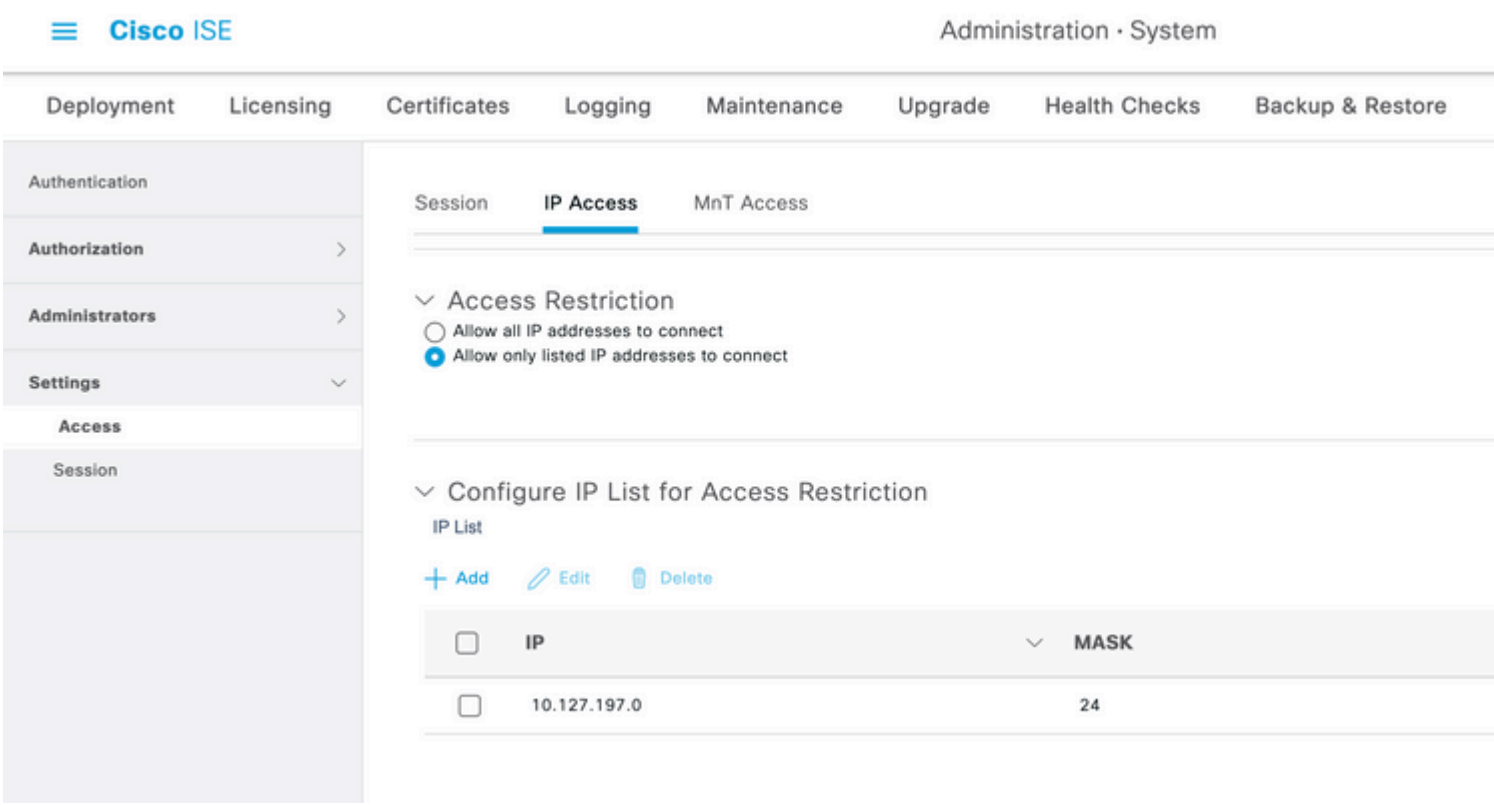
Por exemplo, SNMP v3:

<#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
```

Portas e acessibilidade

O servidor remoto deve ser capaz de acessar o ISE para consultar armadilhas, se necessário. Certifique-se de que o ISE permita que o servidor SNMP tenha acesso IP (se configurado).



Verifique se a porta 161 está aberta no 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

Se o daemon do serviço SNMP estiver travado ou for incapaz de reiniciar, os erros serão vistos no arquivo de registro de mensagens.

```
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=
```

Armadilhas e consultas

Interceptações SNMP genéricas geradas por padrão no 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 = 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

O ISE não tem nenhuma MIB para status de processo ou utilização de disco. O Cisco ISE usa OID HOST-RESOURCES-MIB::hrSWRunName para traps SNMP. snmp walk or snmp get para consultar o status do processo ou a utilização do disco, não pode ser usado no ISE.

Fonte: Guia do administrador

No laboratório, a interceptação (Trap) SNMP foi configurada para ser acionada quando a utilização do disco ultrapassa o limite de 75: sotumu24/admin(config)# snmp-server trap dskThresholdLimit "75".

Os dados para essa interceptação são coletados das saídas mostradas.

Execute estes comandos em uma caixa LINUX externa ou no console do 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 dessas saídas, a utilização do disco é calculada e, quando o valor chega a 75, uma interceptação SNMP é enviada ao HOST do servidor SNMP configurado. Não há recurso MIB para calcular e exibir a utilização do disco diretamente.

Além disso, o processo MIB hrSWRunName é usado para coletar essas informações (de acordo com o Guia de Administração do ISE).

Uma descrição textual desse software em execução, que inclui o fabricante, a revisão e o nome pelo qual ele é comumente conhecido. Se este software foi instalado localmente, deve ser a mesma sequência de caracteres usada no hrSWInstalledName isso corresponde. Os serviços considerados são app-server, rsyslog, redis-server, ad-connector, mnt-collector , mnt-processor , ca-server est-server ,e elasticsearch.

Recursos MIB

O aplicativo ISE está hospedado no RHEL OS(Linux). No entanto, como mencionado no guia de administração do ISE, o ISE usa MIB de recursos de host para reunir informações de interceptação SNMP. Este documento contém a lista de MIBs de recursos de host que podem ser consultados:

SNMP HOST MIB.

A partir do documento, pode-se inferir que não há consultas diretas que possam calcular e exibir os valores de utilização de CPU, Memória ou Disco. No entanto, os dados usados para calcular as saídas estão

presentes nestas tabelas:

- hrSWRunPerf Tabela
- hrDiskStorage Tabela
- Tabela de escalares

Ponteiros adicionais sobre a utilização de memória e disco

Memória usada

Para calcular a memória usada, use:

mem_used = kb_main_total - kb_main_free - kb_main_cached - kb_main_buffers;

kb_main_cached = kb_page_cache + kb_slab_reclaimable;

Memória livre

Há uma pequena diferença entre os valores coletados no servidor SNMP e o root-bash da CLI do ISE. A utilização de memória também tem uma diferença nos valores devido ao slab, que não é contabilizado no SNMP, e mostra o valor total.

Memória livre é uma pequena quantidade de memória que não é usada atualmente e causa essa diferença. Essa é a parte desperdiçada da memória que o sistema não pode utilizar. O ISE é hospedado em um sistema operacional Linux e usa toda a memória física que não é necessária pelos programas atuais como um cache de arquivos, para eficiência. No entanto, se os programas precisarem dessa memória física, o kernel realoca a memória cache do arquivo para a memória anterior. Portanto, a memória usada pelo cache de arquivos é livre, mas não é utilizada até que seja necessária por um programa.

Consulte este link:

Explicação sobre memória livre.

Utilização de disco

Da mesma forma, até 5% do sistema de arquivos é reservado para o usuário raiz a fim de reduzir a fragmentação de arquivos. Esta saída não é vista em 'df'.

Portanto, espera-se ver uma pequena diferença na porcentagem calculada na raiz bash e subsequentemente na saída CLI.

A consulta SNMP não considera esse espaço em disco reservado e calcula a saída com base nos valores exibidos na tabela.

Para obter mais informações, consulte Diferença na saída df e saída df espaço em disco reservado.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.