SNMP-traps configureren en begrijpen om Cisco ISE te bewaken

Inhoud

Inleiding

Dit document beschrijft hoe u Simple Network Management Protocol (SNMP)-traps moet configureren en begrijpen om Cisco ISE te kunnen bewaken.

Voorwaarden

Vereisten

Cisco raadt u aan deze onderwerpen te kennen:

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

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ISE-softwarerelease 3.1
- RHEL 7-server

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

SNMP-traps zijn UDP-berichten die vanaf een SNMP-apparaat worden verzonden naar een externe MIB-server. ISE kan worden geconfigureerd om traps naar een SNMP-server te sturen voor bewaking en probleemoplossing. Dit document is bedoeld om bepaalde basiscontroles bekend te maken om problemen te isoleren en de beperkingen van ISE-vallen te begrijpen.

Configuratie

ISE ondersteunt SNMP v1, v2 en v3. Controleer of SNMP is ingeschakeld op de ISE-CLI en de rest van de configuratie.

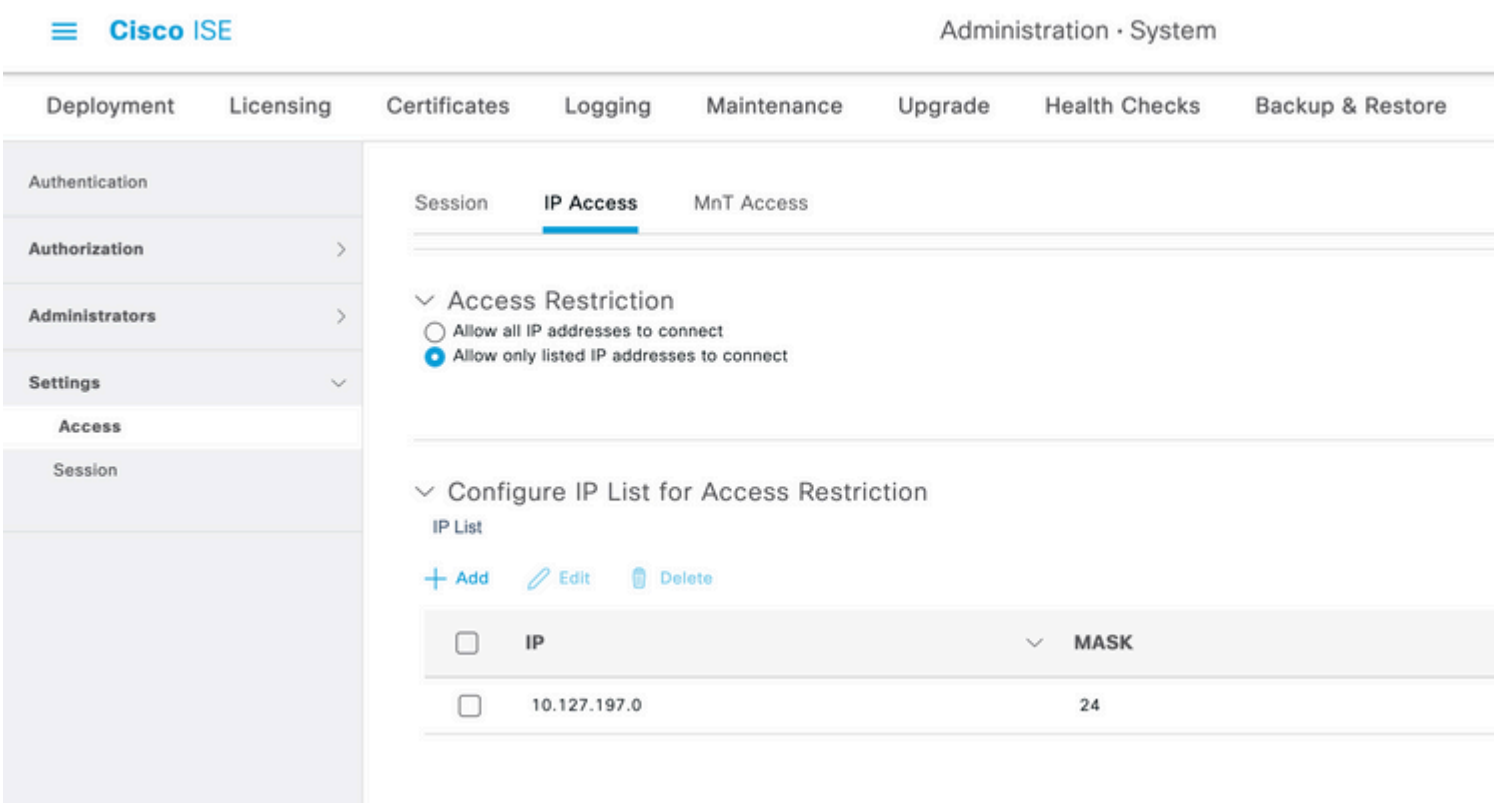
Bijvoorbeeld SNMP v3:

<#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
```

Poorten en bereikbaarheid

De externe server moet de ISE kunnen bereiken om eventueel vallen te kunnen opvragen. Zorg ervoor dat ISE de SNMP-server in IP-toegang biedt (indien geconfigureerd).



Controleer of poort 161 op ISE-CLI is geopend:

```
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
```

Logboeken

Als de SNMP-service daemon vast zit of niet kan herstarten, worden de fouten in het logbestand voor berichten weergegeven.

```
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 en vragen

Generieke SNMP-traps die standaard in Cisco ISE zijn gegenereerd:

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 heeft geen MIB voor processtatus of schijfgebruik. Cisco ISE-gebruik OID HOST-RESOURCES-MIB::hrSWRunName voor SNMP-traps. snmp walk of snmp get opdracht om de processtatus of het schijfgebruik op te vragen, kan niet worden gebruikt in ISE.

Bron: Admin Guide

In het laboratorium is SNMP Trap ingesteld op trigger wanneer het schijfgebruik de drempelwaarde 75 overschrijdt: sotumu24/admin(config)# snmp-server trap dskThresholdLimit "75".

De gegevens voor deze val worden verzameld uit de getoonde uitgangen.

Voer deze opdrachten uit op een externe LINUX-box of SNMP-serverconsole:

```
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
```

Van deze uitgangen wordt het schijfgebruik berekend en wanneer de waarde 75 bereikt, wordt een SNMP-trap naar de geconfigureerde SNMP-Server-HOST verzonden. Er is geen MIB-bron om het schijfgebruik direct te berekenen en weer te geven.

Het MIB-proces hrSWRunName wordt gebruikt om deze informatie te verzamelen (volgens de ISE-beheerdersgids).

Een tekstuele beschrijving van dit lopende stuk software, dat de fabrikant, de herziening, en de naam omvat waardoor het algemeen bekend is. Als deze software lokaal is geïnstalleerd, moet dit dezelfde string zijn als die gebruikt in de hrSWInstalledName dat is hetzelfde. De in aanmerking genomen diensten zijn app-server, rsyslog, redis-server, ad-connector, mnt-collector , mnt-processor , ca-server est-server , en elasticsearch.

MIB-bronnen

ISE-toepassing wordt gehost op RHEL OS(Linux). Echter, zoals vermeld in de ISE admin gids, ISE gebruikt Host Resources MIB om SNMP Trap informatie te verzamelen. Dit document heeft de lijst met hostbronnen MIB die kunnen worden opgevraagd:

SNMP-HOST MIB.

Uit het document kan worden afgeleid dat er geen directe query's zijn die de waarden van CPU-, geheugen- of schijfgebruik kunnen berekenen en weergeven. De gegevens die voor de berekening van de output

worden gebruikt, zijn echter in deze tabellen opgenomen:

- hrSWRunPerf Tabel
- hrDiskStorage Tabel
- Schaaldertabel

Aanvullende aanwijzers voor geheugen- en schijfgebruik

Gebruikt geheugen

Om het gebruikte geheugen te berekenen, gebruikt u:

mem_used = kb_main_total - kb_main_free - kb_main_cached - kb_main_buffers;

kb_main_cached = kb_page_cache + kb_slab_reclaimable;

Vrij geheugen

Er is een klein verschil tussen de waarden die worden verzameld in de SNMP-server en de ISE CLI root-bash. Het gebruik van het geheugen heeft ook een verschil in de waarden toe te schrijven aan plak, die niet in SNMP wordt rekenschap gegeven, en het toont de totale waarde.

Gratis geheugen is een kleine hoeveelheid geheugen die momenteel niet wordt gebruikt en dit verschil veroorzaakt. Dit is het verloren deel van het geheugen dat het systeem niet kan gebruiken. ISE wordt gehost op een Linux OS en gebruikt alle fysiek geheugen dat niet nodig is voor de huidige programma's als een bestandscache, voor efficiëntie. Als programma's dit fysieke geheugen echter nodig hebben, zal de kernel het cachegeheugen van het bestand opnieuw toewijzen aan de eerste. Het geheugen dat wordt gebruikt door de bestandscache is gratis maar niet gebruikt totdat het nodig is voor een programma.

Raadpleeg deze link:

Gratis geheugenuitleg.

Schijfgebruik

Op dezelfde manier is maximaal 5% van het bestandssysteem gereserveerd voor de root gebruiker om de fragmentatie van bestanden te verminderen. Deze output wordt niet weergegeven in 'df'.

Daarom wordt verwacht dat er een klein verschil is in het percentage berekend in de wortelbasis en vervolgens in de CLI-output.

SNMP-query houdt geen rekening met deze gereserveerde schijfruimte en berekent de uitvoer op basis van de waarden die in de tabel worden weergegeven.

Raadpleeg voor meer informatie het verschil in PDF-uitvoer en de gereserveerde schijfruimte voor PDF-uitvoer.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.