Configurazione e comprensione delle trap SNMP per il monitoraggio di Cisco ISE

Sommario

Introduzione

Questo documento descrive come configurare e comprendere le trap Simple Network Management Protocol (SNMP) per monitorare Cisco ISE.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ISE, release 3.1
- server RHEL 7

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Le trap SNMP sono messaggi UDP inviati da un dispositivo SNMP a un server MIB remoto. ISE può essere configurato per inviare trap a un server SNMP per il monitoraggio e la risoluzione dei problemi. Questo documento ha lo scopo di familiarizzare con alcuni controlli di base per isolare i problemi e comprendere i limiti delle trap ISE.

Configurazione

ISE supporta SNMP v1, v2 e v3. Verificare se SNMP è abilitato sulla CLI di ISE e sul resto della configurazione.

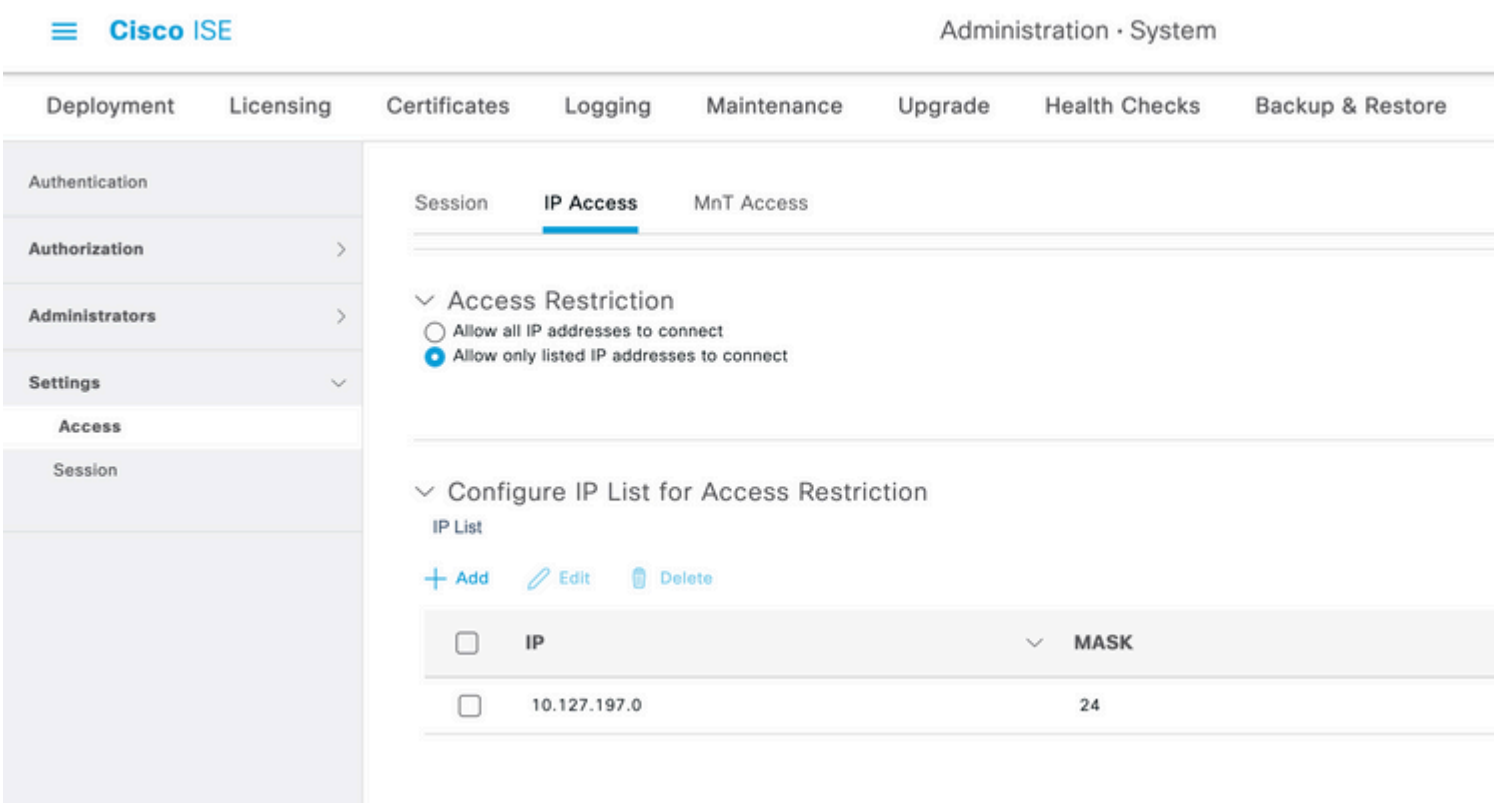
Ad esempio, SNMP v3:

<#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
```

Porte e accessibilità

Il server remoto deve essere in grado di raggiungere l'ISE per poter interrogare i trap, se necessario.
Verificare che ISE consenta al server SNMP di accedere tramite IP (se configurato).



Verificare se la porta 161 è aperta sulla CLI di 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
```

Log

Se il daemon del servizio SNMP è bloccato o non è possibile riavviarlo, gli errori vengono visualizzati nel file di log dei messaggi.

```
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=
```

Trap e query

Trap SNMP generiche generate per impostazione predefinita 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::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

ISE non dispone di MIB per lo stato del processo o l'utilizzo del disco. Cisco ISE utilizza OID HOST-RESOURCES-MIB::hrSWRunName per i trap SNMP. snmp walk o snmp get per verificare lo stato del processo o l'utilizzo del disco, non può essere usato in ISE.

Fonte: Guida dell'amministratore

In laboratorio, SNMP Trap è stato impostato per attivarsi quando l'utilizzo del disco supera il limite di soglia 75: sotumu24/admin(config)# snmp-server trap dskThresholdLimit "75".

I dati per questa trap vengono raccolti dagli output mostrati.

Eseguire i seguenti comandi su una casella LINUX esterna o su una console del server 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
```

Da questi output, viene calcolato l'utilizzo del disco e, quando il valore raggiunge 75, viene inviata una trap SNMP all'HOST del server SNMP configurato. Non è disponibile alcuna risorsa MIB per calcolare e visualizzare direttamente l'utilizzo del disco.

Inoltre, il processo MIB hrSWRunName viene utilizzato per raccogliere queste informazioni (come indicato nella ISE Admin Guide).

Descrizione testuale del software in esecuzione, che include il produttore, la revisione e il nome con cui è comunemente noto. Se il software è stato installato localmente, deve essere la stessa stringa utilizzata nel hrSWInstalledName che corrisponde. I servizi presi in considerazione sono app-server, rsyslog, redis-server, ad-connector, mnt-collector , mnt-processor , ca-server est-server ,e elasticsearch.

Risorse MIB

L'applicazione ISE è ospitata su RHEL OS(Linux). Tuttavia, come accennato nella guida per l'amministratore ISE, ISE utilizza il MIB delle risorse host per raccogliere le informazioni sulle trap SNMP. Questo documento contiene l'elenco dei MIB delle risorse host su cui è possibile eseguire una query:

MIB HOST SNMP.

Dal documento si può dedurre che non esistono query dirette in grado di calcolare e visualizzare i valori relativi all'utilizzo della CPU, della memoria o del disco. Tuttavia, i dati utilizzati per calcolare gli output

sono presenti nelle seguenti tabelle:

- hrSWRunPerf Tabella
- hrDiskStorage Tabella
- Tabella Scalari

Puntatori aggiuntivi per l'utilizzo della memoria e del disco

Memoria utilizzata

Per calcolare la memoria utilizzata, utilizzare:

mem_used = kb_main_total - kb_main_free - kb_main_cached - kb_main_buffers;

kb_main_cached = kb_page_cache + kb_slab_reclaimable;

Memoria disponibile

C'è una leggera differenza tra i valori raccolti nel server SNMP e i root-based di ISE CLI. L'utilizzo della memoria presenta inoltre una differenza nei valori dovuti alla memoria allocata, che non viene presa in considerazione nel protocollo SNMP, e mostra il valore totale.

La memoria libera è una piccola quantità di memoria attualmente non utilizzata e causa questa differenza. Questa è la parte di memoria sprecata che il sistema non è in grado di utilizzare. ISE è ospitata su un sistema operativo Linux e, per una maggiore efficienza, usa tutta la memoria fisica non necessaria ai programmi correnti come cache dei file. Tuttavia, se i programmi necessitano di questa memoria fisica, il kernel rialloca la memoria cache del file al primo. Pertanto, la memoria utilizzata dalla cache dei file è libera ma non utilizzata fino a quando non è richiesta da un programma.

Fare riferimento a questo collegamento:

Spiegazione memoria libera.

Utilizzo del disco

Analogamente, fino al 5% del file system è riservato all'utente root al fine di ridurre la frammentazione dei file. Questo output non è visibile in 'df'.

Pertanto, ci si aspetta di vedere una piccola differenza nella percentuale calcolata nella base principale e successivamente nell'output CLI.

La query SNMP non considera questo spazio riservato su disco e calcola l'output in base ai valori visualizzati nella tabella.

Per ulteriori informazioni, vedere Differenza nell'output df e spazio riservato su disco nell'output df.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).