SNMP-Traps zur Überwachung der Cisco ISE konfigurieren und verstehen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Simple Network Management Protocol (SNMP)-Traps zur Überwachung der Cisco ISE konfiguriert und verstanden werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in den folgenden Bereichen verfügen:

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

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco ISE Version 3.1
- RHEL 7 Server

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

SNMP-Traps sind UDP-Nachrichten, die von einem SNMP-fähigen Gerät an einen Remote-MIB-Server gesendet werden. Die ISE kann so konfiguriert werden, dass Traps an einen SNMP-Server gesendet werden, um diese zu überwachen und Fehler zu beheben. In diesem Dokument werden einige der grundlegenden Prüfungen erläutert, um Probleme zu isolieren und die Einschränkungen von ISE-Traps zu verstehen.

Konfiguration

ISE unterstützt SNMP v1, v2 und v3. Überprüfen Sie, ob SNMP für die ISE-CLI und den Rest der Konfiguration aktiviert ist.

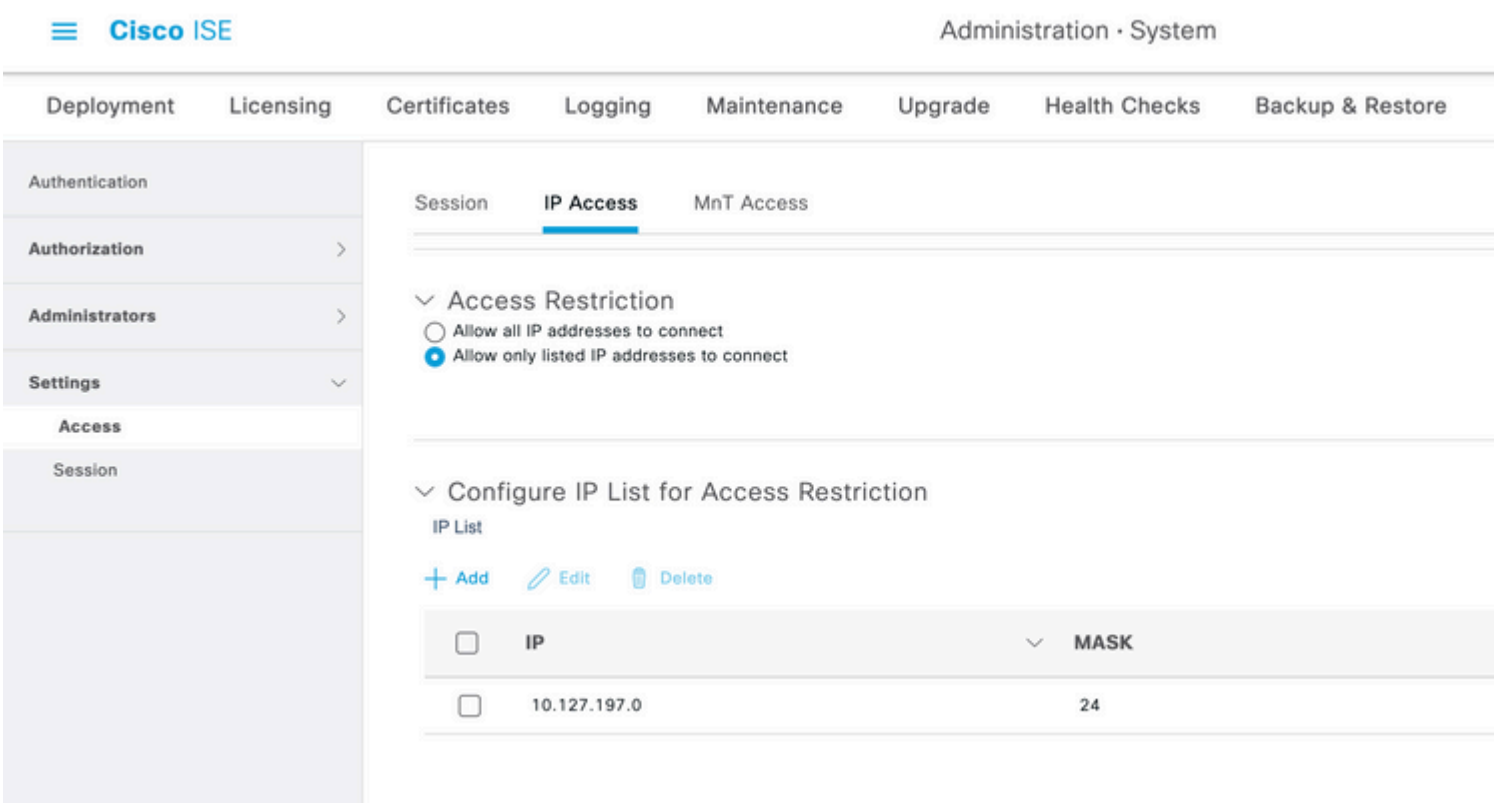
SNMP v3:

<#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 und Erreichbarkeit

Der Remote-Server muss in der Lage sein, die ISE zu erreichen, um bei Bedarf Traps abzufragen. Stellen Sie sicher, dass die ISE dem SNMP-Server den IP-Zugriff erlaubt (falls konfiguriert).



Überprüfen Sie, ob Port 161 in der ISE-CLI geöffnet ist:

```
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
```

Protokolle

Wenn der SNMP-Dienst-Daemon hängen bleibt oder nicht neu gestartet werden kann, werden die Fehler in der Nachrichtenprotokolldatei angezeigt.

```
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 und Abfragen

Generische SNMP-Traps, die standardmäßig in der Cisco ISE generiert werden:

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

Die ISE verfügt über keine MIB für den Prozessstatus oder die Festplattennutzung. Einsatz der Cisco ISE OID HOST-RESOURCES-MIB::hrSWRunName für SNMP-Traps. snmp walk Oder snmp get kann in ISE nicht verwendet werden, um den Prozessstatus oder die Festplattennutzung abzufragen.

Quelle: Administratorhandbuch

In der Übung wurde festgelegt, dass SNMP-Trap ausgelöst wird, wenn die Festplattennutzung den Schwellenwert 75 überschreitet: sotumu24/admin(config)# snmp-server trap dskThresholdLimit "75".

Die Daten für diese Trap werden aus den dargestellten Ausgängen gesammelt.

Führen Sie die folgenden Befehle in einem externen LINUX-System oder einer externen SNMP-Serverkonsole aus:

```
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
```

Anhand dieser Ausgaben wird die Festplattenauslastung berechnet. Wenn der Wert 75 erreicht, wird ein SNMP-Trap an den konfigurierten SNMP-Server-HOST gesendet. Es gibt keine MIB-Ressource, um die Festplattenauslastung direkt zu berechnen und anzuzeigen.

Darüber hinaus wird der MIB-Prozess hrSWRunName wird zum Sammeln dieser Informationen verwendet (gemäß ISE-Administratorhandbuch).

Eine Textbeschreibung dieser laufenden Software, die den Hersteller, die Revision und den Namen enthält, unter dem sie allgemein bekannt ist. Wenn diese Software lokal installiert wurde, muss es sich um dieselbe Zeichenfolge handeln wie in der hrSWInstalledName entspricht. Die in Betracht gezogenen Leistungen sind: app-server, rsyslog, redis-server, ad-connector, mnt-collector , mnt-processor , ca-server est-server und elasticsearch.

MIB-Ressourcen

Die ISE-Anwendung wird auf RHEL OS (Linux) gehostet. Wie jedoch im ISE-Administrationsleitfaden erwähnt, verwendet die ISE zur Erfassung von SNMP-Trap-Informationen die Host Resources MIB. Dieses Dokument enthält eine Liste der Host-Ressourcen-MIBs, die abgefragt werden können:

SNMP-HOST-MIB.

Aus dem Dokument kann abgeleitet werden, dass es keine direkten Abfragen gibt, die die Werte der CPU-, Arbeitsspeicher- oder Festplattenauslastung berechnen und anzeigen können. Die Daten, die zur Berechnung

der Outputs verwendet werden, sind jedoch in den folgenden Tabellen enthalten:

- hrSWRunPerf Tabelle
- hrDiskStorage Tabelle
- Tabelle Scalars

Zusätzliche Zeiger zur Arbeitsspeicher- und Festplattenauslastung

Verwendeter Arbeitsspeicher

Um den verwendeten Speicher zu berechnen, verwenden Sie:

mem_used = kb_main_total - kb_main_free - kb_main_cached - kb_main_buffers;

kb_main_cached = kb_page_cache + kb_slab_reclaimable;

Freier Speicher

Es besteht ein geringfügiger Unterschied zwischen den im SNMP-Server erfassten Werten und dem ISE CLI-Root-Bash. Die Speichernutzung unterscheidet sich ebenfalls durch die Slab-Werte, die im SNMP nicht berücksichtigt werden, und zeigt den Gesamtwert an.

Freier Speicher ist eine kleine Speichermenge, die derzeit nicht verwendet wird und verursacht diesen Unterschied. Dies ist der vergeudete Teil des Speichers, den das System nicht nutzen kann. Die ISE wird auf einem Linux-Betriebssystem gehostet und verwendet den gesamten physischen Speicher, der von den aktuellen Programmen nicht benötigt wird, aus Effizienzgründen als Datei-Cache. Wenn Programme jedoch diesen physischen Speicher benötigen, ordnet der Kernel den Dateicachespeicher dem ersten neu zu. Daher ist der Speicher, der vom Dateicache verwendet wird, frei, aber nicht ausgelastet, bis er von einem Programm benötigt wird.

Weitere Informationen finden Sie unter diesem Link:

Freie Gedächtniserklärung.

Festplattenauslastung

Ebenso sind bis zu 5 % des Dateisystems für den Root-Benutzer reserviert, um die Dateifragmentierung zu reduzieren. Diese Ausgabe wird in 'df' nicht angezeigt.

Daher wird eine geringe Differenz zwischen dem berechneten Prozentsatz im Root-Bash und der anschließenden CLI-Ausgabe erwartet.

Die SNMP-Abfrage berücksichtigt diesen reservierten Speicherplatz nicht und berechnet die Ausgabe auf Grundlage der in der Tabelle angezeigten Werte.

Weitere Informationen finden Sie unter Unterschiede in der df-Ausgabe und reservierter Speicherplatz auf der df-Ausgabe.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.