Configurer et comprendre les déroutements SNMP pour surveiller Cisco ISE

Table des matières

Introduction

Ce document décrit comment configurer et comprendre les déroutements SNMP (Simple Network Management Protocol) afin de surveiller Cisco ISE.

Conditions préalables

Exigences

Cisco vous recommande d'avoir connaissance des sujets suivants :

- Linux de base
- SNMP
- Identity Services Engine (ISE)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco ISE, version 3.1
- Serveur RHEL 7

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre lâ€™incidence possible des commandes.

Informations générales

Les déroutements SNMP sont des messages UDP envoyés par un périphérique SNMP à un serveur MIB distant. ISE peut être configuré pour envoyer des déroutements à un serveur SNMP afin de surveiller et de dépanner. Ce document vise à familiariser certains contrôles de base pour isoler les problèmes et comprendre les limites des pièges ISE.

Configuration

ISE prend en charge SNMP v1, v2 et v3. Vérifiez si SNMP est activé sur l'interface de ligne de commande ISE et le reste de la configuration.

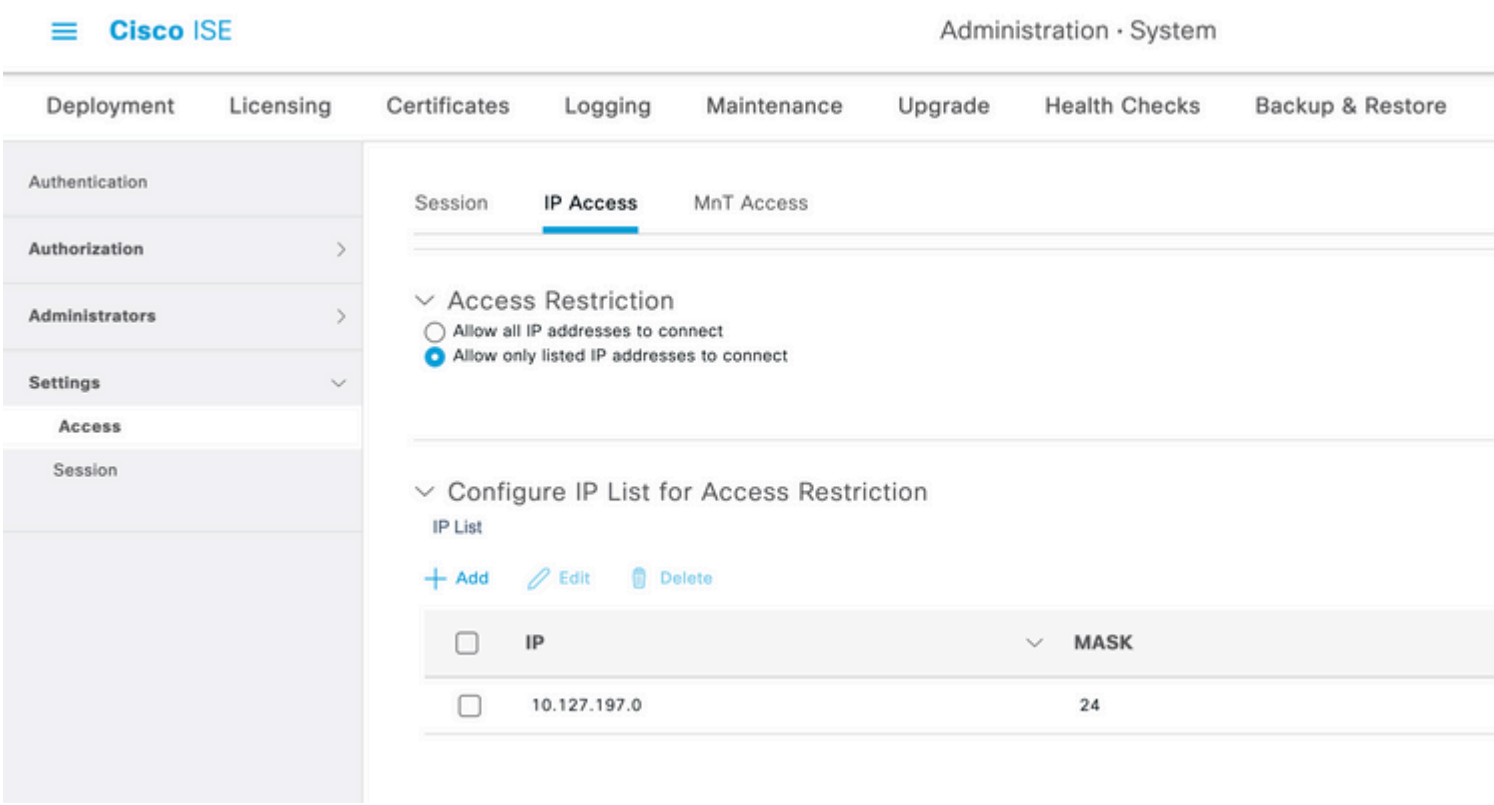
Par exemple, SNMP v3 :

<#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 et accessibilité

Le serveur distant doit être en mesure d'atteindre l'ISE afin d'interroger les déroutements si nécessaire. Assurez-vous qu'ISE autorise le serveur SNMP en accès IP (si configuré).



Vérifiez si le port 161 est ouvert sur l'interface de ligne de commande 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
```

Journaux

Si le démon du service SNMP est bloqué ou ne peut pas redémarrer, les erreurs sont visibles dans le fichier journal des messages.

```
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=
```

Interruptions et requêtes

Déroutements SNMP génériques générés par défaut dans 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 ne dispose pas de MIB pour l'état des processus ou l'utilisation des disques. Cisco ISE utilise OID HOST-RESOURCES-MIB::hrSWRunName pour les déroutements SNMP. snmp walk ou snmp get afin d'interroger l'état du processus ou l'utilisation du disque, ne peut pas être utilisée dans ISE.

Source : Guide d'administration

Au cours des travaux pratiques, le déroutement SNMP a été défini pour se déclencher lorsque l'utilisation du disque dépasse la limite de seuil 75 : sotumu24/admin(config)# snmp-server trap dskThresholdLimit "75".

Les données de ce déroutement sont collectées à partir des résultats affichés.

Exécutez ces commandes sur un boîtier LINUX externe ou une console de serveur 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
```

À partir de ces résultats, l'utilisation du disque est calculée et lorsque la valeur atteint 75, un déroutement SNMP est envoyé à l'hôte SNMP-Server configuré. Il n'existe aucune ressource MIB permettant de calculer et d'afficher directement l'utilisation du disque.

En outre, le processus MIB hrSWRunName est utilisé pour collecter ces informations (conformément au guide d'administration d'ISE).

Description textuelle de ce logiciel en cours d'exécution, qui inclut le fabricant, la révision et le nom sous lequel il est généralement connu. Si ce logiciel a été installé localement, il doit s'agir de la même chaîne que celle utilisée dans le hrSWInstalledName qui correspond. Les prestations prises en compte sont : app-server, rsyslog, redis-server, ad-connector, mnt-collector , mnt-processor , ca-server est-server ,et elasticsearch.

Ressources MIB

L'application ISE est hébergée sur le système d'exploitation RHEL (Linux). Cependant, comme indiqué dans le guide d'administration d'ISE, ISE utilise la base de données MIB Host Resources pour collecter des informations sur les déroutements SNMP. Ce document contient la liste des ressources hôtes MIB pouvant être interrogées :

MIB HÔTE SNMP.

D'après le document, il est possible de déduire qu'il n'existe aucune requête directe capable de calculer et

d'afficher les valeurs d'utilisation du processeur, de la mémoire ou du disque. Cependant, les données utilisées pour calculer les sorties sont présentes dans ces tableaux :

- hrSWRunPerf Tableau
- hrDiskStorage Tableau
- Tableau Scalars

Pointeurs supplémentaires sur l'utilisation de la mémoire et des disques

Mémoire utilisée

Afin de calculer la mémoire utilisée, utilisez :

mem_used = kb_main_total - kb_main_free - kb_main_cached - kb_main_buffers;

kb_main_cached = kb_page_cache + kb_slab_reclaimable;

Mémoire libre

Il existe une légère différence entre les valeurs collectées dans le serveur SNMP et le root-bash de l'interface de ligne de commande ISE. L'utilisation de la mémoire a également une différence dans les valeurs dues à la dalle, qui n'est pas prise en compte dans le SNMP, et elle montre la valeur totale.

La mémoire libre est une petite quantité de mémoire qui n'est pas utilisée actuellement et qui entraîne cette différence. Il s'agit de la partie gaspillée de la mémoire que le système ne peut pas utiliser. ISE est hébergé sur un système d'exploitation Linux et utilise toute la mémoire physique qui n'est pas nécessaire aux programmes actuels comme cache de fichiers, pour plus d'efficacité. Cependant, si les programmes ont besoin de cette mémoire physique, le noyau réalloue la mémoire cache du fichier à la première. Par conséquent, la mémoire utilisée par le cache de fichiers est libre mais inutilisée jusqu'à ce qu'elle soit nécessaire à un programme.

Reportez-vous à ce lien :

Explication de la mémoire libre.

Utilisation du disque

De même, jusqu'à 5 % du système de fichiers est réservé à l'utilisateur racine afin de réduire la fragmentation des fichiers. Ce résultat n'apparaît pas dans 'df'.

Par conséquent, on s'attend à ce qu'il y ait une petite différence entre le pourcentage calculé dans le bash racine et le résultat de l'interface de ligne de commande.

La requête SNMP ne tient pas compte de cet espace disque réservé et calcule le résultat en fonction des valeurs affichées dans le tableau.

Pour plus d'informations, référez-vous à Différence dans la sortie df et l'espace disque réservé à la sortie df.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.