配置和瞭解SNMP陷阱以監控思科ISE

目錄

簡介

本文檔介紹如何配置和理解簡單網路管理協議(SNMP)陷阱以監控思科ISE。

必要條件

需求

思科建議您瞭解以下主題：

- 基本Linux
- SNMP
- 身分識別服務引擎 (ISE)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ISE版本3.1
- RHEL 7伺服器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

SNMP陷阱是從啟用了SNMP的裝置傳送到遠端MIB伺服器的UDP消息。 可以將ISE配置為向SNMP伺服器傳送陷阱，以便進行監控和故障排除。本文檔旨在熟悉一些基本檢查以隔離問題並瞭解ISE陷阱的侷限性。

組態

ISE支援SNMP v1、v2和v3。檢查ISE CLI及其餘配置上是否啟用了SNMP。

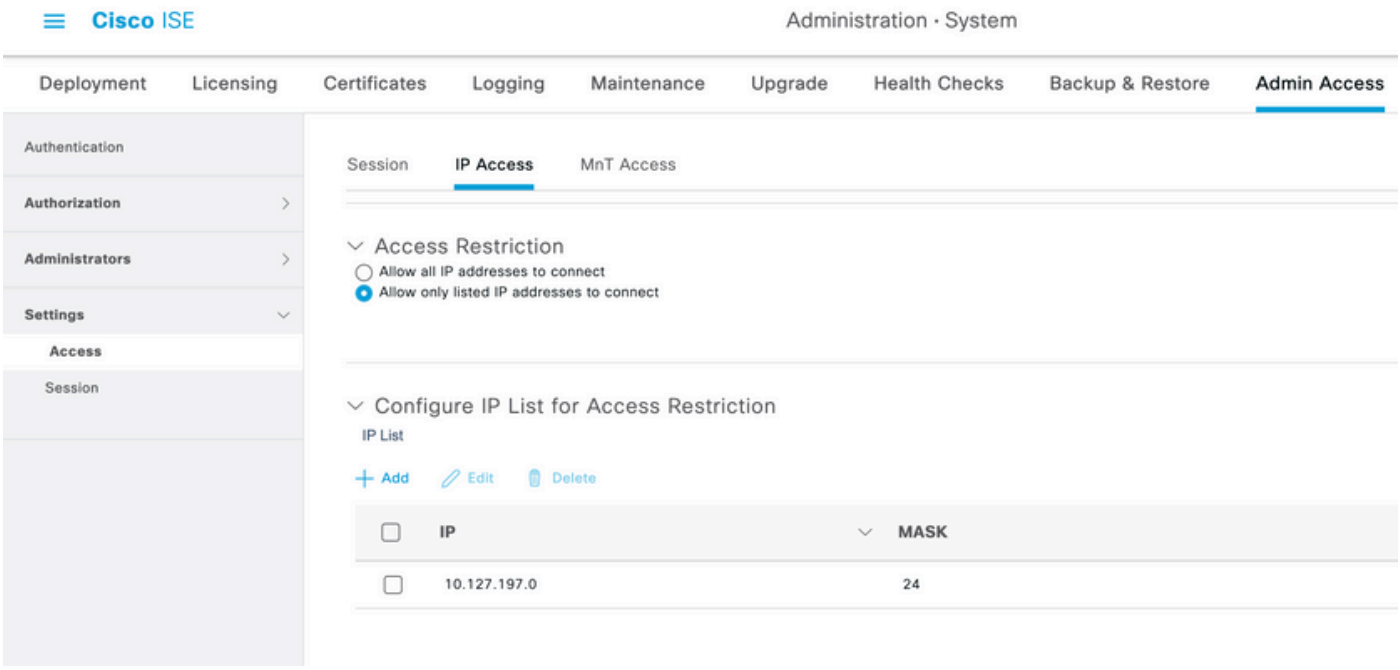
例如，SNMP v3:

<#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 plai


>> 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
```

埠和可達性

如果需要，遠端伺服器必須能夠訪問ISE才能查詢陷阱。確保ISE允許SNMP伺服器進行IP訪問（如果已配置）。



檢查ISE CLI上的埠161是否開啟：

```
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
```

記錄檔

如果SNMP服務守護程式停滯或無法重新啟動，將在消息日誌檔案中看到這些錯誤。

```
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
```

陷阱和查詢

思科ISE中預設生成的通用SNMP陷阱：

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::sysUpTimeInstance = Timeticks: (478) 0:00:04.78 SNMPv2-MIB::snmpTrapOID.0 = OID: NET-SNMP-AGENT-MIB::nsNotifyRestart SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpNotificationPrefix
.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::sysUpTimeInstance = Timeticks: (479) 0:00:04.79 SNMPv2-MIB::snmpTrapOID.0 = OID: NET-SNMP-AGENT-MIB::nsNotifyShutdown SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpNotificationPrefix
.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::sysUpTimeInstance = Timeticks: (478) 0:00:04.78 SNMPv2-MIB::snmpTrapOID.0 = OID: IF-MIB::linkUp IF-MIB::ifIndex.12 = INTEGER: 12 IF-MIB::ifAdminStatus.12 = INTEGER: up(1) IF-MIB::ifOperStatus.12 = INTEGER: up(1) SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
.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::sysUpTimeInstance = Timeticks: (479) 0:00:04.79 SNMPv2-MIB::snmpTrapOID.0 = OID: IF-MIB::linkDown IF-MIB::ifIndex.5 = INTEGER: 5 IF-MIB::ifAdminStatus.5 = INTEGER: up(1) IF-MIB::ifOperStatus.5 = INTEGER: down(2) SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
.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::sysUpTimeInstance = Timeticks: (8) 0:00:00.08 SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-MIB::coldStart SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10

ISE沒有任何MIB用於進程狀態或磁碟利用率。Cisco ISE使用 OID HOST-RESOURCES-MIB::hrSWRunName SNMP陷阱。 snmp walk 或 snmp get 命令不能在ISE中使用，以便查詢進程狀態或磁碟利用率。

來源：管理指南

在實驗中，SNMP陷阱被設定為當磁碟利用率超過閾值限制75時觸發： sotumu24/admin(config)# snmp-server trap dskThresholdLimit "75".

此陷阱的資料是從圖中所示的輸出中收集的。

在外部LINUX機箱或SNMP伺服器控制檯上運行以下命令：

```
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/ae1cef55c92ba90ae6c848bd74c9277c2fb52
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
```

從這些輸出中，計算磁碟利用率，當值達到75時，會向配置的SNMP伺服器主機傳送SNMP陷阱。沒有MIB資源可以直接計算和顯示磁碟利用率。

此外，MIB流程 hrSWRunName 用於收集此資訊（根據ISE管理員指南）。

此運行軟體的文字說明，包括製造商、修訂版本和它通常使用的名稱。如果此軟體是在本地安裝的，則此字串必須與在 hrSWInstalledName 對應。所考慮之服務包括 app-server中， rsyslog中， redis-server中， ad-connector中， mnt-collector 中， mnt-processor 中， ca-server est-server ,和 elasticsearch.

MIB資源

ISE應用程式託管在RHEL OS(Linux)上。但是，如ISE管理指南所述，ISE使用主機資源MIB收集SNMP陷阱資訊。本文檔包含可查詢的主機資源MIB清單：

SNMP主機MIB。

從本文檔可以推斷，沒有直接查詢可以計算和顯示CPU、記憶體或磁碟利用率的值。但是，用於計算輸出的資料將顯示在以下表中：

- hrSWRunPerf 表
- hrDiskStorage 表
- Scalars表

記憶體和磁碟利用率的其他指標

已用記憶體

要計算已用記憶體，請使用：

mem_used = kb_main_total - kb_main_free - kb_main_cached - kb_main_buffers;

kb_main_cached = kb_page_cache + kb_slab_reclaimable;

可用記憶體

在SNMP伺服器和ISE CLI root-bash中收集的值之間存在細微差異。記憶體使用率也存在由於slab（未在SNMP中記入）而產生的值差異，它顯示總值。

可用記憶體是當前未使用的少量記憶體，會導致此差異。這是系統無法使用的記憶體的浪費部分。ISE託管在Linux作業系統上，使用當前程式不需要的全部實體記憶體作為檔案快取，以提高效率。但是，如果程式需要此實體記憶體，核心會將檔案快取記憶體重新分配給前者。因此，檔案快取記憶體使用的儲存器是空閒的，但是未使用，直到程式需要它為止。

請參閱以下連結：

可用記憶體說明。

磁碟利用率

同樣，為根使用者保留的檔案系統最多5%，以減少檔案碎片。'df'中未看到此輸出。

因此，在根bash中計算出的百分比以及隨後的CLI輸出中，預計會出現細微的差異。

SNMP查詢不考慮此保留的磁碟空間，而是根據表中顯示的值計算輸出。

如需詳細資訊，請參閱df輸出和df輸出保留磁盤空間中的差異。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。