Cisco ISEを監視するためのSNMPトラップの設定と理解

内容

はじめに

このドキュメントでは、Cisco ISEを監視するためにSimple Network Management Protocol(SNMP)トラップを設定し理解する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 基本的なLinux
- SNMP
- Identity Services Engine（ISE）

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ISE、リリース 3.1
- RHEL 7サーバ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

SNMPトラップは、SNMP対応デバイスからリモートMIBサーバに送信されるUDPメッセージで

す。 ISEは、監視とトラブルシューティングのためにSNMPサーバにトラップを送信するように設定できます。このドキュメントの目的は、問題を切り分けるための基本的なチェックの一部を理解し、ISEトラップの制限を理解することです。

コンフィギュレーション

ISEはSNMP v1、v2、およびv3をサポートします。ISE CLIおよび残りの設定でSNMPが有効になっているかどうかを確認します。

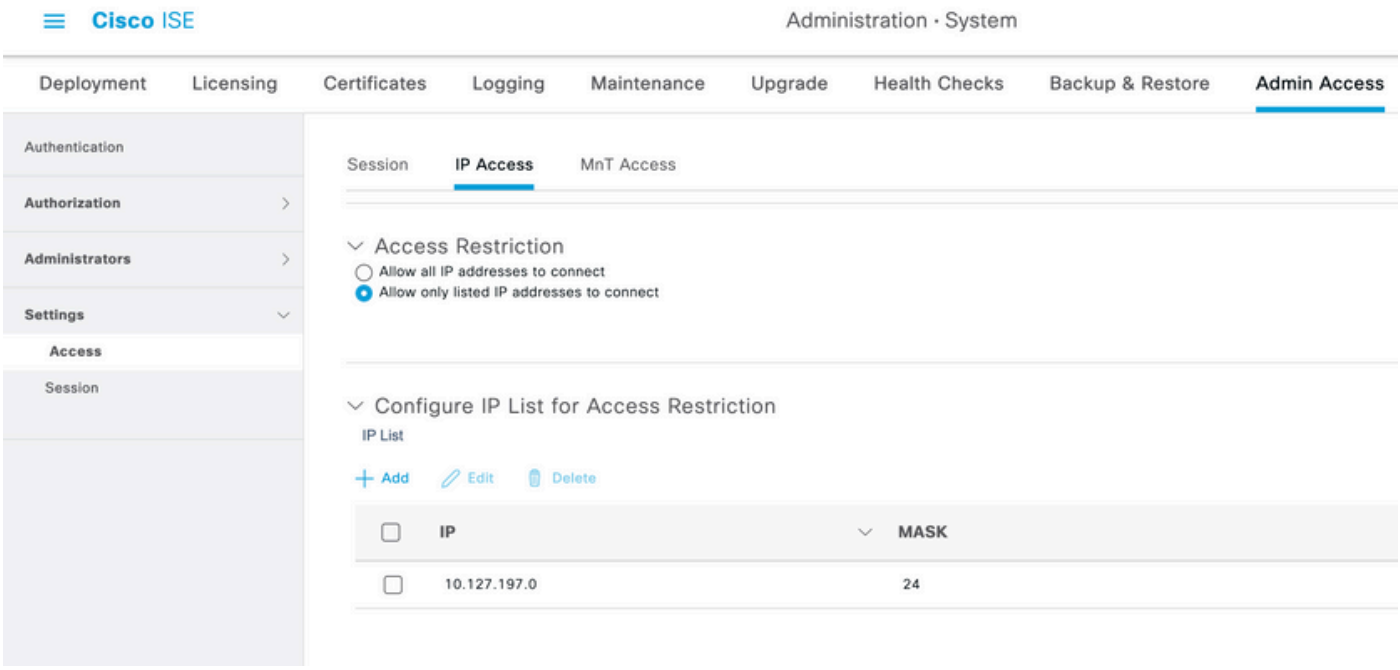
たとえば、SNMP v3:

<#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
```

ポートと到達可能性

リモートサーバは、必要に応じてトラップをクエリーするためにISEに到達できる必要があります。ISEがIPアクセスでSNMPサーバを許可することを確認します（設定されている場合）。



ISE CLIでポート161が開いているかどうかを確認します。

```
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
```

ログ

SNMPサービスデーモンが停止しているか、再起動できない場合、エラーはメッセージログファイルに記録されます。

```
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
```

トラップとクエリー

Cisco ISEでデフォルトで生成される汎用SNMPトラップ：

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には、プロセスのステータスやディスク使用率に関するMIBはありません。Cisco ISEは OID HOST-RESOURCES-MIB::hrSWRunName SNMPトラップ用。 snmp walk または snmp get コマンドは、プロセスのステータスやディスク使用率を照会するために、ISEでは使用できません。

出典：Admin Guide

ラボでは、SNMPトラップは、ディスク使用率がしきい値の制限である75を超えたときにトリガーされるように設定されています。 sotumu24/admin(config)# snmp-server trap dskThresholdLimit "75"を参照。

このトラップのデータは、示されている出力から収集されます。

外部のLINUXボックスまたはSNMPサーバコンソールで次のコマンドを実行します。

```
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
```

これらの出力からディスク使用率が計算され、値が75に達すると、SNMPトラップが設定されたSNMPサーバのホストに送信されます。ディスク使用率を直接計算して表示するためのMIBリソースはありません。

さらに、MIBプロセス hrSWRunName この情報の収集に使用されます（『ISE Admin Guide』を参照）。

この実行中のソフトウェアの説明。製造元、リビジョン、およびよく知られている名前が含まれます。このソフトウェアがローカルにインストールされている場合、この文字列は hrSWInstalledName 対応しています。考慮されるサービスは次のとおりです app-server、 rsyslog、 redis-server、 ad-connector、 mnt-collector 、 mnt-processor 、 ca-server est-server ,と elasticsearchを参照。

MIBリソース

ISEアプリケーションはRHEL OS(Linux)でホストされます。ただし、ISE管理ガイドで説明されているように、ISEはホストリソースMIBを使用してSNMPトラップ情報を収集します。このドキュメントでは、クエリー可能なHost Resources MIBのリストを示します。

SNMPホストMIB。

このドキュメントから、CPU、メモリ、またはディスク使用率の値を計算して表示できる直接的なクエリがないことが推測できます。ただし、出力の計算に使用されるデータは次のテーブルに存在します。

- hrSWRunPerf テーブル
- hrDiskStorage テーブル
- Scalarsテーブル

メモリおよびディスク使用率に関する追加ポインタ

使用メモリ

使用メモリを計算するには、次のコマンドを使用します。

mem_used = kb_main_total - kb_main_free - kb_main_cached - kb_main_buffers;

kb_main_cached = kb_page_cache + kb_slab_reclaimable;

Free Memory

SNMPサーバで収集される値とISE CLIのroot-bashで収集される値には、わずかな違いがあります。メモリ使用率は、SNMPでは考慮されていないslabによる値にも差があり、合計値を示します。

空きメモリは、現在使用されていない少量のメモリであり、この違いを引き起こします。これは、システムが使用できないメモリの無駄な部分です。 ISEはLinux OS上でホストされ、効率を高めるために、現在のプログラムで必要とされないすべての物理メモリをファイルキャッシュとして使用します。しかし、プログラムがこの物理メモリを必要とする場合、カーネルはファイルキャッシュメモリを前者に再割り当てします。したがって、ファイルキャッシュによって使用されるメモリは空いていますが、プログラムによって必要とされるまで使用されません。

次のリンクを参照してください。

空きメモリの説明。

ディスク使用率

同様に、ファイルの断片化を減らすために、ファイルシステムの最大5 %がルートユーザ用に予約されています。この出力は「df」には表示されません。

したがって、root bashで計算されたパーセンテージと、その後のCLI出力で計算されたパーセンテージの差は小さいことが予想されます。

SNMPクエリでは、この予約されたディスク領域は考慮されず、テーブルに表示された値に基づいて出力が計算されます。

詳細については、「df出力の違い」と「df出力の予約済みディスクスペース」を参照してください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。