Cisco ISE를 모니터링 할 SNMP 트랩 구성 및 이해

목차

소개

이 문서에서는 Cisco ISE를 모니터링 하기 위해 SNMP (Simple Network Management Protocol) 트랩을 구성 하고 이해 하는 방법에 대해 설명 합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대해 알고 있는 것이 좋습니다.

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

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISE, 릴리스 3.1
- RHEL 7 서버

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

SNMP 트랩은 SNMP 지원 디바이스에서 원격 MIB 서버로 전송되는 UDP 메시지입니다. ISE는 모니터링 및 문제 해결을 위해 SNMP 서버로 트랩을 전송하도록 구성할 수 있습니다. 이 문서에서는

문제를 격리하고 ISE 트랩의 한계를 파악하기 위한 몇 가지 기본 검사를 숙지합니다.

설정

ISE는 SNMP v1, v2 및 v3을 지원합니다. SNMP가 ISE CLI에서 활성화되었는지 확인하고 나머지 컨피그레이션도 확인합니다.

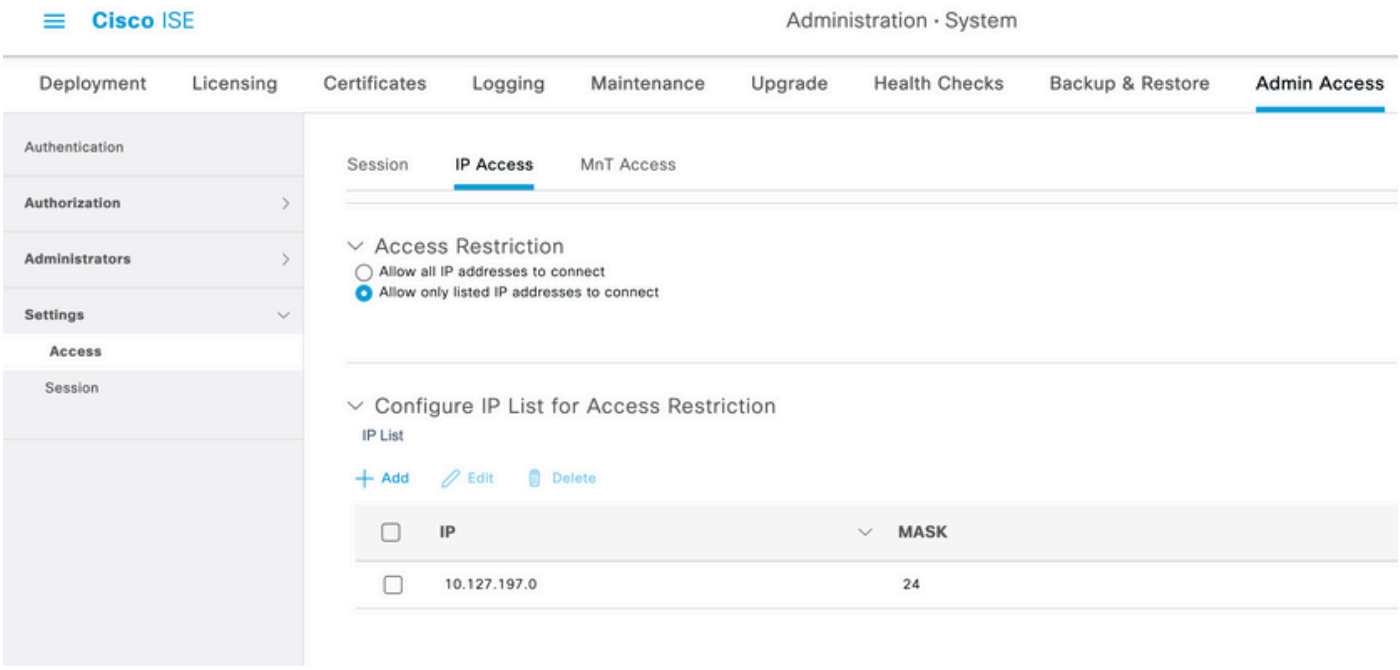
예를 들어, SNMP v3:

<#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
```

포트 및 연결 가능성

필요한 경우 트랩을 쿼리하려면 원격 서버가 ISE에 연결할 수 있어야 합니다. ISE가 IP 액세스에서 SNMP 서버를 허용하는지 확인합니다(구성된 경우).



ISE CLI에서 포트 161이 열려 있는지 확인합니다.

```
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
```

로그

SNMP 서비스 데몬이 중단되었거나 재시작할 수 없는 경우 메시지 로그 파일에 오류가 표시됩니다.

```
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
```

트랩 및 쿼리

Cisco ISE에서 기본적으로 생성되는 일반 SNMP 트랩:

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

ISE에는 프로세스 상태 또는 디스크 사용률에 대한 MIB가 없습니다. Cisco ISE는 OID HOST-RESOURCES-MIB::hrSWRunName SNMP 트랩. snmp walk 또는 snmp get 프로세스 상태 또는 디스크 사용률을 쿼리하기 위해 명령을 ISE에서 사용할 수 없습니다.

출처: Admin Guide

Lab에서 SNMP 트랩은 디스크 사용률이 임계값 제한(75)을 초과할 때 트리거되도록 설정되었습니다. sotumu24/admin(config)# snmp-server trap dskThresholdLimit "75".

이 트랩의 데이터는 표시된 출력에서 수집됩니다.

외부 LINUX 상자 또는 SNMP 서버 콘솔에서 다음 명령을 실행합니다.

```
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
```

이러한 출력에서 디스크 사용률이 계산되고 값이 75에 도달하면 SNMP 트랩이 구성된 SNMP-Server HOST로 전송됩니다. 디스크 사용률을 직접 계산하고 표시하기 위한 MIB 리소스가 없습니다.

또한 MIB 프로세스는 hrSWRunName 이 정보를 수집하는 데 사용됩니다(ISE 관리 가이드에 따름).

이 실행 중인 소프트웨어에 대한 텍스트 설명으로, 제조업체, 개정판 및 일반적으로 알려진 이름을 포함합니다. 이 소프트웨어가 로컬로 설치된 경우 이 문자열은 hrSWInstalledName 그렇습니다. 고려되는 서비스는 다음과 같습니다 app-server, rsyslog, redis-server, ad-connector, mnt-collector , mnt-processor , ca-server est-server 및 elasticsearch.

MIB 리소스

ISE 애플리케이션은 RHEL OS(Linux)에서 호스팅됩니다. 그러나 ISE 관리 설명서에 설명된 대로 ISE는 호스트 리소스 MIB를 사용하여 SNMP 트랩 정보를 수집합니다. 이 문서에는 쿼리할 수 있는 호스트 리소스 MIB 목록이 있습니다.

SNMP 호스트 MIB.

이 문서에서는 CPU, 메모리 또는 디스크 사용률 값을 계산하고 표시할 수 있는 직접 쿼리가 없음을 유추할 수 있습니다. 그러나 출력을 계산하는 데 사용되는 데이터는 다음 테이블에 있습니다.

- hrSWRunPerf 표
- hrDiskStorage 표
- Scalars 테이블

메모리 및 디스크 사용률에 대한 추가 포인터

사용된 메모리

사용된 메모리를 계산하려면 다음을 사용합니다.

mem_used = kb_main_total - kb_main_free - kb_main_cached - kb_main_buffers;

kb_main_cached = kb_page_cache + kb_slab_reclaimable;

사용 가능한 메모리

SNMP 서버와 ISE CLI 루트 기반에서 수집된 값 사이에는 약간의 차이가 있습니다. 메모리 사용률도 SNMP에서 설명되지 않는 슬래브로 인해 값의 차이가 있으며 총 값을 보여 줍니다.

여유 메모리는 현재 사용되지 않는 소량의 메모리이며 이러한 차이를 유발합니다. 시스템에서 사용할 수 없는 메모리의 낭비된 부분입니다. ISE는 Linux OS에서 호스팅되며 효율성을 위해 현재 프로그램에서 필요하지 않은 모든 물리적 메모리를 파일 캐시로 사용합니다. 그러나 프로그램에서 이 물리적 메모리가 필요한 경우 커널은 파일 캐시 메모리를 전자에 재할당합니다. 따라서 파일 캐시에서 사용하는 메모리는 사용 가능하지만 프로그램에서 필요할 때까지 사용되지 않습니다.

다음 링크를 참조하십시오.

여유 메모리 설명.

디스크 사용률

마찬가지로 파일 시스템의 최대 5%는 파일 조각화를 줄이기 위해 루트 사용자를 위해 예약됩니다. 이 출력은 'df'에 표시되지 않습니다.

따라서 루트 베이스와 CLI 출력에서 계산된 백분율에서 작은 차이가 나타날 것으로 예상됩니다.

SNMP 쿼리는 이 예약된 디스크 공간을 고려하지 않으며 테이블에 표시된 값을 기반으로 출력을 계산합니다.

자세한 내용은 Difference in df output and df output reserved disk space를 참조하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.