Cisco ACI 패브릭에서 SNMP 문제 해결

소개

이 문서에서는 Cisco ACI for ACI 릴리스 5.x 이상에서 SNMP를 구성, 확인 및 트러블슈팅하는 방법에 대해 설명합니다. SNMP 정책 모델, 필수 관리 계약, 트랩 컨피그레이션, CLI 및 MO(Managed Object) 쿼리를 사용한 운영 확인, 리프/스파인 스위치와 APIC 컨트롤러에서 가장 일반적인 장애 시나리오에 대한 구조화된 문제 해결 워크플로를 다룹니다.

배경 정보

이 문서의 자료는 ACI의 Cisco ACI Solutions Delivery Team 내부 기술 SNMP에서 발췌한 것입니다. Cisco APIC System Management Configuration Guide(릴리스 5.x) 및 Cisco ACI MIB Quick Reference Guide를 통해 Tomas de Leon이 작성한 개요, 컨피그레이션, 문제 해결 및 주의/문제.

개요

ACI의 SNMP 아키텍처

SNMP(Simple Network Management Protocol)는 네트워크 관리 및 모니터링을 제어하는 UDP 기반 프로토콜입니다. ACI에서 SNMP는 관리되는 각 엔티티에서 독립적으로 작동합니다. 모든 리프 스위치, 스파인 스위치 및 APIC 컨트롤러는 자체 SNMP 에이전트입니다. 각각 독립적으로 폴링하거나 모니터링해야 합니다.

ACI는 다음 SNMP 기능을 지원합니다.

- 읽기 작업(Get, GetNext, BulkGet, Walk) - 리프/스파인 스위치 및 APIC 컨트롤러에서 지원됩니다.
- 알림(트랩) - 리프/스파인 스위치 및 APIC 컨트롤러에서 지원되는 SNMPv1, v2c 및 v3 트랩.
- SNMPv3 — 리프/스파인 스위치 및 APIC 컨트롤러에서 지원됩니다.
- 쓰기 작업(설정) — ACI 디바이스에서 지원되지 않습니다.
- IPv6 — SNMP는 IPv4를 통해서만 지원됩니다.

참고: APIC 클러스터에서 각 APIC는 자신에게 로컬인 MIB 개체를 제공합니다. 각 APIC에 개별적으로 폴링해야 합니다. 클러스터 전반의 SNMP 어그리게이션이 없습니다. 마찬가지로 각

✎ leaf 및 spine 스위치는 독립적으로 쿼리해야 합니다.

APIC의 SNMPD 아키텍처

APIC에서 snmpd 프로세스를 실행하며, 여기에는 두 가지 내부 구성 요소가 있습니다.

- 에이전트 — SNMP 프로토콜 처리 및 세션 관리를 처리하는 오픈 소스 net-snmp 에이전트(버전 5.7.6 이상)입니다.
- DME(Data Model Engine) - APIC MIT(Management Information Tree)와의 인터페이스를 통해 MO(Managed Object)를 읽고 MO 특성을 SNMP Object 형식으로 변환합니다. SNMP 트랩은 MO에서 발생한 이벤트 및 fault에서 생성됩니다.

SNMP 정책 모델 및 구축 체인

ACI는 SNMP에 정책 기반 모델을 사용합니다. SNMP 컨피그레이션은 snmpPol 관리 객체로 추상화되며, 어떤 노드에도 구축되기 전에 패브릭의 포드 정책 그룹과 연결되어야 합니다. 전체 구축 체인은 다음과 같습니다.

1. SNMP 정책(`snmpPol`) — 관리 상태, 커뮤니티 문자열, 클라이언트 그룹 정책(ACL) 및 SNMPv3 사용자를 정의합니다.
2. Pod Policy Group — 다른 포드 레벨 정책(BGP, ISIS, NTP 등)과 함께 SNMP 정책을 참조합니다.
3. 포드 프로파일 선택기 — 패브릭 포드에 포드 정책 그룹을 적용합니다.

또한 SNMP 트랩 컨피그레이션에는 다음이 필요합니다.

1. SNMP 모니터링 대상 그룹(`snmpGroup`) — 트랩 대상 호스트, 포트, SNMP 버전 및 커뮤니티를 정의합니다.
2. Monitoring Sources(`snmpSrc`) — 대상 그룹을 세 개의 고유한 모니터링 정책 범위에 연결합니다. Fabric Default(패브릭 기본값), Fabric Common Policy(패브릭 공통 정책), Access Policy Default(액세스 정책 기본값)입니다.

APIC 노드에는 UDP 포트 161(SNMP 요청) 및 UDP 포트 162(SNMP 트랩)를 허용하는 관리 계약이 필요합니다. 리프 및 스파인 노드에는 올바른 iptables 규칙이 필요합니다. 이 규칙은 클라이언트 그룹 정책이 구성될 때 자동으로 프로그래밍됩니다.

지원되는 MIB

APIC에서 지원되는 MIB는 다음과 같습니다.

- 엔티티 MIB — PhysicalTable
- Cisco Entity Ext MIB — PhysicalProcessorTable, LEDTable
- Cisco Entity FRU Control MIB — PowerSupplyGroupTable, PowerStatusTable, FanTrayStatusTable, PhysicalTable
- Cisco Entity Sensor MIB - SensorValueTable, SensorThresholdTable
- Cisco Process MIB — CPUTotalTable, ProcessTable, ProcessExtRevTable, ThreadTable

리프 및 스파인 스위치는 IF-MIB, IP-MIB, CISCO-CDP-MIB, CISCO-ENTITY-QFP-MIB 및 전체 CISCO-ENTITY-FRU-CONTROL-MIB 제품군을 비롯한 표준 NX-OS MIB를 표시합니다.

APIC에서 생성되는 SNMP 트랩은 다음과 같습니다. `cefcFRUInserted`, `cefcFURemoved`, `cefcFanTrayStatusChange`, `cefcModuleStatusChange`, `entSensorThresholdNotification`, `cefcPowerStatusChange`, `cpmCPURisingThreshold`, `cpmCPUFallingThreshold`.

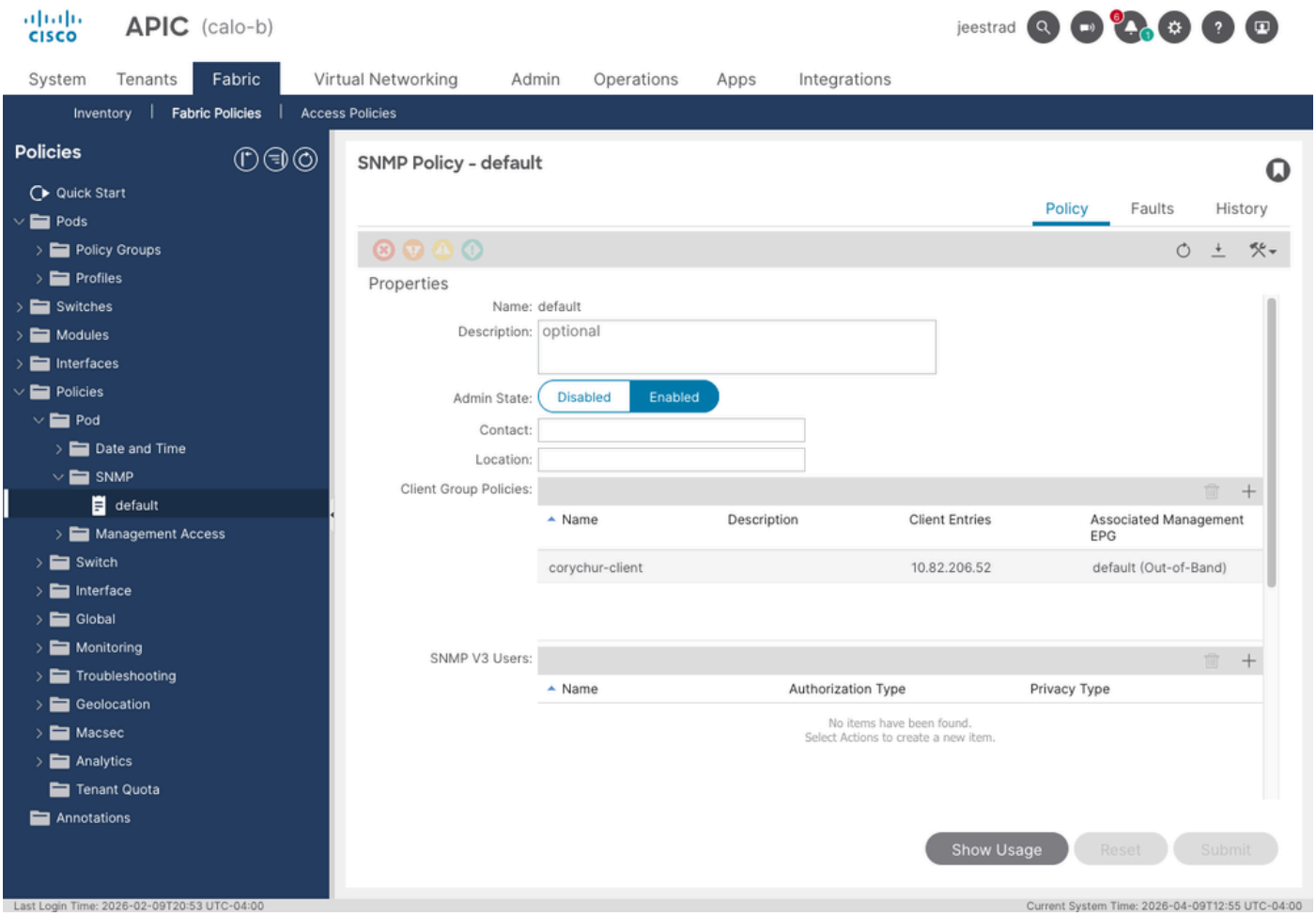
ACI에서 SNMP 구성

참고: 이 섹션에서는 컨피그레이션 워크플로의 요약을 다음에 나오는 확인 및 문제 해결 섹션에 대한 컨텍스트로 제공합니다. 포괄적인 컨피그레이션 절차는 Cisco APIC System Management 컨피그레이션 가이드를 참조하십시오.

1단계: SNMP 정책 구성

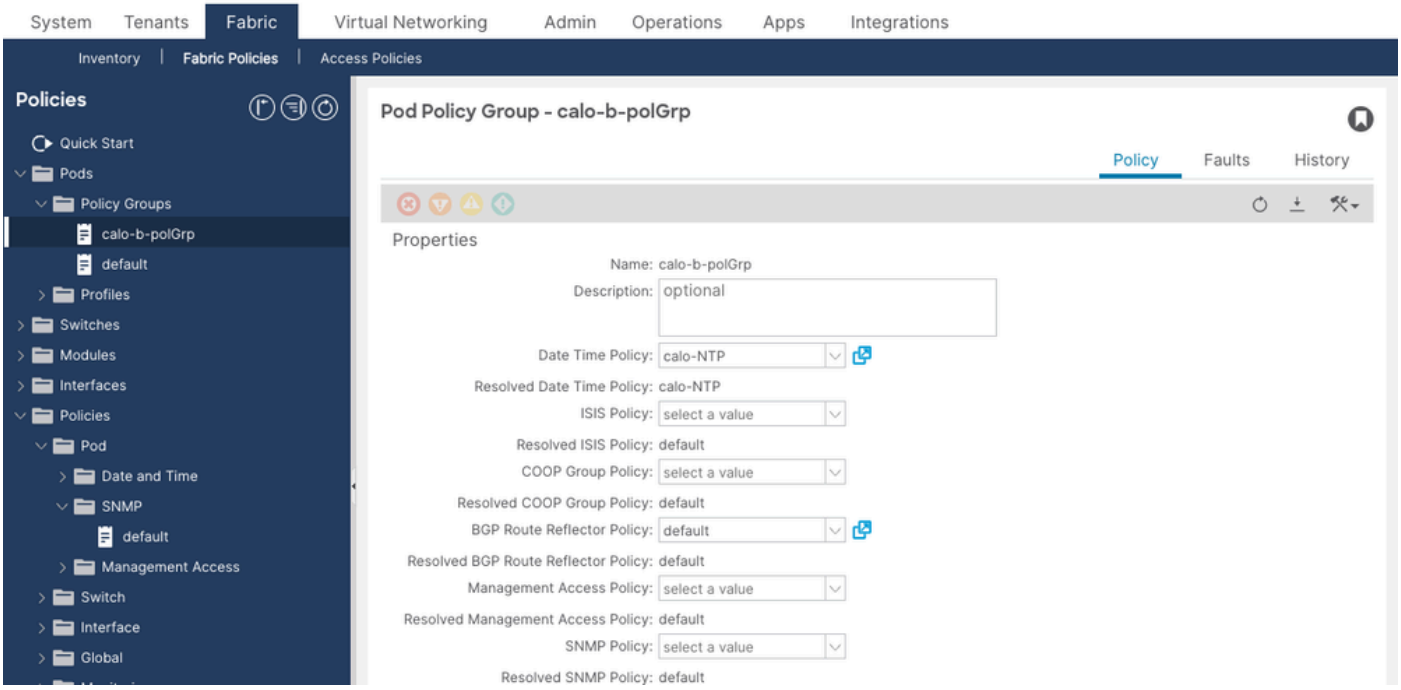
Fabric(패브릭) > Fabric Policies(패브릭 정책) > Policies(정책) > Pod(포드) > SNMP로 이동합니다. 일반적으로 default로 명명된 SNMP 정책을 선택하거나 생성합니다. 구성:

- Admin State — Enabled로 설정합니다.
- 커뮤니티 정책 — NMS에서 사용하는 커뮤니티 문자열을 추가합니다.
- 클라이언트 그룹 정책 — 하나 이상의 클라이언트 그룹 프로필을 정의하며, 각각 허용되는 SNMP 클라이언트 IP 및 관련 관리 EPG(Out-of-Band 또는 In-Band)를 지정합니다.
- SNMPv3 사용자 — SNMPv3을 사용하는 경우 여기에 인증 및 프라이버시 매개변수와 함께 사용자를 추가합니다.



2단계: SNMP 정책을 포드 정책 그룹과 연결

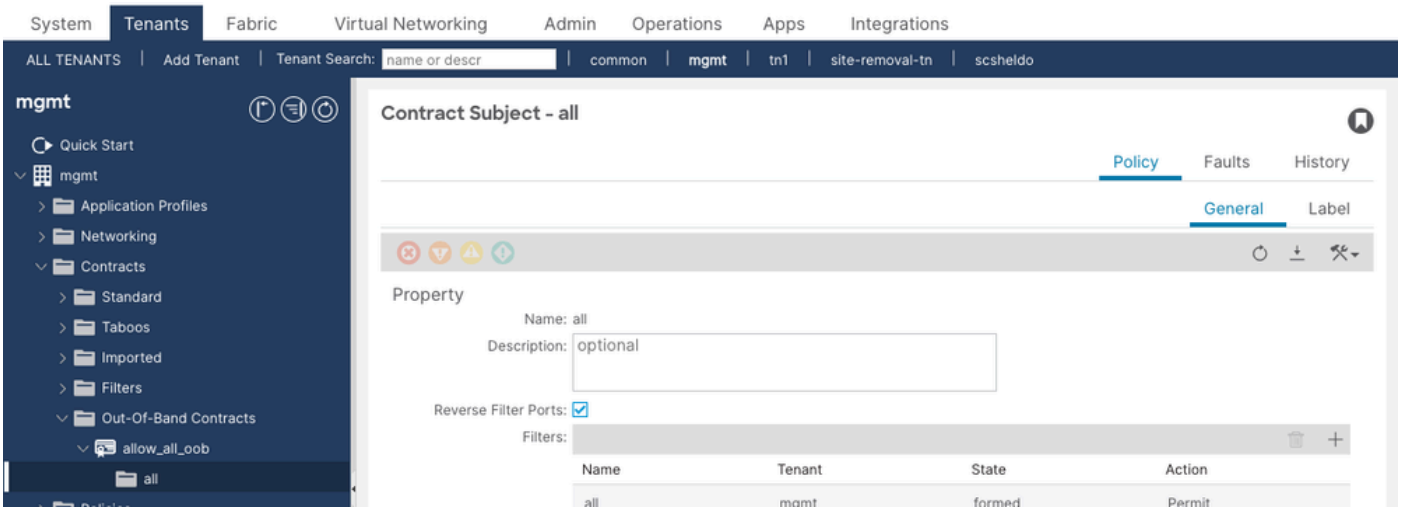
Fabric(패브릭) > Fabric Policies(패브릭 정책) > Pods(포드) > Policy Groups(정책 그룹)로 이동합니다. 활성 포드 정책 그룹(일반적으로 default로 지정됨)을 선택합니다. 1단계에서 생성한 SNMP 정책을 가리키도록 SNMP Policy(SNMP 정책) 필드를 설정합니다. Resolved SNMP Policy(확인된 SNMP 정책) 필드에 올바른 정책 이름이 표시되는지 확인합니다.



그런 다음 Fabric(패브릭) > Fabric Policies(패브릭 정책) > Pods(포드) > Profiles(프로파일)로 이동하고 기본 포드 프로파일을 확장하며 활성 선택기가 올바른 포드 정책 그룹을 참조하는지 확인합니다.

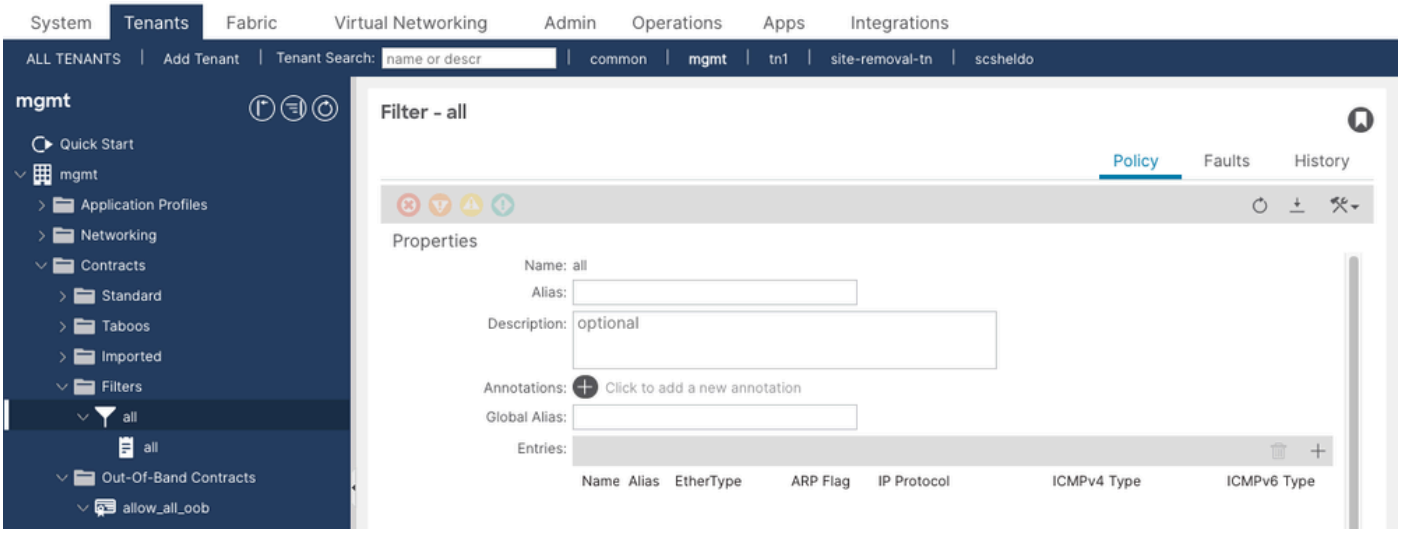
3단계: UDP 포트 161에 대한 관리 계약 구성

Tenants(테넌트) > mgmt(관리) > Contracts(계약) > Out-Of-Band Contracts(대역 외 계약)로 이동합니다. 활성 OOB 계약의 Subject(주체)가 UDP 포트 161(SNMP 요청)을 허용하는 필터 항목을 참조하는지 확인합니다. APIC에서 이 계약이 없으면 모든 SNMP GET/WALK 패킷이 자동으로 삭제됩니다.



계약 주체에 연결된 필터 항목은 EtherType IP, 프로토콜 UDP 및 목적지 포트 161이 포함된 항목을 포함해야 합니다. 위의 예는 모두 허용(지정되지 않은 프로토콜) 필터를 보여줍니다. 이 필터는

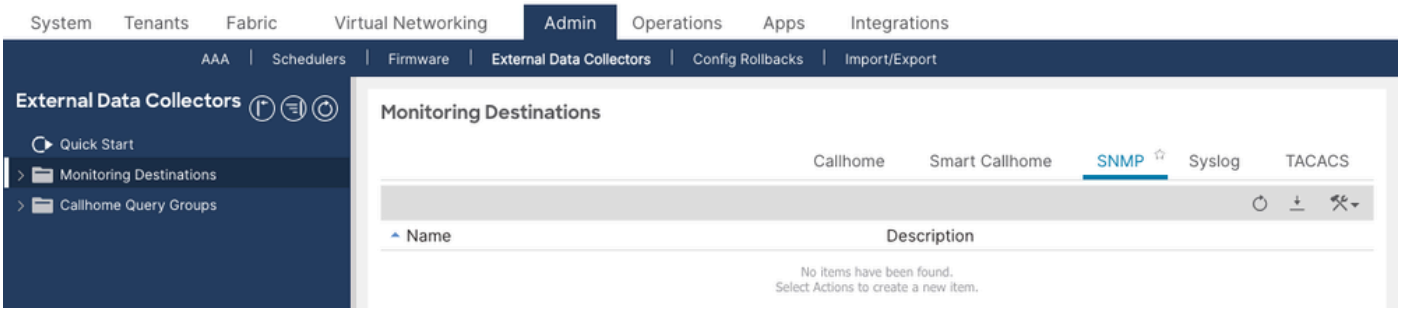
SNMP를 허용하지만 생산에 권장되는 것보다 광범위합니다. 특정 UDP/161 및 UDP/162 항목이 있는 전용 SNMP 필터 항목이 선호됩니다.



참고: 이전 ACI 펌웨어 버전에서는 특정 포트가 리프 및 스파인 노드에서 항상 열려 있었고 SNMP에 관리 계약이 필요하지 않았습니다. ACI 5.x에서는 APIC 노드에 대한 계약이 필요합니다. 리프 및 스파인 노드는 관리 계약이 아닌 클라이언트 그룹 정책에서 파생된 iptable 규칙을 사용합니다.

4단계: SNMP 트랩 대상 구성

Admin(관리) > External Data Collectors(외부 데이터 수집기) > Monitoring Destinations(모니터링 대상) > SNMP로 이동합니다. 마우스 오른쪽 버튼을 클릭하고 Create SNMP Monitoring Destination Group(SNMP 모니터링 대상 그룹 생성)을 선택합니다. SNMP 탭에는 구성된 모든 대상 그룹이 표시됩니다. 테이블이 비어 있으면 트랩 대상이 아직 구성되지 않았음을 의미합니다.



정의:

- 그룹 이름
- 트랩 대상: 호스트 이름/IP, UDP 포트(기본값 162), SNMP 버전, 커뮤니티 문자열, 관리 EPG

5단계: 모니터링 소스 구성

모니터링 소스는 SNMP 대상 그룹을 어떤 이벤트와 결함이 트랩을 생성할지를 제어하는 모니터링 정책에 연결합니다. 다음 세 위치 모두에서 모니터링 소스를 구성해야 합니다. 그렇지 않으면 일부 노드 유형의 트랩이 전송되지 않습니다.

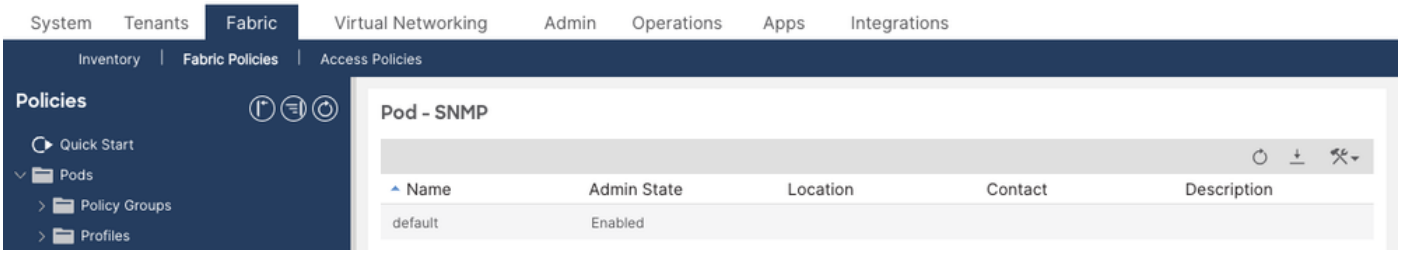
- Fabric(패브릭) > Fabric Policies(패브릭 정책) > Policies(정책) > Monitoring(모니터링) > default(기본값) > Callhome/Smart Callhome/SNMP/Syslog/TACACS(패브릭 인프라 이벤트 포함)
- Fabric(패브릭) > Fabric Policies(패브릭 정책) > Policies(정책) > Monitoring(모니터링) > Common Policy(공통 정책) > Callhome/Smart Callhome/SNMP/Syslog/TACACS(Callhome/Smart Callhome/SNMP/Syslog/TACACS)(패브릭 전반의 공통 이벤트 포함)
- Fabric(패브릭) > Access Policies(액세스 정책) > Policies(정책) > Monitoring(모니터링) > default(기본값) > Callhome/Smart Callhome/SNMP/Syslog(액세스/인프라 이벤트 포함)

각 위치에서 소스 유형으로 SNMP를 선택하고 4단계에서 생성한 대상 그룹을 참조하는 새 SNMP 소스를 생성합니다.

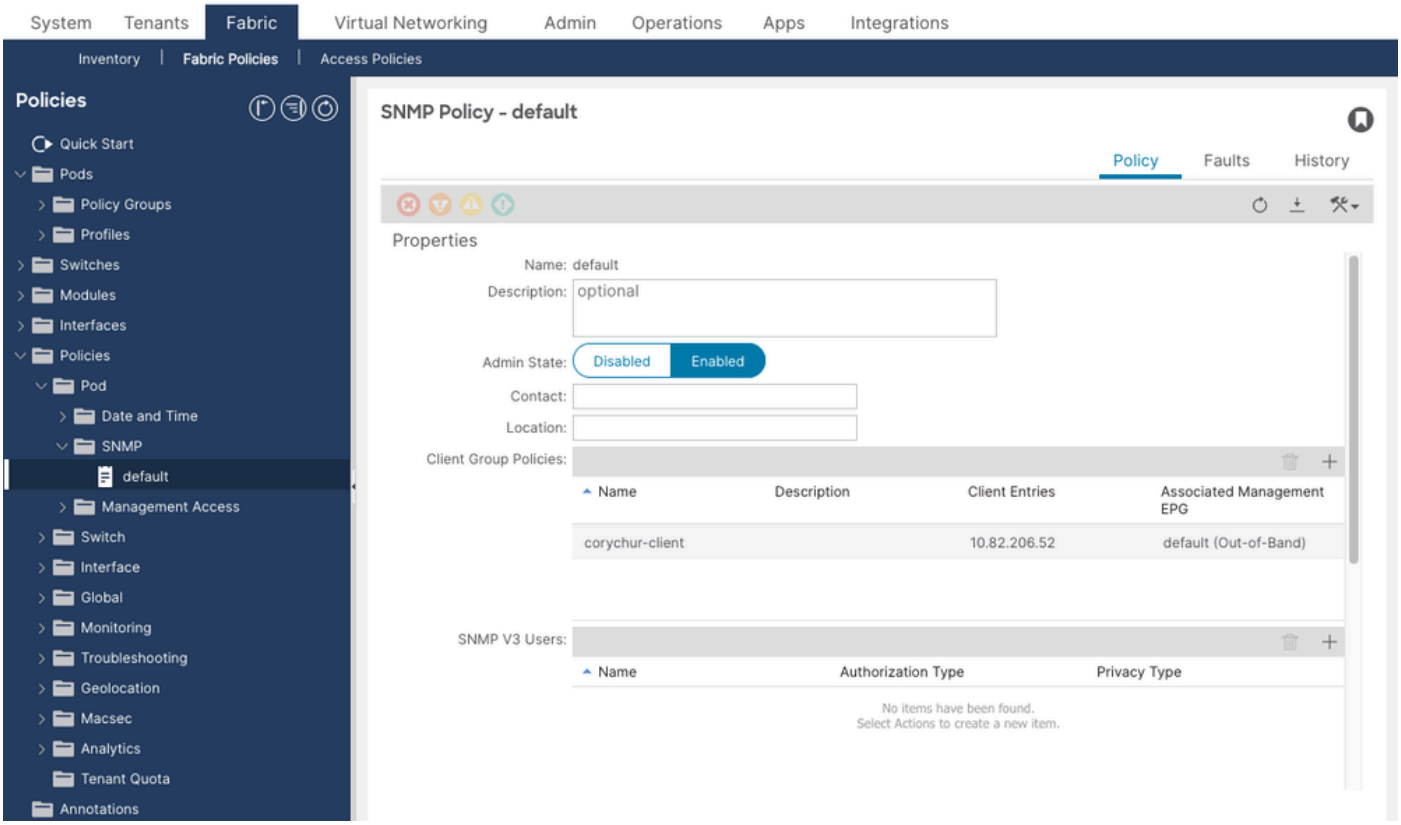
컨피그레이션 확인

SNMP 정책 구축 확인

Fabric(패브릭) > Fabric Policies(패브릭 정책) > Policies(정책) > Pod(포드) > SNMP로 이동하고 기본 SNMP 정책이 있으며 Admin State(관리 상태)가 Enabled(활성화됨)로 설정되었는지 확인합니다. Policy Groups(정책 그룹) 목록에는 관리자 상태와 함께 구성된 모든 SNMP 정책이 한 눈에 표시됩니다.



자세한 확인을 위해 정책 이름을 클릭하여 엽니다. Admin State(관리 상태) 토글이 Enabled(활성화됨)로 설정되어 있고, Client Group Policies(클라이언트 그룹 정책)에서 허용되는 모든 NMS 호스트를 관련 관리 EPG와 함께 나열하는지 확인합니다.



모든 APIC에서 다음 MO 쿼리를 실행하여 SNMP 정책이 패브릭에 있고 활성화되어 있는지 확인합니다.

<#root>

```
apic1#

moquery -c snmpPol

Total Objects shown: 1

# snmp.Pol
name          : default
adminSt       : enabled                    <--- must be "enabled"
contact       : NOC Team
descr         : ACI Fabric SNMP Policy
dn            : uni/fabric/snmppol-default
loc           : DC1 ACI Fabric
monPolDn      : uni/fabric/monfab-default
```

adminSt가 비활성화된 경우 SNMP는 어떤 노드에서도 작동하지 않습니다. APIC GUI의 Fabric(패브릭) > Fabric Policies(패브릭 정책) > Policies(정책) > Pod(포드) > SNMP > default(기본값)에서 활성화합니다.

커뮤니티 문자열 구성 확인

<#root>

apic1#

moquery -c snmpCommunityP

Total Objects shown: 1

```
# snmp.CommunityP
name         : public                      <--- confirm this matches your NMS community string
dn           : uni/fabric/snmppol-default/community-public
descr        : SNMP Community String
```

반환된 커뮤니티가 없거나 이름이 NMS에서 사용 중인 것과 일치하지 않는 경우 SNMP 정책에서 커뮤니티 문자열을 추가하거나 수정합니다.

클라이언트 그룹 정책 확인(SNMP 액세스 제어)

클라이언트 그룹 정책은 SNMP GET/WALK 액세스를 위한 ACL로 작동합니다. 각 정책은 관리 VRF를 통해 리프/스파인 노드를 폴링할 수 있는 클라이언트 IP 주소를 지정합니다. 리프/스파인 노드에서 이러한 정책은 iptables 규칙으로 변환됩니다.

<#root>

apic1#

moquery -c snmpClientGrpP -x query-target=children

Total Objects shown: 3

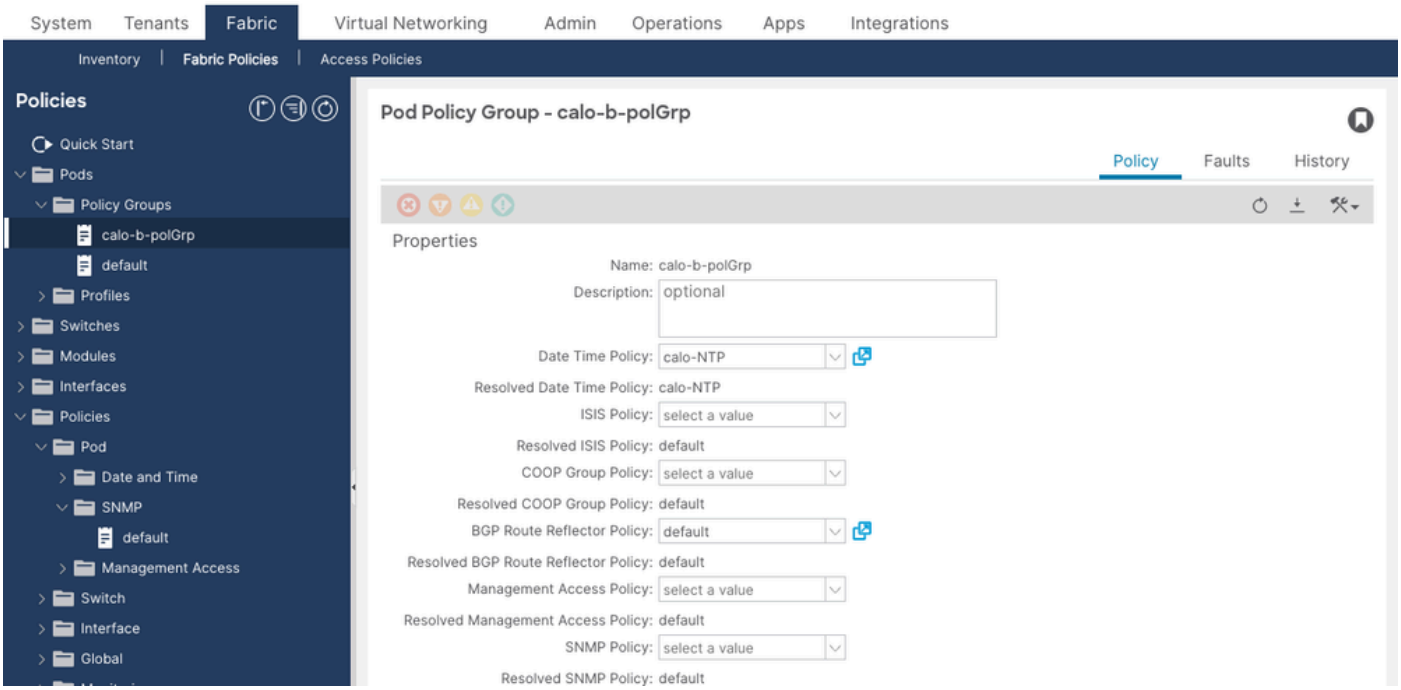
```
# snmp.ClientP
addr         : 10.1.1.50                   <--- NMS server IP
dn           : uni/fabric/snmppol-default/clgrp-NMS-Clients/client-[10.1.1.50]
name         : nms-server1

# snmp.ClientP
addr         : 10.1.1.51
dn           : uni/fabric/snmppol-default/clgrp-NMS-Clients/client-[10.1.1.51]
name         : nms-server2

# snmp.ClientGrpP
name         : NMS-Clients
dn           : uni/fabric/snmppol-default/clgrp-NMS-Clients
```

NMS 서버 IP가 클라이언트 항목에 있는지 확인합니다. 클라이언트 IP가 없는 경우 해당 호스트의 SNMP GET/WALK 요청은 리프/스파인 노드에서 iptable에 의해 삭제됩니다.

참고: SNMPv3 주의 — 클라이언트 그룹 정책은 SNMPv3을 사용할 때 APIC에 적용되지 않습니다. 클라이언트 그룹 컨피그레이션과 상관없이 APIC에 대한 모든 SNMPv3 GET/WALK가 허용됩니다. APIC의 SNMPv3에 대한 클라이언트 그룹 시행은 알려진 제한 사항입니다. 리프 및 스파인 스위치에서 클라이언트 그룹 시행은 SNMPv2c 및 SNMPv3 모두에 대해 동일하게 작동합니다.

Pod 정책 그룹이 SNMP 정책을 참조하는지 확인

Fabric(패브릭) > Fabric Policies(패브릭 정책) > Pods(포드) > Policy Groups(정책 그룹)로 이동하고 활성 포드 정책 그룹을 엽니다. SNMP Policy(SNMP 정책) 드롭다운 필드가 원하는 SNMP 정책으로 설정되어 있고 Resolved SNMP Policy(확인된 SNMP 정책) 필드에 동일한 이름이 표시되는지 확인합니다. 누락되거나 해결되지 않은 정책은 SNMP 컨피그레이션이 스위치에 푸시되지 않음을 의미합니다.



위의 스크린샷에서 SNMP Policy(SNMP 정책) 필드는 "select a value(값 선택)"(비어 있음)를 표시하고 Resolved SNMP Policy(확인된 SNMP 정책)는 "default(기본값)"를 표시합니다. 즉, 정책이 패브릭 기본값에서 상속되지만 명시적으로 설정되지 않음을 의미합니다. 모호성을 방지하려면 SNMP Policy 필드를 명시적으로 설정하는 것이 좋습니다.

REST API를 통해 확인:

<#root>

apic1#

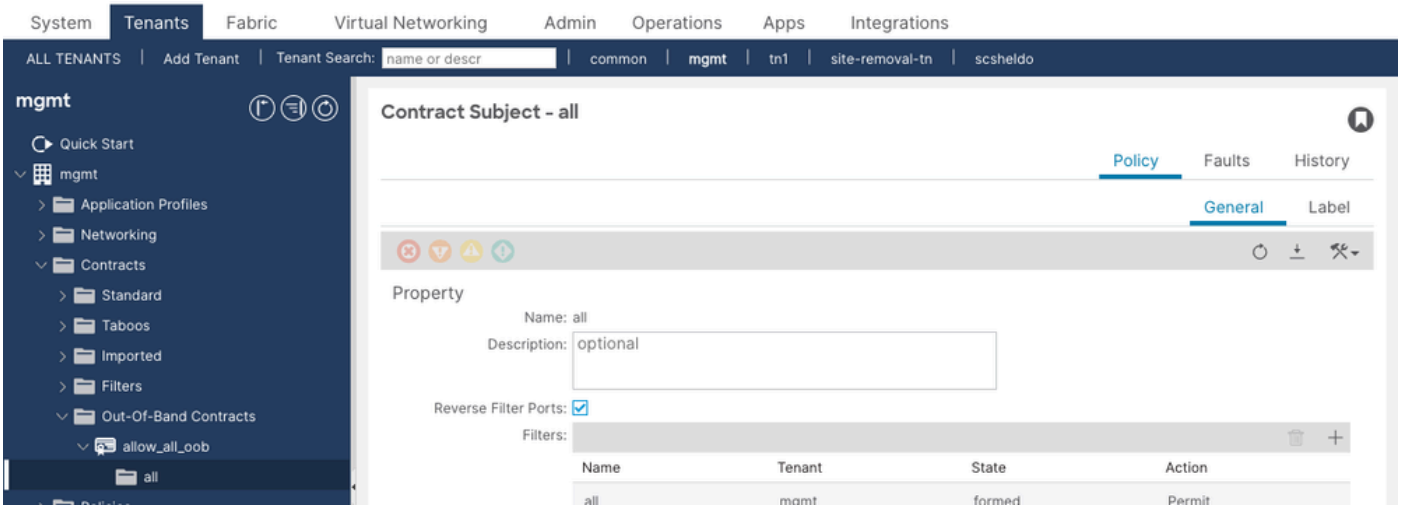
moquery -c fabricPodPGrp -x rsp-subtree=full

```
# fabric.PodPGrp
name          : default
dn            : uni/fabric/funcprof/podpgrp-default

  # fabric.RsSnmpPol
  tnSnmpPolName : default                  <--- must reference the SNMP policy
  state         : formed                   <--- must be "formed"
```

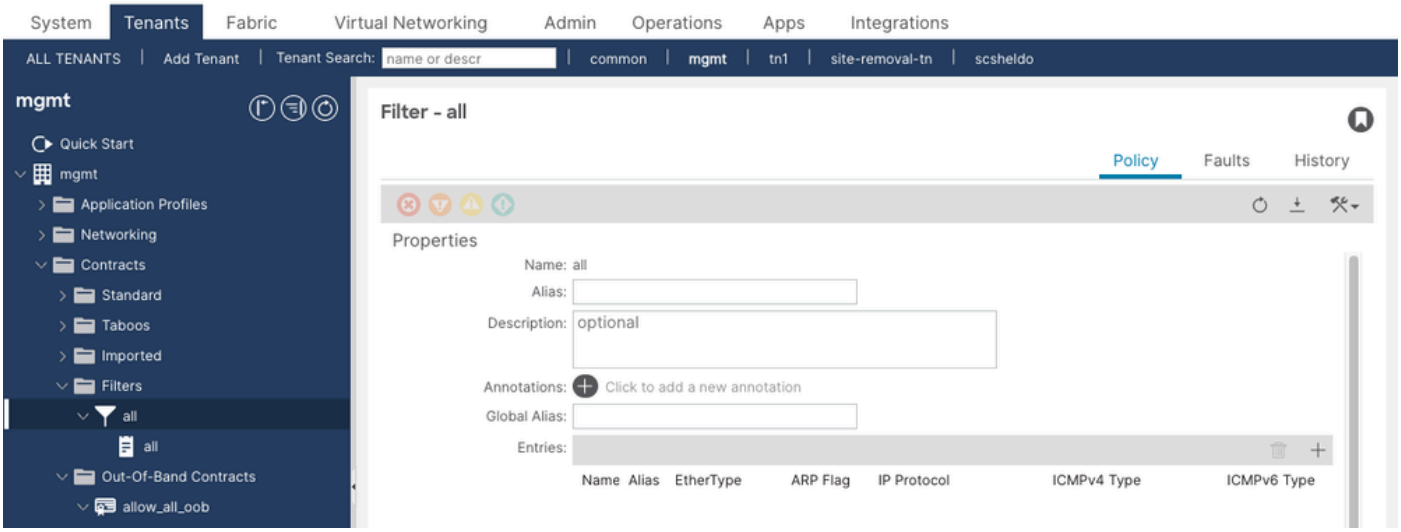
상태가 구성되지 않은 경우 SNMP 정책 관계가 끊어집니다. Pod Policy Group(포드 정책 그룹)에서 SNMP 정책을 다시 선택하고 전송합니다.

UDP 161(APIC 노드)에 대한 관리 계약 확인

Tenants(테넌트) > mgmt(관리) > Contracts(계약) > Out-Of-Band Contracts(대역 외 계약)(INB 관리를 사용하는 경우 In-Band Contracts)로 이동합니다. 활성 OOB 계약을 열고 Policy(정책) 탭을 클릭합니다. Subject가 UDP 포트 161을 허용하는 필터를 참조하는지 확인합니다.



주제가 참조하는 필터를 확장하고 해당 항목에 EtherType IP, Protocol UDP, Destination Port 161의 항목이 포함되어 있는지 확인합니다. 필터 항목은 APIC에 대한 OOB 관리 계약을 통해 허용되는 트래픽을 결정합니다.



필터는 다음과 같이 표시되어야 합니다.

- 이더 타입: IP
- IP 프로토콜: UDP
- 대상 포트: 161
- 대상 포트: 161

또한 APIC에서 OOB 인터페이스를 통해 SNMP 트랩을 아웃바운드로 보내도록 하려면 UDP 포트 162가 허용되는지 확인합니다.

MO 쿼리를 통해 확인:

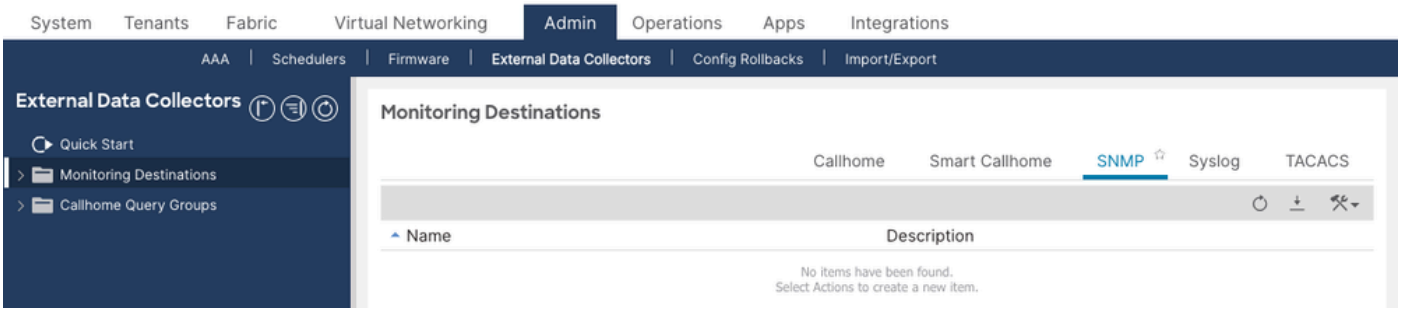
<#root>

```
apic1#

moquery -c vzEntry -x query-target-filter='and(eq(vzEntry.dFromPort,"161"),eq(vzEntry.prot,"17"))'

Total Objects shown: 2

# vz.Entry
name         : snmp-get
dn           : uni/tn-mgmt/flt-snmp-filter/e-snmp-get
dFromPort    : 161                          <--- destination port 161
dToPort      : 161
prot         : 17                           <--- UDP
stateful     : no
```

결과가 반환되지 않으면 UDP 161에 대한 필터가 없습니다. 관리 계약에 하나를 추가합니다.

SNMP 트랩 대상 컨피그레이션 확인

Admin(관리) > External Data Collectors(외부 데이터 수집기) > Monitoring Destinations(모니터링 대상) > SNMP로 이동하여 구성된 모든 SNMP 대상 그룹을 확인합니다. 목록이 비어 있으면 트랩 대상이 구성되지 않고 어떤 노드에서도 트랩이 전송되지 않습니다.



<#root>

```
apic1#

moquery -c snmpTrapDest

Total Objects shown: 1

# snmp.TrapDest
host         : 10.1.1.50                  <--- NMS trap receiver IP
port         : 162                         <--- trap UDP port
ver          : v2c                         <--- SNMP version
secName      : public                      <--- community string (v2c) or username (v3)
v3SecLvl     : noauth
notifT       : traps
vrfName      : mgmt:inb                    <--- VRF used to reach the trap receiver
epgDn        : uni/tn-mgmt/mgmtp-default/inb-default
dn           : uni/fabric/snmpgroup-NMS-DestGrp/trapdest-10.1.1.50-port-162
```

트랩 대상 IP, 포트, 버전, 커뮤니티 문자열 및 관리 VRF(`mgmt:inb` 또는 OOB를 위한 관리)가 사용자 환경과 일치하는지 확인합니다. VRF는 대상에 할당된 관리 EPG와 일치해야 합니다.

모니터링 소스가 3개 범위 모두에 구성되었는지 확인

SNMP 소스는 세 가지 모니터링 정책 범위에 모두 있어야 합니다. 범위에서 소스가 누락되면 관련 이벤트의 트랩이 전달되지 않습니다.

<#root>

```
apic1#
```

```
moquery -c snmpSrc | egrep "snmp.Src|name|dn|incl|minSev|monPolDn"

# snmp.Src
name          : NMS-snmpSrc
dn            : uni/fabric/monfab-default/snmpsrc-NMS-snmpSrc        <--- Fabric Default
incl          : audits,events,faults
minSev        : info
monPolDn      : uni/fabric/monfab-default

# snmp.Src
name          : NMS-snmpSrc
dn            : uni/fabric/moncommon/snmpsrc-NMS-snmpSrc              <--- Fabric Common
incl          : audits,events,faults
minSev        : info
monPolDn      : uni/fabric/moncommon

# snmp.Src
name          : NMS-snmpSrc
dn            : uni/infra/moninfra-default/snmpsrc-NMS-snmpSrc        <--- Access Default
incl          : audits,events,faults
minSev        : info
monPolDn      : uni/infra/moninfra-default
```

3개 중 하나라도 누락된 경우 GUI를 사용하여 해당 모니터링 정책에서 누락된 SNMP 소스를 생성합니다.

운영 확인

APIC(show snmp summary)를 사용하여 SNMP 상태 확인

각 APIC에서 직접 이 명령을 실행하여 SNMP 에이전트가 실행 중이고 컨피그레이션이 적용되었는지 확인합니다.

<#root>

```
apic1#

show snmp summary

Active Policy:
default, Admin State: enabled             <--- admin state must be "enabled"

Local SNMP engineID: [Hex] 0x8000000980e2b692088976c75600000000

---------------------------------------
Community           Description
---------------------------------------
public              SNMP Community String  <--- community must be present

------------------------------------------------------------
User                Authentication   Privacy
```

```
-------------------------------------------------------------
                                          <--- empty if using v2c only

-------------------------------------------------------------
Client-Group        Mgmt-Epg              Clients
-------------------------------------------------------------
NMS-Clients         default (In-Band)     10.1.1.50,10.1.1.51  <--- verify client IPs

-------------------------------------------------------------
Host                Port    Version   Level       SecName
-------------------------------------------------------------
10.1.1.50           162     v2c       noauth      public        <--- trap destination
```

출력에서 확인할 사항:

- Admin State(관리 상태)를 활성화해야 합니다.
- 커뮤니티는 NMS가 사용하도록 구성된 항목과 일치해야 합니다.
- Client-Group은 올바른 관리 EPG를 사용하여 허용된 모든 NMS IP를 나열해야 합니다.
- 호스트(트랩 대상)는 NMS 트랩 수신기를 올바른 포트 및 버전으로 나열해야 합니다.

show snmp summary(Leaf/Spine)를 사용하여 SNMP 상태 확인

<#root>

```
leaf101#

show snmp summary

Admin State : enabled, running (pid:8192)  <--- must show "enabled, running" with a PID

Local SNMP engineID: [Hex] 80000009037C69F6105BF9

-----------------------------------------------------------------------
Community       Context         Status
-----------------------------------------------------------------------
public                          ok                                    <--- community status must be "o

-----------------------------------------------------------------------
Client          VRF             Status
-----------------------------------------------------------------------
10.1.1.50       mgmt:inb        ok                                    <--- client entry must be "ok"
10.1.1.51       mgmt:inb        ok

-------------------------------------------------------------------------------
Host            Port    Ver     Level   SecName         VRF
-------------------------------------------------------------------------------
10.1.1.50       162     v2c     noauth  public          mgmt:inb      <--- trap destination
```

출력에서 확인할 사항:

- Admin State(관리 상태)가 pid로 실행 중이어야 합니다. 비활성화된 것으로 표시되는 경우 SNMP 정책이 적용되지 않거나 포드 정책 체인이 끊어집니다.
- Community Status(커뮤니티 상태)는 정상이어야 합니다. 오류 상태는 정책 구축 문제를 나타냅니다.
- 각 NMS 호스트의 클라이언트 VRF는 관리 EPG의 VRF와 일치해야 합니다(대역 내의 경우 mgmt:inb, OOB의 경우 관리).
- 트랩 호스트는 올바른 VRF 컨텍스트로 대상을 나열해야 합니다.

snmpd 프로세스가 실행 중인지 확인

리프 또는 스파인의 경우:

<#root>

```
leaf101#

ps aux | grep snmp

root      5881  2.5 1907404  411444 ?    Ssl  Apr05   /isan/bin/snmpd -f -s -d udp:161 udp6:161 tcp:161

leaf101#

pidof snmpd

5881
```

APIC의 경우:

<#root>

```
apic1#

ps aux | grep snmp

ifc   32182  1.4   0.1  641196  239716  ?   Ssl  Apr10   /mgmt//bin/snmpd.bin \
  -f -p /tmp/snmpd2.pid -a -A -LE 0-2 -c /data//snmp/snmpd.conf
```

leaf 또는 spine에서 snmpd 프로세스가 발견되지 않으면 해당 노드에서 SNMP가 실행되고 있지 않습니다. SNMP 정책 Admin State(관리 상태)가 활성화되어 있고 포드 정책 체인이 올바르게 구성되었는지 확인합니다.

스포일러 (읽으려면 강조 표시)

SNMP 포트가 수신 대기 중인지 확인

<#root>

```
leaf101#

netstat -lutn | grep 161

Active Internet connections (only servers)
Proto  Recv-Q  Send-Q  Local Address    Foreign Address  State
tcp         0       0  0.0.0.0:161      0.0.0.0:*        LISTEN   <--- SNMP agent is accepting requests
udp         0       0  0.0.0.0:161      0.0.0.0:*
udp6        0       0  :::161           :::*
```

포트 161이 LISTEN 상태에 나열되지 않으면 snmpd 프로세스가 실행되고 있지 않거나 포트에 바인딩하지 못했습니다.

리프/스파인에 대한 iptables 규칙 확인

클라이언트 그룹 정책은 각 leaf 및 spine에서 iptable 규칙으로 변환됩니다. 다음을 사용하여 규칙을 검사합니다.

<#root>

```
leaf101#

iptables -S | grep -i snmp

-N snmp_rules
-N vrf_2_snmp_rules
-N vrf_9_snmp_rules
-A INPUT -p udp -m udp --dport 161 -j snmp_rules    <--- SNMP port 161 redirects to snmp_rules chain
-A snmp_rules -m vrf --vrf 2 -j vrf_2_snmp_rules    <--- VRF 2 = OOB management
-A snmp_rules -m vrf --vrf 9 -j vrf_9_snmp_rules    <--- VRF 9 = In-Band management
-A snmp_rules -j DROP                                <--- default drop; only permitted clients pass
-A vrf_2_snmp_rules -s 10.1.1.50/32 -j ACCEPT       <--- permitted NMS client (OOB VRF)
-A vrf_9_snmp_rules -s 10.1.1.50/32 -j ACCEPT       <--- permitted NMS client (INB VRF)
```

패브릭에 대한 올바른 VRF ID를 식별하려면 다음을 실행합니다.

<#root>

```
leaf101#

show vrf

VRF-Name                VRF-ID  State   Reason
management              2       Up      --
mgmt:inb                9       Up      --
```

iptables 규칙의 VRF ID는 show vrf reports와 일치해야 합니다. 클라이언트 IP가 iptables 규칙에 없을 경우, snmpd 프로세스가 실행 중인 경우에도 해당 호스트의 SNMP 요청이 자동으로 삭제됩니다.

카운터를 사용하여 SNMP 패킷이 일치하는지 또는 삭제되었는지 확인합니다.

<#root>

```
leaf101#

iptables -nvL | grep -A 20 "Chain snmp_rules"

Chain snmp_rules (1 references)
 pkts bytes target         prot opt in     out    source       destination
    1    73 vrf_9_snmp_rules all -- *      *      0.0.0.0/0    0.0.0.0/0    vrf 9
    0     0 DROP             all -- *      *      0.0.0.0/0    0.0.0.0/0    <--- if pkts>0 here, client
```

참고: SNMP가 실행 중이지만 iptables에 snmp_rules 체인이 표시되지 않거나 체인이 비어 있으면 snmpd 프로세스를 다시 시작하여 iptables 규칙 리프로그래밍을 강제 수행할 수 있습니다. snmpd PID에 SIGKILL을 전송하는 것은 안전합니다. ACI 프로세스 관리자(폴리싱된)가 자동으로 다시 시작합니다. pidof snmpd를 실행하여 PID를 얻은 다음 -9 [snmpd_pid]를 삭제합니다. 10-15초 후 pidof snmpd를 사용하여 새 PID를 확인합니다.

SNMP 포트가 수신 leaf101# netstat -lutn인지 확인합니다. | grep 161 활성 인터넷 연결(서버만 해당) Proto Recv-Q Send-Q Local Address Foreign Address State tcp 0 0 0.0.0.0:161 0.0.0:0* LISTEN <— SNMP 에이전트가 udp 0.0.0.0:161 0.0.0:* udp6 0 0 ::161 ::* 포트 161이 LISTEN 상태에 나열되지 않으면 snmpd 프로세스가 실행되고 있지 않거나 포트에 바인딩하지 못했습니다. Leaf/Spine 클라이언트 그룹 정책의 iptables 규칙이 각 leaf 및 spine의 iptables 규칙으로 변환되는지 확인합니다. 다음을 사용하여 규칙을 검사합니다. leaf101# iptables -S | grep -i snmp -N snmp_rules -N vrf_2_snmp_rules -N vrf_9_snmp_rules -A INPUT -p udp -m udp —dport 161 -j snmp_rules <— SNMP 포트 161은 snmp_rules 체인으로 리디렉션됩니다. -A snmp_rules -m vrf —vrf 2 -j vrf_2_snmp_rules <— VRF 2 = OOB management -A snmp_rules -m vrf —vrf 9 -j vrf_9_snmp rules <— VRF 9 = In-Band management -A snmp_rules -j DROP <— default drop; 허용된 클라이언트만 통과 -A vrf_2_snmp_rules -s 10.1.1.50/32 -j ACCEPT <— permitted NMS client (OOB VRF) -A vrf_9_snmp_rules -s 10.1.1.50/32 -j ACCEPT <— permitted NMS client (INB VRF) 패브릭의 올바른 VRF ID를 식별하려면 다음을 실행합니다. leaf101# show vrf VRF-Name VRF-ID State Reason management 2 Up — mgmt:inb 9 Up — iptables 규칙의 VRF ID가 show vrf reports와 일치해야 합니다. 클라이언트 IP가 iptables 규칙에 없을 경우, snmpd 프로세스가 실행 중인 경우에도 해당 호스트의 SNMP 요청이 자동으로 삭제됩니다. 카운터를 사용하여 SNMP 패킷이 일치하는지 또는 삭제되었는지 확인합니다. leaf101# iptables -nvL | grep -A 20 "Chain snmp_rules" Chain snmp_rules (1 references) pkts bytes target prot opt in out source destination 1 73 vrf_9_snmp_rules all — * 0.0.0.0/0 0.0.0.0/0 vrf 9 0 0 0 DROP all — * 0.0.0.0/0 0.0.0.0/0 <— pkts>0 here, client IPs missing 참고: SNMP가 실행 중이지만 iptables에 snmp_rules 체인이 표시되지 않거나 체인이 비어 있으면 snmpd 프로세스를 다시 시작하여 iptables 규칙 리프로그래밍을 강제 수행할 수 있습니다. SIGKILL을 snmpd PID로 전송하는 것은 안전합니다. ACI 프로세스 관리자(폴리싱된)가 자동으로 이를 다시 시작합니다. pidof snmpd를 실행하여 PID를 얻은 다음 -9 [snmpd_pid]를 삭제합니다. 10-15초 후 pidof snmpd를 사용하여 새 PID를 확인합니다.

SNMP 포트에 대한 네트워크 연결 확인

<#root>

```
leaf101#

netstat -ai | grep eth0

Iface  MTU  Met  RX-OK  RX-ERR  RX-DRP  RX-OVR  TX-OK  TX-ERR  TX-DRP  TX-OVR  Flg
eth0   1500   0  501277      0       0       0  633546      0       0       0  BMRU

leaf101#

netstat -ai | grep kpm_inb

Iface     MTU  Met    RX-OK  RX-ERR  RX-DRP  RX-OVR    TX-OK  TX-ERR  TX-DRP  TX-OVR  Flg
kpm_inb  9300   0  10361421     0       0       0   8958506      0     126       0  BMRU
```

관리 인터페이스가 활성 상태이고(RX-ERR 증가 없음) 트래픽을 전달하는지 확인합니다. eth0은 OOB 관리 인터페이스입니다. kpm_inb는 스위치의 대역 내 관리 인터페이스입니다.

tcpdump를 사용하여 SNMP 트랩 전송 확인

트랩이 생성되고 리프 또는 스파인 노드에서 전송되는지 확인하려면 해당 인터페이스에서 트래픽을 캡처합니다. 노드를 관리자로 액세스하고 다음을 사용합니다.

<#root>

```
leaf101#

tcpdump -i kpm_inb -f port 162 -vv

tcpdump: listening on kpm_inb, link-type EN10MB (Ethernet), capture size 65535 bytes
17:21:49.810052 IP (tos 0x0, ttl 64, id 63116, proto UDP, length 218)
    172.18.242.14.35582 > 10.1.1.50.snmp-trap: { SNMPv2c C=public
    { V2Trap(171) R=253 system.sysUpTime.0=5888267
      S:1.1.4.1.0=E:cisco.9.276.0.1
      interfaces.ifTable.ifEntry.ifIndex.436224000=436224000
      interfaces.ifTable.ifEntry.ifOperStatus.436224000=2 }}        <--- verify trap is being sent to N
```

OOB의 경우

<#root>

```
leaf101#
```

```
tcpdump -i eth0 -f port 162 -vv
```

스포일러 (읽으려면 강조 표시)

APIC 트랩(INB)의 경우

<#root>

```
apic1#

tcpdump -i bond0.1100 -f port 162

20:01:08.453473 IP apic1-inb.cisco.com.59417 > 10.1.1.50.snmptrap: C=public V2Trap(85) S:
1.1.4.1.0=E:cisco.9.117.2.0.2 E:cisco.9.117.1.1.2.1.1.10548=1 E:cisco.9.117.1.1.2.1.2.10548=2
```

참고: APIC에서 bond0.1100은 대역 내 관리 인터페이스 VLAN 하위 인터페이스입니다. 1100을 대역 내 관리 EPG에 대해 구성된 VLAN encap으로 교체합니다. APIC에서 OOB 캡처의 인터페이스 이름으로 oobmgmt를 사용합니다.

APIC 트랩(INB)의 경우 apic1# tcpdump -i bond0.1100 -f 포트 162 20:01:08.453473 IP apic1-inb.cisco.com.59417 > 10.1.1.50.snmptrap: C=공용 V2Trap(85) S: 1.1.4.1.0=E:cisco.9.117.2.0.2 E:cisco.9.117.1.1.2.1.1.10548=1 E:cisco.9.117.1.1.2.1.2.10548=2 참고: APIC에서 bond0.1100은 대역 내 관리 인터페이스 VLAN 하위 인터페이스입니다. 1100을 대역 내 관리 EPG에 대해 구성된 VLAN encap으로 교체합니다. APIC에서 OOB 캡처의 인터페이스 이름으로 oobmgmt를 사용합니다.

tcpdump로 SNMP GET/WALK 요청 확인

<#root>

```
leaf101#

tcpdump -i kpm_inb -f port 161 -vv

17:26:08.548149 IP 10.1.1.50.64245 > leaf101.cisco.com.snmp: { SNMPv2c C=public
  { GetRequest(28) R=949769396 system.sysDescr.0 }}              <--- GET request received
17:26:08.552290 IP leaf101.cisco.com.snmp > 10.1.1.50.64245: { SNMPv2c C=public
  { GetResponse(191) R=949769396
    system.sysDescr.0="Cisco NX-OS(tm) aci, Software (aci-n9000-system), \
Version 15.0(1k), RELEASE SOFTWARE" }}                          <--- response returned; SNMP working
```

GetRequest는 표시되지만 GetResponse는 표시되지 않는 경우 요청이 수신되지만 응답하지 않습니다. snmpd 프로세스 및 커뮤니티 문자열을 확인합니다. 요청과 응답이 모두 표시되지 않으면 노드에 도달하기 전에 요청이 차단됩니다(라우팅 및 iptable 확인).

문제 해결 워크플로

분류 결정 트리

엔지니어가 SNMP가 작동하지 않는다고 보고할 때 이 진단트리를 사용합니다. 관찰된 증상부터 시작하여 가지에 따라 격리합니다.

증상: SNMP GET/WALK 요청에 응답 없음

1. APIC에서 SNMP Admin State(SNMP 관리 상태)를 선택합니다. moquery `-c snmpPol`을 실행합니다. adminSt가 비활성화된 경우 이를 활성화하고 7단계로 진행합니다.
2. snmpd 프로세스를 확인합니다. 영향을 받는 노드에서 `ps aux`를 실행합니다 `| grep snmp` 또는 `pidof snmpd`. 실행 중인 프로세스가 없으면 SNMP 정책이 구축되지 않습니다. Pod 정책 체인(SNMP Policy → Pod Policy Group → Pod Profile)을 확인합니다.
3. 포트 161이 수신 대기 중인지 확인하십시오. netstat `-lutn` 실행 `| grep 161`. 포트 161이 LISTEN 상태가 아닌 경우 snmpd 프로세스가 실패했습니다. /var/log/dme/log/svc_ifc_dbgrelem.log*에서 로그를 수집하고 프로세스를 다시 시작합니다.
4. 라우팅을 확인합니다. `show ip route vrf management` 및 `show ip route vrf mgmt:inb`를 실행합니다. NMS 호스트에 대한 경로가 올바른 VRF에 있는지 확인합니다.
5. APIC의 관리 계약을 확인합니다. 대상이 APIC(leaf/spine이 아님)인 경우 OOB 또는 INB 관리 계약에서 UDP 161이 허용되는지 확인합니다.
6. 노드에서 tcpdump를 수행합니다. tcpdump `-i kpm_inb -f port 161 -vv`(또는 OOB의 경우 `eth0`)를 실행합니다. GetRequest가 나타나지만 GetResponse가 뒤따르지 않는 경우, 요청이 노드에 도달하지만 snmpd가 응답하지 않는 경우 — 커뮤니티 문자열을 확인합니다. 요청이 전혀 표시되지 않으면 업스트림(라우팅 또는 계약)에서 문제가 발생합니다.
7. 허용된 클라이언트에서 테스트. 클라이언트 그룹에 나열된 NMS 호스트에서 snmpget `-v2c -c [community] [node-ip] SNMPv2-MIB::sysDescr.0`을 실행합니다. 성공적으로 응답하면 SNMP가 완전히 작동하고 있음을 확인할 수 있습니다.

증상: NMS에서 수신된 SNMP 트랩 없음

1. 트랩 대상 컨피그레이션을 확인합니다. moquery `-c snmpTrapDest`를 실행합니다. NMS IP, 포트, 버전 및 커뮤니티가 NMS 예상 값과 일치하는지 확인합니다.
2. 모니터링 소스가 세 가지 범위에 모두 있는지 확인하십시오. moquery `-c snmpSrc` 실행 `| egrep "snmp.Src|name|dn"`. uni/fabric/monfab`-default`, uni`/fabric/moncommon`, uni/infra/moninfra-default에 대한 `monPolDn` 값이 있는 항목이 있는지 확인합니다. 누락된 항목이 있으면 해당 모니터링 정책에 SNMP 소스를 추가합니다.
3. snmpd 프로세스를 확인합니다. 트랩을 전송해야 하는 노드에서 snmpd가 실행 중인지 확인합니다.
4. 테스트 이벤트를 생성하고 tcpdump를 사용하여 캡처합니다. 인터페이스를 플랩하거나 상태를 변경하여 이벤트를 생성합니다. 노드에서 tcpdump `-i kpm_inb -f port 162 -v`를 실행합니다.

와이어에 트랩 트래픽이 나타나지 않으면 이벤트가 트랩을 생성하지 않습니다. 모니터링 소스 incl 속성(결함 또는 이벤트를 포함해야 함)을 다시 확인하십시오.
5. 트랩 수신기와의 연결을 확인합니다. 관리 VRF에서 트랩 수신기에 연결할 수 있는지 확인합니다. `show ip route vrf mgmt:inb`는 NMS 호스트에 대한 경로를 표시해야 합니다.
6. 트랩이 tcpdump에는 나타나지만 NMS에는 나타나지 않는 경우, 네트워크 측에서 문제가 발생합니다. 방화벽, 라우팅 또는 NMS 컨피그레이션입니다 NMS가 ACI 노드의 관리 소스 IP에서 UDP 162를 수신 대기하고 있는지 확인합니다.

일반적인 시나리오

시나리오 1: SNMP 정책이 활성화되었지만 리프/스파인에서 데이터가 반환되지 않음

문제/장애: APIC의 SNMP 정책에는 Admin State(관리 상태)가 enabled(활성화됨)로 표시됩니다. NMS는 리프의 관리 IP에 연결할 수 있습니다. `snmp`는 응답 없이 시간 초과됩니다.

컨피그레이션 확인: Pod Policy Group이 SNMP 정책을 참조하고 Resolved SNMP Policy(확인된 SNMP 정책)에 올바른 이름이 표시되는지 확인합니다. Pod Policy Group(포드 정책 그룹)의 SNMP Policy(SNMP 정책) 필드가 비어 있거나 관계가 형성되지 않은 경우 스위치에서 snmpd 프로세스가 시작되지 않을 수 있습니다.

운영 확인: 영향받는 리프에 SSH를 적용하고 show snmp `summary`를 실행합니다. 출력에 Admin `State`(관리자 상태)가 표시되면 `disabled`(비활성화됨)는 APIC에서 enabled(활성화됨)로 표시되지만 정책이 구축되지 않았습니다. Pod 정책 체인에서 누락되었거나 잘못 참조된 Pod 정책 그룹을 확인합니다.

근본 원인: SNMP 정책이 Pod Policy Group에 연결되어 있지 않거나 Pod Profile Selector가 올바른 Pod Policy Group을 이 Pod에 적용하지 않습니다.

해결책:

1. Fabric(패브릭) > Fabric Policies(패브릭 정책) > Pods(포드) > Policy Groups(정책 그룹) > default(기본값)로 이동합니다.
2. SNMP Policy(SNMP 정책) 필드가 활성화된 SNMP 정책을 가리키는지 확인합니다.
3. Fabric(패브릭) > Fabric Policies(패브릭 정책) > Pods(포드) > Profiles(프로파일)로 이동하고 활성 선택기가 이 포드 정책 그룹을 참조하는지 확인합니다.
4. 저장 후 2분 이내에 `leaf`에 snmp 요약을 표시합니다.

시나리오 2: SNMP GET/WALK는 일부 NMS 호스트에서는 작동하지만 다른 호스트에서는 작동하지 않음

문제/장애: 하나의 NMS 서버가 ACI 노드를 폴링할 수 있습니다. 다른 서브넷의 두 번째 NMS 서버는 응답을 받지 않습니다.

컨피그레이션 확인: APIC에서 `moquery -c snmpClientGrpP -x query-target=`children을 실행합니다. 두 번째 NMS 서버의 IP가 클라이언트 항목으로 나열되는지 확인합니다. 이 IP가 없는 경우 해당 IP는 snmp_rules 체인의 맨 아래에 있는 iptables DROP 규칙에 의해 차단됩니다.

운영 확인: 영향받는 leaf에서 OOB 또는 INB 관리 계약에 UDP 161이 허용되는지 확인합니다. SNMP 포트가 있는 계약 또는 필터가 없으면 요청이 삭제됩니다.

근본 원인: 두 번째 NMS 서버 IP가 클라이언트 그룹 정책에 없습니다.

해결책: 누락된 NMS IP를 SNMP 클라이언트 그룹 정책의 Fabric(패브릭) > Fabric Policies(패브릭 정책) > Policies(정책) > Pod(포드) > SNMP > default(기본값) > Client Group Policies(클라이언트 그룹 정책) 아래에 있는 클라이언트 항목으로 추가합니다. 모든 노드의 iptables 규칙은 정책을 저장한 후 몇 분 내에 업데이트됩니다.

시나리오 3: SNMP 트랩이 수신되지 않음 — 트랩이 생성되지만 전달되지 않음

문제/장애: APIC 결함 테이블에 결함이 표시됩니다. `moquery -c snmpTrapDest`는 올바른 NMS IP를 표시합니다. NMS는 트랩을 수신하지 않습니다.

컨피그레이션 확인: moquery `-c snmpSrc` 실행 | `egrep "snmp.Src|name|dn"`. 모니터링 소스가 세 가지 범위(monfab-default, `moncommon`, `moninfra-default`)에 모두 있는지 확인합니다. 일반적인 감독은 액세스 정책 이벤트를 놓치는 Fabric Default 정책에서만 소스를 구성하는 것입니다.

운영 확인: 테스트 이벤트를 트리거합니다(예: 인터페이스를 admin-down 상태로 전환). 관련 노드에서 tcpdump `-i kpm_inb -f port 162`를 실행합니다. 트랩 패킷이 노드의 인터페이스에 나타나는 경우 ACI 측이 작동하고 문제가 NMS에 대한 네트워크 경로(방화벽, 라우팅)에 있습니다. 와이어에 트랩이 나타나지 않으면 ACI 모니터링 소스가 없거나 이벤트 유형이 소스의 incl 특성에 `포함되지` 않습니다.

근본 원인 1: 하나 이상의 모니터링 원본이 필요한 범위에 없습니다.

근본 원인 2: 모니터링 소스 `incl` 특성은 생성되는 이벤트 유형을 제외합니다(예: `incl: 장애`가 `없는` 이벤트는 장애 기반 트랩이 전송되지 않음을 의미합니다.

해결책:

1. 세 가지 범위(Fabric Default(패브릭 기본값), Fabric Common(패브릭 공통), Access

Default(액세스 기본값)) 각각에 대해 GUI에서 누락된 모니터링 소스를 추가합니다. 대상 그룹을 구성된 SNMP 대상 그룹으로 설정합니다.

2. 포괄적인 트랩 커버리지를 위해 `incl` 특성에 감사, 이벤트, 결함이 포함되는지 확인합니다.
3. 변경 후 테스트 이벤트를 다시 트리거하고 tcpdump를 다시 선택합니다.

스포일러 (읽으려면 강조 표시)

참고: APIC에서 tcpdump/code> 명령은 루트 사용자만 사용할 수 있습니다. APIC 및 Switches iptables 명령은 루트 사용자만 사용할 수 있습니다.

시나리오 4: APIC에서 작동하지 않는 SNMPv3 클라이언트 그룹 시행

문제/장애: 클라이언트 그룹 정책에 없는 SNMP 클라이언트는 동일한 쿼리가 리프/스파인 노드에서 실패하더라도 SNMPv3을 사용하여 APIC에 성공적으로 쿼리할 수 있습니다.

근본 원인: 이것은 **알려진 경고입니다.** 클라이언트 그룹 정책(iptables 기반 소스 IP 시행)은 APIC 컨트롤러에 대한 SNMPv3 GET/Walk에 적용되지 않습니다. 모든 호스트는 클라이언트 그룹 컨피그레이션과 상관없이 SNMPv3을 통해 APIC에 쿼리할 수 있습니다. 리프 및 스파인 스위치에서 클라이언트 그룹 시행은 SNMPv2c 및 SNMPv3에 대해 동일하게 작동합니다.

완화: APIC에서 관리 계약 필터를 사용하여 소스 서브넷별 SNMP 액세스를 제한합니다. 클라이언트 그룹은 리프/스파인 노드에 효과적입니다. SNMPv3를 사용하는 APIC의 경우 액세스 제어 메커니즘으로 관리 계약 소스 기반 필터링을 사용합니다.

시나리오 5: SNMP 쿼리는 성공했지만 MIB 데이터가 완전하지 않거나 오래됨

문제/장애: SNMP GET/WALK는 데이터를 반환하지만 특정 MIB OID는 빈 값이나 오래된 값을 반환합니다. 특히 인터페이스 통계나 작동 상태 데이터는 현재 패브릭 상태를 반영하지 않습니다.

운영 확인: 쿼리할 APIC를 확인합니다. 각 APIC는 로컬 데이터에 대한 MIB 객체만 반환합니다. 쿼리 중인 APIC에 대해 show snmp summary를 실행하고 결과를 예상한 결과와 비교합니다. 스위치 레벨 데이터(IF-MIB, entityMIB)의 경우 APIC가 아니라 스위치를 직접 쿼리합니다.

근본 원인: 리프 레벨 MIB 데이터에 대한 APIC 쿼리 각 APIC는 자체 관리 객체에 대해서만 MIB 객체를 제공합니다. 각 leaf 및 spine을 직접 폴링하여 스위치 레벨 데이터(인터페이스 통계, CPU, 메모리, 환경 센서)를 검색해야 합니다.

해결책: 인터페이스 및 하드웨어 MIB 데이터에 대해 리프 및 스파인 관리 IP를 직접 폴링하도록 NMS를 구성합니다. APIC 관리 IP는 APIC 네이티브 MIB(APIC 서버 하드웨어와 관련된 엔티티, FRU, 프로세스, 센서)에만 사용합니다.

시나리오 6: SNMP는 리프/스파인에서 작동하지만 APIC에서는 작동하지 않음

문제/장애: NMS에서 리프 및 스파인 노드로 SNMPv2c GET이 성공합니다. 동일한 NMS에서 APIC를 폴링할 수 없습니다.

컨피그레이션 확인: APIC SNMP에는 UDP 161을 허용하는 명시적 관리 계약이 필요합니다. Tenants(테넌트) **> mgmt(관리)로** 이동하여 OOB/INB 계약과 UDP 161에 대한 필터를 확인합니다.

운영 확인: APIC에서 iptables -S를 실행합니다 | grep 161. UDP 161에 대한 ACCEPT 규칙이 fp-137(또는 동등 OOB 계약) 체인 아래에 나타나지 않으면 UDP 161에 대한 계약 필터가 없거나 구축되지 않았습니다.

```
<#root>

apic1#

iptables -S | grep 161

-A fp-137 -s 10.0.0.0/8 -p udp -m udp --dport 161 -j ACCEPT     <--- permit SNMP from the management su
-A fp-137 -s 172.18.0.0/16 -p udp -m udp --dport 161 -j ACCEPT  <--- permit SNMP from INB management su
```

이러한 규칙이 없는 경우 UDP 161에 대한 필터 항목을 관리 계약 제목에 추가하고 다시 검증합니다.

근본 원인: 관리 계약이 누락되었거나 잘못 구성되었습니다. ACI 5.x에서 APIC 노드는 관리 계약을 엄격하게 적용합니다. 명시적 허가가 없으면 SNMP 패킷이 삭제됩니다.

해결책:

1. Tenants(테넌트) **> mgmt(관리) > Security Policies(보안 정책) > Out-Of-Band Contracts(대역 외 계약)로 이동합니다.**
2. OOB contract(OOB 계약)를 확장하고 Subject(주체)를 선택한 다음 UDP **포트 161**에 대한 필터를 확인/**추가합니다.**
3. NMS가 INB 관리를 통해 APIC에 도달하는 경우 In-Band 계약에 대해 반복합니다.
4. iptables -S로 확인합니다. 저장 후 APIC에서 grep 161을 선택합니다.

시나리오 7: SNMP Iptables 규칙이 없거나 잘못되었습니다.

문제/장애: show snmp summary는 SNMP 정책이 적용되었지만 iptables -S를 표시합니다. | grep snmp는 규칙을 반환하지 않거나 NMS 클라이언트 IP가 규칙에 없습니다.

운영 확인: snmpd가 pidof snmpd와 실행 중인지 확인합니다. snmpd가 실행 중이지만 iptables에 SNMP 규칙이 없는 경우, 클라이언트 그룹 정책이 구축되기 전에 프로세스가 시작되었습니다. 재시작 횟수가 250회 미만인 경우 snmpd를 재시작하여 규칙 재프로그래밍을 적용합니다.

```
<#root>

leaf101#

pidof snmpd

5881

leaf101# show system internal sysmgr service name snmpd
Service "snmpd" ("snmpd", 127):
UUID = 0x1A, PID = 5881, SAP = 1545
State: SRV_STATE_HANDSHAKED (entered at time Mon Aug 25 19:23:50 2025).

Restart count: 3


Time of last restart: Mon Aug 25 19:23:48 2025.
Previous PID: 32080
Reason of last termination: SYSMGR_DEATH_REASON_FAILURE_SIGNAL
Tag = N/A
Plugin ID: 0
leaf101#

kill -9 5881
```

ACI 프로세스 관리자가 snmpd를 자동으로 재시작합니다. 다시 시작한 후 다음을 확인합니다.

```
<#root>

leaf101#

iptables -S | grep -i snmp
```

이제 snmp_rules 체인 및 VRF별 클라이언트 ACCEPT 규칙이 표시됩니다.

근본 원인: 클라이언트 그룹 정책이 노드에 완전히 구축되기 전에 snmpd 프로세스가 다시 시작되었거나 시작되어 iptables가 SNMP 액세스 규칙 없이 유지됩니다.

참고: APIC에서 tcpdump/code> 명령은 루트 사용자만 사용할 수 있습니다. APIC 및 Switches iptables 명령의 경우 루

트 사용자만 사용할 수 있습니다. 시나리오 4: SNMPv3 클라이언트 그룹 시행이 APIC 문제에서 작동하지 않음: 클라이언트 그룹 정책에 없는 SNMP 클라이언트는 동일한 쿼리가 리프/스파인 노드에서 실패하더라도 SNMPv3을 사용하여 APIC에 성공적으로 쿼리할 수 있습니다. 근본 원인: 이것은 알려진 경고문이다. 클라이언트 그룹 정책(iptables 기반 소스 IP 시행)은 APIC 컨트롤러에 대한 SNMPv3 GET/Walk에 적용되지 않습니다. 모든 호스트는 클라이언트 그룹 컨피그레이션과 상관없이 SNMPv3을 통해 APIC에 쿼리할 수 있습니다. 리프 및 스파인 스위치에서 클라이언트 그룹 시행은 SNMPv2c 및 SNMPv3에 대해 동일하게 작동합니다. 완화: APIC에서 관리 계약 필터를 사용하여 소스 서브넷별 SNMP 액세스를 제한합니다. 클라이언트 그룹은 리프/스파인 노드에 효과적입니다. SNMPv3를 사용하는 APIC의 경우 액세스 제어 메커니즘으로 관리 계약 소스 기반 필터링을 사용합니다. 시나리오 5: SNMP 쿼리는 성공했지만 MIB 데이터가 완전하지 않거나 오래된 문제입니다. SNMP GET/WALK는 데이터를 반환하지만 특정 MIB OID는 빈 값이나 오래된 값을 반환합니다. 특히 인터페이스 통계나 작동 상태 데이터는 현재 패브릭 상태를 반영하지 않습니다. 운영 확인: 쿼리할 APIC를 확인합니다. 각 APIC는 로컬 데이터에 대한 MIB 객체만 반환합니다. 쿼리 중인 APIC에 대해 show snmp summary를 실행하고 결과를 예상한 결과와 비교합니다. 스위치 레벨 데이터(IF-MIB, entityMIB)의 경우 APIC가 아니라 스위치를 직접 쿼리합니다. 근본 원인: 리프 레벨 MIB 데이터에 대한 APIC 쿼리 각 APIC는 자체 관리 객체에 대해서만 MIB 객체를 제공합니다. 각 leaf 및 spine을 직접 폴링하여 스위치 레벨 데이터(인터페이스 통계, CPU, 메모리, 환경 센서)를 검색해야 합니다. 해결책: 인터페이스 및 하드웨어 MIB 데이터에 대해 리프 및 스파인 관리 IP를 직접 폴링하도록 NMS를 구성합니다. APIC 관리 IP는 APIC 네이티브 MIB(APIC 서버 하드웨어와 관련된 엔티티, FRU, 프로세스, 센서)에만 사용합니다. 시나리오 6: SNMP는 리프/스파인에서 작동하지만 APIC 문제에서는 작동하지 않습니다. NMS에서 리프 및 스파인 노드로 SNMPv2c GET이 성공합니다. 동일한 NMS에서 APIC를 폴링할 수 없습니다. 컨피그레이션 확인: APIC SNMP를 사용하려면 UDP 161을 허용하는 명시적 관리 계약이 필요합니다. Tenants(테넌트) > mgmt로 이동하여 OOB/INB 계약과 UDP 161에 대한 필터를 확인합니다. 운영 확인: APIC에서 iptables -S를 실행합니다 | grep 161. fp-137(또는 이에 상응하는 OOB 계약) 체인 아래에 UDP 161에 대한 ACCEPT 규칙이 나타나지 않으면 UDP 161에 대한 계약 필터가 없거나 배포되지 않습니다. apic1# iptables -S | grep 161 -A fp-137 -s 10.0.0.0/8 -p udp -m udp —dport 161 -j ACCEPT <— 관리 서브넷에서 SNMP 허용 -A fp-137 -s 172.18.0.0/16 -p udp -m udp —dport 161 -j ACCEPT <— INB 관리 서브넷에서 SNMP 허용 이 규칙이 없는 경우 관리 계약 제목에 UDP 161에 대한 필터 항목을 추가하고 다시 검증합니다. 근본 원인: 관리 계약이 누락되었거나 잘못 구성되었습니다. ACI 5.x에서 APIC 노드는 관리 계약을 엄격하게 적용합니다. 명시적 허가가 없으면 SNMP 패킷이 삭제됩니다. 해결책: Tenants(테넌트) > mgmt(관리) > Security Policies(보안 정책) > Out-Of-Band Contracts(대역 외 계약)로 이동합니다. OOB contract를 확장하고 Subject를 선택한 다음 UDP 포트 161에 대한 필터를 확인/추가합니다. NMS가 INB 관리를 통해 APIC에 도달하는 경우 In-Band contract에 대해 반복합니다. iptables -S로 확인 | 저장 후 APIC에서 grep 161을 선택합니다. 시나리오 7: SNMP Iptables 규칙이 없거나 잘못된 문제: show snmp summary - SNMP 정책이 적용되었지만 iptables -S가 표시됩니다. | grep snmp는 규칙을 반환하지 않거나 NMS 클라이언트 IP가 규칙에 없습니다. 운영 확인: snmpd가 pidof snmpd와 실행 중인지 확인합니다. snmpd가 실행 중이지만 iptables에 SNMP 규칙이 없는 경우, 클라이언트 그룹 정책이 구축되기 전에 프로세스가 시작되었습니다. 재시작 횟수가 250회 미만인 경우 snmpd를 재시작하여 규칙 재프로그래밍을 적용합니다. leaf101# pidof snmpd 5881leaf101# show system internal sysmgr service name snmpdService "snmpd" ("snmpd", 127):UUID = 0x1A, PID = 5881, SAP = 1545State: SRV_STATE_HANDSHAKED(2025년 8월 25일 월요일 19:23:50에 입력됨).재시작 수: 3마지막 재시작 시간: 2025년 8월 25일 월요일 19:23:48.이전 PID: 32080마지막 종료 이유: SYSMGR_DEATH_REASON_FAILURE_SIGNALTag = 해당 사항 없음 로그인 ID: 0 leaf101# kill -9 5881 ACI 프로세스 관리자가 snmpd를 자동으로 재시작합니다. 다시 시작한 후 다음을 확인합니다. leaf101# iptables -S | grep -i snmp snmp snmp snmp_rules 체인 및 per-VRF client ACCEPT 규칙이 표시됩니다. 근본 원인: 클라이언트 그룹 정책이 노드에 완전히 구축되기 전에 snmpd 프로세스가 다시 시작되었거나 시작되어 iptables가 SNMP 액세스 규칙 없이 유지됩니다.

확장 문제 해결을 위한 로그 파일

위의 확인 단계에서 문제가 해결되지 않을 경우 리프, 스파인 및 APIC 노드의 다음 로그 파일에는 SNMP 관련 진단 정보가 포함되어 있습니다.

<#root>

leaf101#

zgrep "snmp" /var/log/dme/log/svc_ifc_dbgrelem.log*

leaf101#

zgrep "snmpd" /var/log/dme/log/svc_ifc_dbgrelem.log*

leaf101#

zgrep "snmpd_log" /var/log/dme/log/*

이러한 로그에는 show snmp summary를 통해 표시되지 않는 snmpd restart 이벤트, 정책 구축 이벤트 및 커뮤니티/클라이언트 컨피그레이션 오류가 포함됩니다.

참조

- Cisco APIC System Management 컨피그레이션 가이드, 릴리스 5.x – SNMP 관리
- Cisco ACI MIB 빠른 참조 설명서

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.