ACI에서 SNMP 구성

목차

소개

이 문서에서는 ACI의 SNMP(Simple Network Management Protocol) 및 SNMP 트랩의 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 패브릭 검색이 완료되었습니다.
- APIC(Application Policy Infrastructure Controller) 및 패브릭 스위치에 대한 대역 내/대역 외 연결
- SNMP 트래픽을 허용하도록 구성된 대역 내/대역 외 계약(UDP 포트 161 및 162)

- 기본 관리 테넌트에서 APIC 및 패브릭 스위치에 대해 구성된 고정 노드 관리 주소(이 기능이 없으면 APIC에서 SNMP 정보 가져오기가 실패함)
- SNMP 프로토콜 워크플로 이해

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- APIC
- 브라우저
- 5.2(8e)를 실행하는 ACI(Application Centric Infrastructure)
- Snmpwalk 명령을 사용합니다

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.

구성

Cisco ACI는 MIB(Management Information Base) 및 알림(트랩)을 비롯한 SNMPv1, v2c 및 v3 지원을 제공합니다. SNMP 표준에서는 다양한 MIB를 지원하는 모든 서드파티 애플리케이션이 ACI 리프 및 스파인 스위치와 APIC 컨트롤러를 관리하고 모니터링할 수 있습니다.

그러나 SNMP 쓰기 명령(Set)은 ACI에서 지원되지 않습니다.

SNMP 정책은 리프 및 스파인 스위치와 APIC 컨트롤러에 개별적으로 적용되고 실행됩니다. 각 ACI 디바이스에는 자체 SNMP 엔티티가 있으므로 APIC 클러스터의 여러 APIC는 스위치와 함께 별도로 모니터링해야 합니다. 그러나 SNMP 정책 소스는 전체 ACI 패브릭에 대한 모니터링 정책으로 생성됩니다.

기본적으로 SNMP는 폴링에 **UDP** 포트 **161**을 사용하고 TRAP에 포트 **162**를 사용합니다.

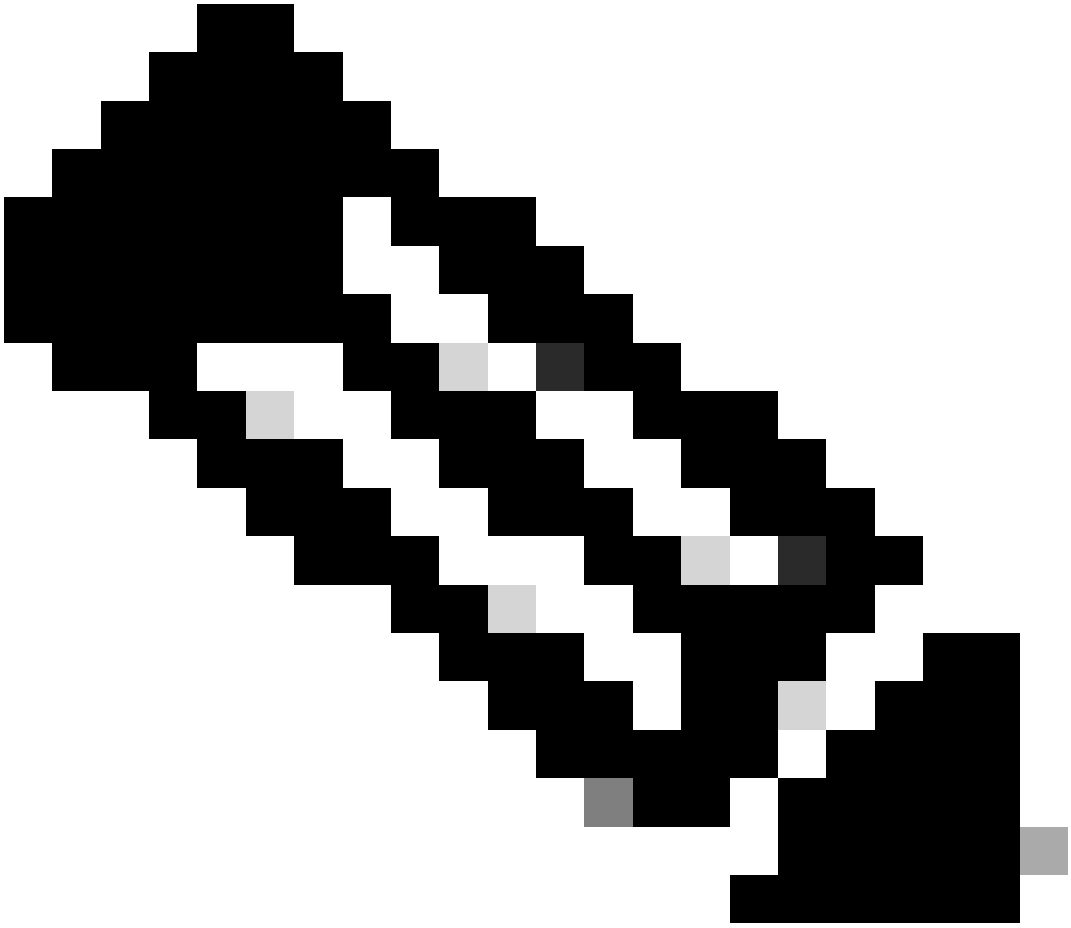
SNMP 범위 이해

ACI에서 SNMP의 한 가지 빠른 기본 개념은 SNMP 정보를 가져올 수 있는 범위가 두 개라는 것입니다.
1. 글로벌
2. VRF(Virtual Routing and Forwarding) 컨텍스트

전역 **범위**는 리프/스파인 노드의 인터페이스 수, 인터페이스 인덱스, 인터페이스 이름, 인터페이스 상태 등과 같은 섀시 MIB를 가져오는 것입니다.

VRF 컨텍스트 범위별 MIB는 IP 주소 및 라우팅 프로토콜 정보와 같은 VRF별 정보를 가져옵니다.

Cisco ACI MIB 지원 목록에는 지원되는 APIC 및 패브릭 스위치 전역 및 VRF 컨텍스트 MIB의 전체 목록이 있습니다.

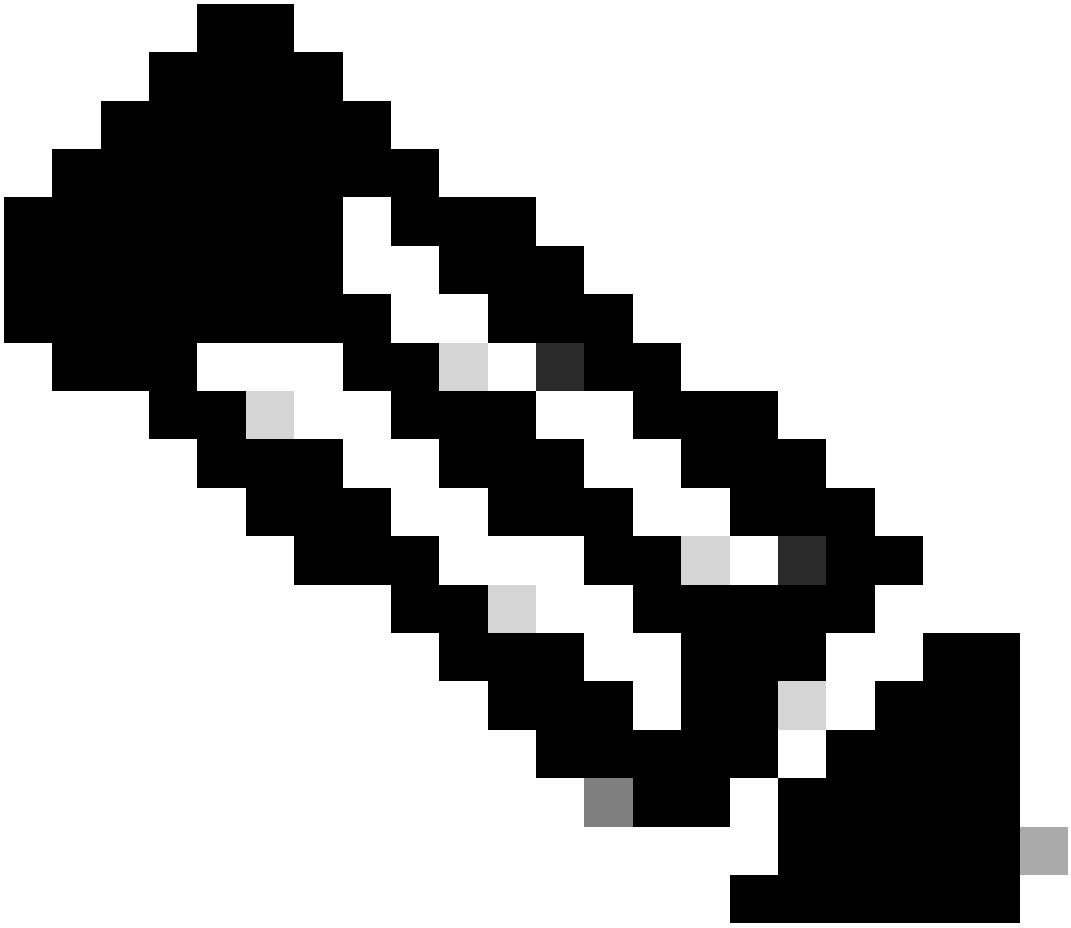


참고: 전역 범위가 있는 MIB는 시스템에 하나의 인스턴스만 있습니다. 전역 MIB의 데이터는 전체 시스템과 관련이 있습니다.

VRF별 범위가 있는 MIB는 시스템에서 VRF별 인스턴스를 가질 수 있습니다. VRF 특정 MIB의 데이터는 해당 VRF에만 관련됩니다.

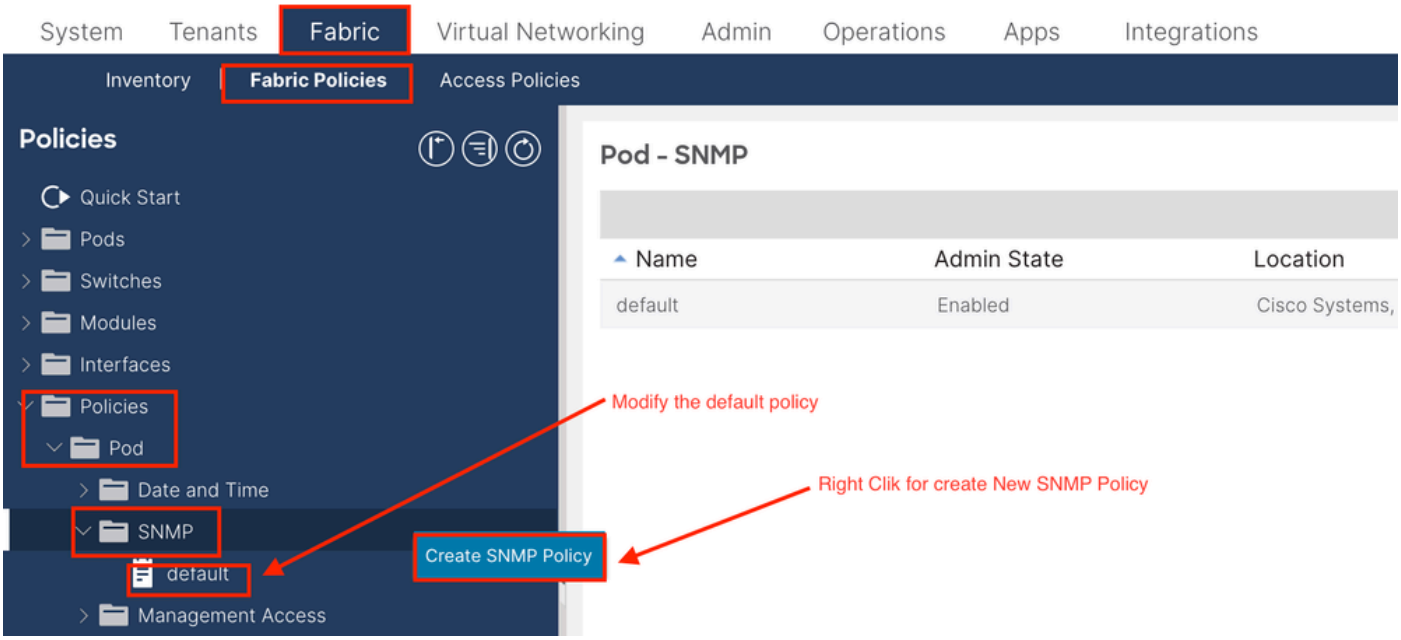
컨피그레이션 단계(전역 및 VRF 컨텍스트 범위 모두)

1단계. SNMP 패브릭 정책 구성



참고: 여기서는 SNMP 커뮤니티 정책 및 SNMP 클라이언트 그룹 정책과 같은 SNMP 설정을 지정합니다.

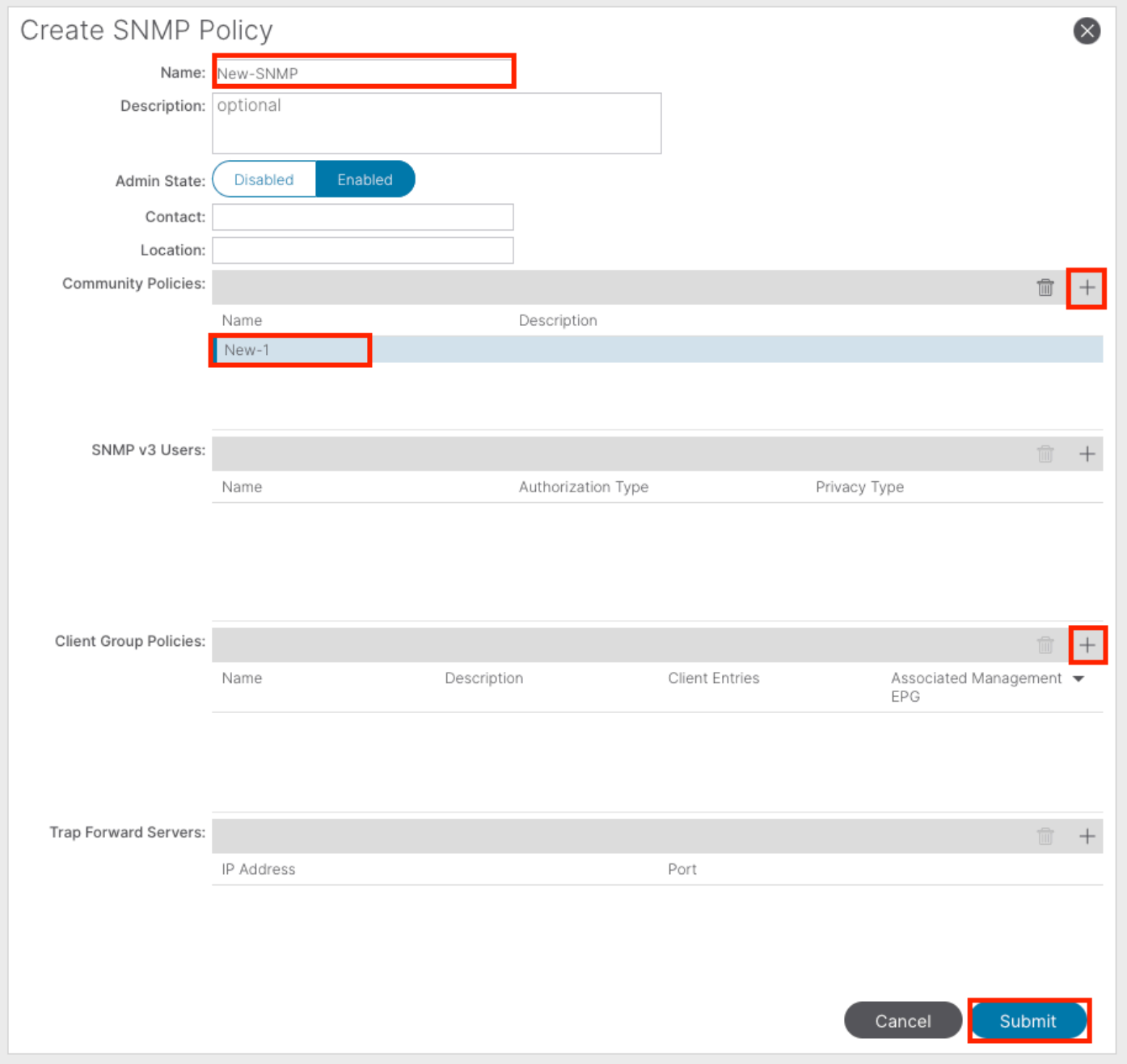
SNMP를 구성하는 첫 번째 단계는 필요한 SNMP 패브릭 정책을 생성하는 것입니다. SNMP 패브릭 정책을 생성하려면 APIC 웹 GUI 경로로 이동합니다Fabric > Fabric Policies > Policies > Pod > SNMP.



새 SNMP 정책을 생성하거나 기본 SNMP 정책을 수정할 수 있습니다.

이 문서에서 SNMP 정책은 **New-SNMP라고** 하며 SNMP 버전 v2c를 사용하므로 여기서 필요한 필드는 커뮤니티 정책 및 클라이언트 그룹 정책뿐입니다.

Community Policy Name 필드는 사용할 SNMP 커뮤니티 문자열을 정의합니다. 우리의 경우, **New-1**. 이 두 커뮤니티 문자열은 나중에 어디에서 나타나는지 알 수 있습니다.



Name(이름) - SNMP 정책의 이름입니다. 이 이름은 1~64자의 영숫자로 지정할 수 있습니다.

설명 - SNMP 정책에 대한 설명입니다. 설명은 0~128자의 영숫자로 구성할 수 있습니다.

Admin State(관리 상태) - SNMP 정책의 관리 상태입니다. 상태를 활성화 또는 비활성화할 수 있습니다. 상태는 다음과 같습니다.

- enabled(활성화됨) - 관리자 상태가 활성화됨
- disabled(비활성화됨) - 관리 상태가 비활성화됨

기본값은 **disabled**입니다.

Contact - SNMP 정책의 연락처 정보입니다.

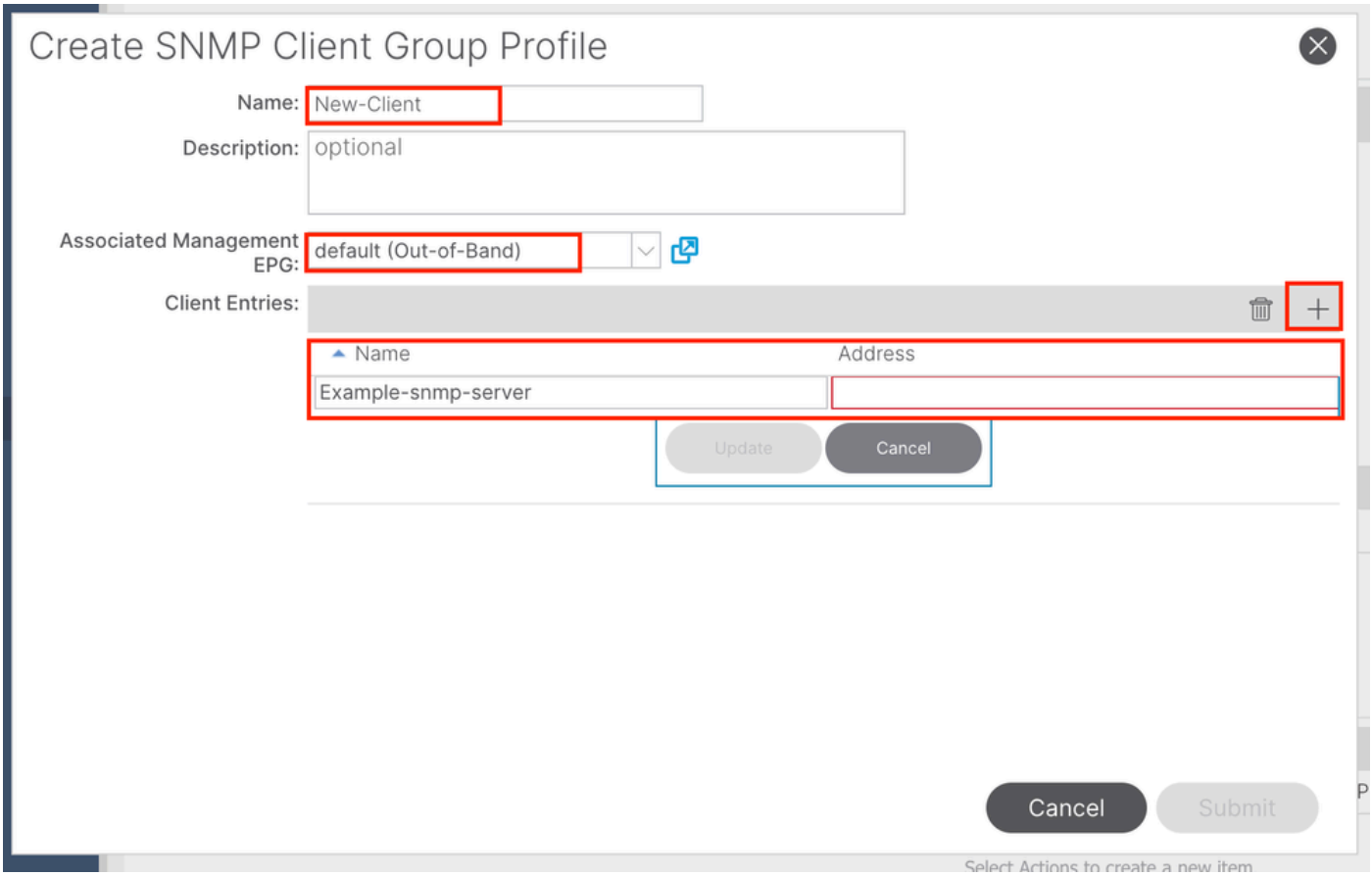
Location - SNMP 정책의 위치입니다.

SNMP v3 Users(SNMP v3 사용자) - SNMP 사용자 프로필은 네트워크의 디바이스를 모니터링하기 위해 사용자를 SNMP 정책과 연결하는 데 사용됩니다.

Community Policies(커뮤니티 정책) - SNMP 커뮤니티 프로필을 사용하면 모니터링을 위해 라우터 또는 스위치 통계에 액세스할 수 있습니다.

클라이언트 그룹 정책:

다음 단계는 클라이언트 그룹 정책/프로필을 추가하는 것입니다. 클라이언트 그룹 정책/프로필의 목적은 APIC 및 패브릭 스위치에서 SNMP 데이터를 가져올 수 있는 IP/서브넷을 정의하는 것입니다.



Name(이름) - 클라이언트 그룹 프로필의 이름입니다. 이 이름은 1~64자의 영숫자로 지정할 수 있습니다.

설명 - 클라이언트 그룹 프로필에 대한 설명입니다. 설명은 0~128자의 영숫자로 구성할 수 있습니다.

EPG(Associated Management End Point Group) - VRF에 액세스할 수 있는 엔드포인트 그룹의 고유 이름입니다. 지원되는 최대 문자열 길이는 255자의 ASCII 문자입니다. 기본값은 관리 테넌트 대역 외 관리 액세스 EPG입니다.

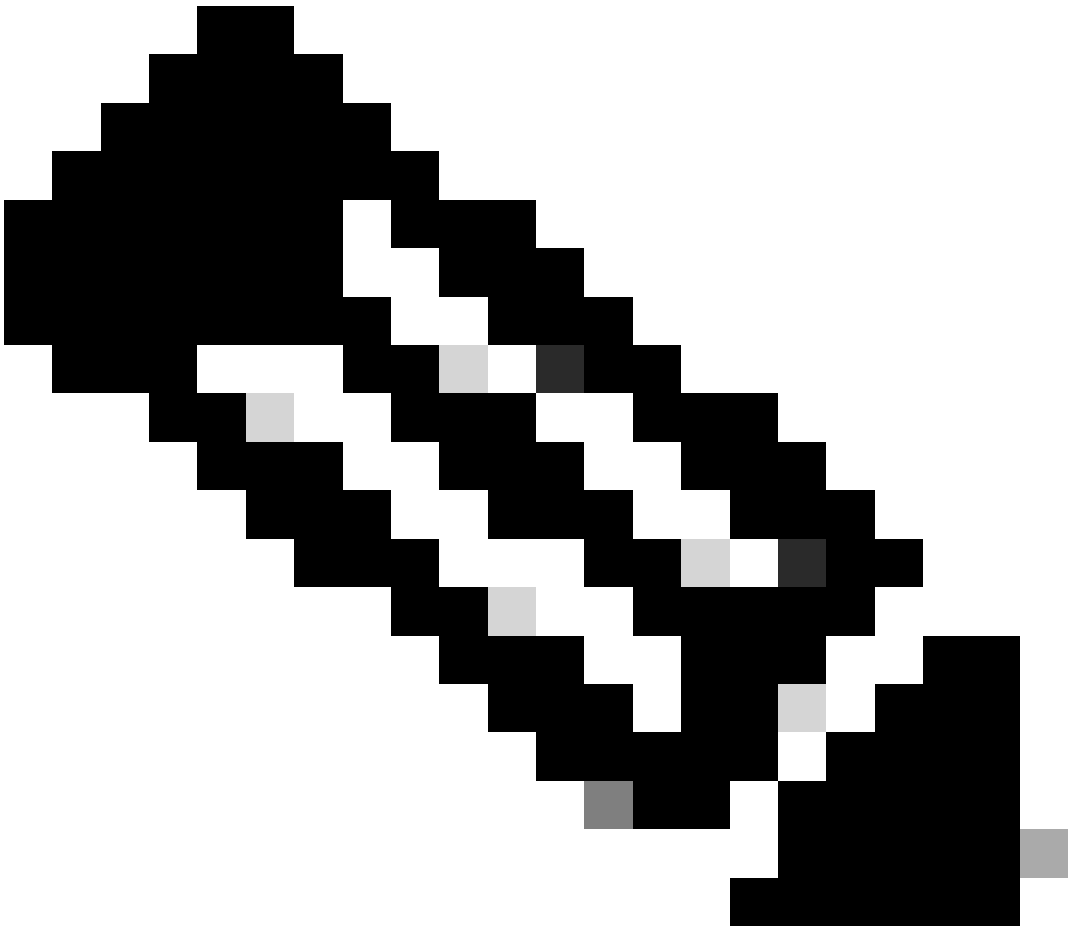
Client Entries(클라이언트 항목) - SNMP 클라이언트 프로파일 IP 주소입니다.

이 문서에서 클라이언트 그룹 정책/프로필은 **New-Client입니다**.

클라이언트 그룹 정책/프로필에서 기본 관리 EPG를 연결해야 합니다. 선택하는 관리 EPG에 SNMP 트래픽(UDP 포트 161 및 162)을 허용하는 데 필요한 계약이 있는지 확인해야 합니다. 기본 대역 외 관리 EPG는 데모용으로 문서에서 사용됩니다.

마지막 단계는 특정 IP 또는 전체 **서브넷 액세스**가 ACI SNMP 데이터를 가져올 수 있도록 클라이언트 항목을 정의하는 것입니다. 특정 IP 또는 전체 서브넷을 정의하기 위한 구문이 있습니다.

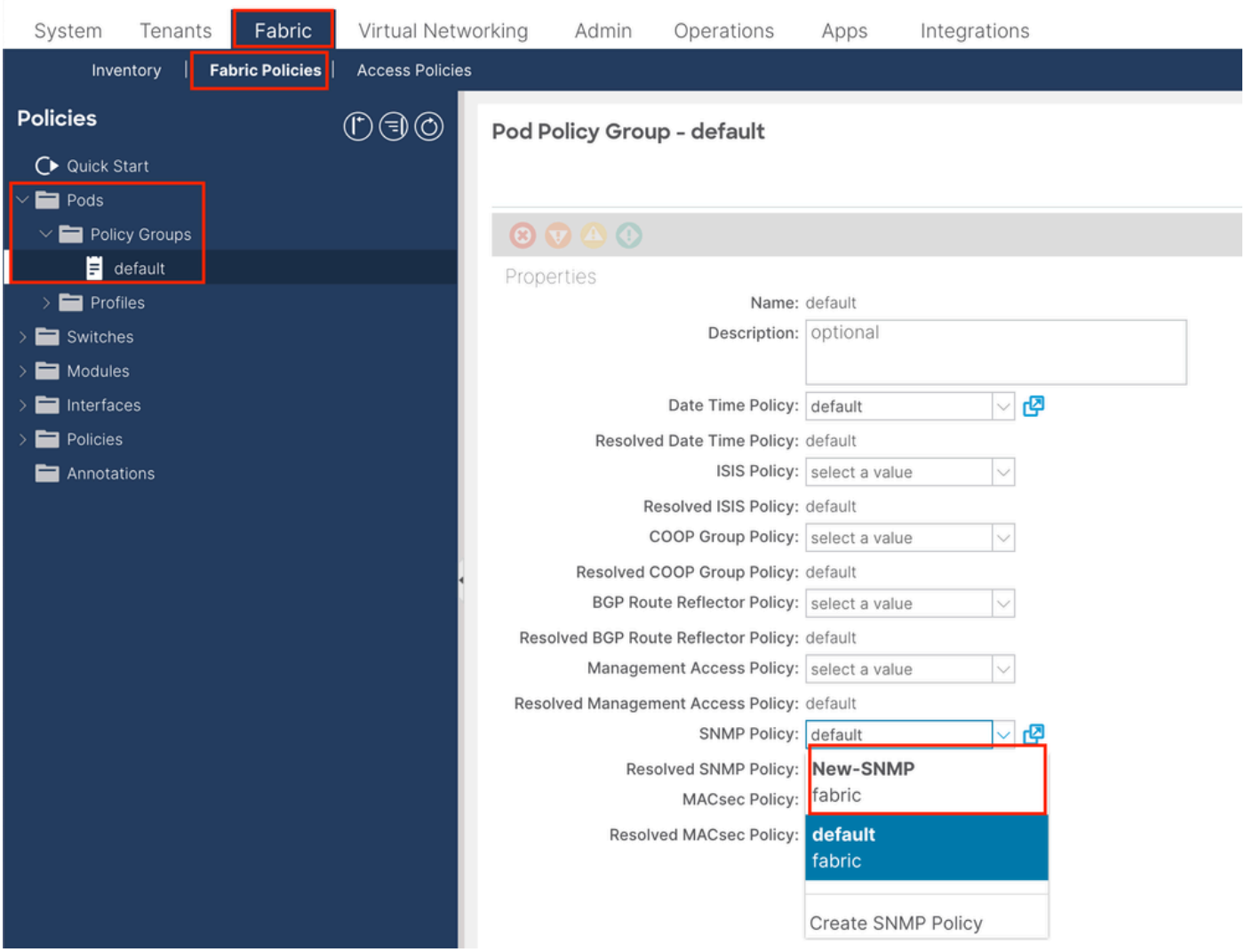
- 특정 호스트 IP: 192.168.1.5
- 전체 서브넷: 192.168.1.0/24



참고: 모든 서브넷을 허용하기 위해 클라이언트 항목에서 0.0.0.0을 사용할 수는 없습니다(모든 서브넷이 SNMP MIB에 액세스하도록 허용하려면 클라이언트 항목을 비워 두십시오).

2단계. SNMP 정책을 포드 정책 그룹(패브릭 정책 그룹)에 적용

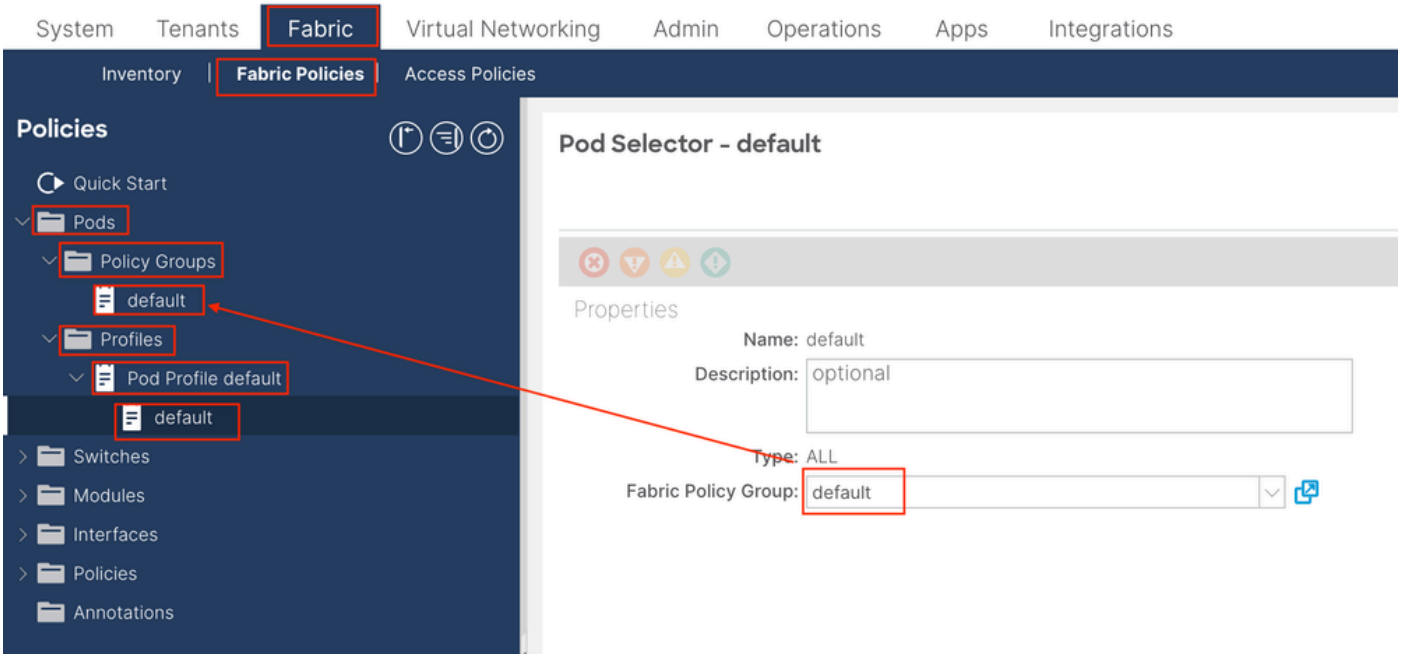
이 컨피그레이션을 적용하려면 APIC 웹 GUI 경로(Fabric > Fabric Policies > Pods > Policy Groups > POD_POLICY_GROUP 문서의 기본값)로 이동합니다.



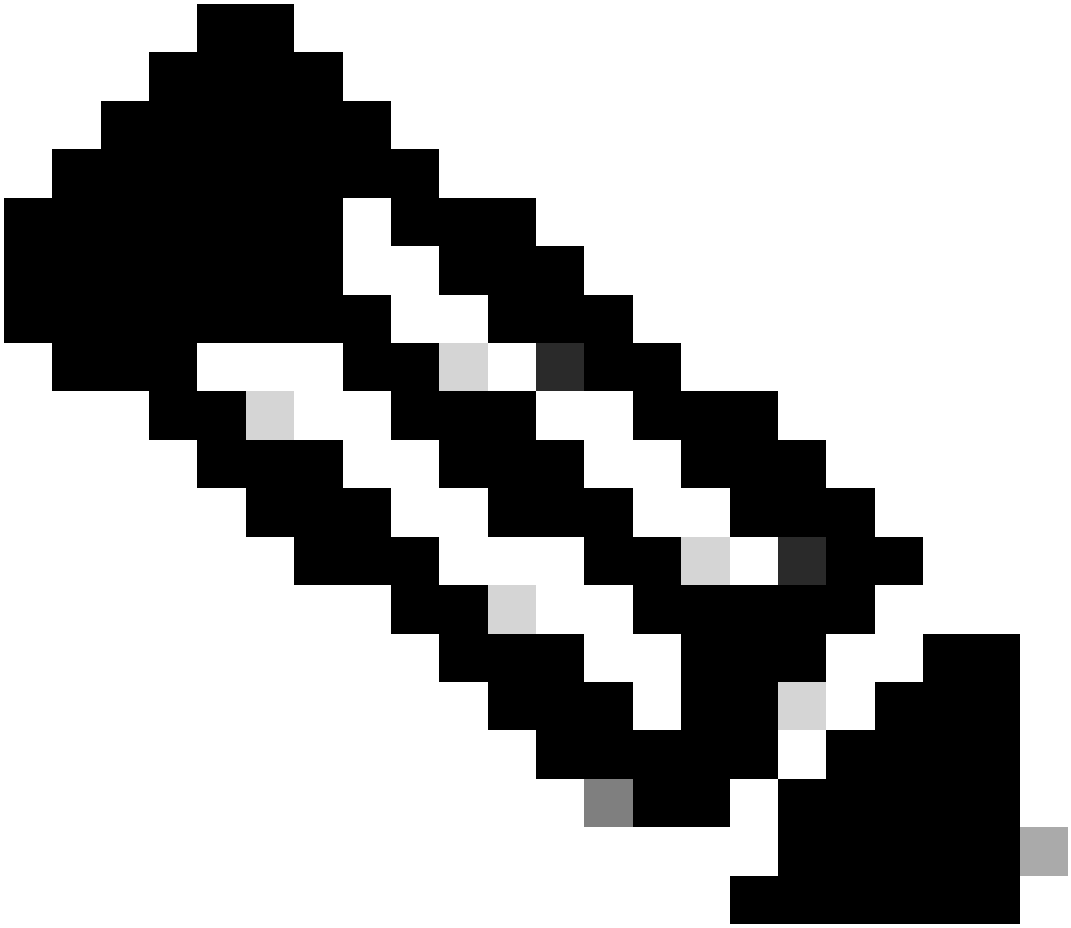
오른쪽 창에 SNMP 정책에 대한 필드가 표시됩니다. 드롭다운에서 새로 생성한 SNMP 정책을 선택하고 변경 사항을 제출합니다.

3단계. 포드 정책 그룹을 포드 프로필과 연결

이 문서에서는 기본 포드 프로파일을 사용하여 간소화합니다. 이렇게 하려면 APIC 웹 GUI 경로(Fabric > Fabric Policies > Pods > Profiles > POD_PROFILE 문서의 기본값)로 이동합니다.



이 단계에서는 전역 MIB에 대한 기본 SNMP를 구성합니다.

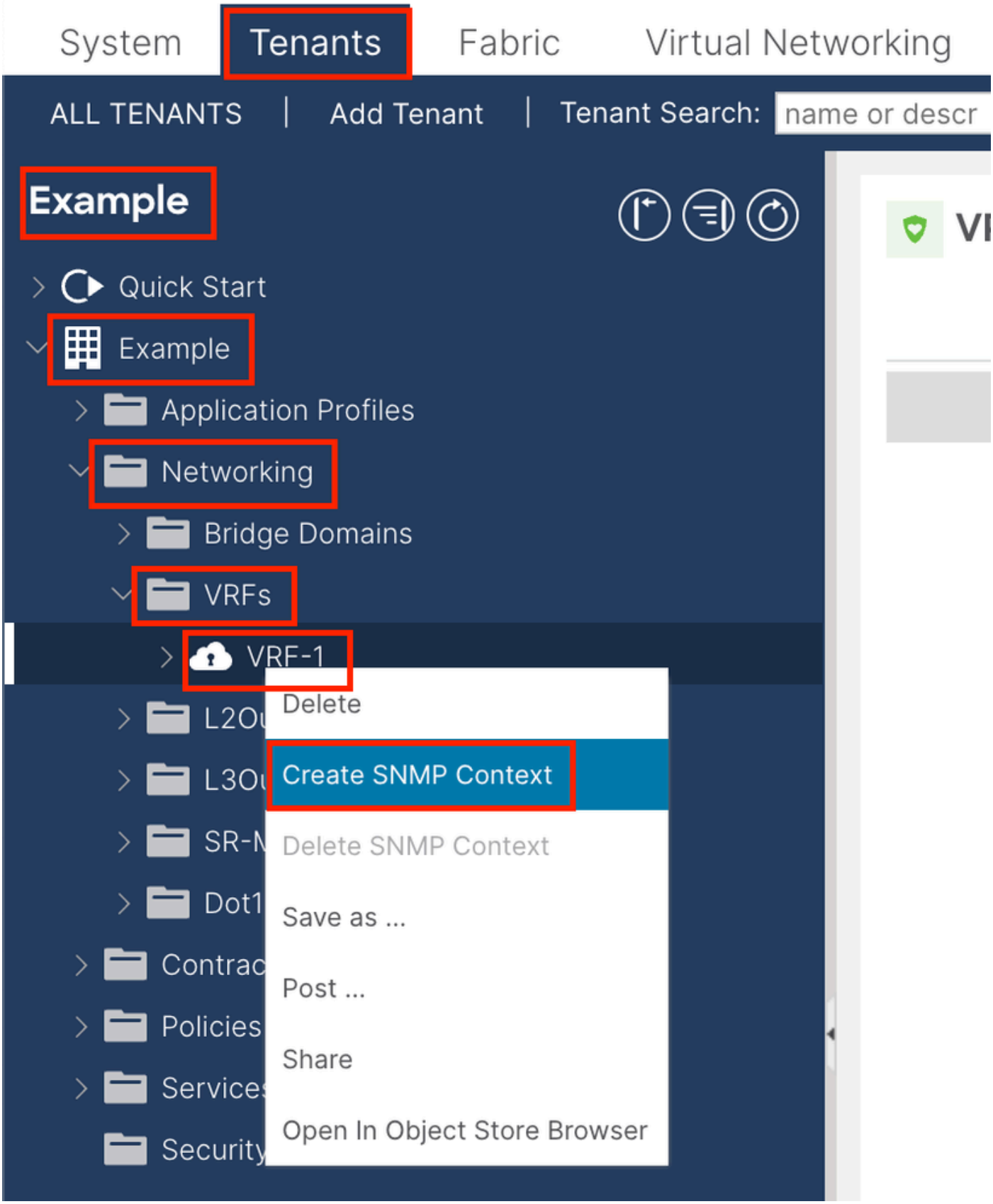


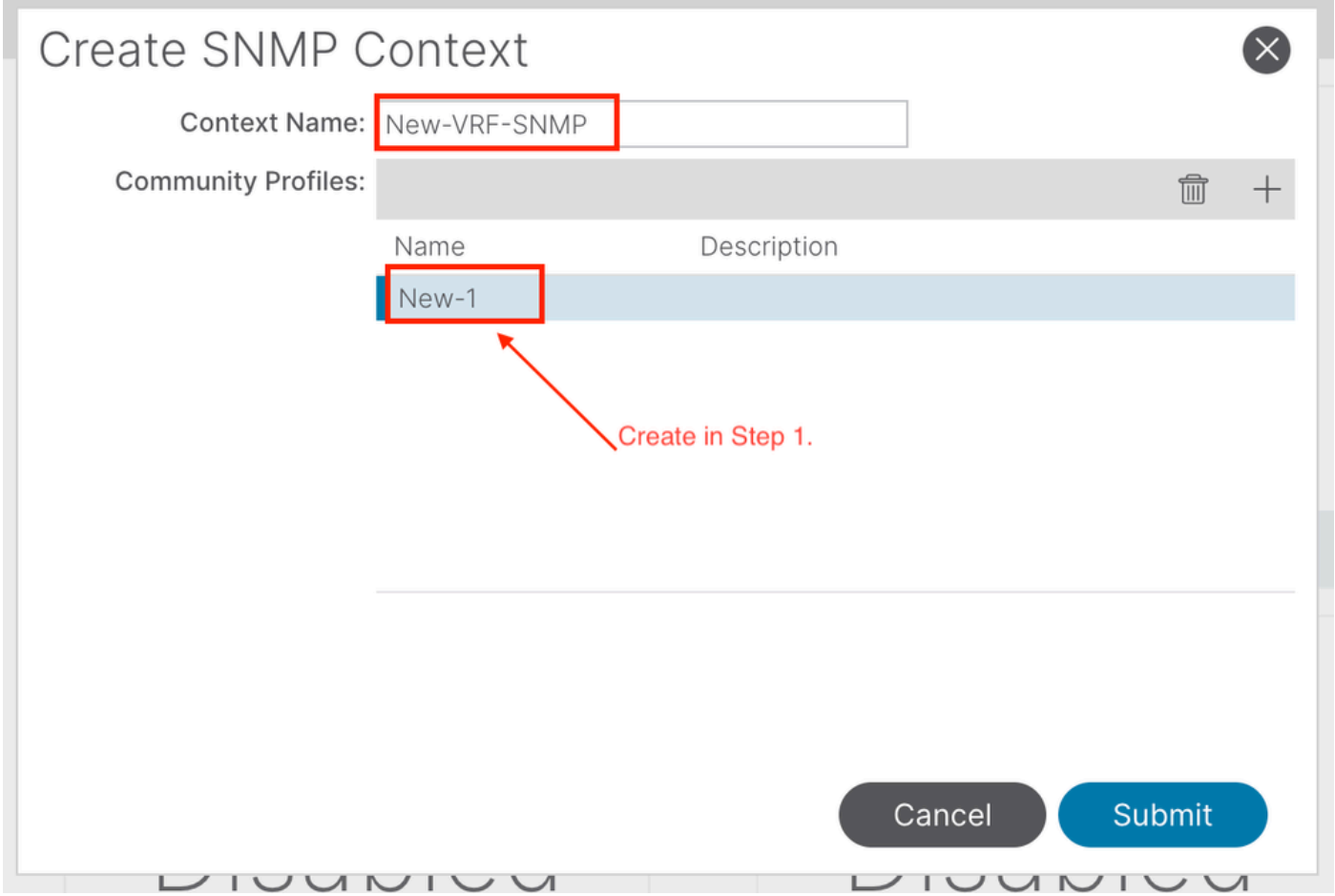
참고: 이 시점에서 SNMP 구성에 필요한 모든 단계(1~3단계)가 완료되었으며 전역 MIB 범위가 암시적으로 사용되었습니다. 그러면 모든 ACI 노드 또는 APIC에 대해 SNMP 워크가 수행됩니다.

4단계. VRF 컨텍스트 범위 구성

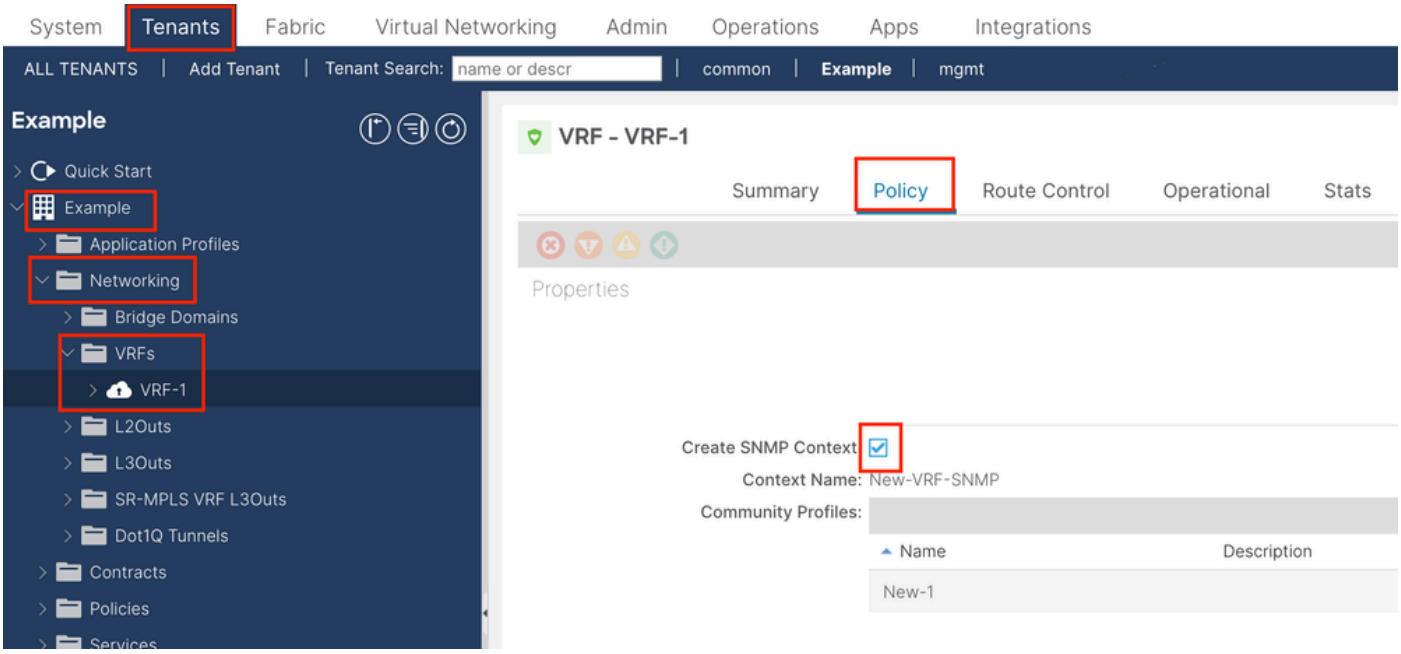
커뮤니티 문자열을 VRF Context에 연결한 후에는 특정 커뮤니티 문자열을 사용하여 전역 범위 SNMP 데이터를 가져올 수 없습니다. 따라서 전역 범위와 VRF 컨텍스트 SNMP 데이터를 모두 가져오려면 두 개의 SNMP 커뮤니티 문자열을 만들어야 합니다.

이 경우, 이전에 생성된 커뮤니티 문자열(1단계), 즉 (**New-1**)은 Example 사용자 지정 테넌트의 VRF 컨텍스트 범위 및 VRF-**1** 사용자 지정 VRF에 **New-1을** 사용합니다. 이렇게 하려면 APIC 웹 GUI 경로로 이동합니다Tenants > Example > Networking > VRFs > VRF-1 (right click) > Create SNMP Context .


System
Tenants
Fabric
Virtual Networking
ALL TENANTS
Add Tenant
Tenant Search:
name or descr
Example
Quick Start
Example
Application Profiles
Networking
Bridge Domains
VRFs
VRF-1
Delete
Create SNMP Context
Delete SNMP Context
Save as ...
Post ...
Share
Open In Object Store Browser



컨피그레이션을 제출한 후 VRF를 마우스 왼쪽 버튼으로 클릭하고 VRF의 Policy(정책) 탭으로 이동한 다음 창 아래쪽으로 스크롤하여 적용한 SNMP Context 컨피그레이션을 확인할 수 있습니다.

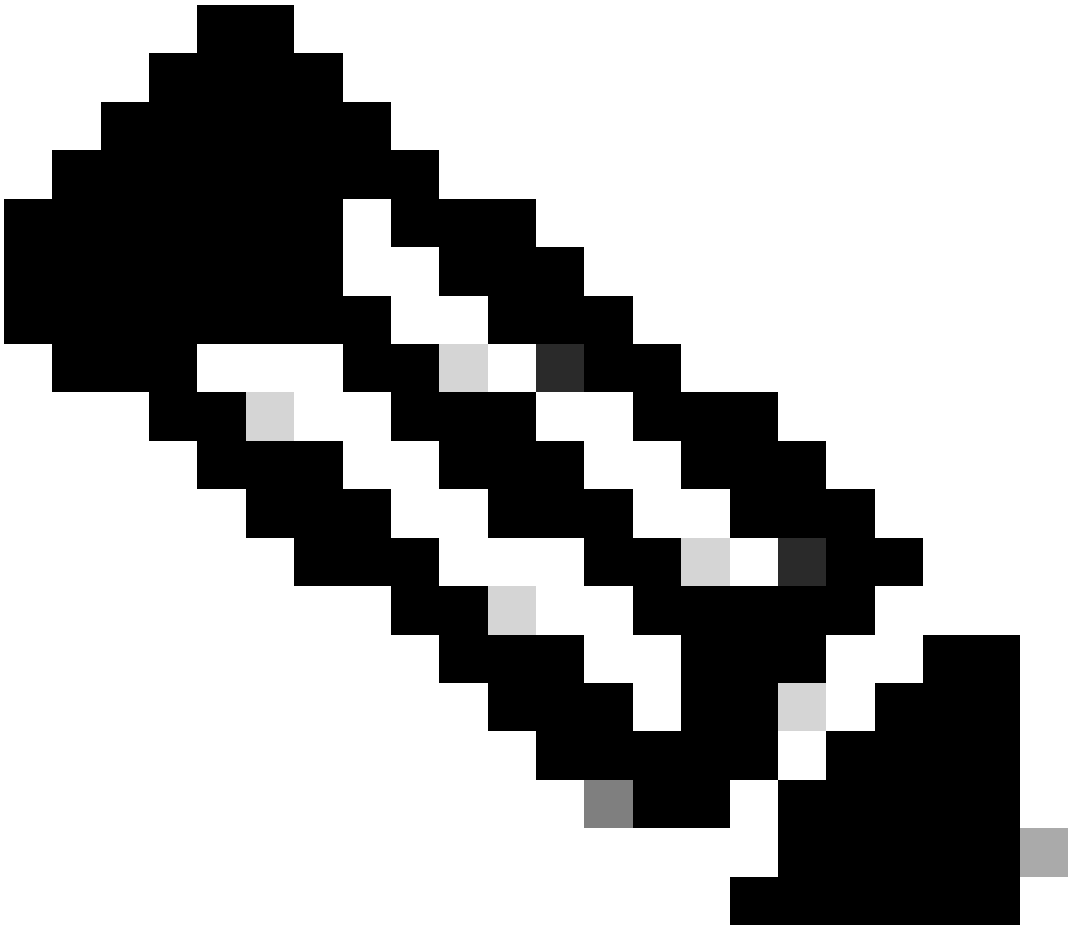


VRF에서 SNMP 컨텍스트를 비활성화하려면 SNMP **컨텍스트 생성** 확인란(스크린샷에 표시됨)의 선택을 취소하거나 VRF를 마우스 오른쪽 버튼으로 클릭하고 SNMP 컨텍스트 삭제를 선택합니다.

GUI를 사용하는 SNMP 트랩 컨피그레이션

SNMP TRAP은 폴링 없이 SNMP 서버(SNMP Destination/Network Management Systems (NMS))로 전송되며, ACI 노드/APIC는 결함/이벤트(정의된 조건)가 발생하면 SNMP TRAP을 전송합니다.

SNMP 트랩은 액세스/패브릭/테넌트 모니터링 정책에서 정책 범위에 따라 활성화됩니다. ACI는 최대 10개의 트랩 수신기를 지원합니다.

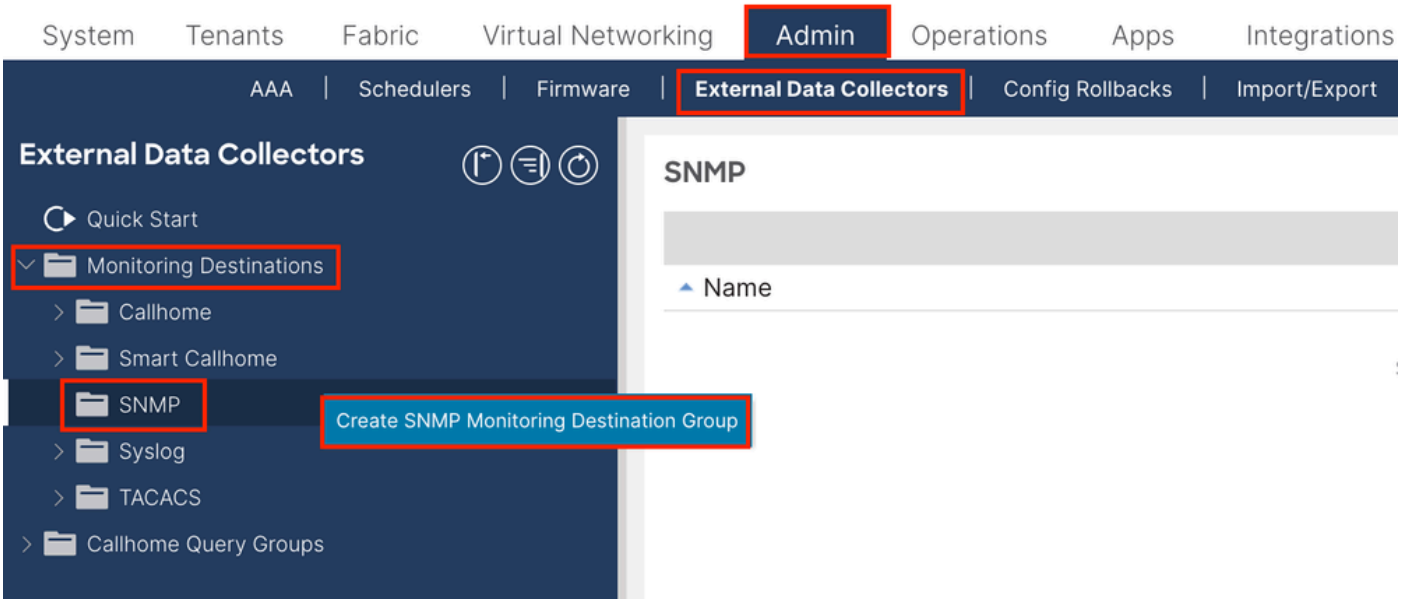


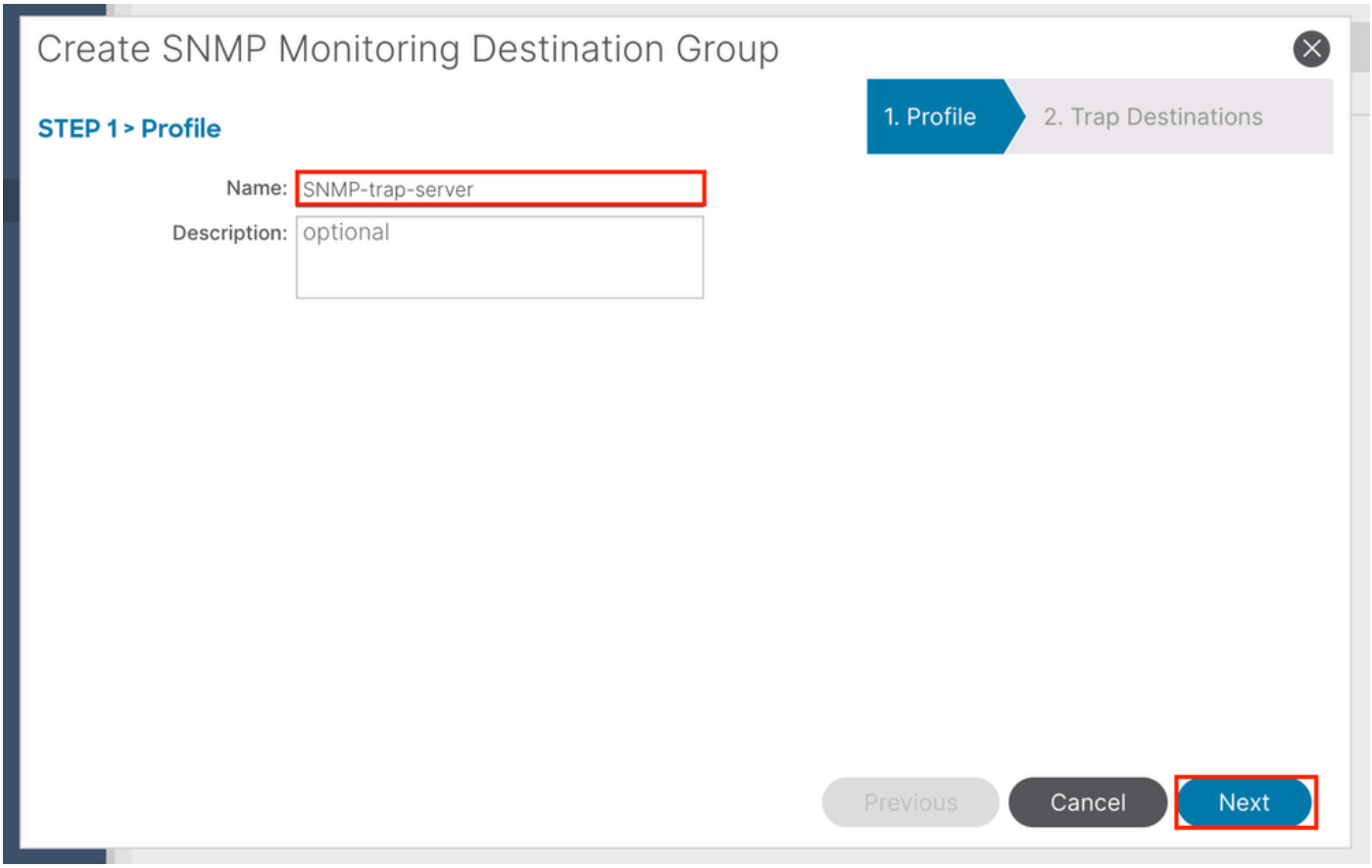
참고: 이전 섹션의 1-3단계가 없으면 SNMP TRAP 컨피그레이션만으로는 충분하지 않습니다. 2단계. SNMP TRAP 컨피그레이션에서는 (액세스/패브릭/테넌트)에 대한 모니터링 정책과 관련이 있습니다.

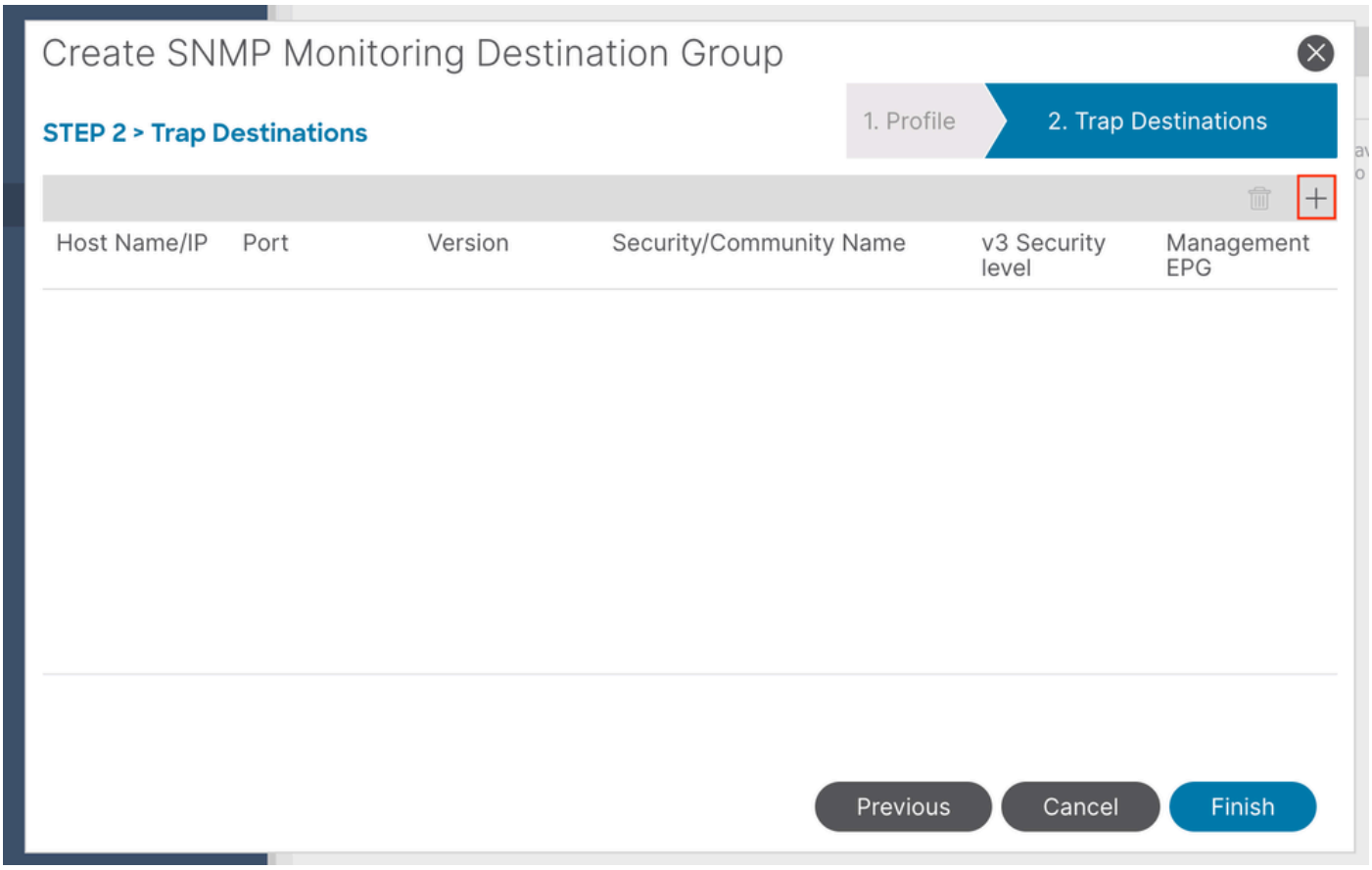
ACI에서 SNMP TRAP을 구성하려면 이전 섹션의 1, 2, 3단계 외에 두 단계가 필요합니다.

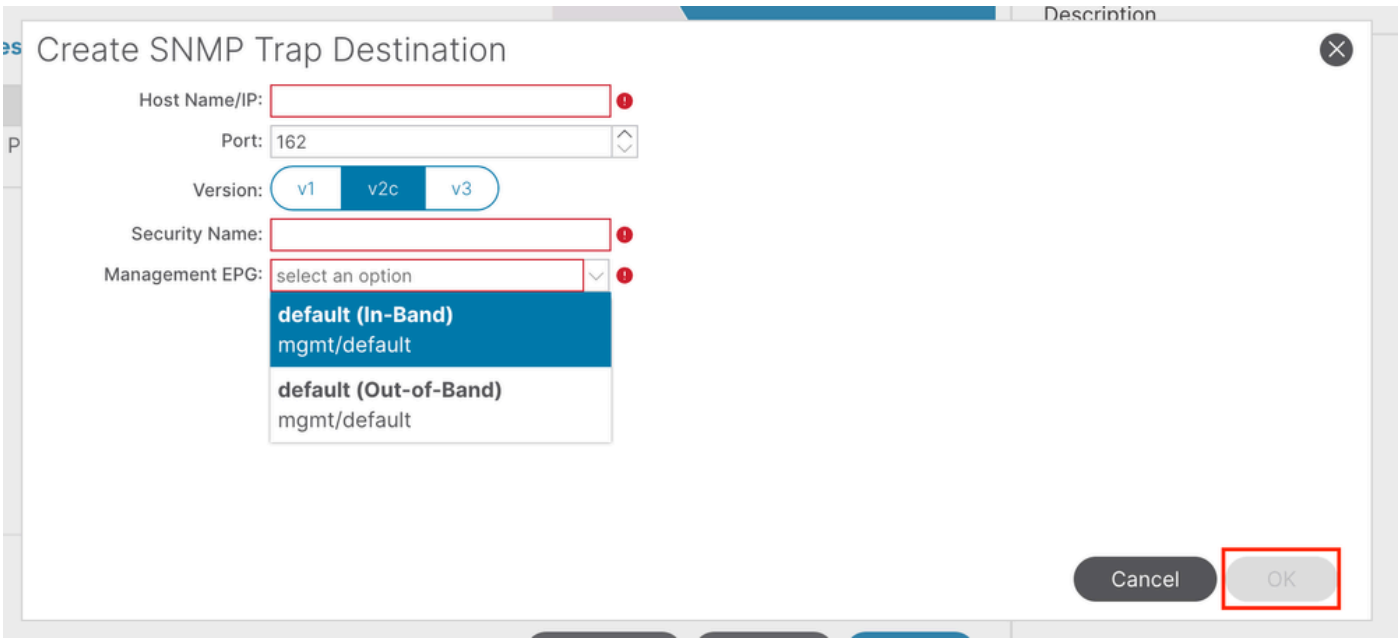
1단계. SNMP 트랩 서버 구성

이렇게 하려면 APIC 웹 GUI 경로로 이동합니다Admin > Eternal Data Collectors > Monitoring Destinations > SNMP.









Host Name/IP - SNMP 트랩 대상의 호스트입니다.

Port - SNMP 트랩 대상의 서비스 포트입니다. 범위는 0(지정되지 않음)부터 65535까지이며 기본값은 162입니다.

Version - SNMP 트랩 대상에 대해 지원되는 CDP 버전입니다. 버전은 다음과 같을 수 있습니다.

- v1 - 사용자 인증에 커뮤니티 문자열 일치를 사용합니다.

- v2c - 사용자 인증에 커뮤니티 문자열 일치를 사용합니다.

- v3 - 네트워크를 통해 프레임을 인증하고 암호화하여 디바이스에 대한 보안 액세스를 제공하는 네트워크 관리를 위한 상호 운용 가능한 표준 기반 프로토콜입니다.

기본값은 **v2c입니다**.

Security Name(보안 이름) - SNMP 트랩 대상 보안 이름(커뮤니티 이름)입니다. @기호를 포함할 수 없습니다.

v.3 Security Level - SNMP 대상 경로에 대한 SNMPv3 보안 레벨입니다. 레벨은 다음과 같을 수 있습니다.

- 인증

- noauth

- 개인

기본값은 noauth**입니다**.

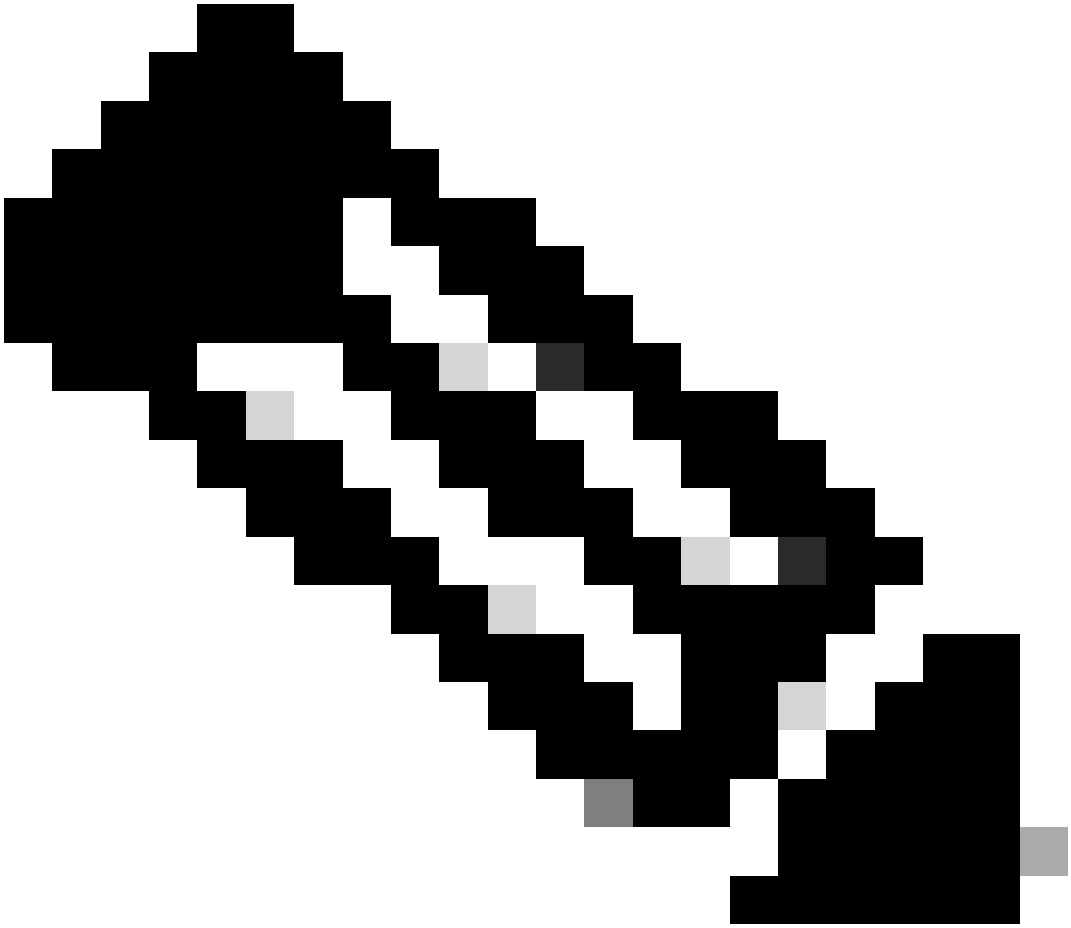
관리 EPG - 원격 호스트에 연결할 수 있는 SNMP 대상의 관리 엔드포인트 그룹 이름입니다.

2단계. (액세스/패브릭/테넌트) 모니터링 정책에서 SNMP 트랩 소스 구성

다음과 같은 세 가지 범위로 모니터링 정책을 생성할 수 있습니다.

- 액세스 - 액세스 포트, FEX, VM 컨트롤러
- 패브릭 - 패브릭 포트, 카드, 섀시, 팬

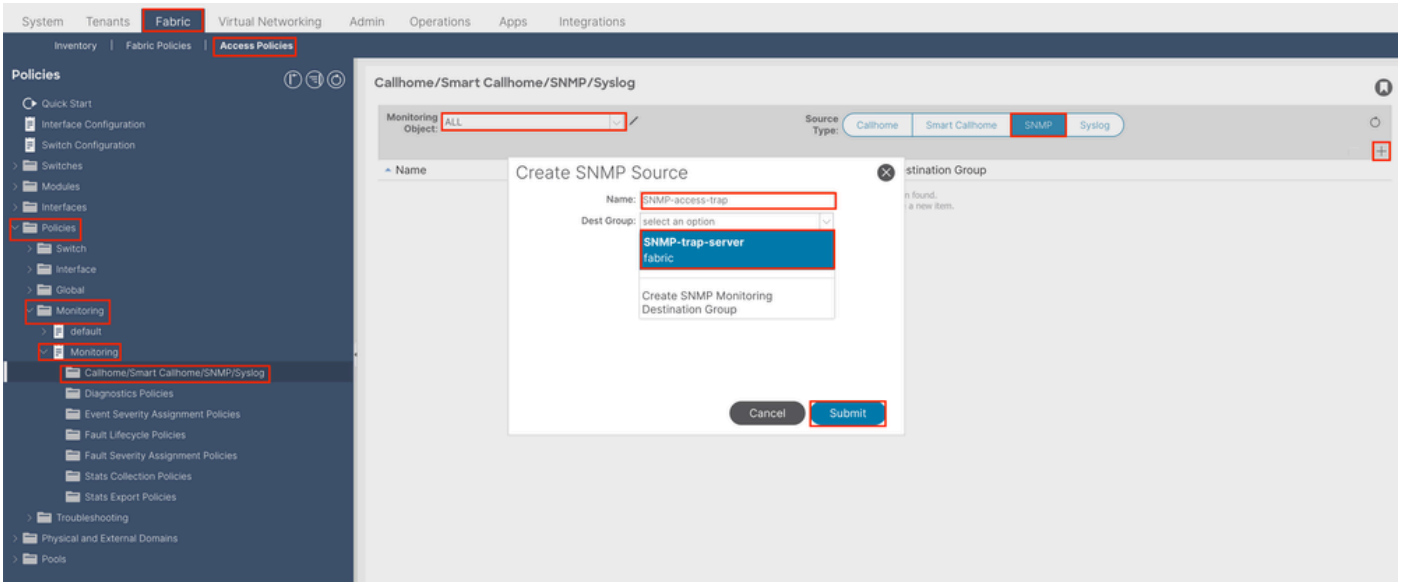
- 테넌트 - EPG, 애플리케이션 프로파일, 서비스

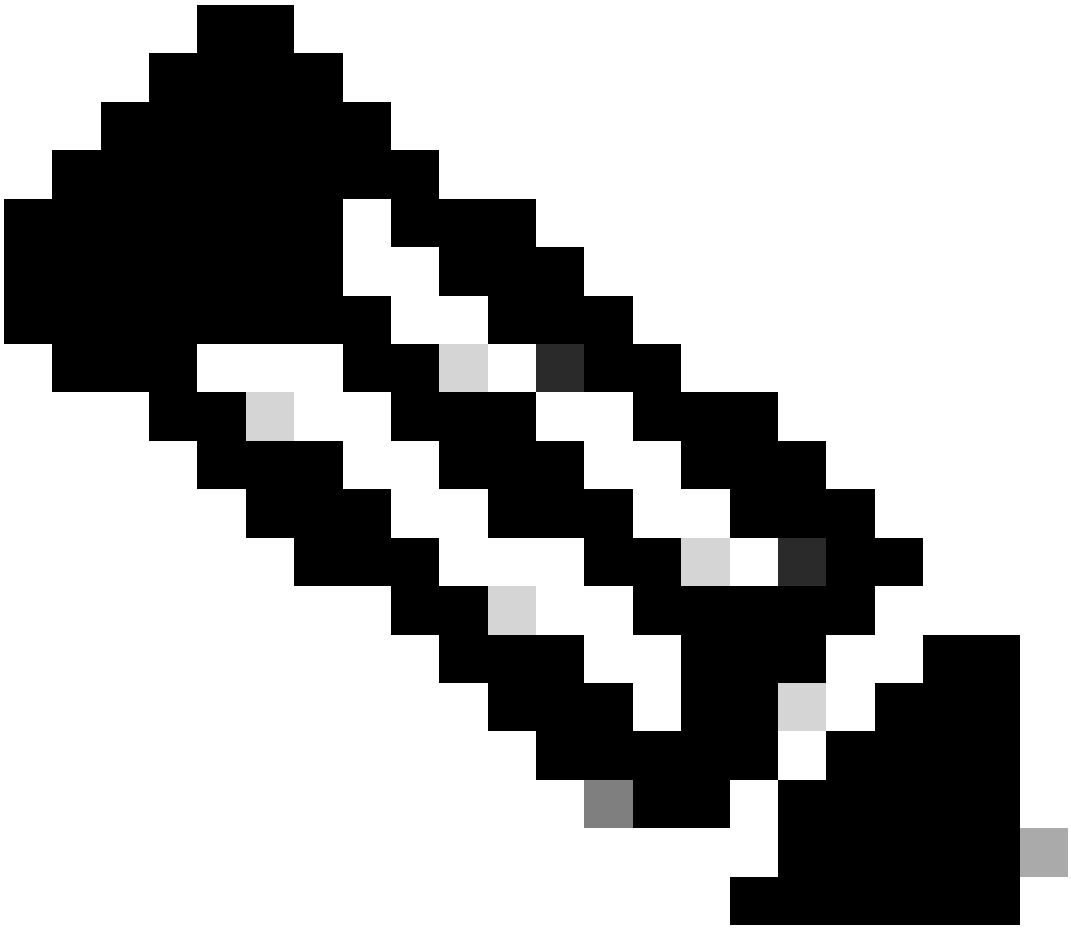


참고: 필요에 따라 구성하기 위해 하나 또는 그 조합을 선택할 수 있습니다.

옵션 1. 액세스 정책에서 SNMP 소스 정의

이렇게 하려면 APIC 웹 GUI 경로로 이동합니다Fabric > Access Polices > Polices > Monitoring > Default > Callhome/Smart Callhome/SNMP/Syslog/TACACS.

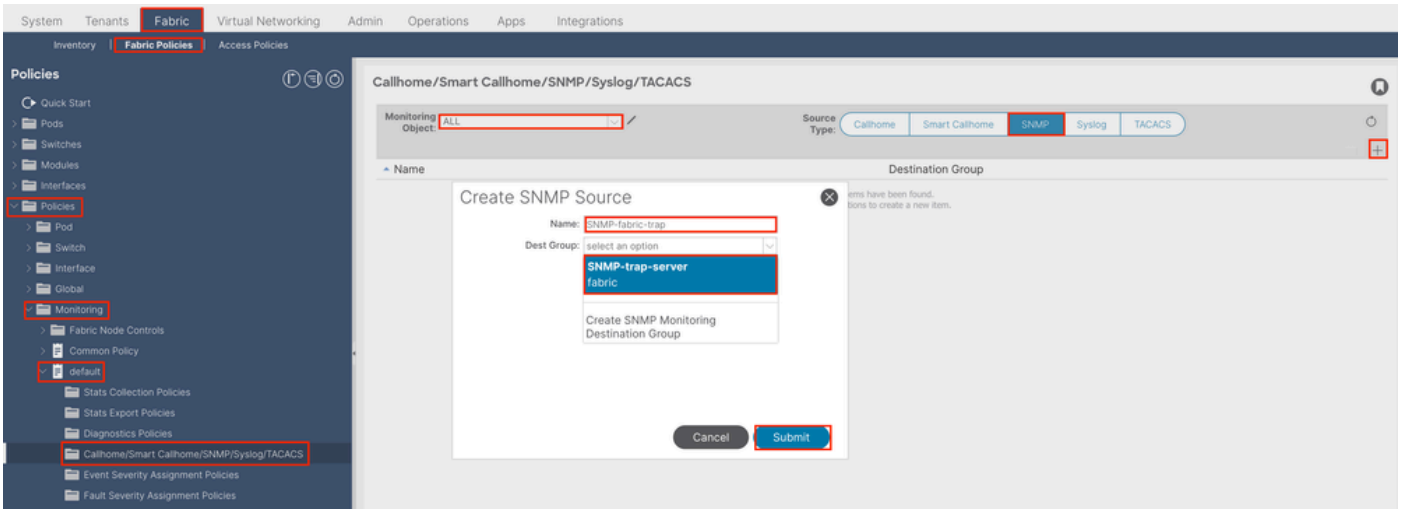

System
Tenants
Fabric
Virtual Networking
Admin
Operations
Apps
Integrations
Inventory
Fabric Policies
Access Policies
Policies
Quick Start
Interface Configuration
Switch Configuration
Switches
Modules
Interfaces
Policies
Switch
Interface
Global
Monitoring
default
Monitoring
Callhome/Smart Callhome/SNMP/Syslog
Diagnostics Policies
Event Severity Assignment Policies
Fault Lifecycle Policies
Fault Severity Assignment Policies
Stats Collection Policies
Stats Export Policies
Troubleshooting
Physical and External Domains
Pools
Callhome/Smart Callhome/SNMP/Syslog
Monitoring Object:
ALL
Source Type:
Callhome
Smart Callhome
SNMP
Syslog
Name
Create SNMP Source
Name:
SNMP-access-trap
Dest Group:
select an option
SNMP-trap-server
fabric
Create SNMP Monitoring Destination Group
Cancel
Submit



참고: 사용자 정의 모니터링 정책(구성된 경우)을 기본 정책 대신 사용할 수 있습니다. 여기서 기본 정책을 사용합니다. 모니터링할 모니터링 객체를 지정할 수 있습니다. 모두 여기에서 사용되었습니다.

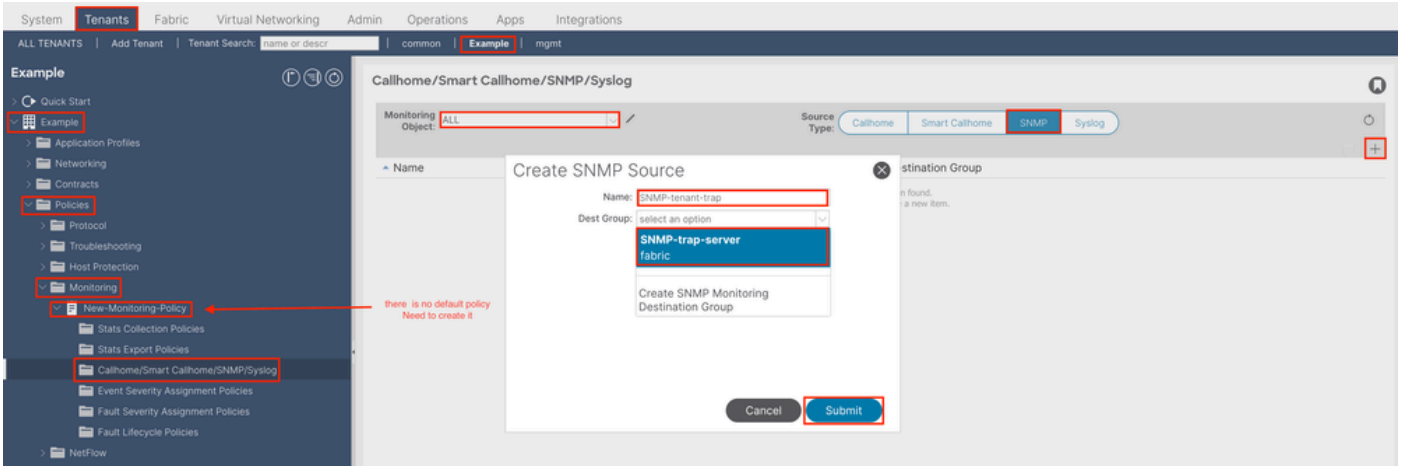
옵션 2. 패브릭 정책에서 SNMP 소스 정의

이렇게 하려면 APIC 웹 GUI 경로로 이동합니다Fabric > Fabric Polices > Polices > Monitoring > Default > Callhome/Smart Callhome/SNMP/Syslog/TACACS.



옵션 3. 테넌트 정책에서 SNMP 소스 정의

이렇게 하려면 APIC 웹 GUI 경로로 이동합니다Tenant > (Tenant Name) > Polices > Monitoring > (Custom monitoring policy) > Callhome/Smart Callhome/SNMP/Syslog/TACACS.



다음을 확인합니다.

snmpwalk 명령을 사용하여 확인

먼저 leaf 스위치의 전역 범위에서 SNMP 데이터를 가져옵니다. snmpwalk 명령을 사용하면 이 작업을 수행할 수 있습니다snmpwalk -v

2c -c New-1 x.x.x.x.

이 분할 명령은 다음을 나타냅니다.

snmpwalk = MacOS/Linux/Windows에 설치된 snmpwalk 실행 파일
-v = 사용할 SNMP 버전을 지정합니다.
2c= SNMP 버전 2c를 사용하도록 지정합니다.
-c= 특정 커뮤니티 문자열을 지정합니다
New-1= 커뮤니티 문자열은 전역 범위 SNMP 데이터를 가져오는 데 사용됩니다.
x.x.x.x= 내 리프 스위치의 대역 외 관리 IP 주소

명령 결과:

```
$ snmpwalk -v 2c -c New-1 x.x.x.x SNMPv2-MIB::sysDescr.0 = STRING: Cisco NX-OS(tm) aci, Software (aci-n
```

스니핑된 명령 출력에서 snmpwalk가 성공적이며 하드웨어별 정보가 풀링되었음을 확인할 수 있습니다. snmpwalk를 계속 진행하면 하드웨어 인터페이스 이름, 설명 등이 표시됩니다.

이제 SNMP 커뮤니티 문자열 New-**1**을 사용하여 VRF용 **New-VRF-SNMP**, 이전에 생성된 SNMP 컨텍스트, VRF 컨텍스트 SNMP 데이터를 **검색합니다**.

동일한 커뮤니티 문자열 **New-1**이 두 개의 다른 SNMP 컨텍스트에 사용되므로 SNMP 데이터를 가져올 SNMP 컨텍스트를 지정해야 합니다. 특정 SNMP 컨텍스트를 지정하는 데 사용해야 하는 snmpwalk 구문이 있습니다snmpwalk -v 2c -c New-1@New-VrF-SNMP 10.x.x.x.

특정 SNMP 컨텍스트에서 가져오려면 다음 형식을 사용합니다. COMMUNITY_NAME_HERE@SNMP_CONTEXT_NAME_HERE .

CLI Show 명령 사용

APIC의 경우:

```
show snmp show snmp policy <SNMP_policy_name> show snmp summary show snmp clientgroups show snmp commun
```

스위치:

```
show snmp show snmp | grep "SNMP packets" show snmp summary show snmp community show snmp host show snm
```

CLI Moquery 명령 사용

APIC/스위치에서:

```
moquery -c snmpGroup #The SNMP destination group, which contains information needed to send traps or in
```

CLI cat 명령 사용

APIC의 경우:

```
cat /aci/tenants/mgmt/security-policies/out-of-band-contracts/summary cat /aci/tenants/mgmt/security-po
```

문제 해결

snmpd 프로세스 확인

스위치:

```
ps aux | grep snmp pidof snmpd
```

APIC의 경우:

```
ps aux | grep snmp
```

정상적인 프로세스라면 Cisco TAC에 문의하십시오.

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.