

在ACI中配置SNMP

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[瞭解SNMP範圍](#)

[配置步驟 \(適用於全局和VRF情景範圍\)](#)

[步驟 1.配置SNMP交換矩陣策略](#)

[步驟 2.將SNMP策略應用於Pod策略組 \(交換矩陣策略組\)](#)

[步驟 3.將Pod策略組與Pod配置檔案關聯](#)

[步驟 4.配置VRF情景範圍](#)

[使用GUI配置SNMP陷阱](#)

[步驟 1.配置SNMP TRAP Server](#)

[步驟 2.在 \(訪問/交換矩陣/租戶\) 監控策略下配置SNMP陷阱源](#)

[選項 1.在訪問策略下定義SNMP源](#)

[選項 2.在Fabric Policies \(交換矩陣策略\) 下定義SNMP源](#)

[選項 3.在租戶策略下定義SNMP源](#)

[驗證](#)

[使用snmpwalk命令進行驗證](#)

[使用CLI Show命令](#)

[使用CLI Moquery命令](#)

[使用CLI cat命令](#)

[疑難排解](#)

[檢查snmpd流程](#)

簡介

本文檔介紹ACI中簡單網路管理協定(SNMP)和SNMP陷阱的配置。

必要條件

需求

思科建議您瞭解以下主題：

- [結構發現已完成](#)
- [與應用策略基礎設施控制器\(APIC\)和交換矩陣交換機的帶內/帶外連線](#)
- [帶內/帶外合約配置為允許SNMP流量 \(UDP埠161和162 \)](#)
- [在預設管理租戶下為APIC和交換矩陣交換機配置的靜態節點管理地址 \(如果沒有此地址，從APIC提取SNMP資訊將失敗 \)](#)

- 瞭解SNMP協定工作流程

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- APIC
- 瀏覽器
- 運行5.2 (8e)的以應用為中心的基礎設施(ACI)
- Snmpwalk 指令

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。

設定

思科ACI提供SNMPv1、v2c和v3支援，包括管理資訊庫(MIB)和通知（陷阱）。SNMP標準允許支援不同MIB的任何第三方應用管理和監控ACI枝葉和主幹交換機以及APIC控制器。

但是，ACI不支援SNMP寫入命令(Set)。

SNMP策略在枝葉和主幹交換機以及APIC控制器上獨立應用和運行。由於每個ACI裝置都有自己的SNMP實體，即一個APIC集群中的多個APIC必須與交換機分開監控。但是，SNMP策略源是作為整個ACI交換矩陣的監控策略建立的。

預設情況下，SNMP使用UDP 埠161 進行輪詢，使用162 埠進行TRAP。

瞭解SNMP範圍

ACI中SNMP的一個快速基本概念是，SNMP資訊可以從兩個範圍中提取：

1. 全球
2. 虛擬路由和轉發(VRF)環境

Global Scope是抽取枝葉/主幹節點的介面數、介面索引、介面名稱、介面狀態等機箱MIB。

VRF上下文範圍特定的MIB提取特定於VRF的資訊，例如IP地址和路由協定資訊。

在[Cisco ACI MIB 支援清單](#)中有受支援的APIC和交換矩陣交換機全局和VRF情景MIB的完整清單。



註：具有全局範圍的MIB在系統中只有一個例項。全局MIB中的資料與整個系統相關。

具有VRF特定範圍的MIB可以在系統中具有每個VRF例項。VRF特定MIB中的資料僅與該VRF相關。

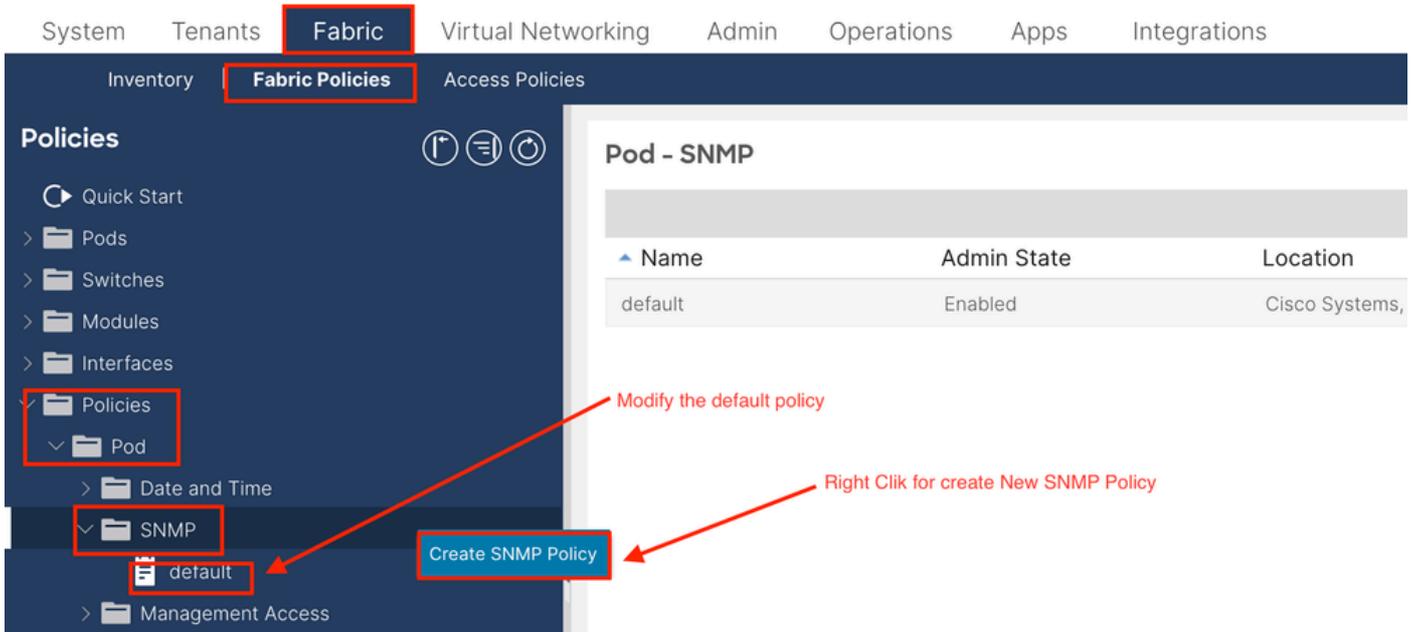
配置步驟 (適用於全局和VRF情景範圍)

步驟 1. 配置SNMP交換矩陣策略



注意：此處指定了SNMP設定，如SNMP社群策略和SNMP客戶端組策略。

配置SNMP的第一步是建立必要的SNMP交換矩陣策略。要建立SNMP交換矩陣策略，請導航到APIC Web GUI路徑；Fabric > Fabric Policies > Policies > Pod > SNMP。



您可以建立新的SNMP策略或修改預設SNMP策略。

在本文檔中，SNMP策略稱為New-SNMP，使用SNMP版本v2c，因此此處需要的唯一欄位是社群策略和客戶端組策略。

Community Policy Name欄位定義要使用的SNMP社群字串。就我們而言，是New-1。你看看這兩個團體後來會變成什麼樣子。

Create SNMP Policy

Name:

Description:

Admin State: Disabled Enabled

Contact:

Location:

Community Policies:

Name	Description
New-1	

SNMP v3 Users:

Name	Authorization Type	Privacy Type
------	--------------------	--------------

Client Group Policies:

Name	Description	Client Entries	Associated Management EPG
------	-------------	----------------	---------------------------

Trap Forward Servers:

IP Address	Port
------------	------

Name - SNMP策略的名稱。此名稱可以是1到64個字母數字字元。

Description - SNMP策略的說明。說明可以是0到128個字母數字字元。

管理狀態- SNMP策略的管理狀態。狀態可以是啟用或停用。狀態包括：

- 已啟用-管理狀態已啟用
- 已停用-管理狀態已停用

預設值為disabled。

Contact - SNMP策略的聯絡人資訊。

Location - SNMP策略的位置。

SNMP v3使用者 - SNMP使用者配置檔案用於將使用者與用於監控網路中裝置的SNMP策略相關聯。

社群策略- SNMP社群配置檔案允許訪問路由器或交換機統計資訊以進行監控。

客戶端組策略：

下一步是增加客戶端組策略/配置檔案。客戶端組策略/配置檔案的目的是定義哪些IP/子網能夠從APIC和交換矩陣交換機提取SNMP資料：

Create SNMP Client Group Profile

Name: New-Client

Description: optional

Associated Management EPG: default (Out-of-Band)

Client Entries:

Name	Address
Example-snmp-server	

Update Cancel

Cancel Submit

Select Actions to create a new item

名稱- 客戶端組配置檔案的名稱。此名稱可以是1到64個字母數字字元。

Description - 客戶端組配置檔案的說明。說明可以是0到128個字母數字字元。

Associated Management End Point Group (EPG) - 可透過其訪問VRF的終端組的可分辨名稱。支援的最大字串長度為255個ASCII字元。預設為管理租戶帶外管理訪問EPG。

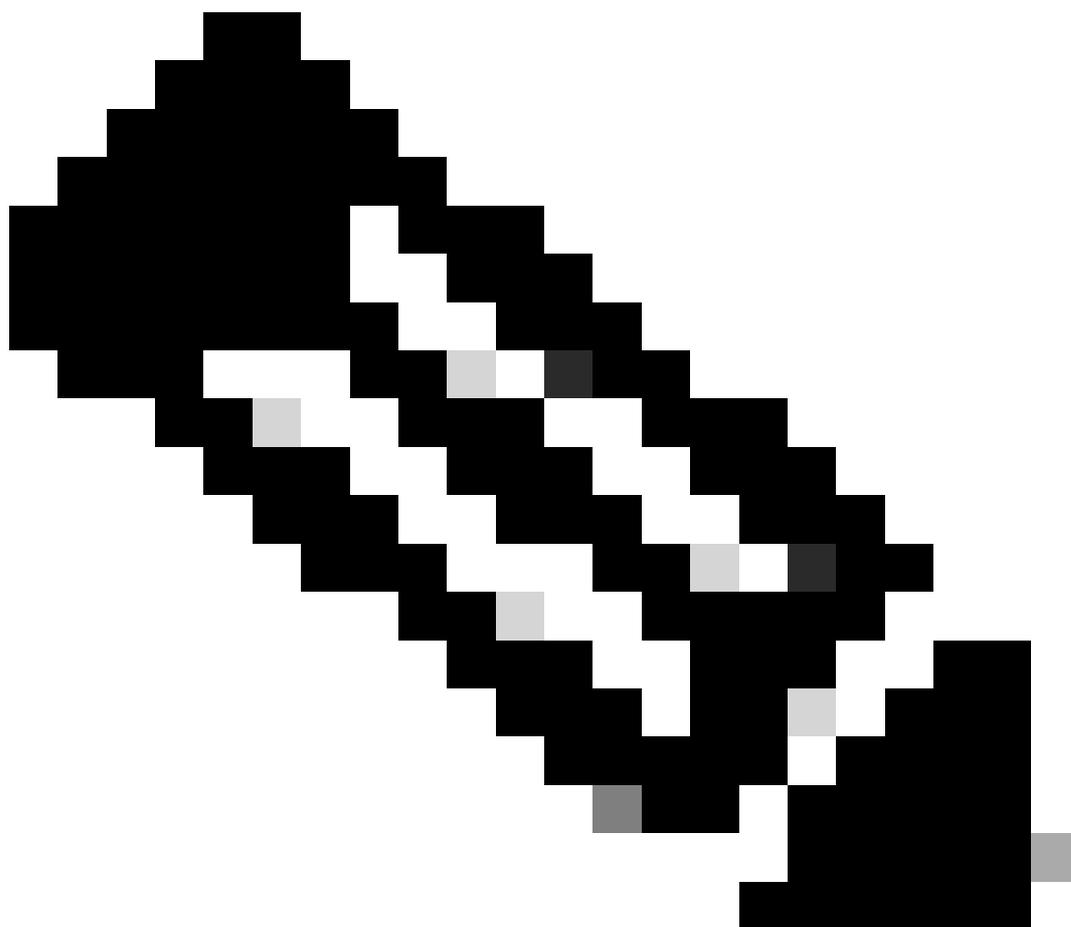
Client Entries - SNMP客戶端配置檔案IP地址。

在本文檔中，客戶端組策略/配置檔案稱為New-Client。

在客戶端組策略/配置檔案中，必須關聯首選管理EPG。您必須確保您選擇的管理EPG具有允許SNMP流量的必要合約 (UDP埠161和162)。本文檔中預設帶外管理EPG用於演示目的。

最後一步是定義客戶端條目，以便允許特定IP或整個子網訪問提取ACI SNMP資料。以下是用於定義特定IP或整個子網的語法：

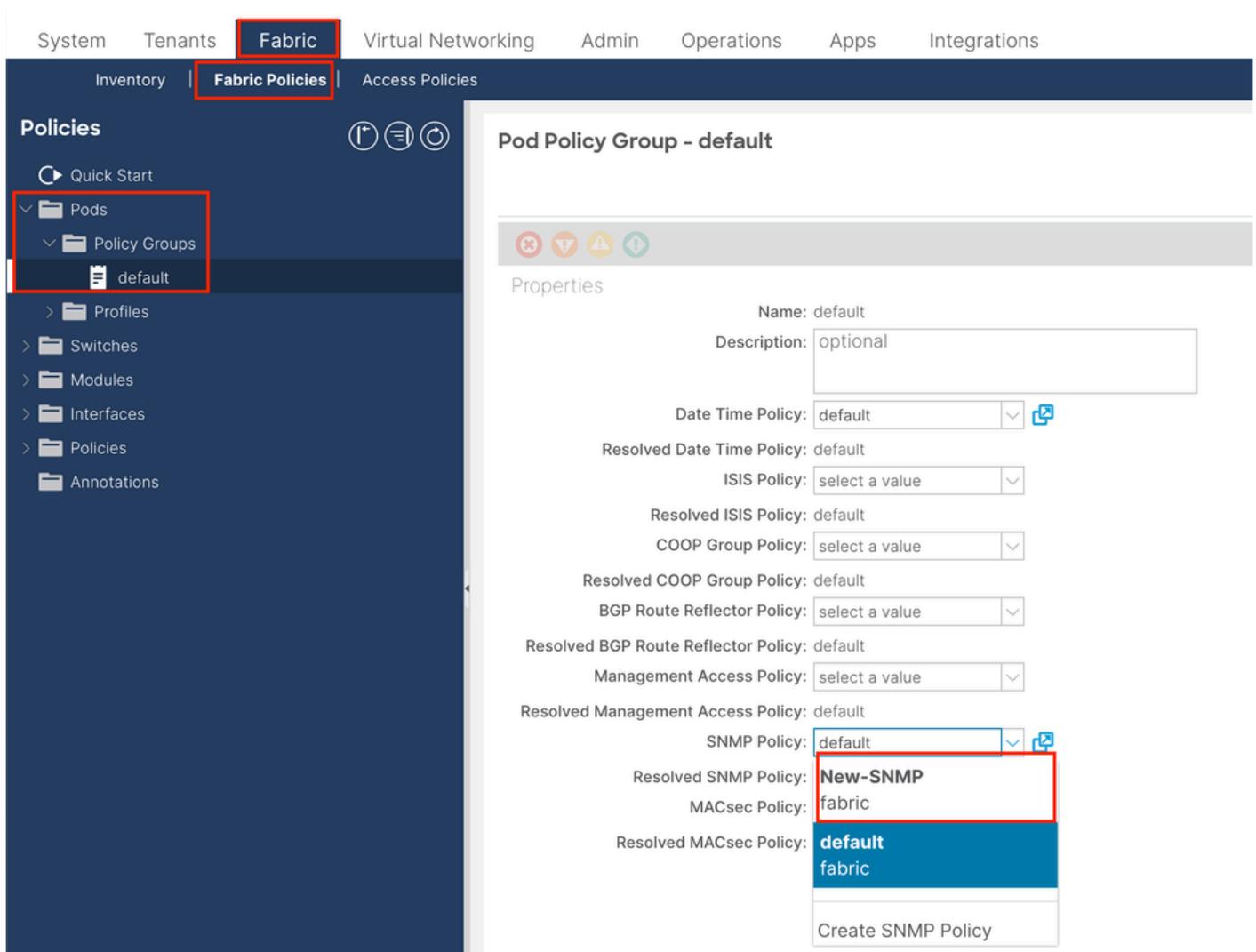
- 特定主機IP：192.168.1.5
- 整個子網：192.168.1.0/24



注意：不能在客戶端條目中使用0.0.0.0以允許所有子網 (如果要允許所有子網訪問SNMP MIB，只需將客戶端條目留空)。

步驟 2.將SNMP策略應用於Pod策略組 (交換矩陣策略組)

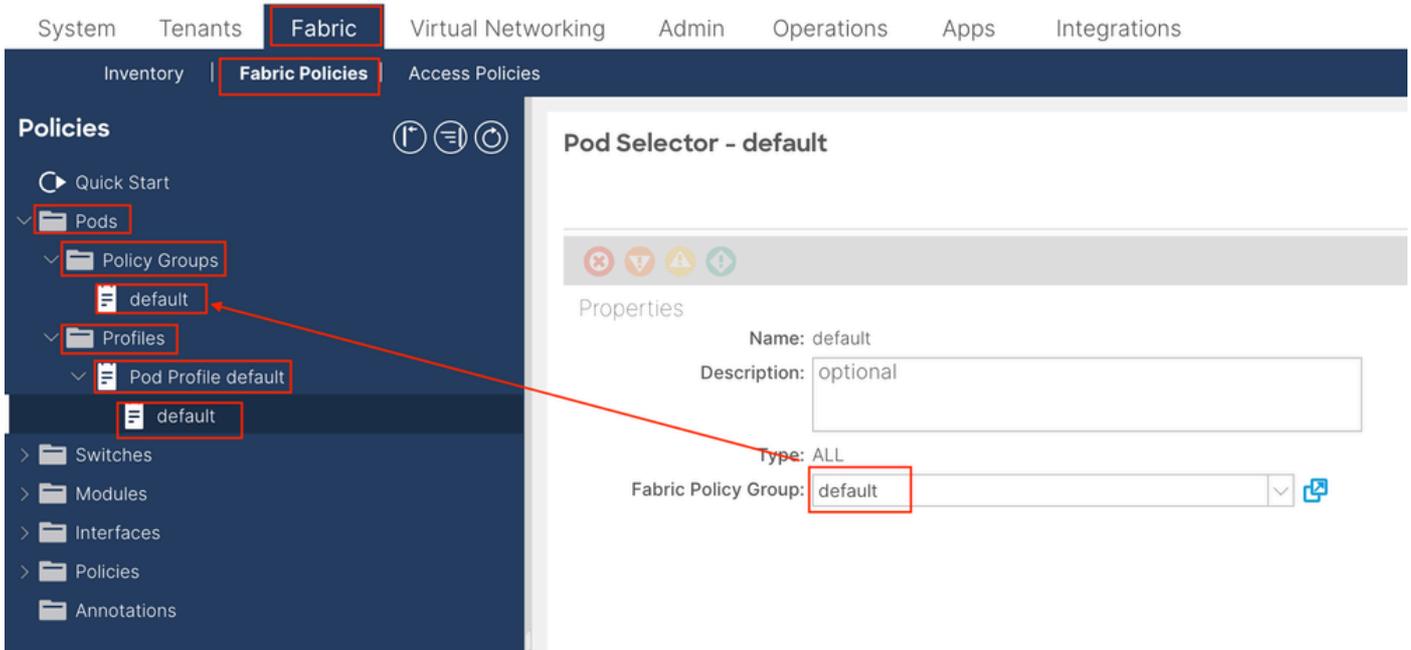
要應用此配置，請導航到APIC Web GUI路徑；Fabric > Fabric Policies > Pods > Policy Groups > POD_POLICY_GROUP (文檔中的預設設定)。



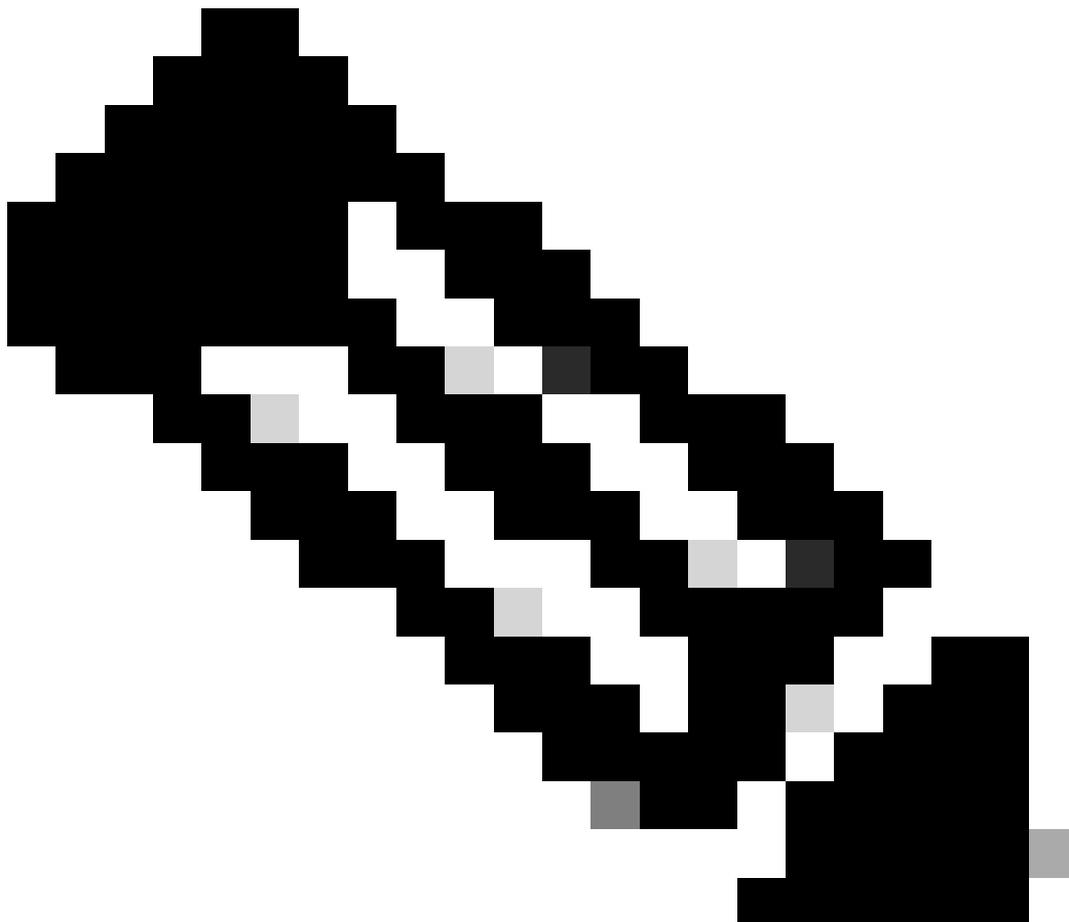
在右側窗格中，您會看到SNMP Policy欄位。從下拉選單中，選擇新建立的SNMP策略並提交更改。

步驟 3.將Pod策略組與Pod配置檔案關聯

為簡單起見，在文檔中採用預設 Pod配置檔案。為此，請導航至APIC Web GUI路徑；Fabric > Fabric Policies > Pods > Profiles > POD_PROFILE (文檔中的預設設定)。



在此階段，配置全局MIB的基本SNMP。



注意：此時，SNMP配置的所有必要步驟（步驟1-3）均已完成，並且已隱式使用全局MIB範圍。這允許為任何ACI節點或APIC執行SNMP漫遊。

步驟 4. 配置VRF情景範圍

一旦您將社群字串與VRF情景相關聯，該特定社群字串便無法用於提取全局範圍SNMP資料。因此，如果您希望提取全局範圍和VRF情景SNMP資料，則需要建立兩個SNMP社群字串。

在本例中，之前建立的社群字串（在步驟1中），即(New-1)，對於VRF上下文範圍，使用New-1，對於示例自定義租戶，使用VRF-1自定義VRF。為此，請導航到APIC Web GUI路徑；Tenants > 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**

> L2Out Delete

> L3Out **Create SNMP Context**

> SR-M Delete SNMP Context

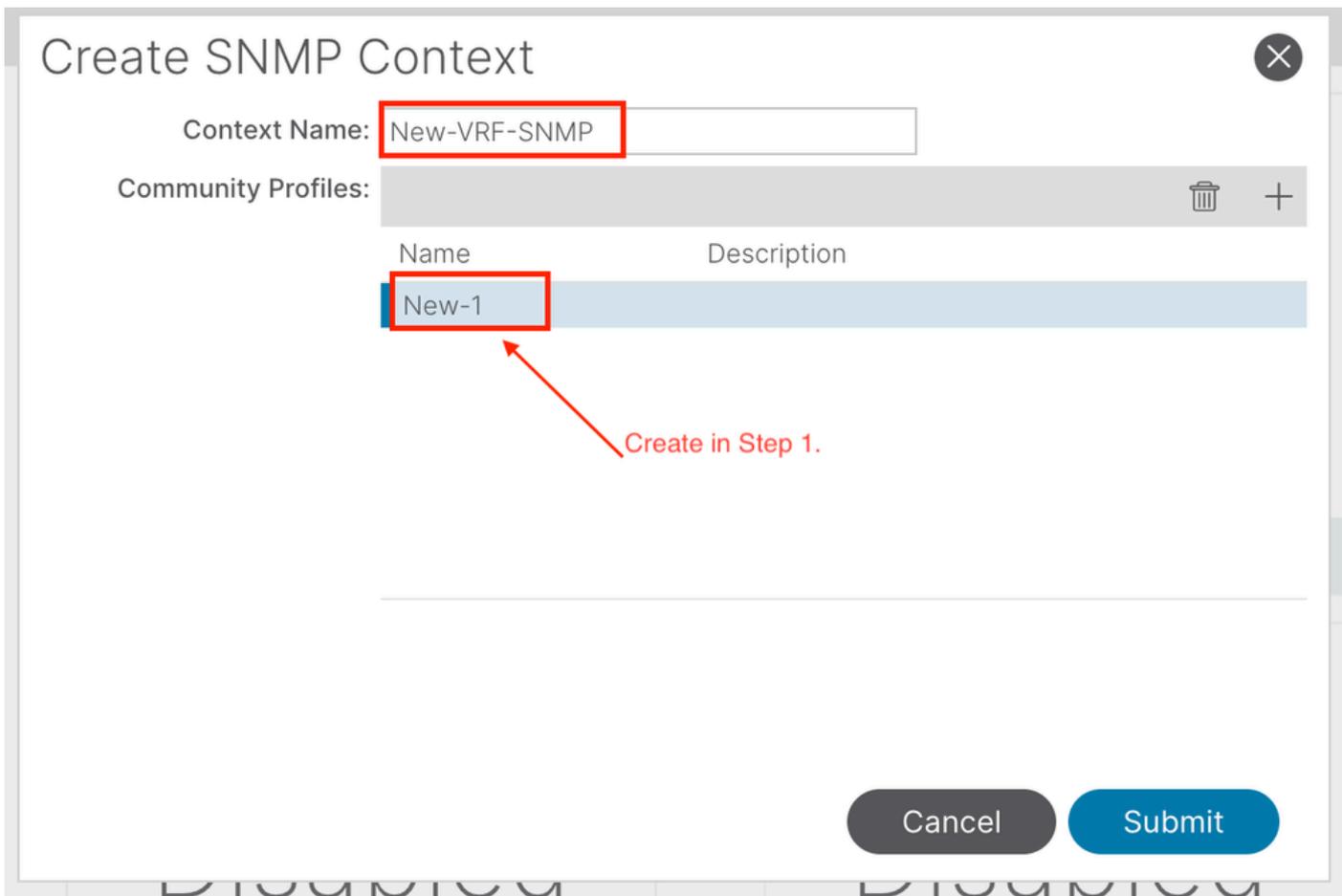
> Dot1 Save as ...

> Contract Post ...

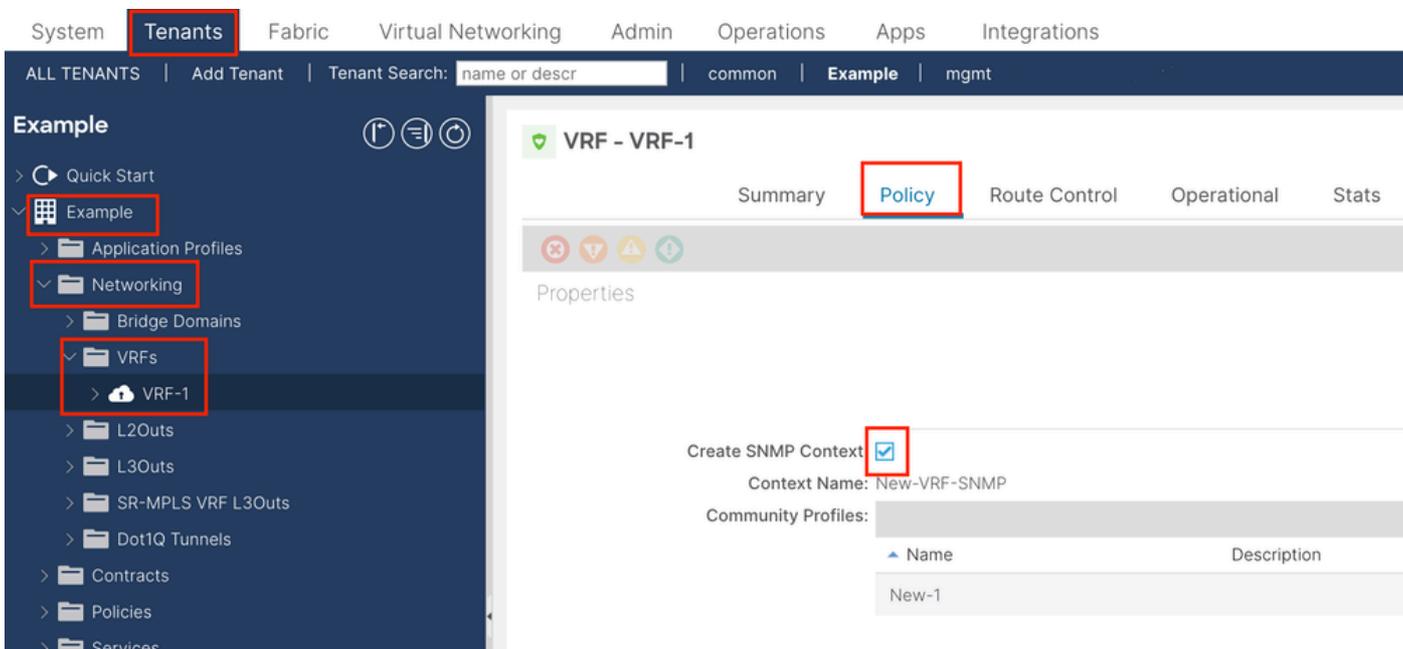
> Policies Share

> Services Open In Object Store Browser

> Security



提交配置後，您可以驗證應用的SNMP情景配置，方法是：左鍵點選VRF，導航到VRF上的Policy頁籤，然後向下滾動到窗格底部：



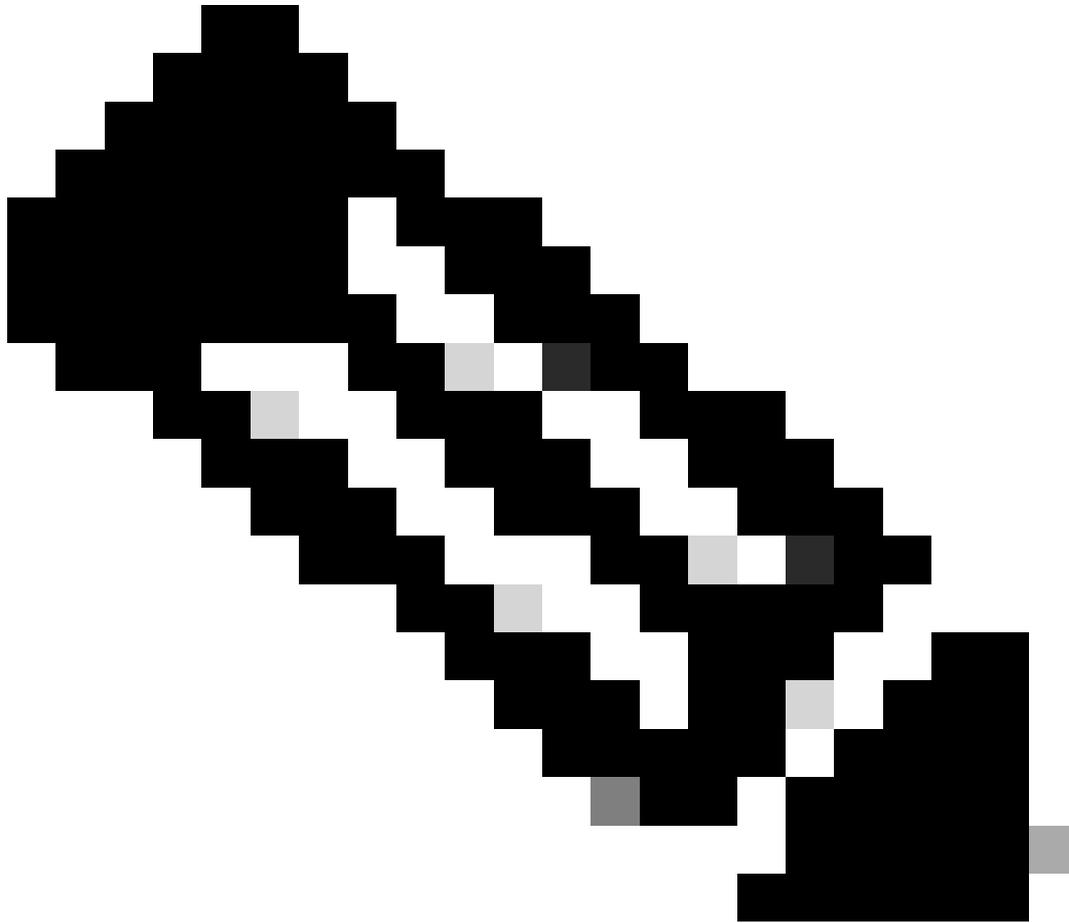
要停用VRF上的SNMP上下文，您可以取消選中Create SNMP Context覆取方塊（參見螢幕截圖），或者按一下右鍵VRF並選擇Delete SNMP Context。

使用GUI配置SNMP陷阱

SNMP TRAP不透過輪詢傳送到SNMP伺服器(SNMP目標/網路管理系統(NMS))，一旦發生故障/事件（已定義條件），ACI節點

/APIC就會傳送SNMP TRAP。

SNMP陷阱根據Access/Fabric/Tenant監控策略下的策略範圍啟用。ACI最多支援10個陷阱接收器。



注意：如果沒有前面部分中的步驟1-3，SNMP TRAPs配置是不夠的。步驟2.在SNMP TRAP配置中，與（接入/交換矩陣/租戶）的監控策略相關。

要在ACI中配置SNMP陷阱，除上節的步驟1、2和3之外還需要兩個步驟。

步驟 1.配置SNMP TRAP Server

為此，請導航到APIC Web GUI路徑；Admin > External Data Collectors > Monitoring Destinations > SNMP。

External Data Collectors

Quick Start

Monitoring Destinations

Callhome

Smart Callhome

SNMP

Syslog

TACACS

Callhome Query Groups

Create SNMP Monitoring Destination Group

SNMP

Name

Create SNMP Monitoring Destination Group

STEP 1 > Profile

1. Profile

2. Trap Destinations

Name: SNMP-trap-server

Description: optional

Previous

Cancel

Next

Create SNMP Monitoring Destination Group

STEP 2 > Trap Destinations

1. Profile 2. Trap Destinations

Host Name/IP	Port	Version	Security/Community Name	v3 Security level	Management EPG	
						+

Previous Cancel Finish

Create SNMP Trap Destination

Host Name/IP:

Port:

Version:

Security Name:

Management EPG:

- default (In-Band) mgmt/default
- default (Out-of-Band) mgmt/default

Cancel OK

Host Name/IP - SNMP陷阱目標的主機。

埠- SNMP陷阱目標的服務埠。範圍為0（未指定）至65535；預設值為162。

版本- SNMP陷阱目標支援的CDP版本。版本可以是：

-

- v1 - 使用社群字串匹配進行使用者身份驗證。

-

v2c - 使用社群字串匹配進行使用者身份驗證。

-

v3 - 基於標準的互操作性網路管理協定，透過結合驗證和加密網路上的幀，提供對裝置的安全訪問。

預設值為v2c。

Security Name - SNMP陷阱目標安全名稱（社群名稱）。它不能包含@符號。

v.3安全等級- SNMP目的地路徑的SNMPv3安全等級。級別可以是：

-

身份驗證

-

noauth

-

priv

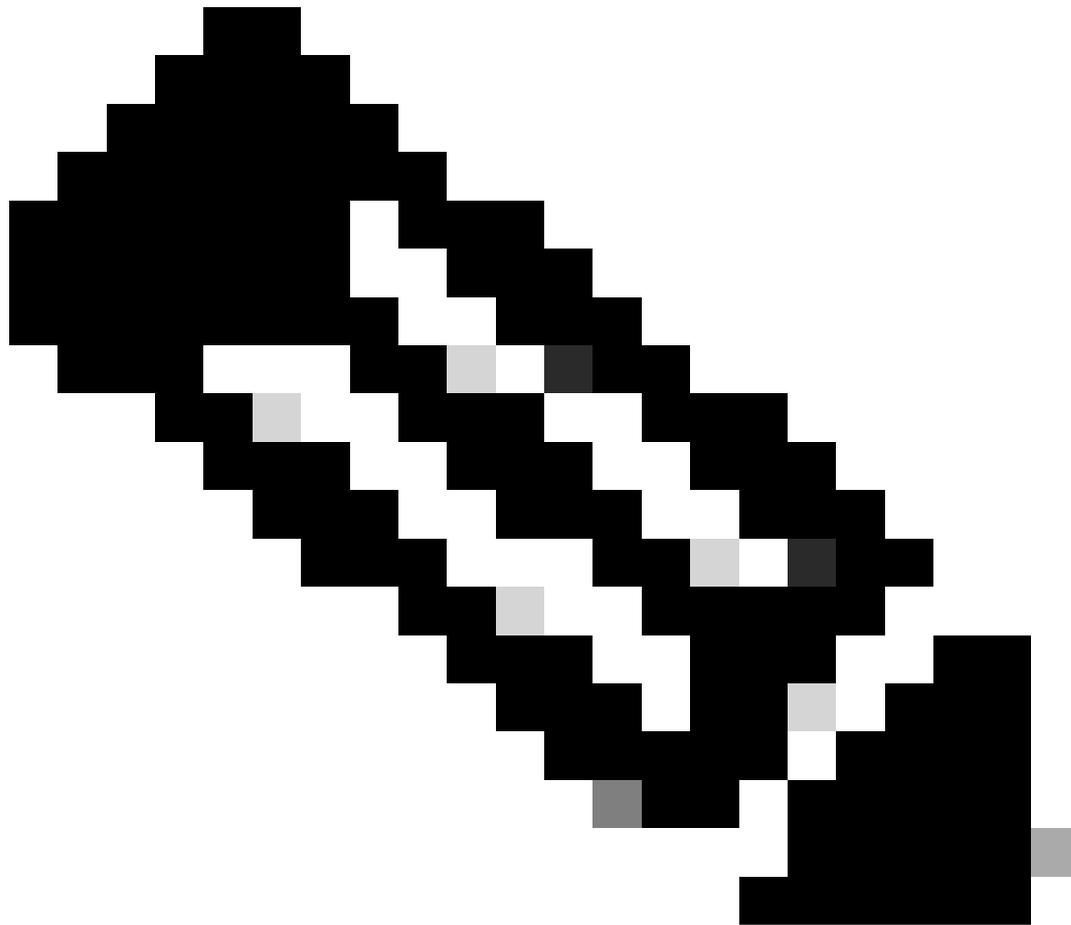
預設值為noauth。

管理EPG - 可訪問遠端主機的SNMP目標管理終端組的名稱。

步驟 2.在（訪問/交換矩陣/租戶）監控策略下配置SNMP陷阱源

您可以使用以下三個作用域建立監視策略：

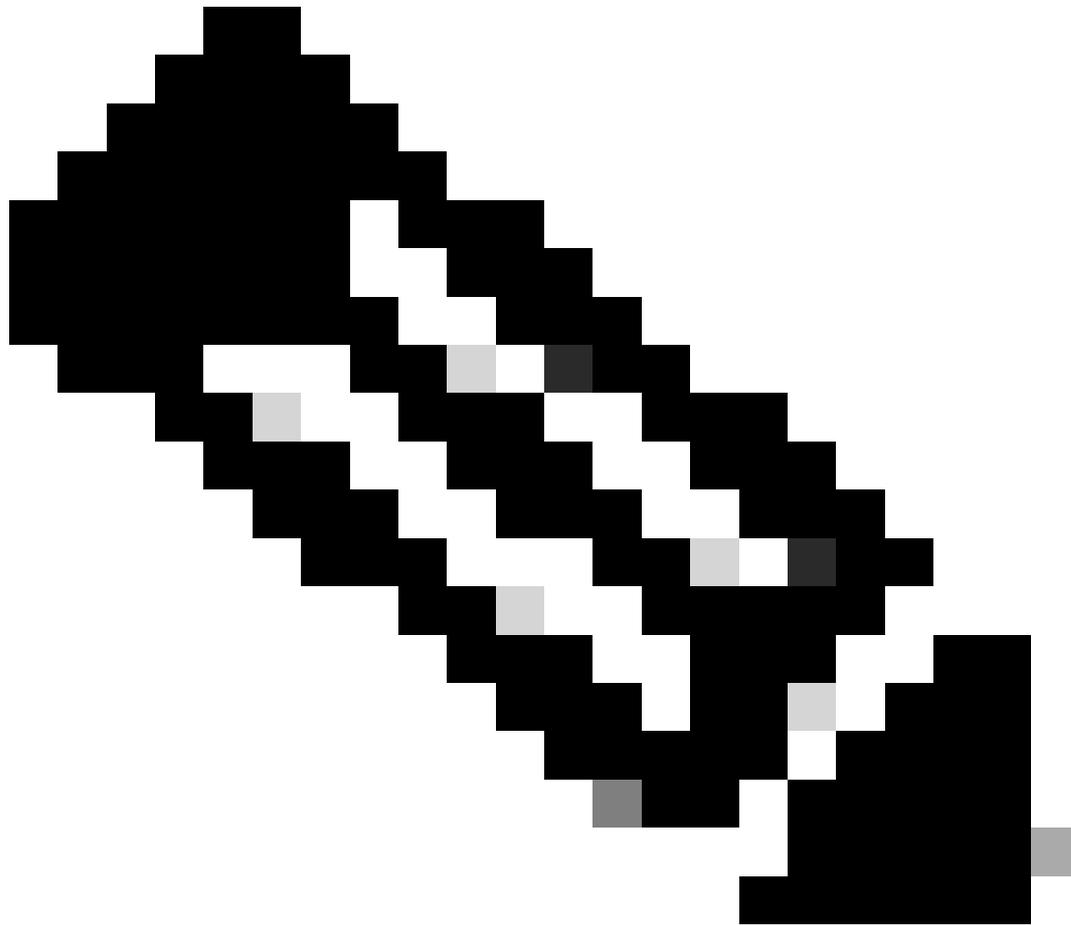
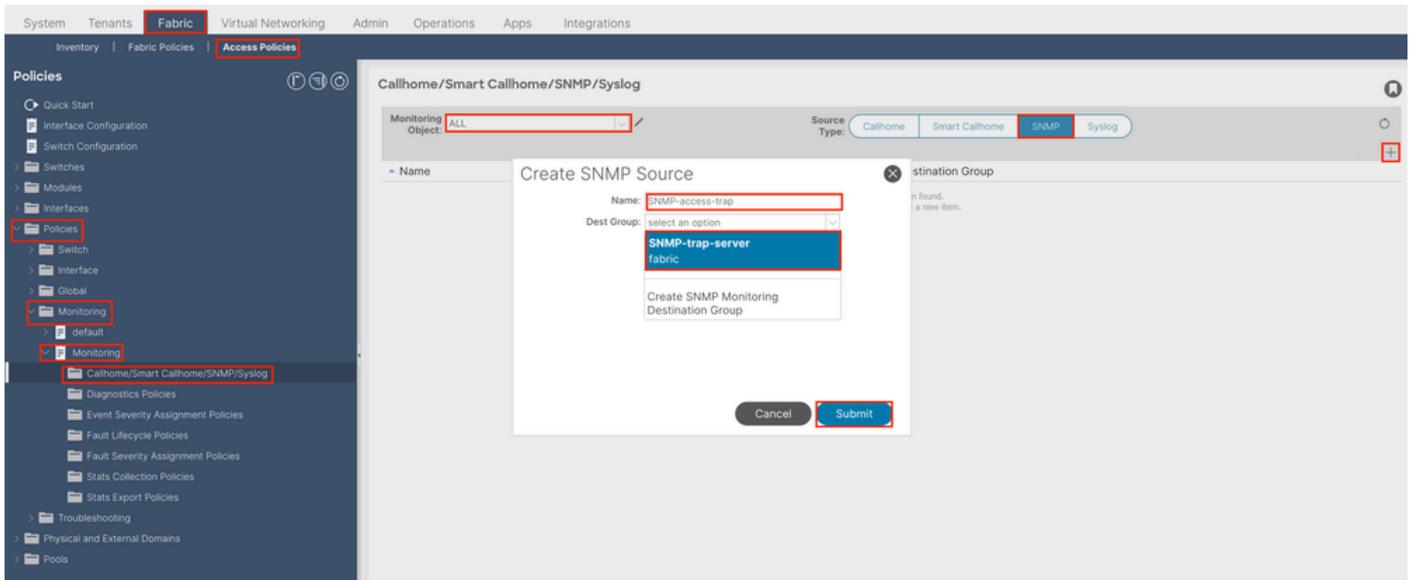
- 接入-接入埠、FEX、VM控制器
- 交換矩陣-交換矩陣埠、卡、機箱、風扇
- 租戶- EPG、應用配置檔案、服務



附註：您可以根據自己的需求選擇其中一個或以上任意組合，以進行設定。

選項 1. 在訪問策略下定義SNMP源

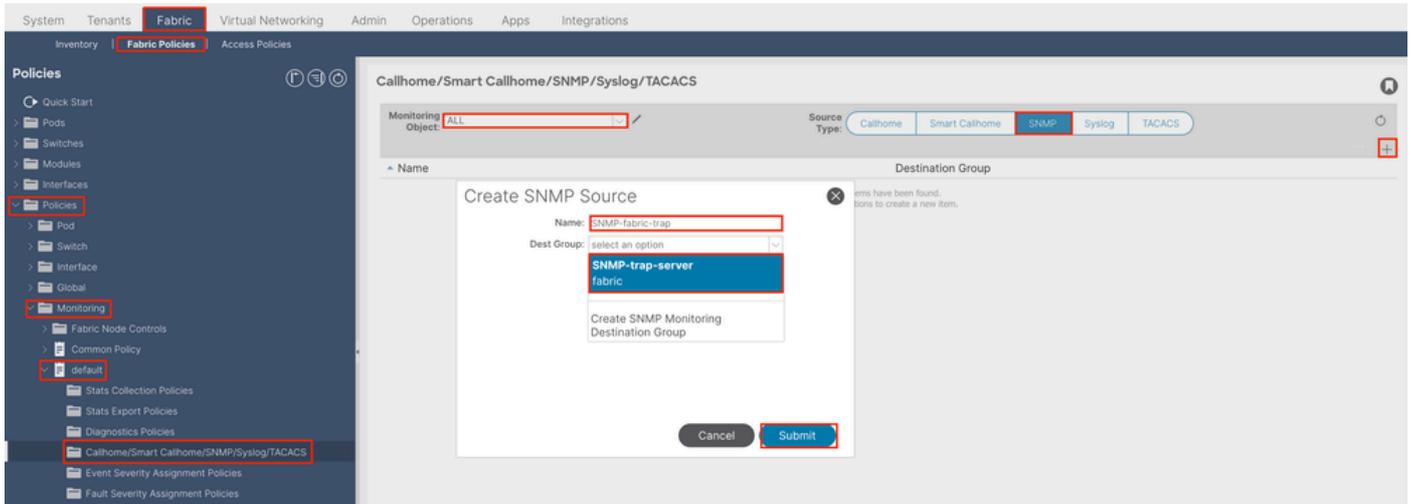
為此，請導航到APIC Web GUI路徑；Fabric > Access Polices > Polices > Monitoring > Default > Callhome/Smart Callhome/SNMP/Syslog/TACACS。



注意：您可以使用自訂的監督原則（若已設定）來取代預設原則，請在此處使用預設原則。您可以指定要監視的監視物件；所有物件均在此使用。

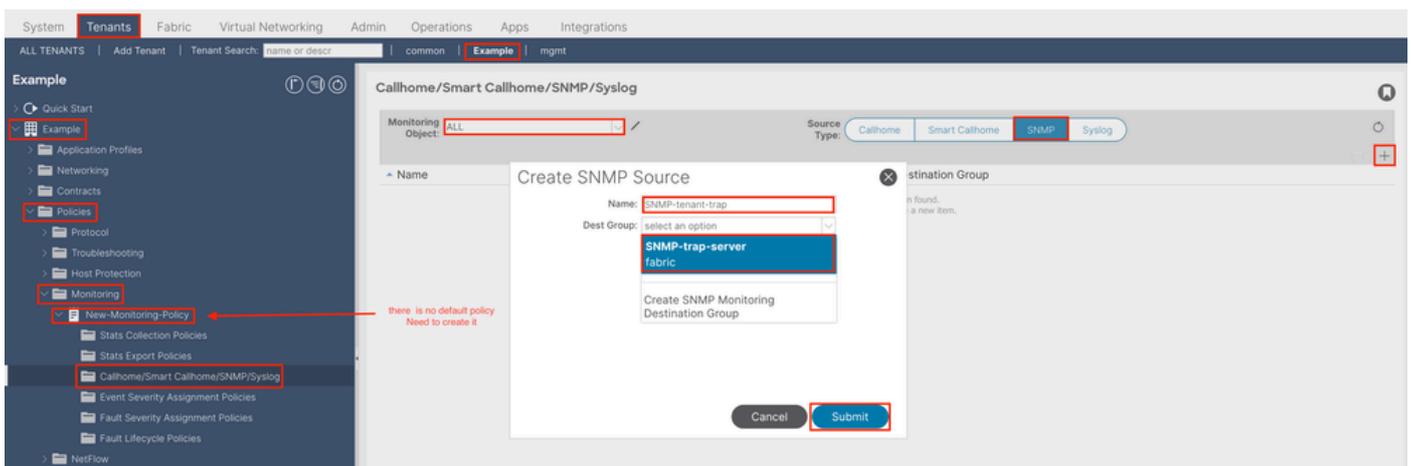
選項 2.在Fabric Policies (交換矩陣策略) 下定義SNMP源

為此，請導航到APIC Web GUI路徑；Fabric > Fabric Polices > Polices > Monitoring > Default > Callhome/Smart Callhome/SNMP/Syslog/TACACS。



選項 3.在租戶策略下定義SNMP源

為此，請導航到APIC Web GUI路徑；Tenant > (Tenant Name) > Polices > Monitoring > (Custom monitoring policy) > Callhome/Smart Callhome/SNMP/Syslog/TACACS。



驗證

使用snmpwalk命令進行驗證

首先，從枝葉交換機的全局範圍提取SNMP資料。使用snmpwalk命令可以做到這一點；snmpwalk -v 2c -c New-1 x.x.x.x。

此細分命令代表：

snmpwalk = 安裝在MacOS/Linux/Windows上的snmpwalk執行檔

-v = 指定要使用的SNMP版本

2c = 指定使用SNMP版本2c

-c = 指定特定的社群字串

New-1 = 社群字串用於提取全局範圍SNMP資料

x.x.x.x = 我的枝葉交換機的帶外管理IP地址

命令結果：

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

在擷取的命令輸出中，您可以看到snmpwalk是成功的，並且提取了特定於硬體的資訊。如果您讓snmpwalk繼續進行，您將看到硬體介面名稱、說明等等。

現在，繼續檢索VRF上下文SNMP資料、之前建立的SNMP上下文、使用SNMP社群字串New-1的VRF的New-VRF-SNMP。

由於在兩個不同的SNMP上下文中使用相同的社群字串New-1，您必須指定從中提取SNMP資料的SNMP上下文。有些snmpwalk語法需要用來指定特定的SNMP環境；snmpwalk -v 2c -c New-1@New-VrF-SNMP 10.x.x.x。

您可以看到，要從特定SNMP情景中提取，您使用如下格式：COMMUNITY_NAME_HERE@SNMP_CONTEXT_NAME_HERE。

使用CLI Show命令

在APIC上：

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

在Switch：

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

使用CLI Moquery命令

在APIC/交換機上：

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

使用CLI cat命令

在APIC上：

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

疑難排解

檢查snmpd流程

在Switch：

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

在APIC上：

```
ps aux | grep snmp
```

如果過程正常，請聯絡思科TAC以獲取更多幫助。

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）。