在ACI中配置SNMP

目录

简介

先决条件

- 要求
- 使用的组件

配置

- 了解SNMP范围
- 配置步骤（适用于全局和VRF情景范围）
  - 步骤1.配置SNMP交换矩阵策略
  - 步骤2.将SNMP策略应用于Pod策略组（交换矩阵策略组）
  - 步骤3.将Pod策略组与Pod配置文件关联
  - 步骤4.配置VRF环境范围
- 使用GUI配置SNMP陷阱
  - 步骤1.配置SNMP TRAP服务器
  - 步骤2.在(Access/Fabric/Tenant)Monitoring Policy下配置SNMP TRAP Source
  - 选项1.在“访问策略”下定义SNMP源
  - 选项2.在“交换矩阵策略”下定义SNMP源
  - 选项3.在“租户策略”下定义SNMP源

验证

- 使用snmpwalk命令进行验证
- 使用CLI Show命令
- 使用CLI Moquery命令
- 使用CLI cat命令

故障排除

- 检查snmpd流程

简介

本文档介绍在ACI中配置简单网络管理协议(SNMP)和SNMP陷阱。

先决条件

要求

Cisco 建议您了解以下主题：

- 交换矩阵发现已完成
- 与应用策略基础设施控制器(APIC)和交换矩阵交换机的带内/带外连接
- 带内/带外合同配置为允许SNMP流量（UDP端口161和162）
- 在默认mgmt租户下为APIC和交换矩阵交换机配置的静态节点管理地址（如果不这样做，从APIC提取SNMP信息失败）

- 了解SNMP协议工作流程

使用的组件

本文档中的信息基于以下软件和硬件版本：

- APIC
- 浏览器
- 运行5.2(8e)的以应用为中心的基础设施(ACI)
- Snmpwalk 命令

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

思科ACI提供SNMPv1、v2c和v3支持，包括管理信息库(MIB)和通知（陷阱）。 SNMP标准允许支持不同MIB的任何第三方应用管理和监控ACI枝叶和主干交换机以及APIC控制器。

但是，ACI不支持SNMP write命令(Set)。

SNMP策略在枝叶和主干交换机以及APIC控制器上独立应用和运行。由于每个ACI设备都有自己的SNMP实体，即APIC集群中的多个APIC必须与交换机分开监控。但是，SNMP策略源创建为整个ACI交换矩阵的监控策略。

默认情况下，SNMP使用UDP端口161进行轮询，使用端口162进行TRAP。

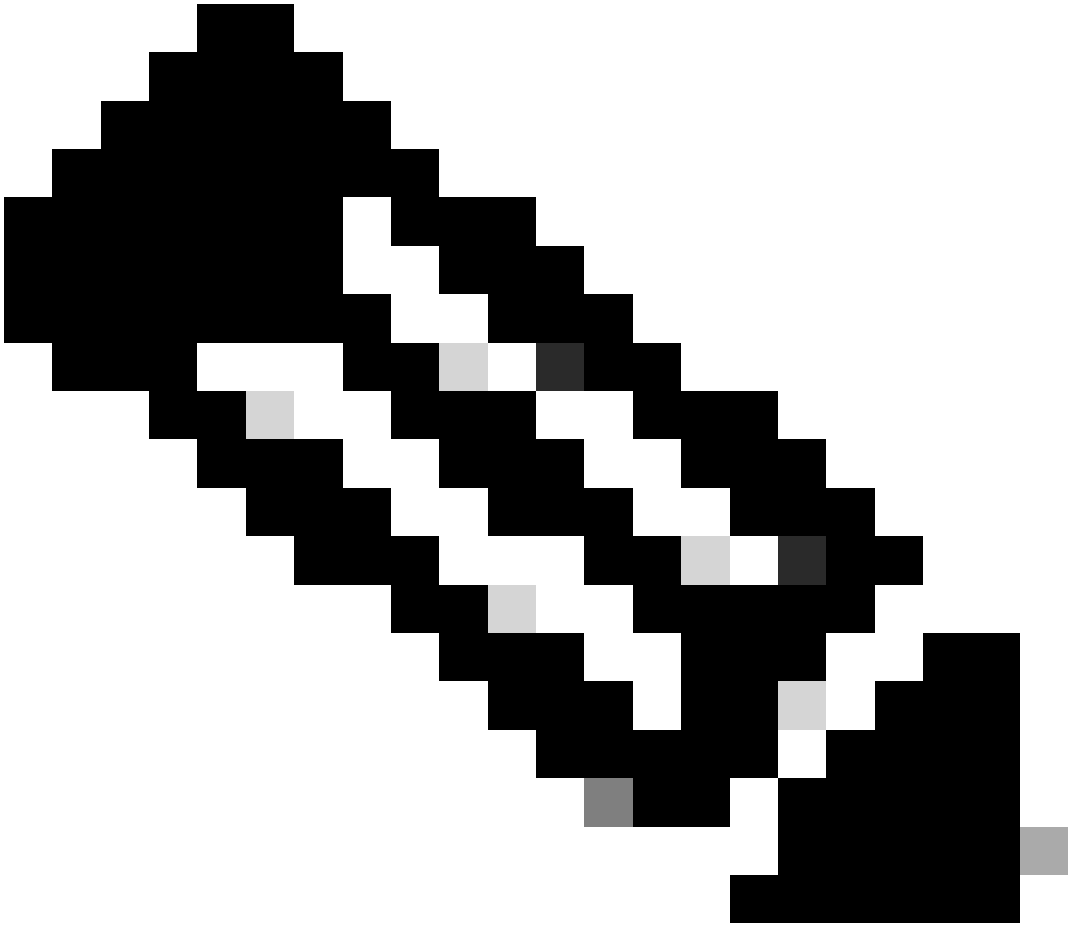
了解SNMP范围

ACI中SNMP的一个快速基本概念是可以从两个范围提取SNMP信息：
1.全球
2.虚拟路由和转发(VRF)情景

Global Scope是拉取机箱MIB，例如枝叶/主干节点的接口数、接口索引、接口名称、接口状态等。

VRF Context Scope 特定MIB提取特定于VRF的信息，例如IP地址和路由协议信息。

Cisco ACI MIB Support List中提供了受支持的APIC和交换矩阵交换机全局和VRF情景MIB的完整列表。

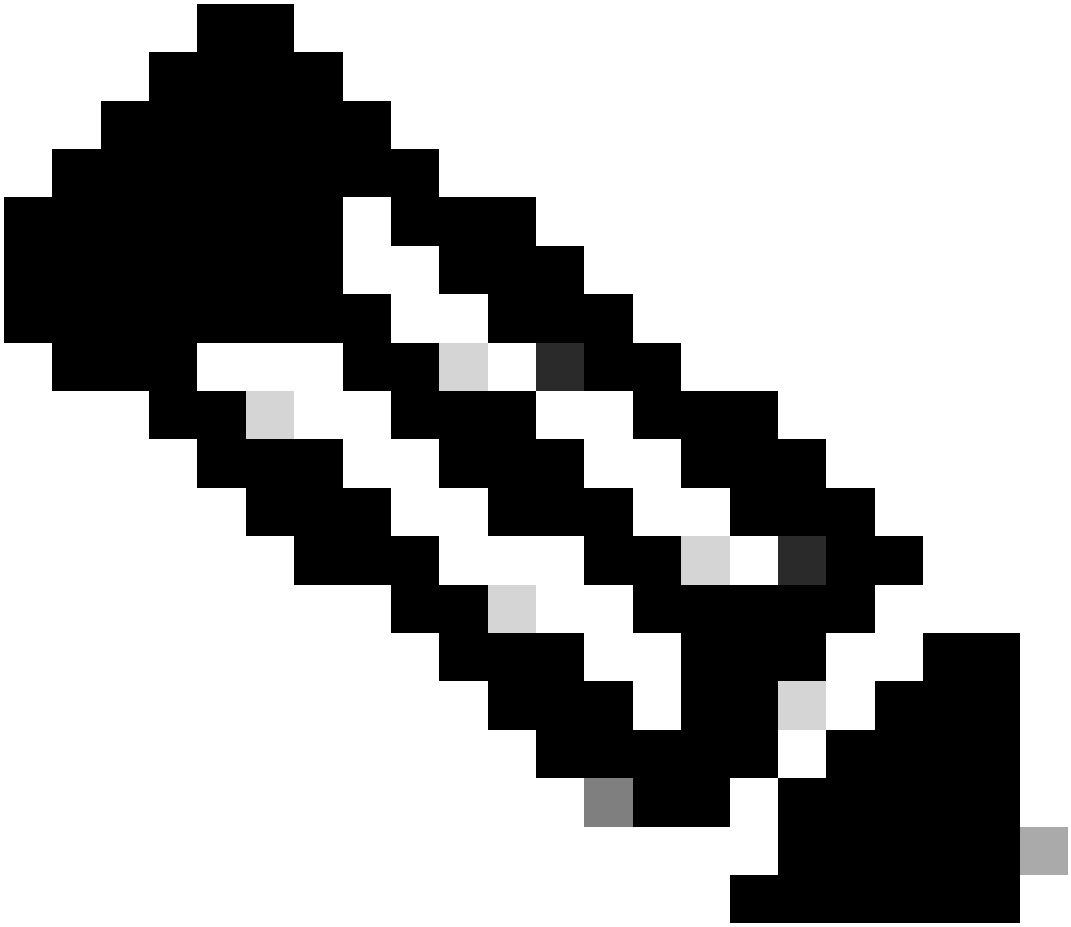


注意：具有全局范围的MIB在系统中只有一个实例。全局MIB中的数据与整个系统相关。

具有VRF特定范围的MIB可以在系统中具有每个VRF实例。VRF特定MIB中的数据仅与该VRF相关。

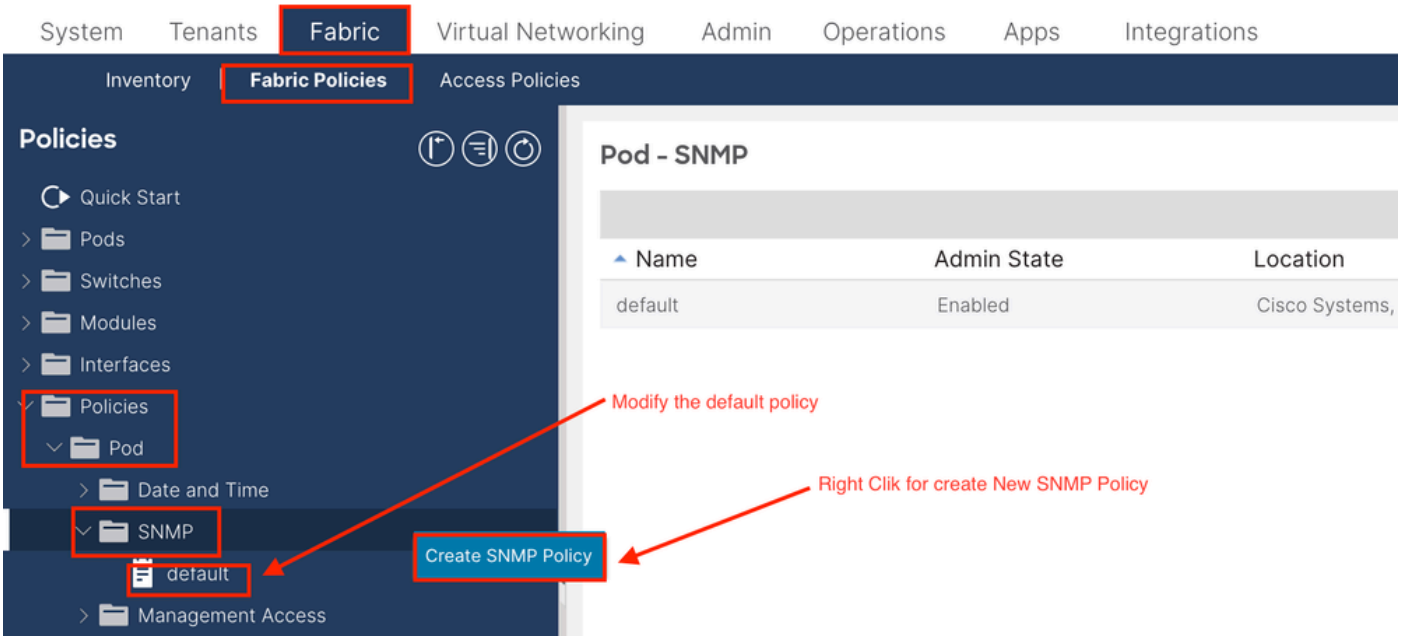
配置步骤（适用于全局和VRF情景范围）

步骤1.配置SNMP交换矩阵策略



注意：此处指定SNMP设置，例如SNMP社区策略和SNMP客户端组策略。

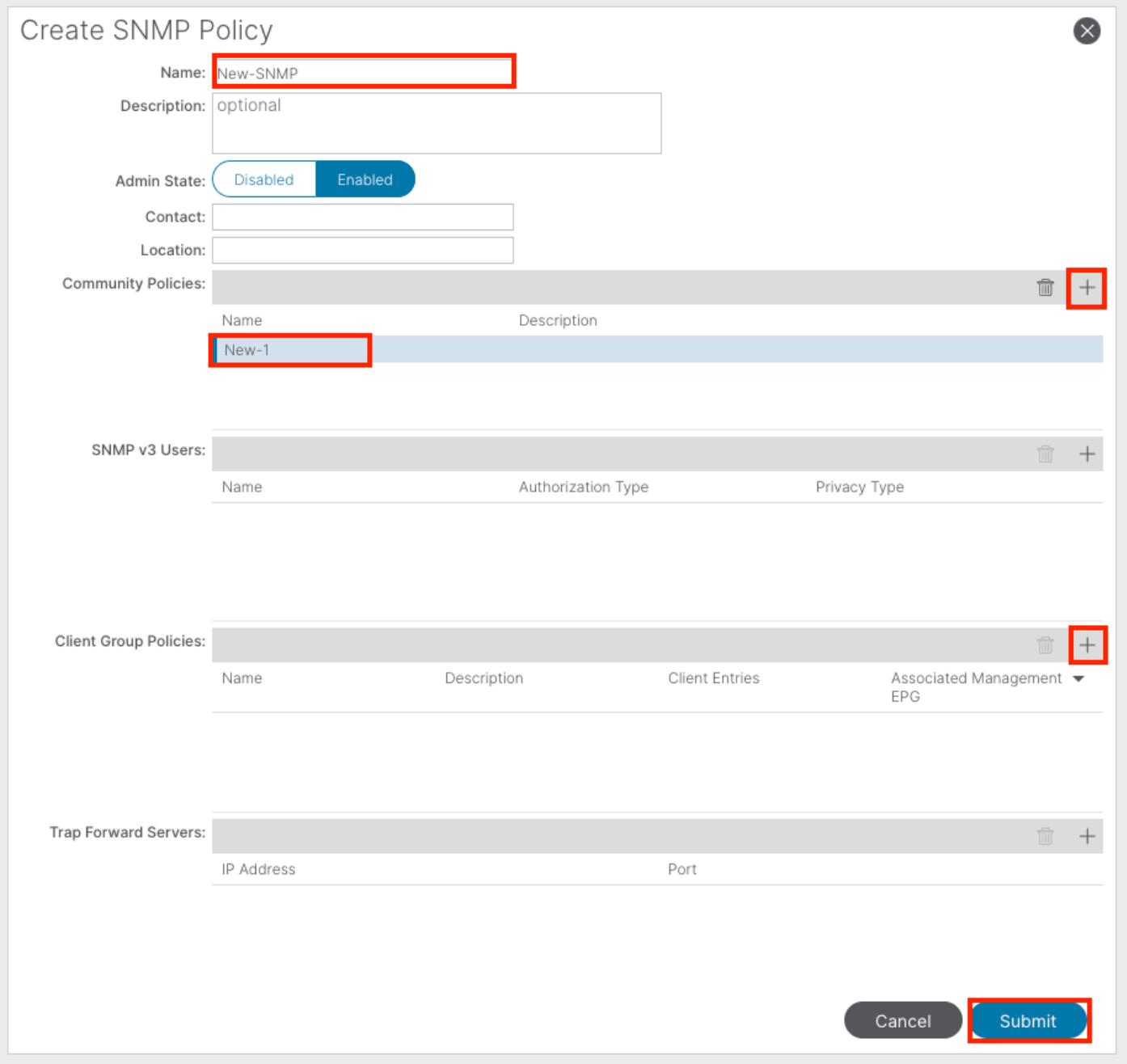
配置SNMP的第一步是创建必要的SNMP交换矩阵策略。要创建SNMP交换矩阵策略，请导航至APIC Web GUI路径；Fabric > Fabric Policies > Policies > Pod > SNMP.



您可以创建新的SNMP策略或修改默认SNMP策略。

在文档中，SNMP策略称为New-SNMP，使用SNMP版本v2c，因此此处需要的字段只有Community Policies和Client Group Policies。

Community Policy Name字段定义要使用的SNMP社区字符串。在我们的例子中，New-1。您会看到这两个社区字符串后面会出现在何处。



名称- SNMP策略的名称。此名称可以是1到64个字母数字字符。

说明- SNMP策略的说明。说明可以是0到128个字母数字字符。

管理状态 — SNMP策略的管理状态。状态可以启用或禁用。状态如下：

- enabled — 管理员状态已启用
- disabled — 管理员状态已禁用

默认值为disabled。

联系人- SNMP策略的联系人信息。

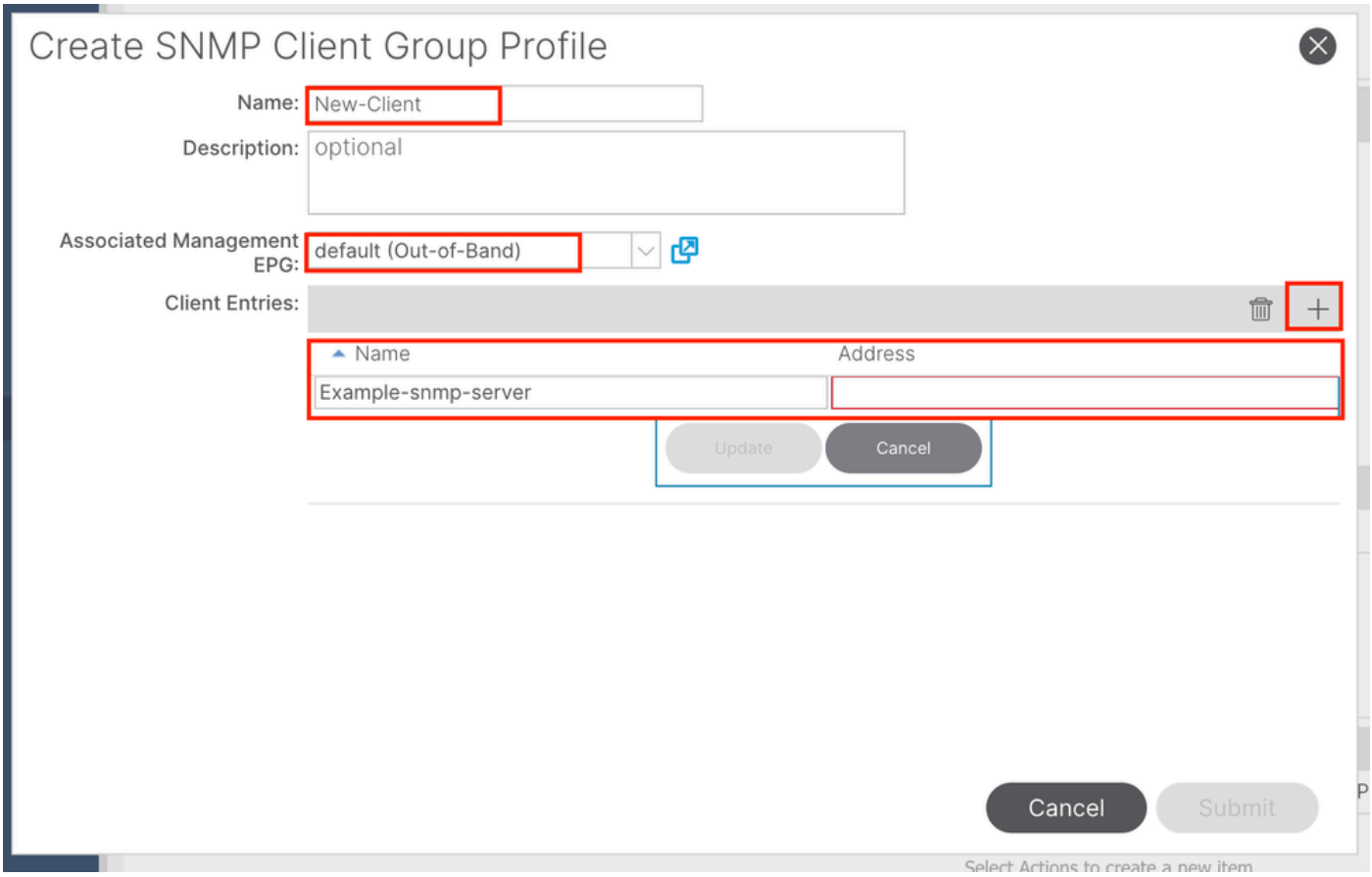
位置- SNMP策略的位置。

SNMP v3用户 — SNMP用户配置文件用于将用户与SNMP策略相关联，用于监控网络中的设备。

社区策略 — SNMP社区配置文件允许访问路由器或交换机统计信息以进行监控。

客户端组策略：

下一步是添加客户端组策略/配置文件。客户端组策略/配置文件的目的是定义哪些IP/子网能够从APIC和交换矩阵交换机提取SNMP数据：



Name — 客户端组配置文件的名称。此名称可以是1到64个字母数字字符。

Description — 客户端组配置文件的说明。说明可以是0到128个字母数字字符。

关联管理终端组(EPG)-可访问VRF的终端组的可分辨名称。支持的最大字符串长度为255个ASCII字符。默认为管理租户带外管理访问EPG。

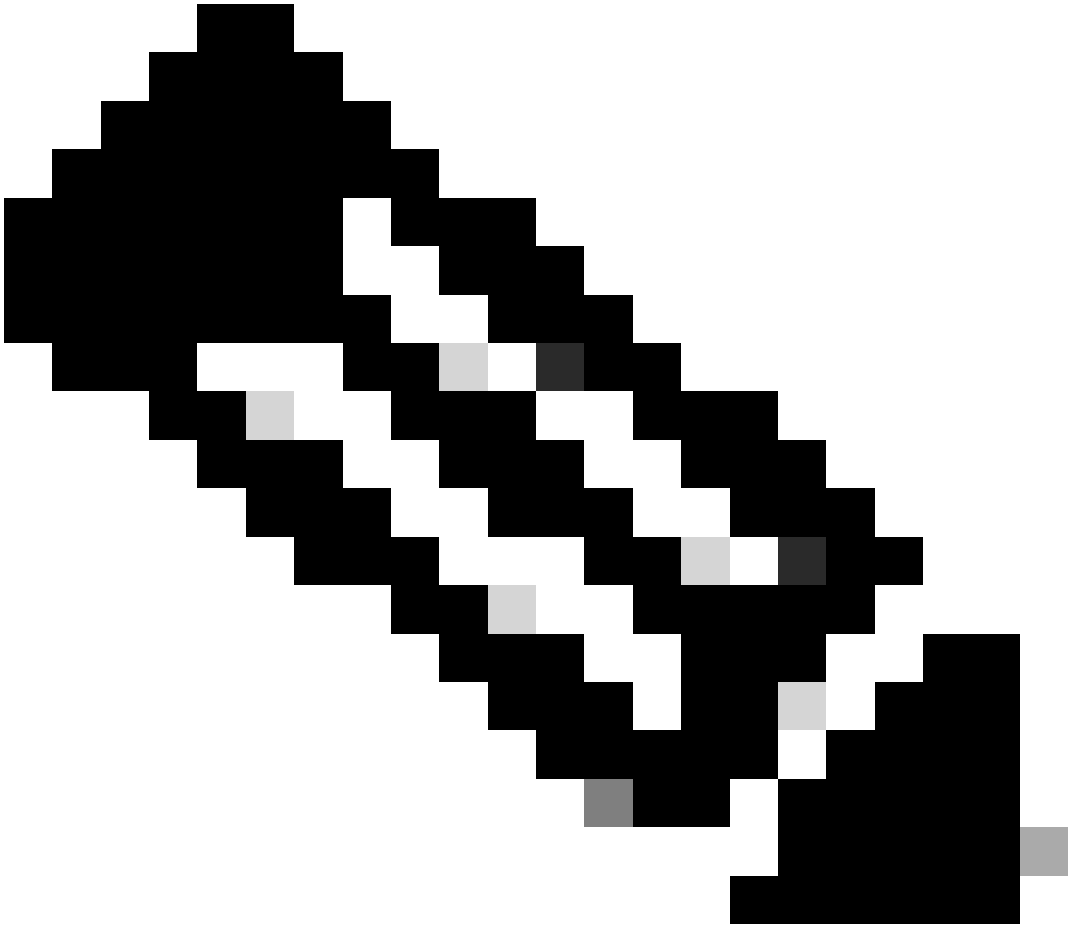
客户端条目 — SNMP客户端配置文件IP地址。

在文档中，客户端组策略/配置文件称为新客户端。

在Client Group Policy/Profile中，您必须关联首选的管理EPG。您必须确保您选择的管理EPG具有允许SNMP流量（UDP端口161和162）的必要合同。 文档中使用了默认的带外管理EPG进行演示。

最后一步是定义您的客户端条目以允许特定IP或整个子网访问来提取ACI SNMP数据。有一个用于定义特定IP或整个子网的语法：

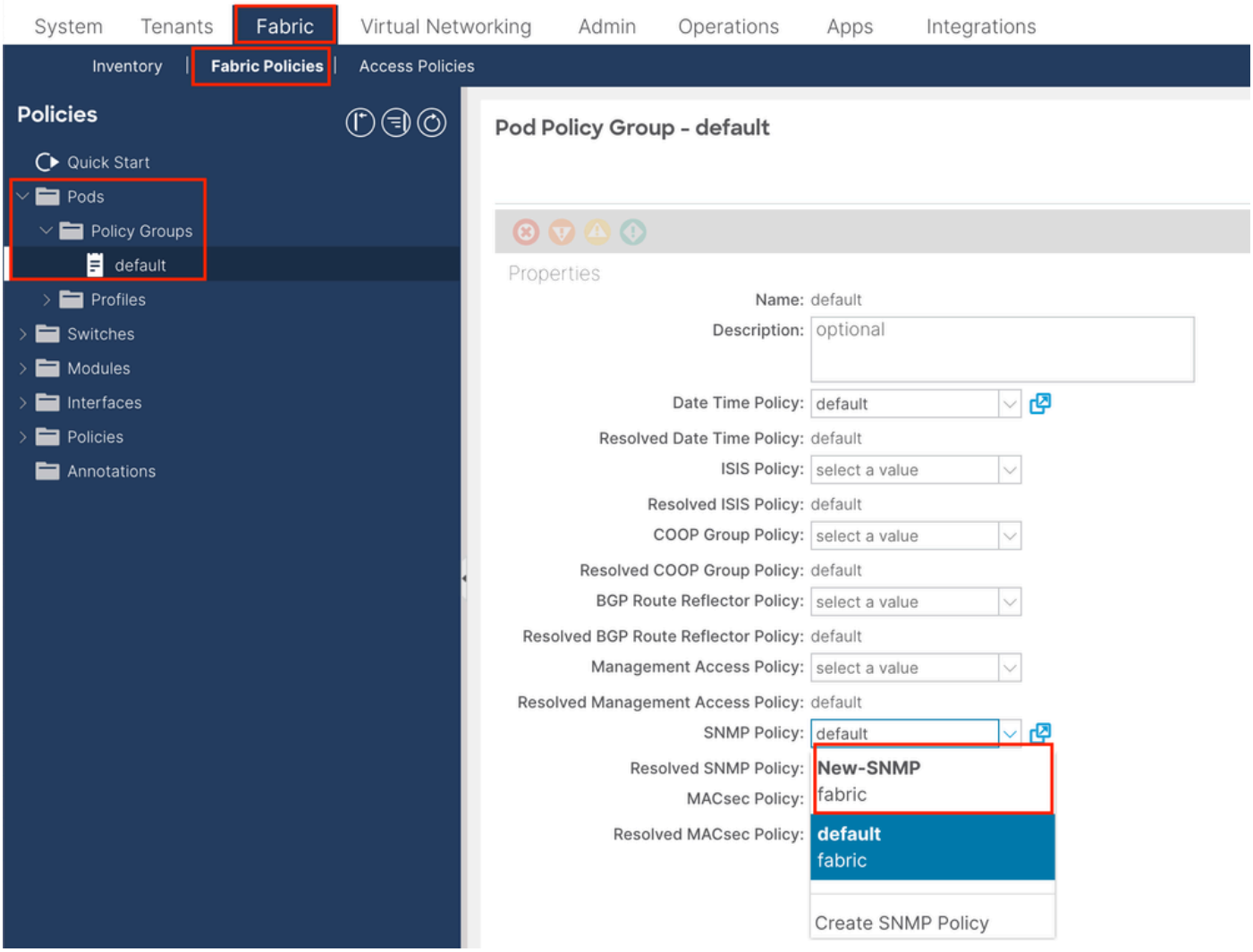
- 特定主机IP:192.168.1.5
- 整个子网：192.168.1.0/24



注意：不能在客户端条目中使用0.0.0.0来允许所有子网（如果要允许所有子网访问SNMP MIB，只需将客户端条目留空）。

步骤2.将SNMP策略应用于Pod策略组（交换矩阵策略组）

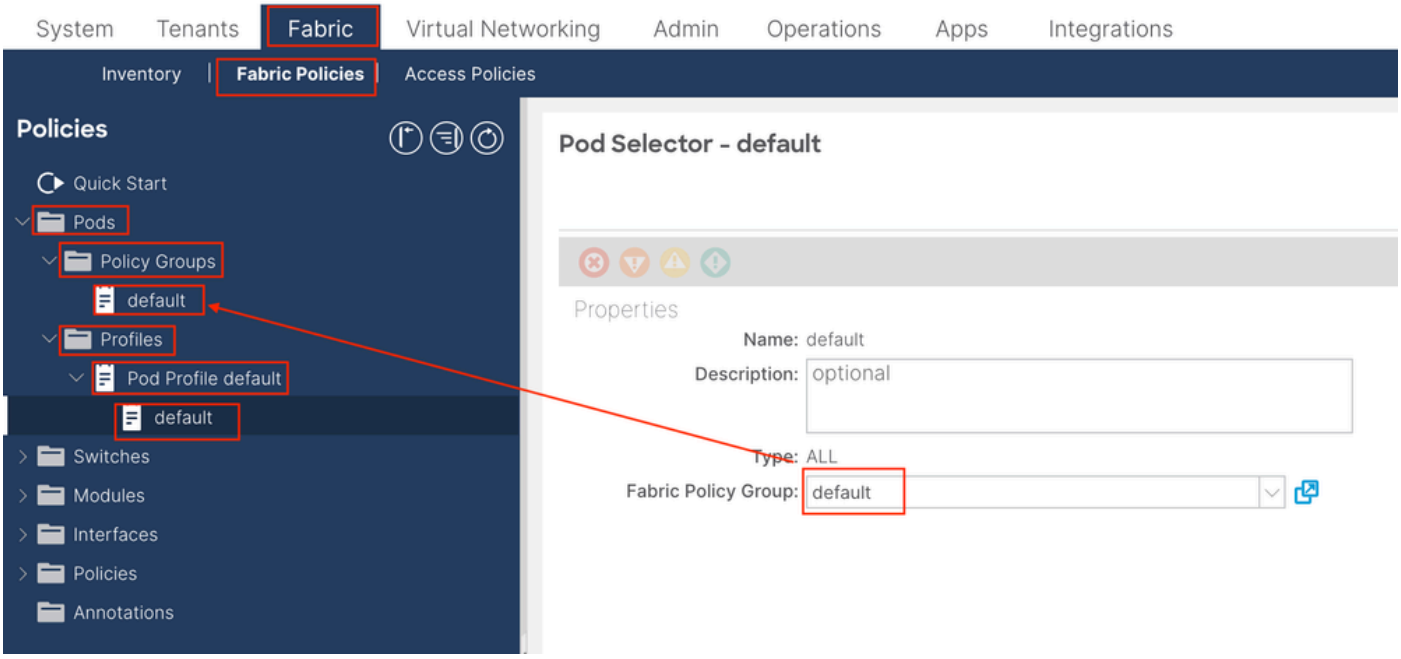
要应用此配置，请导航至APIC Web GUI路径；Fabric > Fabric Policies > Pods > Policy Groups > POD_POLICY_GROUP（文档中的默认值）。



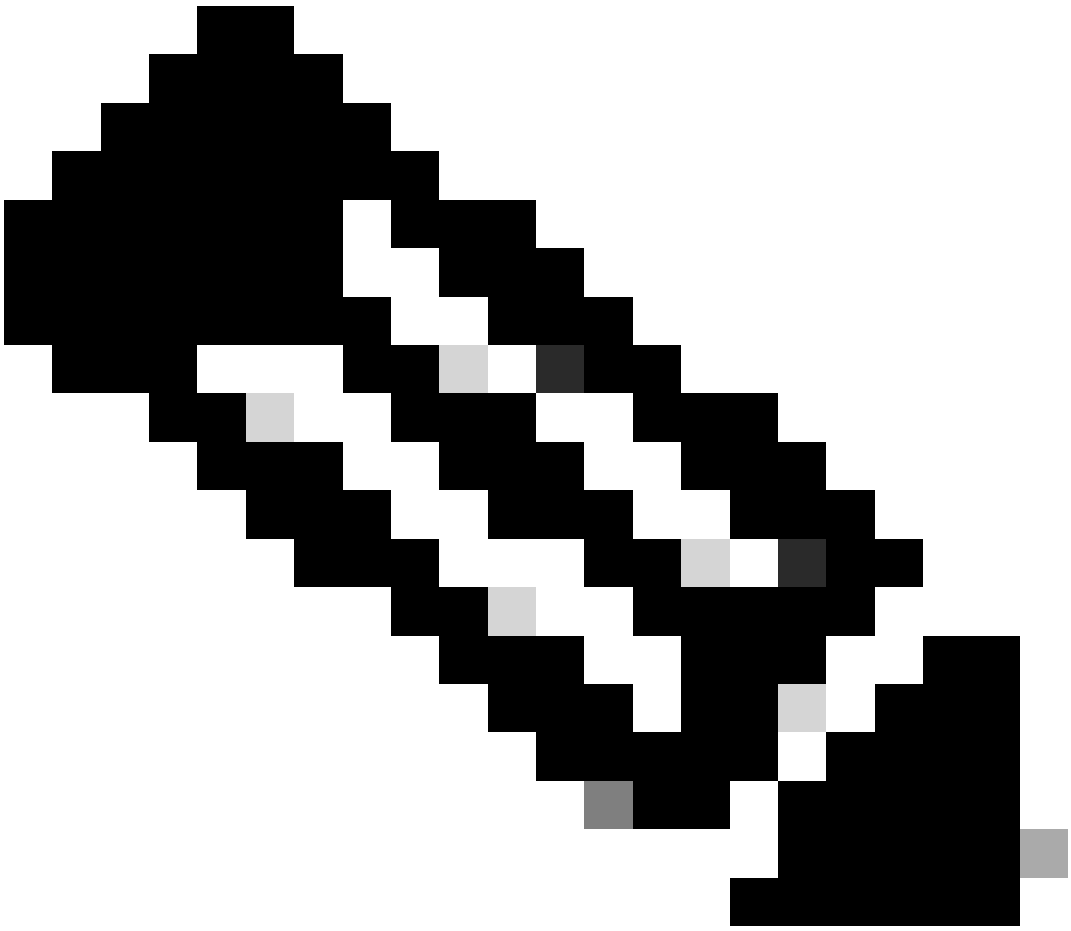
在右侧窗格中，您会看到SNMP Policy的字段。从下拉列表中，选择新创建的SNMP策略并提交更改。

步骤3.将Pod策略组与Pod配置文件关联

在文档中，使用默认Pod配置文件以简化操作。为此，请导航至APIC Web GUI路径；Fabric > Fabric Policies > Pods > Profiles > POD_PROFILE（文档中的默认值）。



在此阶段，配置全局MIB的基本SNMP。

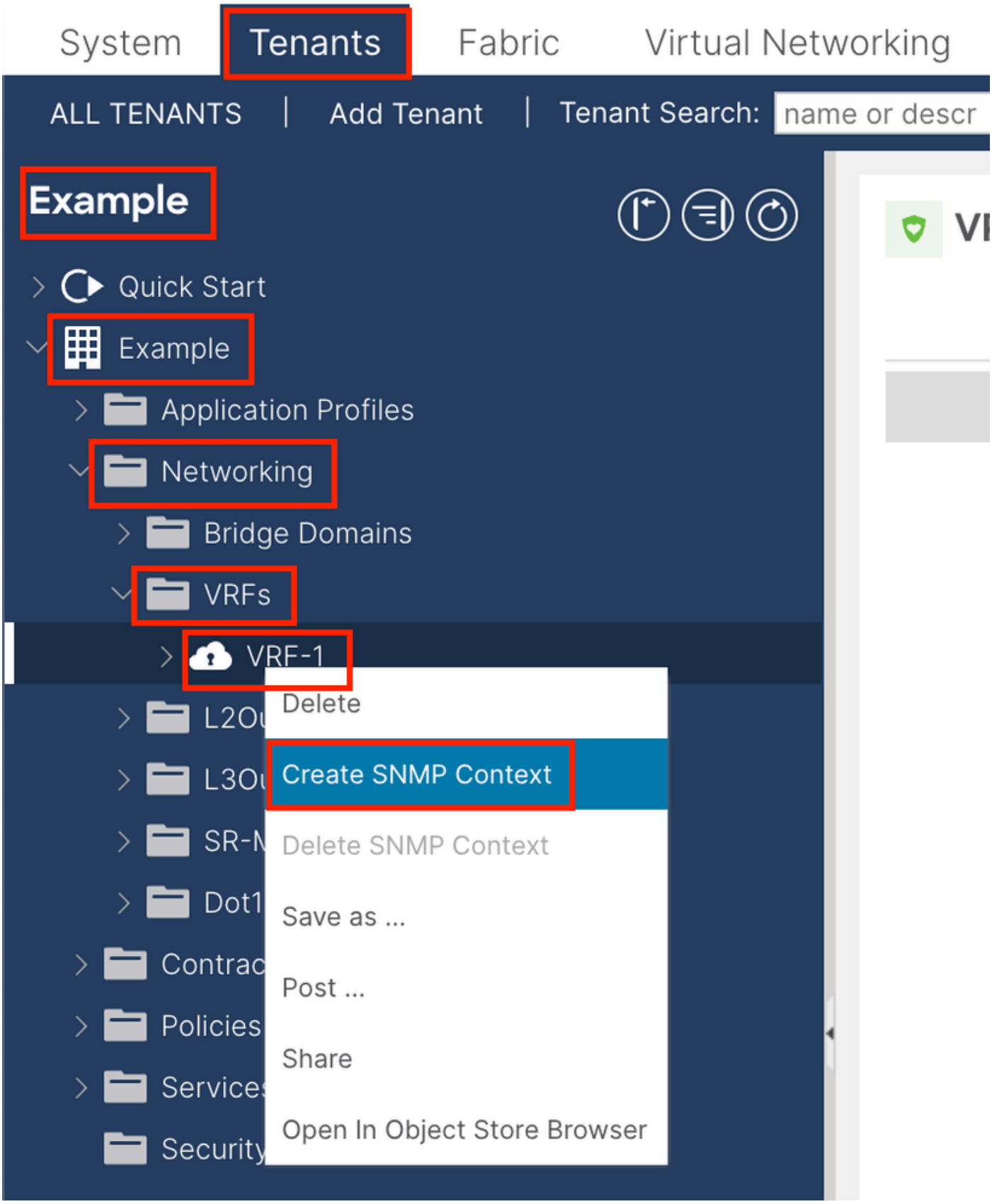


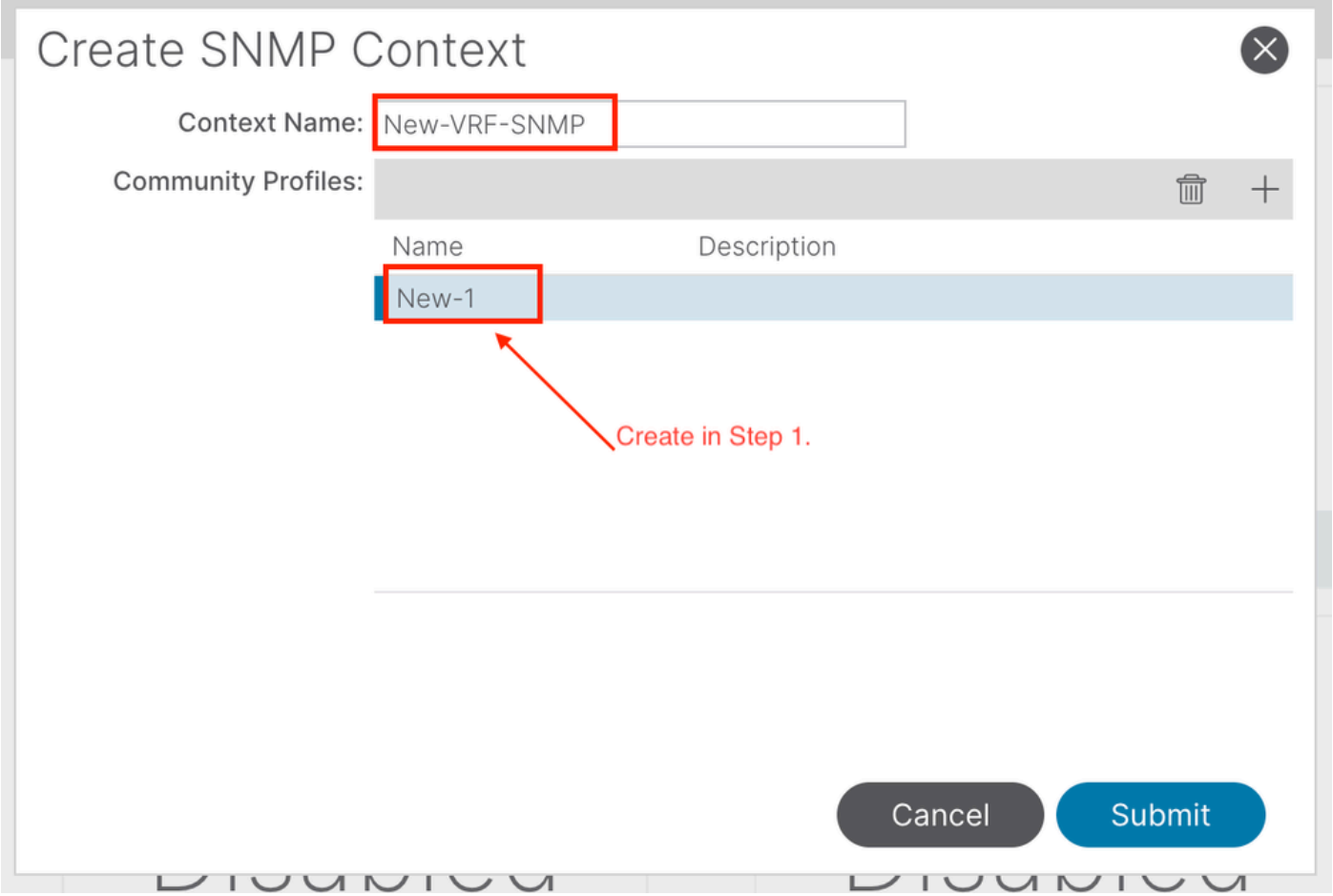
注意：此时，SNMP配置的所有必要步骤（步骤1-3）都已完成，并且已隐式使用全局MIB范围。这允许对任何ACI节点或APIC执行SNMP漫游。

步骤4.配置VRF环境范围

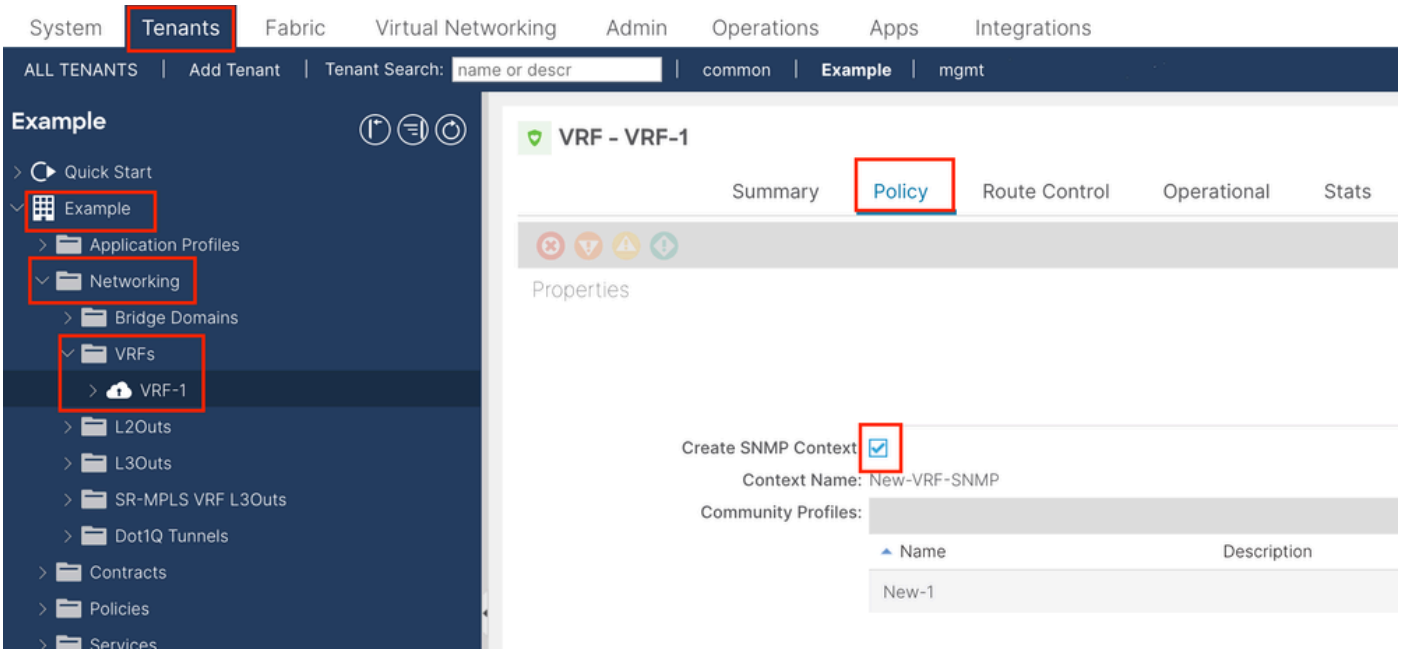
一旦将社区字符串关联到VRF情景，该特定社区字符串将无法用于提取全局范围SNMP数据。因此，如果您希望提取全局范围和VRF情景SNMP数据，则需要创建两个SNMP社区字符串。

在本例中，以前创建的社区字符串（在第1步中）即(New-1)，对VRF上下文范围使用New-1，对Example自定义租户使用VRF-1自定义VRF。为此，请导航至APIC Web GUI路径；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
Delete
Create SNMP Context
Delete SNMP Context
Save as ...
Post ...
Share
Open In Object Store Browser



提交配置后，您可以通过左键点击VRF、导航到VRF上的Policy选项卡并向下滚动至窗格底部来验证应用的SNMP情景配置：

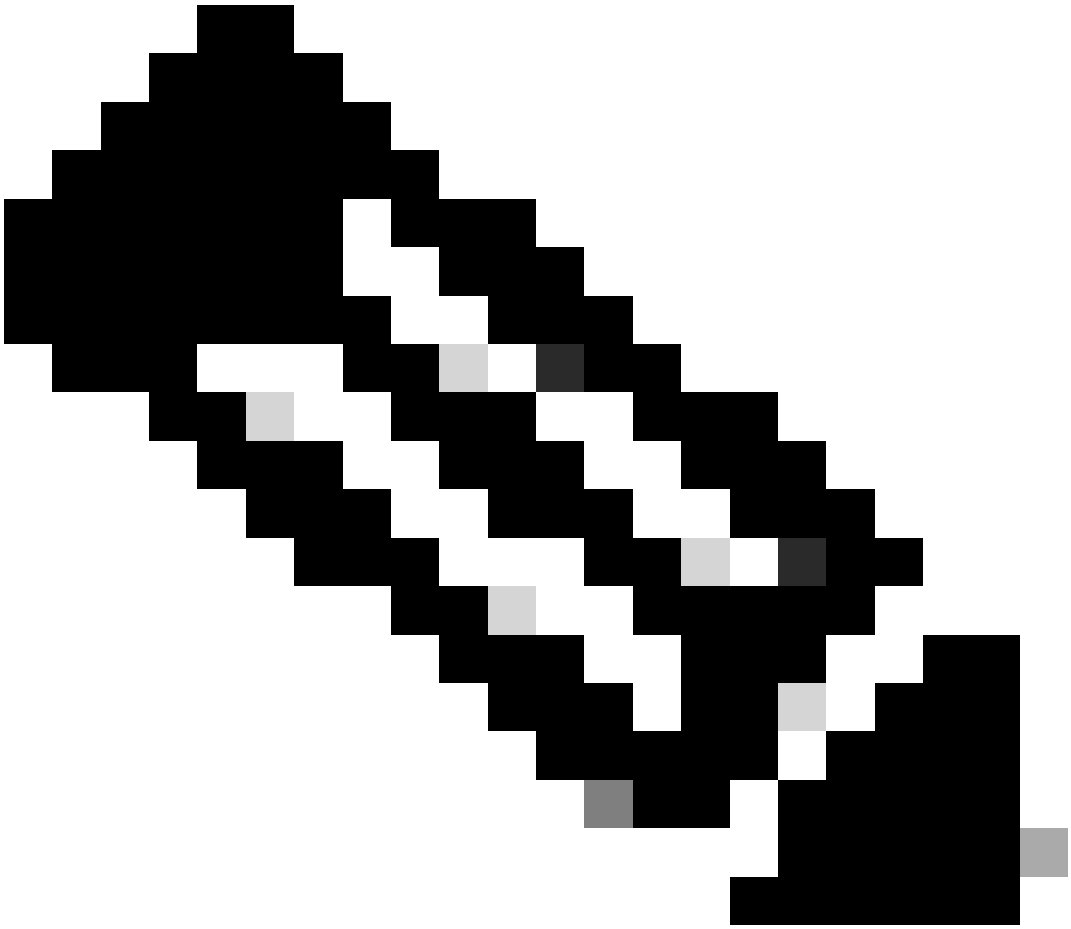


要禁用VRF上的SNMP情景，您可以取消选中创建SNMP情景复选框（显示在屏幕截图中），或右击VRF并选择删除SNMP情景。

使用GUI配置SNMP陷阱

SNMP TRAP无需轮询即可发送到SNMP服务器(SNMP目标/网络管理系统(NMS))，一旦发生故障/事件（已定义的条件），ACI节点/APIC就会发送SNMP TRAP。

SNMP陷阱基于访问/交换矩阵/租户监控策略下的策略范围启用。ACI最多支持10个陷阱接收器。

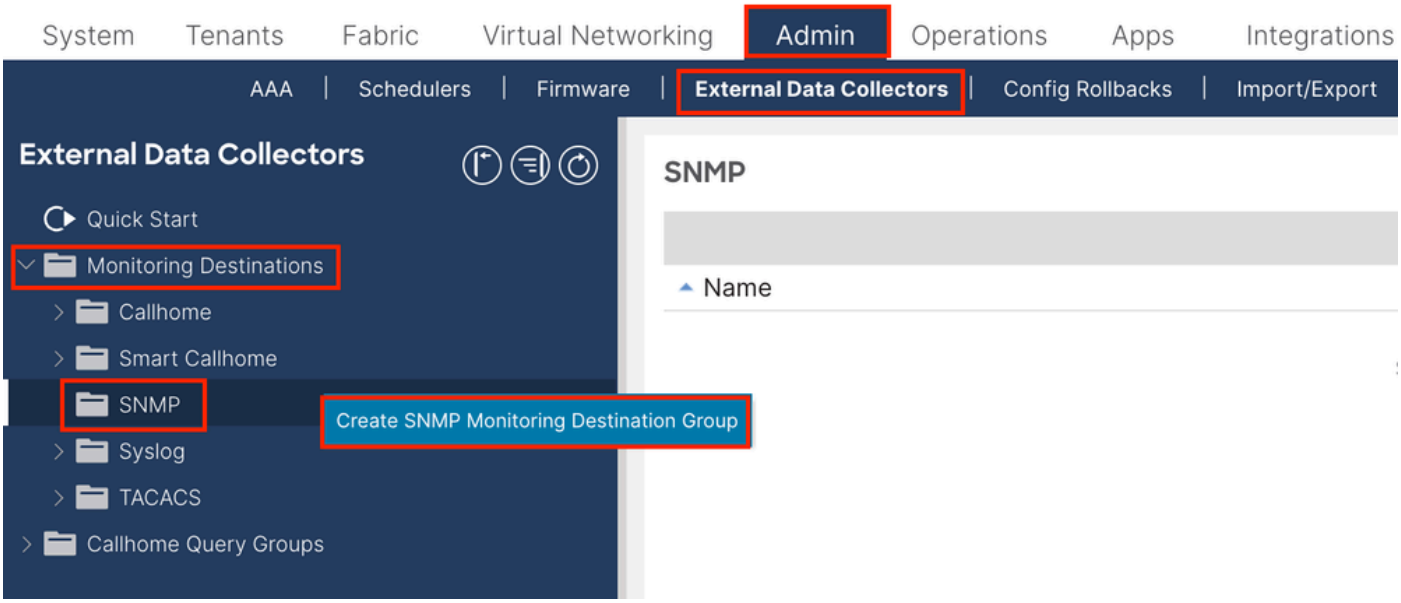


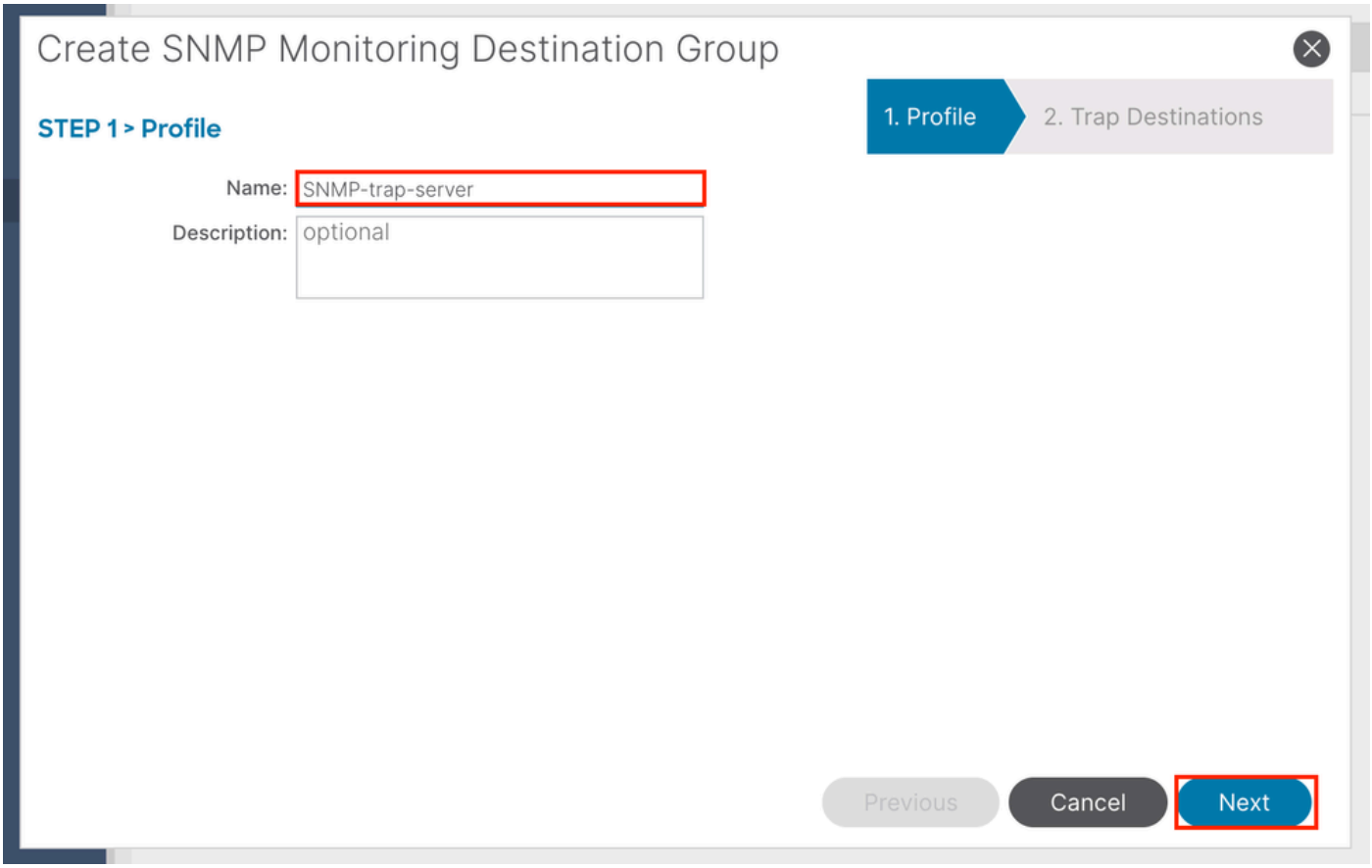
注意：如果没有上一节中的步骤1-3,SNMP TRAPs配置是不够的。步骤2.在SNMP TRAP配置中，与（接入/交换矩阵/租户）的监控策略相关。

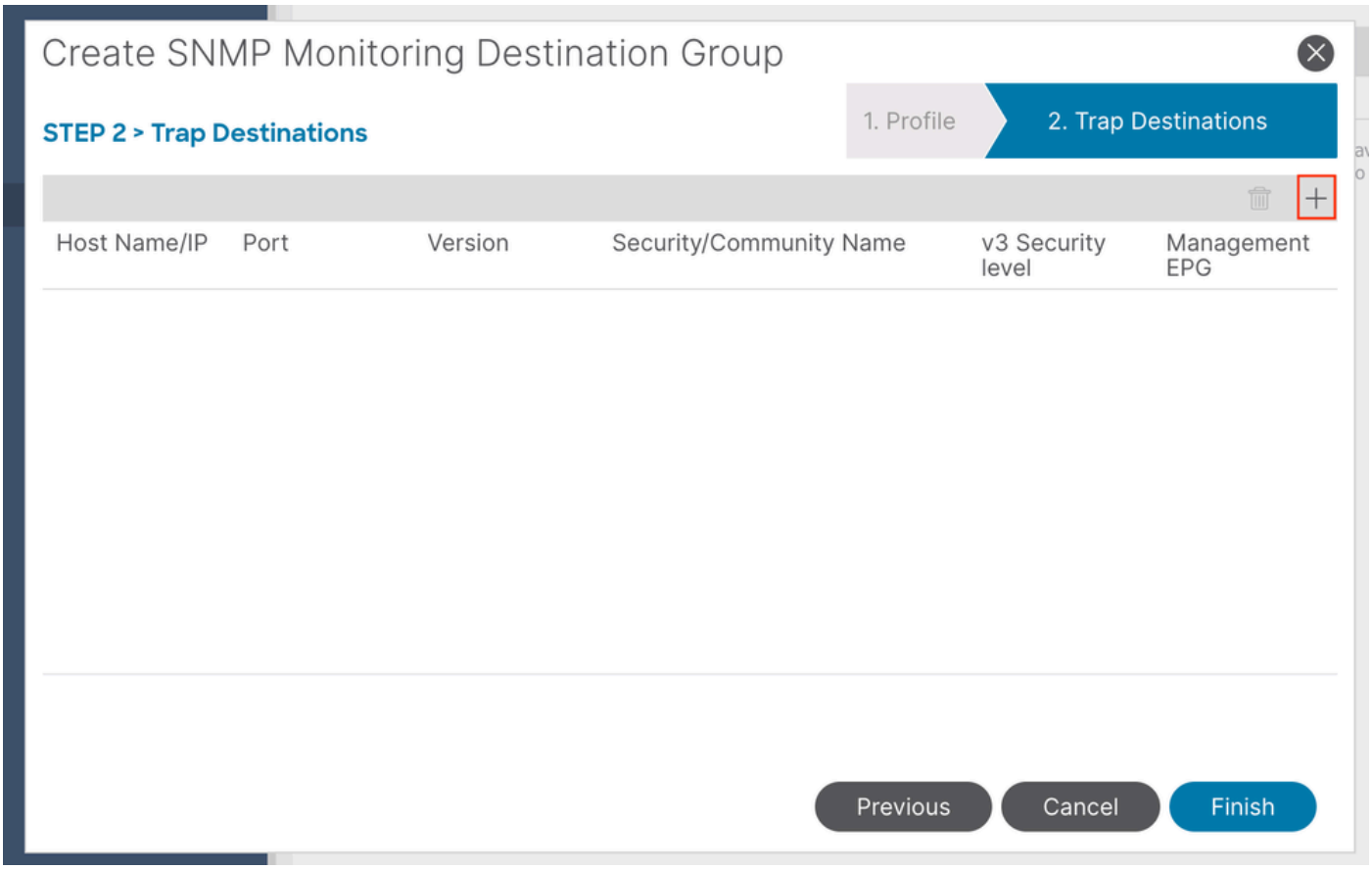
要在ACI中配置SNMP TRAP，除了上节中的步骤1、2和3外，还需要两个步骤。

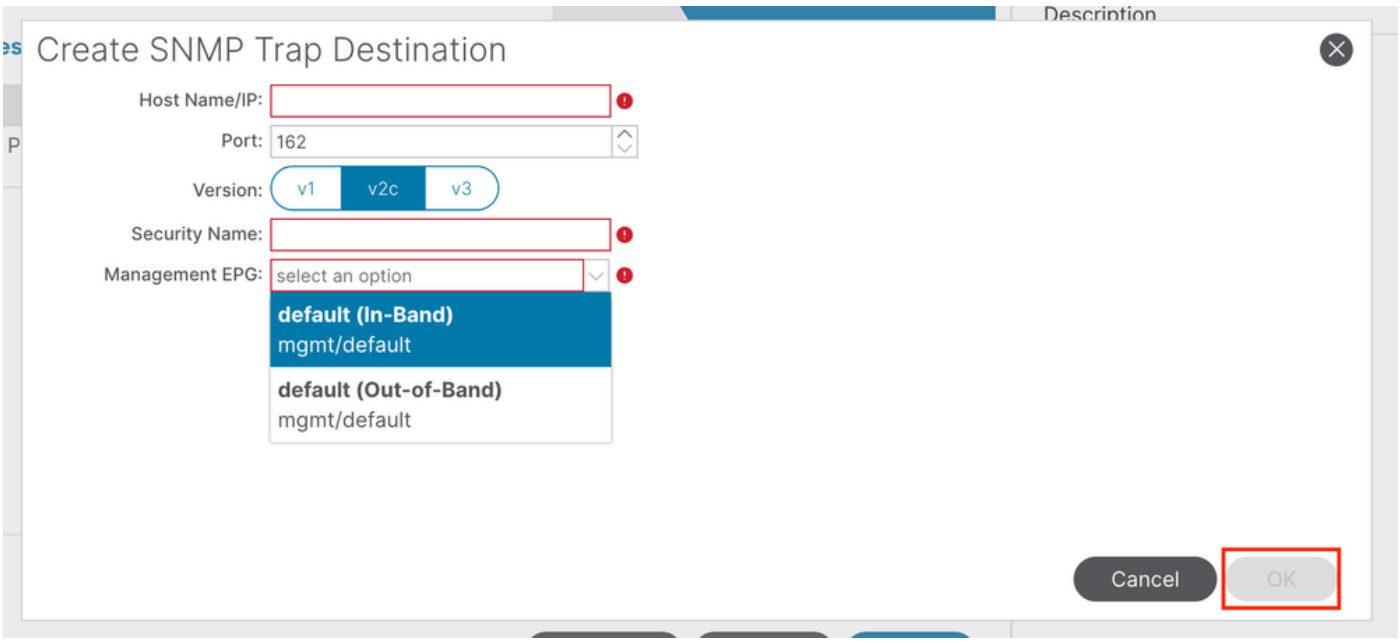
步骤1.配置SNMP TRAP服务器

为此，请导航至APIC Web GUI路径；Admin > Eternal Data Collectors > Monitoring Destinations > SNMP。


System
Tenants
Fabric
Virtual Networking
Admin
Operations
Apps
Integrations
AAA
Schedulers
Firmware
External Data Collectors
Config Rollbacks
Import/Export
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





主机名/IP - SNMP陷阱目标的主机。

端口- SNMP陷阱目标的服务端口。范围为0（未指定）至65535;默认值为 162。

版本 — SNMP陷阱目标支持的CDP版本。版本可以是：

- v1 — 使用社区字符串匹配进行用户身份验证。
- v2c — 使用社区字符串匹配进行用户身份验证。

- v3 -用于网络管理的基于标准的可互操作协议，通过结合身份验证和加密网络上的帧，提供对设备的安全访问。

默认值为v2c。

安全名称- SNMP陷阱目标安全名称（社区名称）。 它不能包含@符号。

v.3安全级别 — SNMP目标路径的SNMPv3安全级别。级别可以是：

- auth
- noauth
- priv

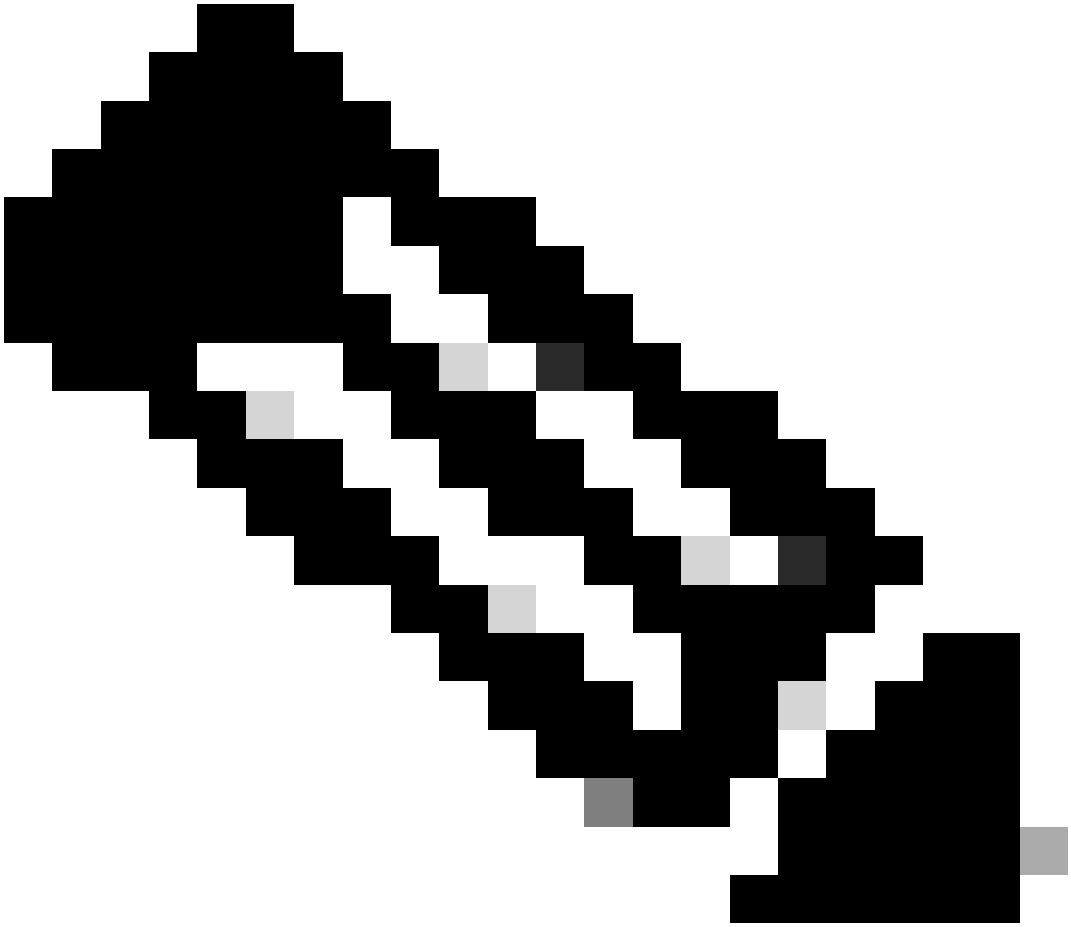
默认值为noauth。

管理EPG — 用于访问远程主机的SNMP目标的管理终端组的名称。

步骤2.在（访问/交换矩阵/租户）监控策略下配置SNMP TRAP源

您可以使用以下三个范围创建监控策略：

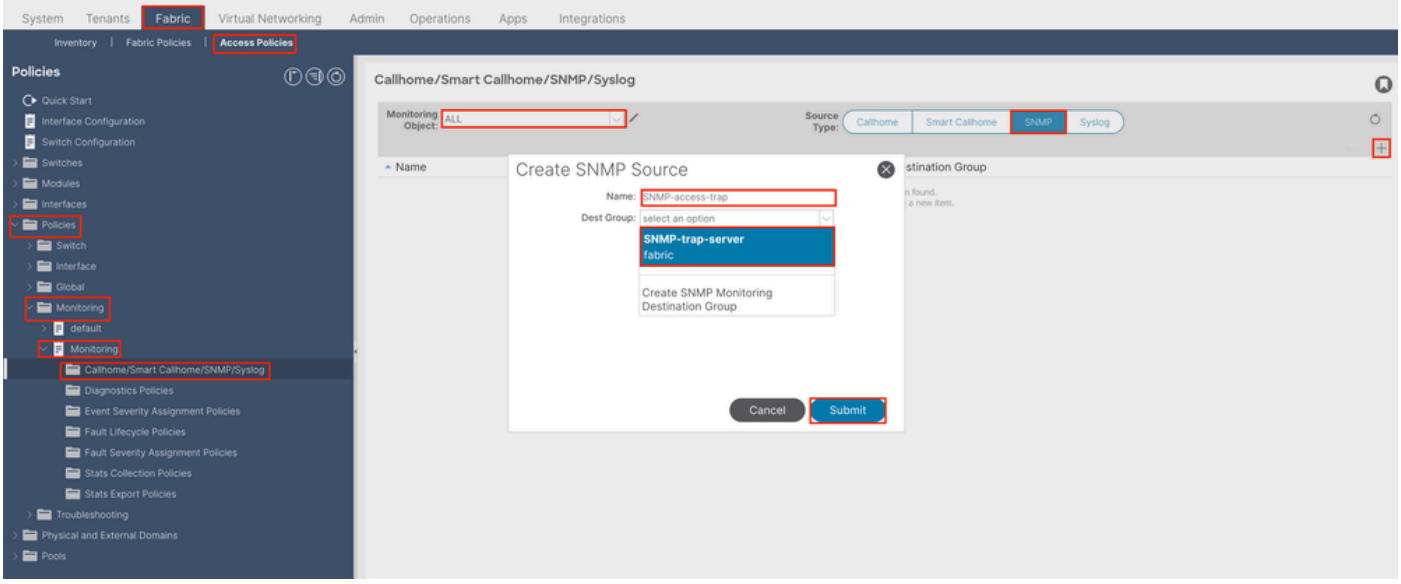
- 接入 — 接入端口、FEX、VM控制器
- 交换矩阵 — 交换矩阵端口、卡、机箱、风扇
- 租户 — EPG、应用配置文件、服务

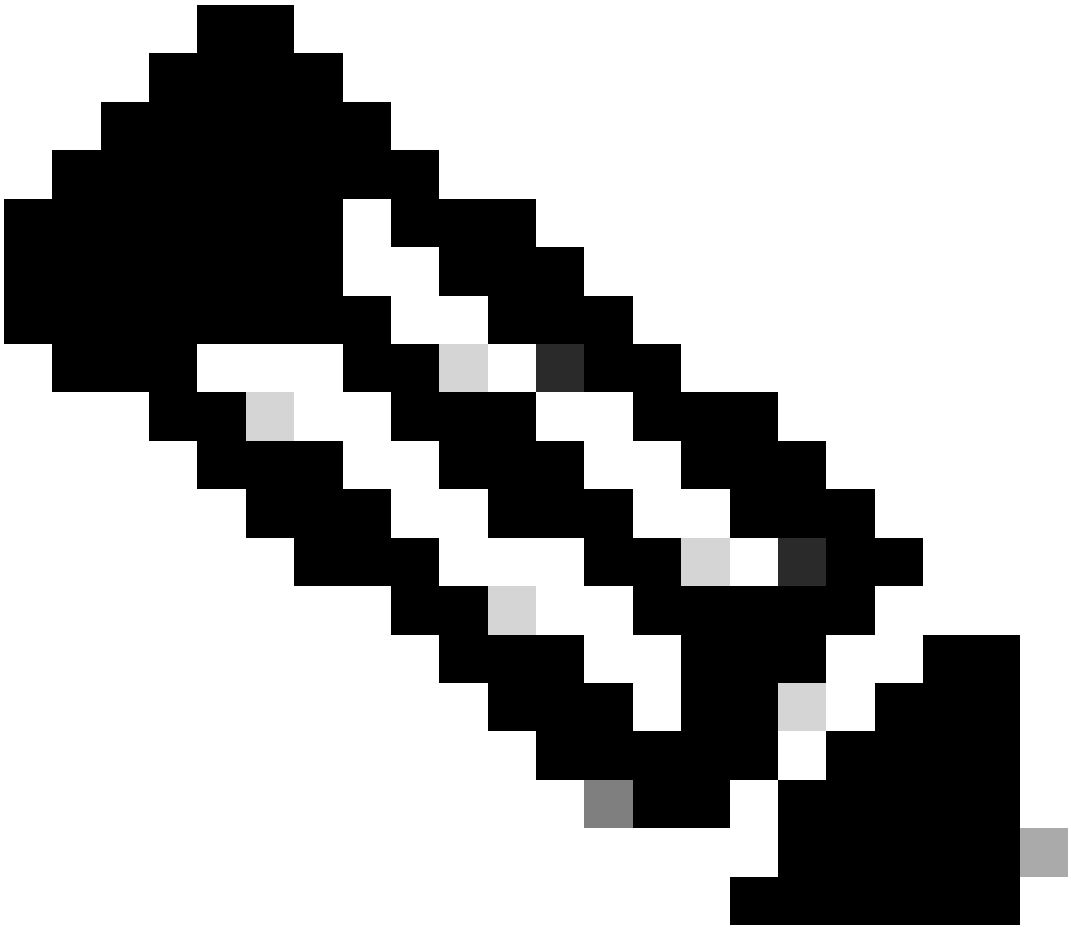


注意：您可以选择任意一个或它们的任意组合，以便根据您的需要进行配置。

选项1.在“访问策略”下定义SNMP源

为此，请导航至APIC Web GUI路径；Fabric > Access Polices > Polices > Monitoring > Default > Callhome/Smart Callhome/SNMP/Syslog/TACACS.

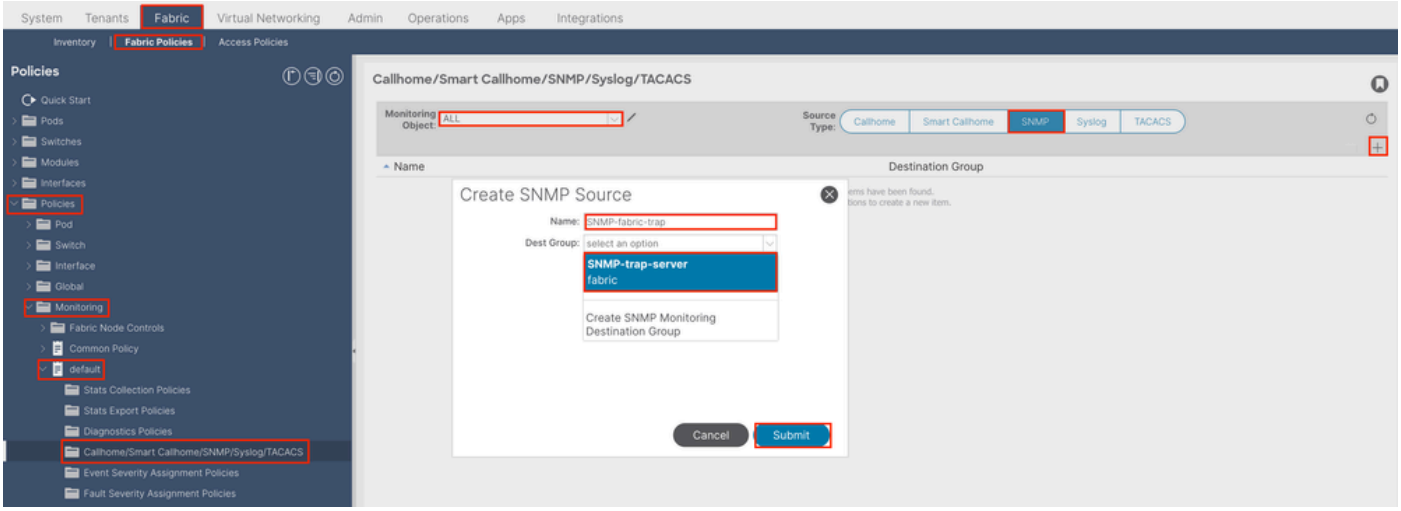




注意：您可以使用自定义的监控策略（如果已配置）而不是默认监控策略，请在此处使用默认策略。您可以指定要监控的监控对象；都是在这里使用的。

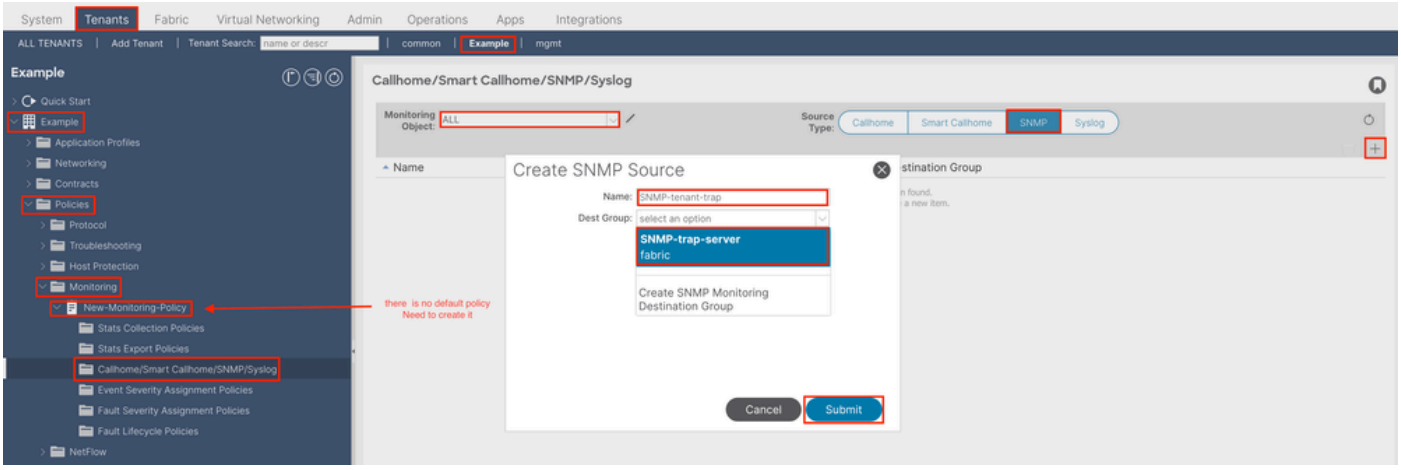
选项2.在“交换矩阵策略”下定义SNMP源

为此，请导航至APIC Web GUI路径；Fabric > Fabric Polices > Polices > Monitoring > Default > Callhome/Smart Callhome/SNMP/Syslog/TACACS.



选项3.在“租户策略”下定义SNMP源

为此，请导航至APIC Web GUI路径；Tenant > (Tenant Name) > Polices > Monitoring > (Custom monitoring policy) > Callhome/Smart Callhome/SNMP/Syslog/TACACS.



验证

使用snmpwalk命令进行验证

首先，观察从枝叶交换机的全局范围中提取SNMP数据。使用snmpwalk命令可以做到这一点；snmpwalk -v 2c -c New-1 x.x.x.x.

此细分命令表示：

snmpwalk =安装在MacOS/Linux/Windows上的snmpwalk可执行文件
-v =指定要使用的SNMP版本

2c=指定使用SNMP版本2c
-c=指定特定社区字符串
New-1=社区字符串用于提取全局范围SNMP数据
x.x.x.x=我的枝叶交换机的带外管理IP地址

命令结果：

```
$ snmpwalk -v 2c -c New-1 x.x.x.x
SNMPv2-MIB::sysDescr.0 = STRING: Cisco NX-OS(tm) aci, Software (aci-n9000-system), Version 15.2(8e), RE
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.12.3.1.3.1626
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (45013216) 5 days, 5:02:12.16
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: leaf1
SNMPv2-MIB::sysLocation.0 = STRING:
SNMPv2-MIB::sysServices.0 = INTEGER: 70
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (3) 0:00:00.03
SNMPv2-MIB::sysORID.1 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.2 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup
SNMPv2-MIB::sysORID.3 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.4 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.5 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORDescr.1 = STRING: The MIB module for SNMPv2 entities
SNMPv2-MIB::sysORDescr.2 = STRING: View-based Access Control Model for SNMP.
SNMPv2-MIB::sysORDescr.3 = STRING: The SNMP Management Architecture MIB.
SNMPv2-MIB::sysORDescr.4 = STRING: The MIB for Message Processing and Dispatching.
SNMPv2-MIB::sysORDescr.5 = STRING: The management information definitions for the SNMP User-based Secur
```

在截取的命令输出中，您可以看到snmpwalk成功并且提取了特定于硬件的信息。如果让snmpwalk继续，您将看到硬件接口名称、说明等。

现在，继续使用SNMP社区字符串New-1检索VRF情景SNMP数据、以前创建的SNMP情景、VRF的New-VRF-SNMP。

由于在两个不同的SNMP情景中使用相同的社区字符串New-1，因此必须指定要从中提取SNMP数据的SNMP情景。您需要使用snmpwalk语法来指定特定SNMP情景；snmpwalk -v 2c -c New-1@New-VrF-SNMP 10.x.x.x.

您可以看到，要从特定SNMP情景中提取，请使用以下格式：.

使用CLI Show命令

在APIC上：

```
show snmp
show snmp policy
```

```
show snmp summary
```

```
show snmp clientgroups
show snmp community
show snmp hosts
show snmp engineid
```

在交换机上：

```
show snmp
show snmp | grep "SNMP packets"
show snmp summary
show snmp community
show snmp host
show snmp engineID
show snmp context
show snmp user
show snmp internal dump-internal-log
show snmp internal globals
show snmp internal trace log
```

使用CLI Moquery命令

在APIC/交换机上：

```
moquery -c snmpGroup         #The SNMP destination group, which contains information needed to send tra
moquery -c snmpTrapDest      #A destination to which traps and informs are sent.
moquery -c snmpRtDestGroup   #A target relation to SNMP destination group. This group contains informat
moquery -c snmpPol           #The SNMP policy, which enables you to monitor client group, v3 user, and/
moquery -c snmpClientGrpP    #A client group, which is a group of client IP addresses that allows SNMP
moquery -c snmpCommunityP    #The SNMP community profile, which enables access to the router or switch
moquery -c snmpRtSnmpPol     #A target relation to an SNMP policy that contains site information and ge
moquery -c snmpClientP       #The client profile information.
moquery -c snmpRsEpg         #A source relation to the endpoint group VRF through which the clients can
moquery -c snmpSrc           #The SNMP source profile, which determines the fault information, severity
moquery -c snmpCtxP          #The SNMP context profile, which enables you to specify a context to monit
```

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-policies/filters/summary
cat /aci/tenants/mgmt/node-management-epgs/default/out-of-band/default/summary
cat /aci/admin/external-data-collectors/monitoring-destinations/snmp/*/snmp-trap-destinations/summary
cat /aci/fabric/fabric-policies/pod-policies/policies/snmp/summary
cat /aci/fabric/fabric-policies/pod-policies/policies/snmp/*/summary
```

```
cat /aci/fabric/fabric-policies/pod-policies/policies/snmp/*/client-group-policies/*/*/summary
cat /aci/fabric/fabric-policies/pod-policies/policy-groups/summary
cat /aci/fabric/fabric-policies/pod-policies/pod-selector-default-all/summary
cat /aci/fabric/fabric-policies/monitoring-policies/monitoring-policy-default/callhome-snmp-syslog/all/
cat /aci/fabric/fabric-policies/monitoring-policies/common-policy/callhome-snmp-syslog/snmp/*/summary
cat /aci/fabric/access-policies/monitoring-policies/default/callhome-snmp-syslog/all/snmp*/summary
```

故障排除

检查snmpd流程

在交换机上：

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

在APIC上：

```
ps aux | grep snmp
```

如果过程正常，请联系思科TAC以获得更多帮助。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。