ACIでのSNMPの設定

内容

はじめに

このドキュメントでは、ACIでの簡易ネットワーク管理プロトコル(SNMP)およびSNMPトラップの設定について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ファブリック検出が完了しました
- Application Policy Infrastructure Controller(APIC)およびファブリックスイッチへのインバンド/アウトオブバンド接続

- SNMPトラフィックを許可するように設定されたインバンド/アウトオブバンド契約（UDPポート161および162）
- デフォルトの管理テナントの下でAPICおよびファブリックスイッチ用に設定されたスタティックノード管理アドレス（これがないと、APICからのSNMP情報の取得に失敗します）
- SNMPプロトコルワークフローを理解する

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- APIC
- ブラウザ
- 5.2(8e)を実行するアプリケーションセントリックインフラストラクチャ(ACI)
- Snmpwalk command

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

Cisco ACIは、Management Information Base（MIB；管理情報ベース）や通知（トラップ）などのSNMPv1、v2c、およびv3をサポートしています。SNMP標準を使用すると、異なるMIBをサポートするサードパーティ製アプリケーションで、ACIリーフ/スパイン型スイッチとAPICコントローラを管理およびモニタできます。

ただし、SNMP書き込みコマンド(Set)はACIではサポートされていません。

SNMPポリシーは、リーフスイッチとスパインスイッチ、およびAPICコントローラに対して個別に適用され、実行されます。各ACIデバイスは独自のSNMPエンティティを持つため、APICクラスタ内の複数のAPICは、スイッチだけでなく個別にモニタする必要があります。ただし、SNMPポリシーソースは、ACIファブリック全体の監視ポリシーとして作成されます。

デフォルトでは、SNMPはポーリングに**UDP** ポート**161** を使用し、トラップにポート**162** を使用します。

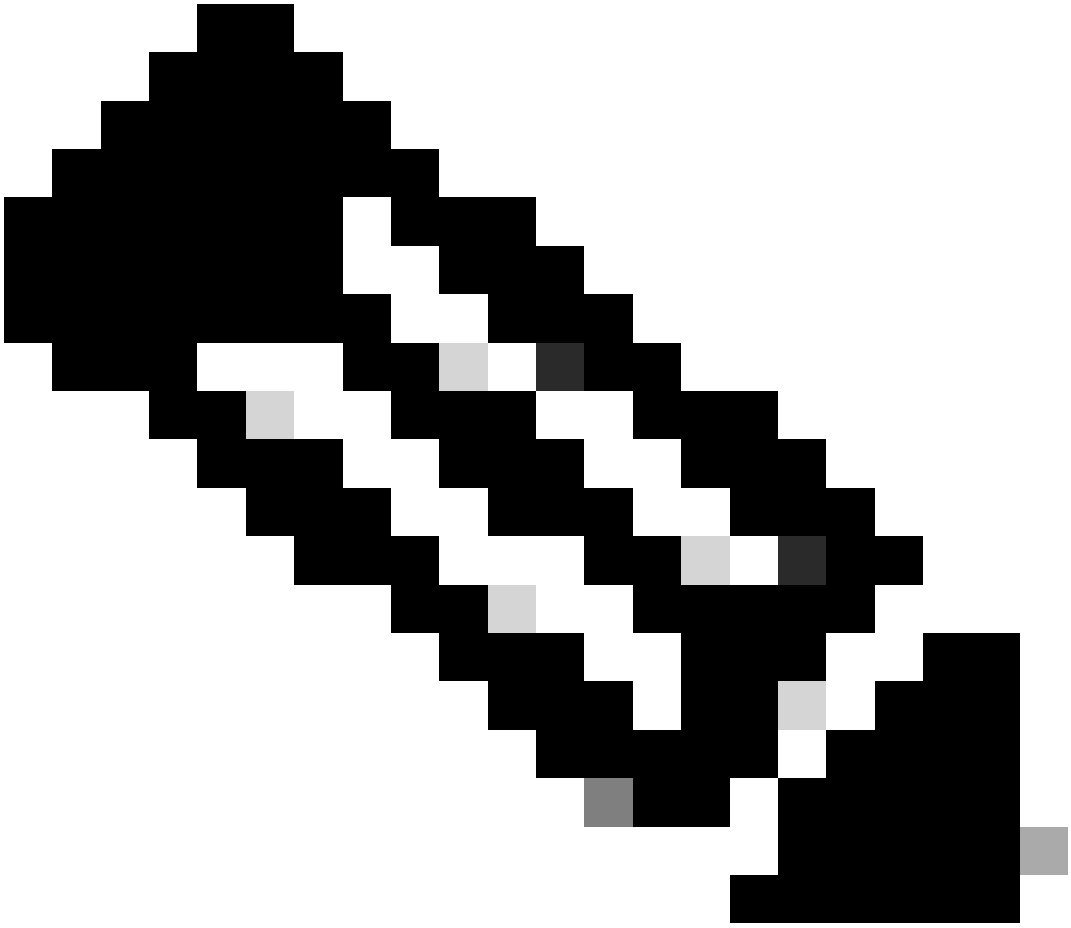
SNMPスコープについて

ACIにおけるSNMPの基本的な概念の1つは、SNMP情報の取得元となるスコープが2つあることです。
1. グローバル
2. Virtual Routing and Forwarding(VRF)コンテキスト

グローバルスコープでは、リーフ/スパインノードのインターフェイス数、インターフェイスインデックス、インターフェイス名、インターフェイスステータスなどのシャーシMIBが抽出されます。

VRF Context **Scope固有のMIB**は、**IP**アドレスやルーティングプロトコル情報など、**VRF**固有の情報をプルします。

Cisco ACI MIBサポートリストには、サポートされているAPICおよびファブリックスイッチのグローバルMIBとVRFコンテキストMIBの完全なリストがあります。

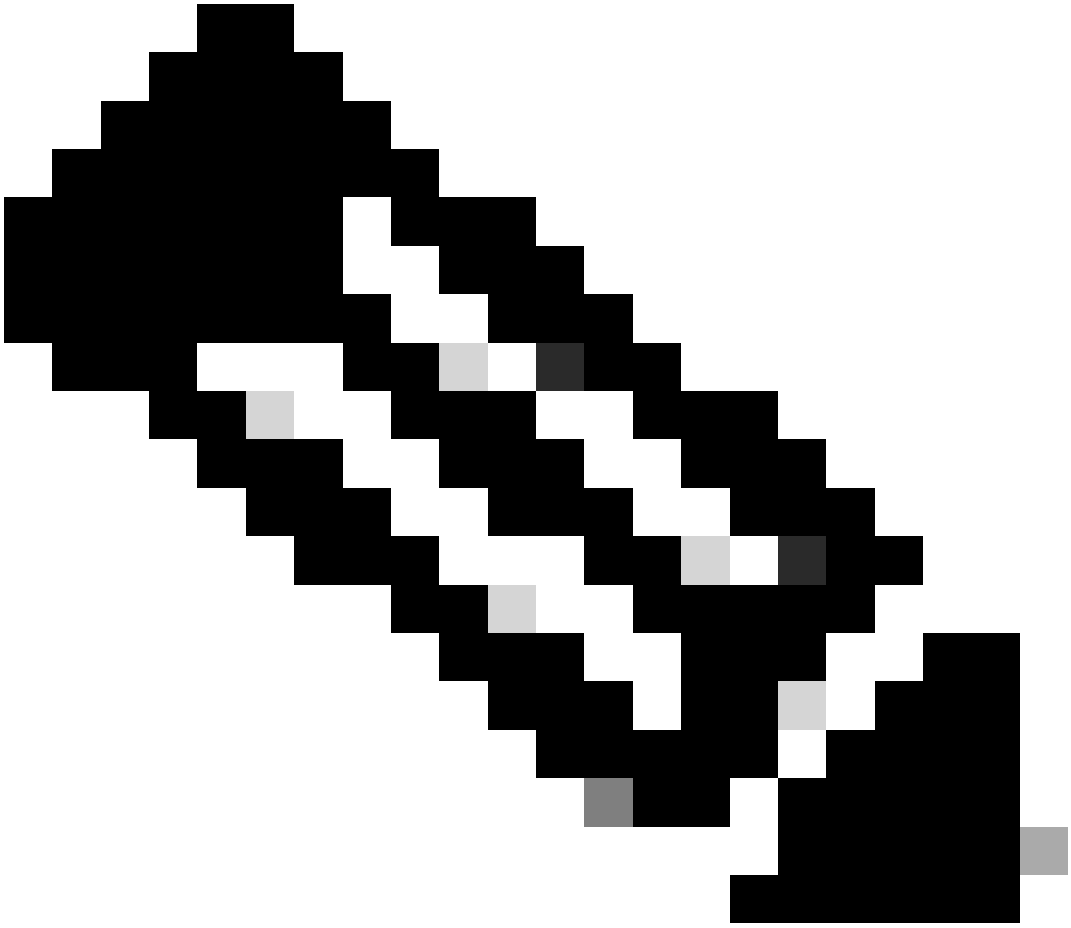


注：グローバルスコープを持つMIBは、システム内に1つのインスタンスしかありません。グローバルMIBのデータは、システム全体に関連しています。

VRF固有のスコープを持つMIBは、システム内にVRF単位のインスタンスを持つことができます。VRF固有のMIB内のデータは、そのVRFにのみ関連します。

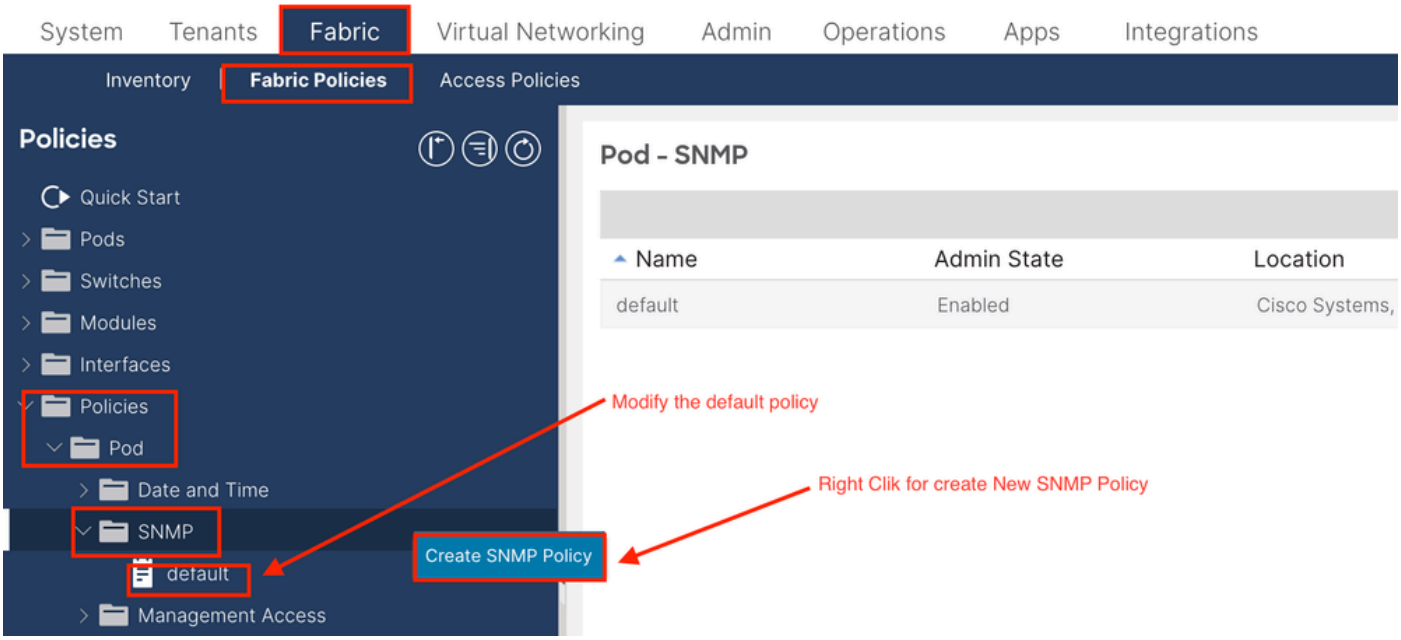
設定手順（グローバルコンテキストとVRFコンテキストの両方のスコープ用）

ステップ 1：SNMPファブリックポリシーの設定



注：ここでは、SNMPコミュニティポリシーやSNMPクライアントグループポリシーなどのSNMP設定を指定します。

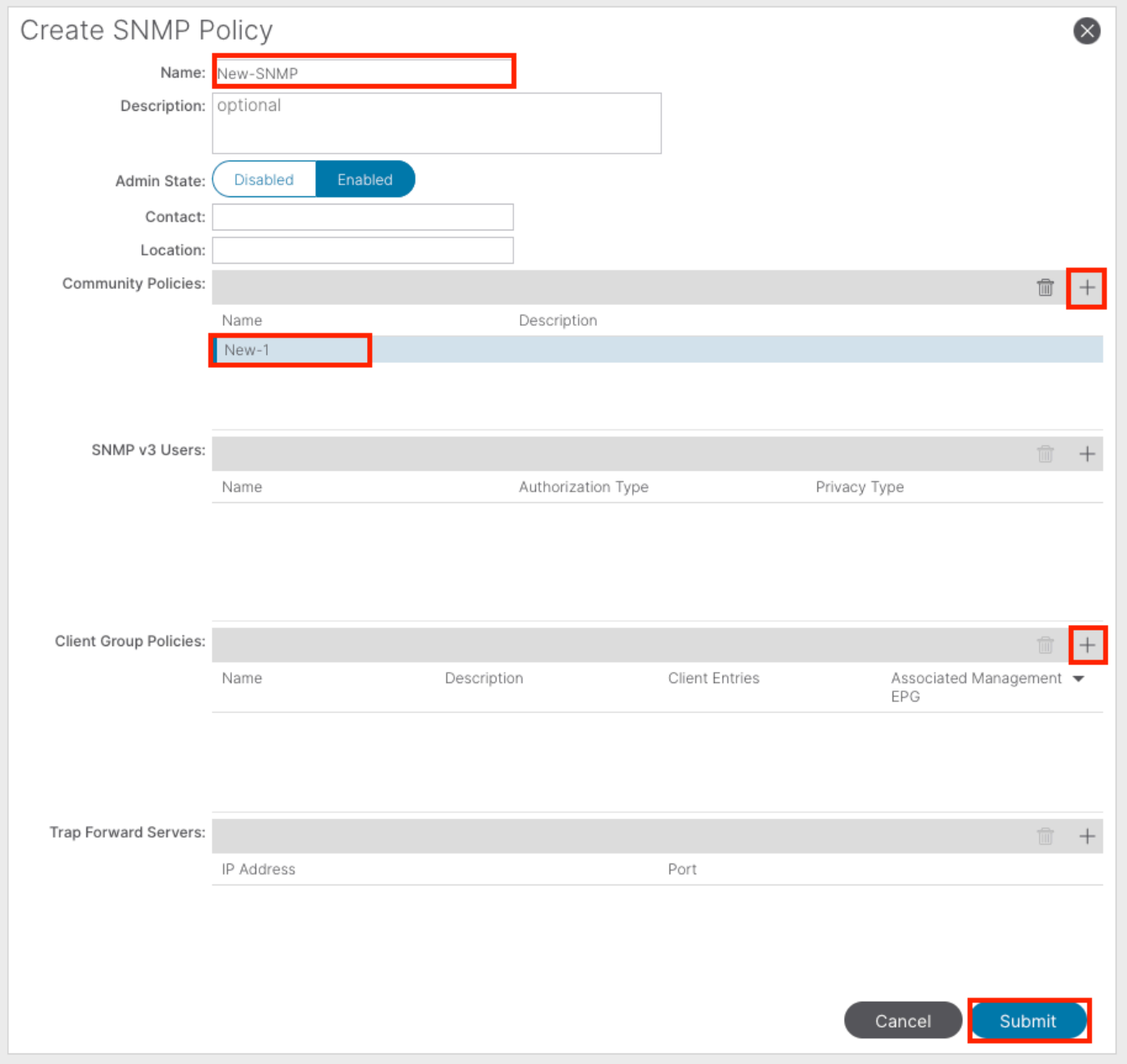
SNMPの設定の最初の手順は、必要なSNMPファブリックポリシーを作成することです。SNMPファブリックポリシーを作成するには、APIC Web GUIパスFabric > Fabric Policies > Policies > Pod > SNMPに移動します。



新しいSNMPポリシーを作成したり、デフォルトのSNMPポリシーを変更したりできます。

このドキュメントでは、SNMPポリシーは**New-SNMP**と呼ばれ、SNMPバージョンv2cを使用します。したがって、ここで必要なフィールドは、コミュニティポリシーとクライアントグループポリシーだけです。

Community Policy Nameフィールドでは、使用するSNMPコミュニティストリングを定義します。この例では、**New-1**です。これら2つのコミュニティストリングは後で説明します。



Name:SNMPポリシーの名前。この名前には、1 ~ 64 文字の英数字を使用できます。

Description:SNMPポリシーの説明。説明には、0 ~ 128文字の英数字を使用できます。

Admin State:SNMPポリシーの管理状態。状態は有効または無効にできます。状態には次のものがあります。

- enabled:admin状態は有効です
- disabled：管理状態は無効です

デフォルトは**disabled**です。

Contact:SNMPポリシーの連絡先情報。

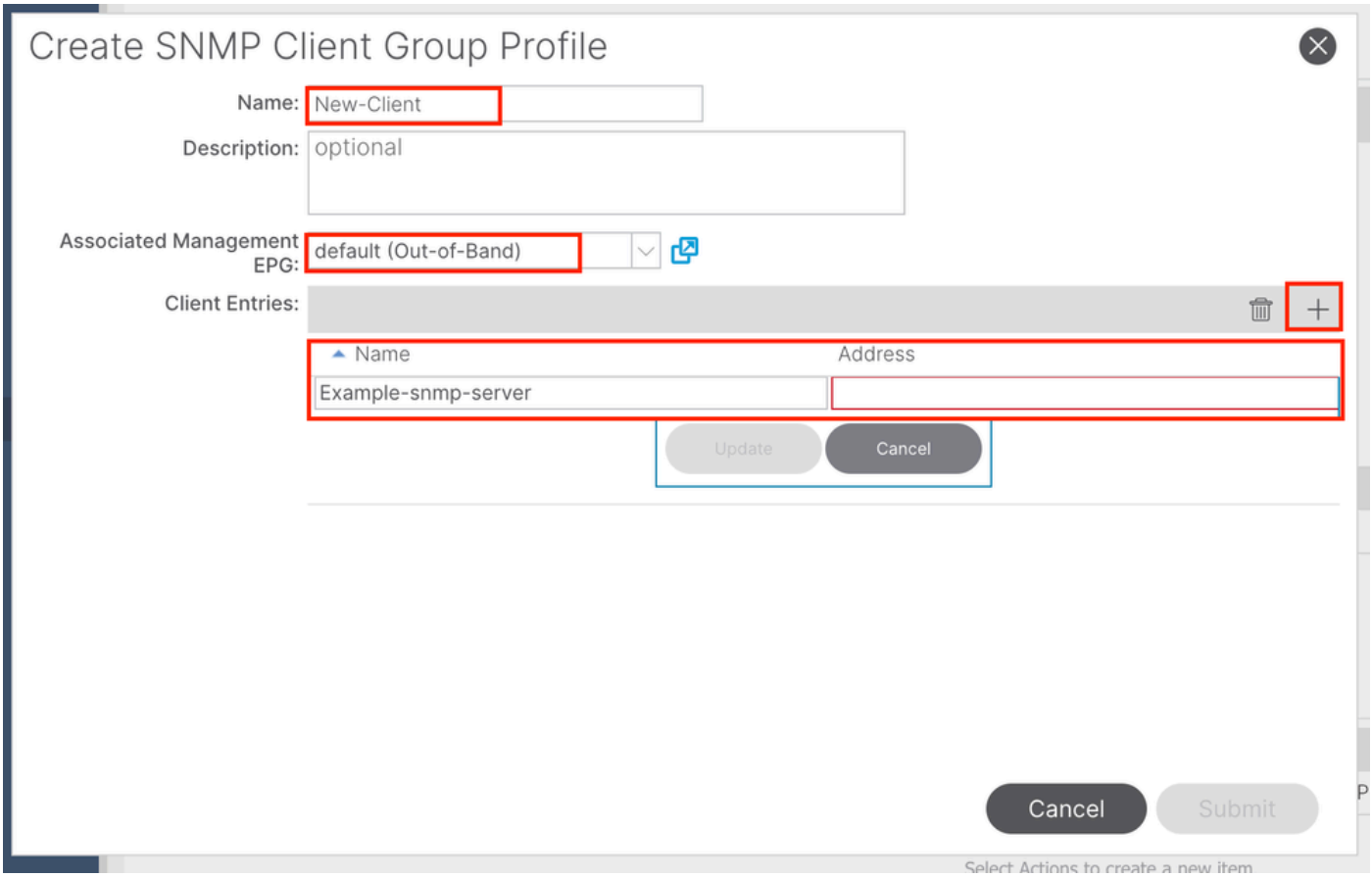
Location:SNMPポリシーの場所。

SNMP v3ユーザ：SNMPユーザプロファイルは、ネットワーク内のデバイスを監視するためにユーザをSNMPポリシーに関連付けるために使用されます。

コミュニティポリシー：SNMPコミュニティプロファイルは、モニタリング用のルータまたはスイッチの統計情報へのアクセスを有効にします。

クライアントグループポリシー：

次の手順では、クライアントグループポリシー/プロファイルを追加します。クライアントのグループポリシーおよびプロファイルの目的は、APICおよびファブリックスイッチからSNMPデータをプルできるIPおよびサブネットを定義することです。



Name：クライアントグループプロファイルの名前。この名前には、1 ~ 64 文字の英数字を使用できます。

Description：クライアントグループプロファイルの説明。説明には、0 ~ 128文字の英数字を使用できます。

関連管理エンドポイントグループ(EPG):VRFへのアクセスに使用されるエンドポイントグループの識別名。サポートされる文字列の最大長は255文字のASCII文字です。デフォルトは、管理テナントのアウトオブバンド管理アクセスEPGです。

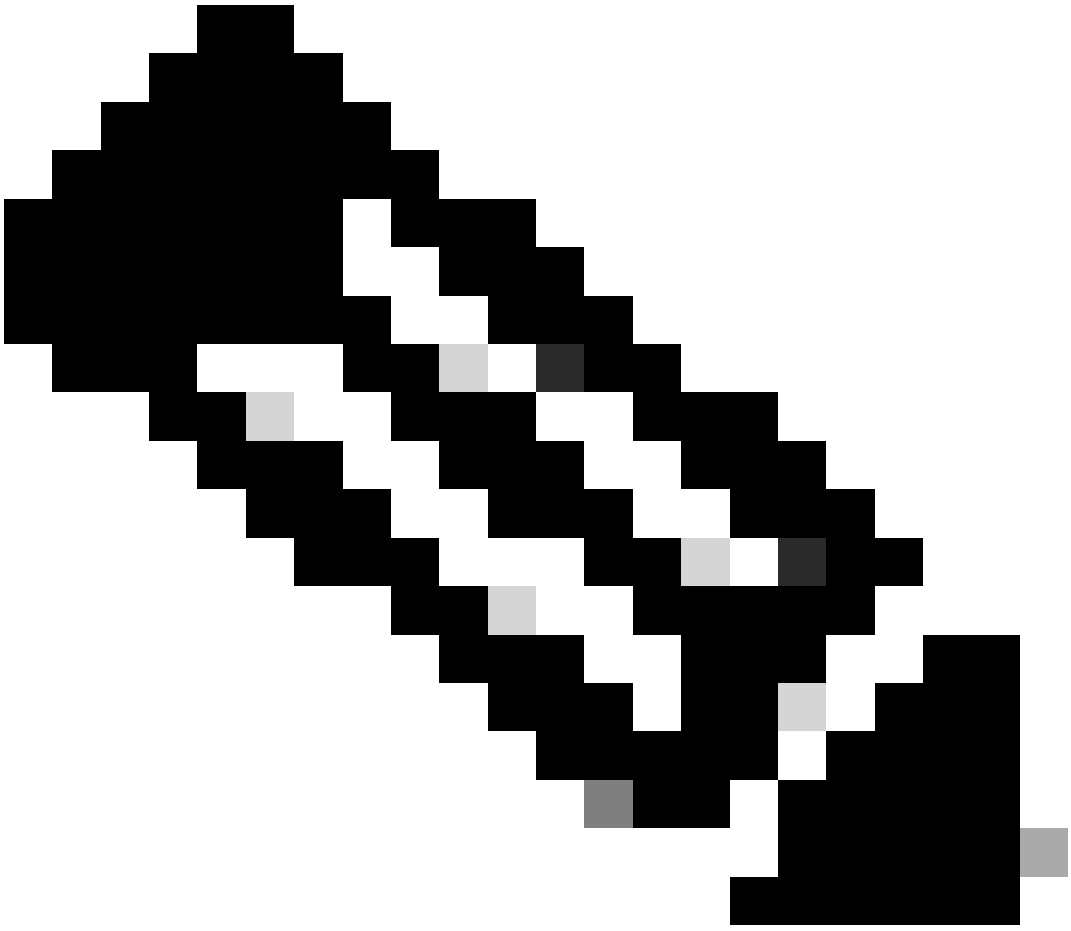
Client Entries:SNMPクライアントプロファイルのIPアドレス。

このドキュメントでは、クライアントのグループポリシーおよびプロファイルは**New-Client**と呼ばれます。

クライアントのグループポリシー/プロファイルで、優先される管理EPGを関連付ける必要があります。選択した管理EPGに、SNMPトラフィック（UDPポート161および162）を許可するために必要なコントラクトがあることを確認する必要があります。このドキュメントでは、説明の目的でデフォルトのアウトオブバンド管理EPGを使用します。

最後のステップでは、特定のIPまたはサブネット全体にアクセスしてACI SNMPデータを取得できるようにクライアントエントリを定義します。特定のIPまたはサブネット全体を定義するための構文があります。

- 特定のホストIP:192.168.1.5
- サブネット全体：192.168.1.0/24

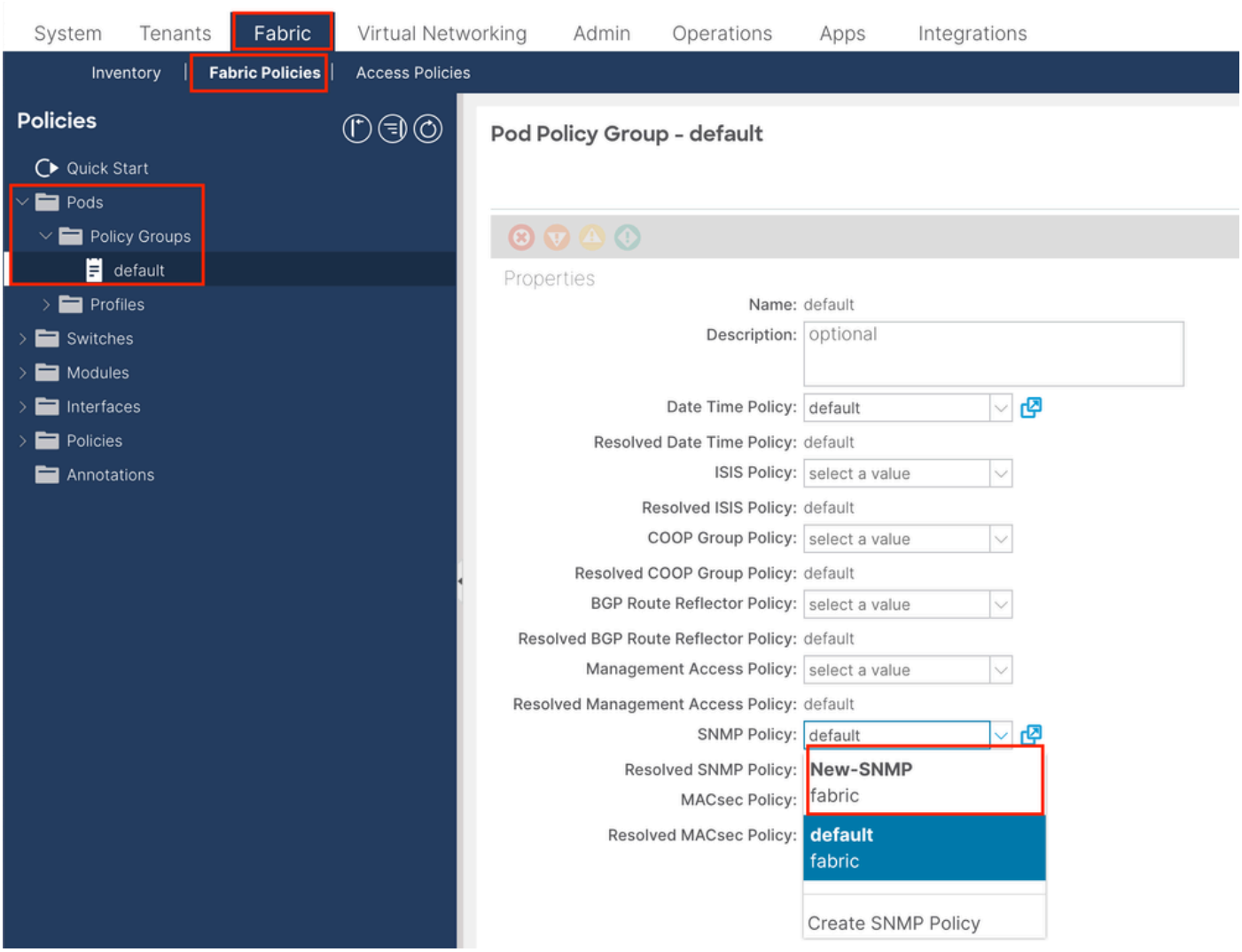


注：クライアントエントリに0.0.0.0を使用してすべてのサブネットを許可することはできません（すべてのサブネット

にSNMP MIBへのアクセスを許可する場合は、クライアントエントリを空のままにしてください）。

ステップ 2：ポッドポリシーグループ（ファブリックポリシーグループ）へのSNMPポリシーの適用

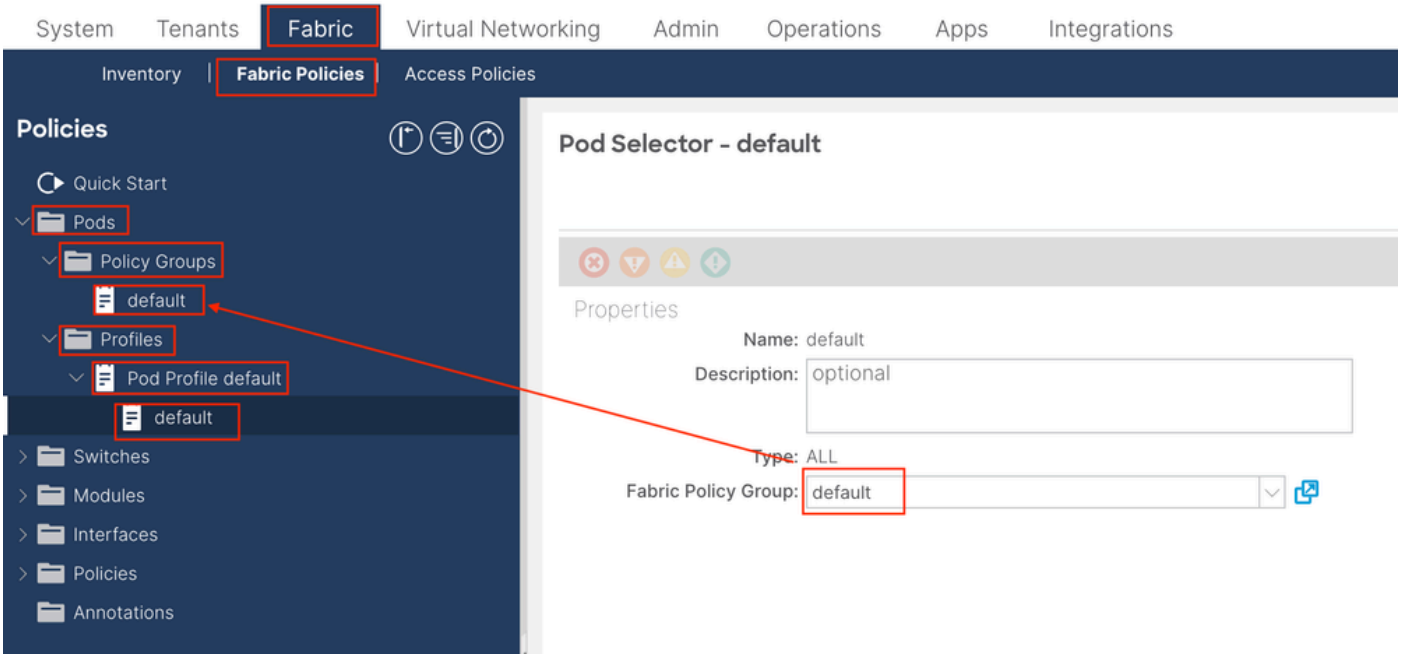
この設定を適用するには、APIC Web GUIのパスFabric > Fabric Policies > Pods > Policy Groups > POD_POLICY_GROUP(ドキュメントのデフォルト)に移動します。



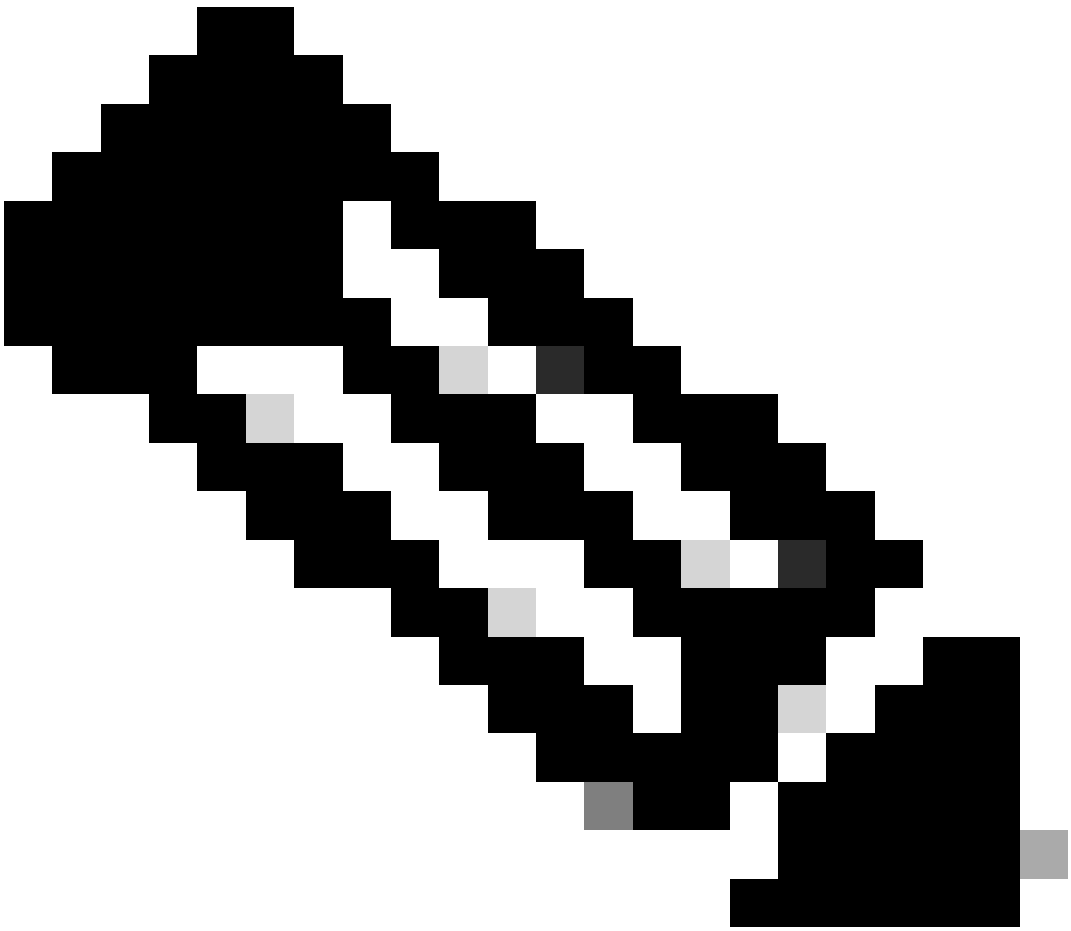
右側のペインに、SNMP Policyのフィールドが表示されます。ドロップダウンから、新しく作成したSNMPポリシーを選択し、変更を送信します。

ステップ 3：ポッドポリシーグループとポッドプロファイルの関連付け

このドキュメントでは、わかりやすくするためにdefaultポッドプロファイルを使用します。これを行うには、APIC Web GUIのパスFabric > Fabric Policies > Pods > Profiles > POD_PROFILE(ドキュメントのデフォルト)に移動します。



この段階では、グローバルMIBの基本的なSNMPを設定します。

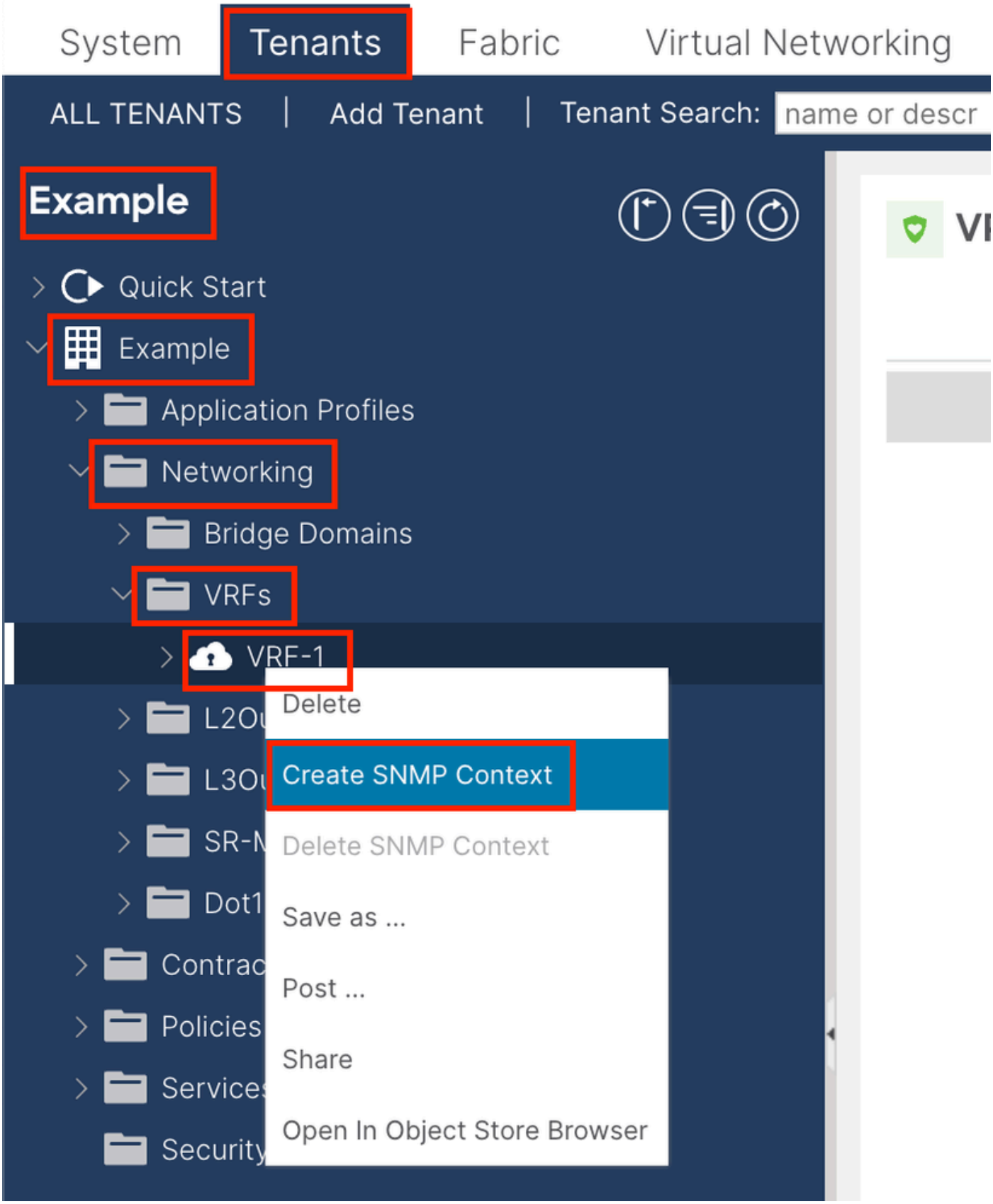


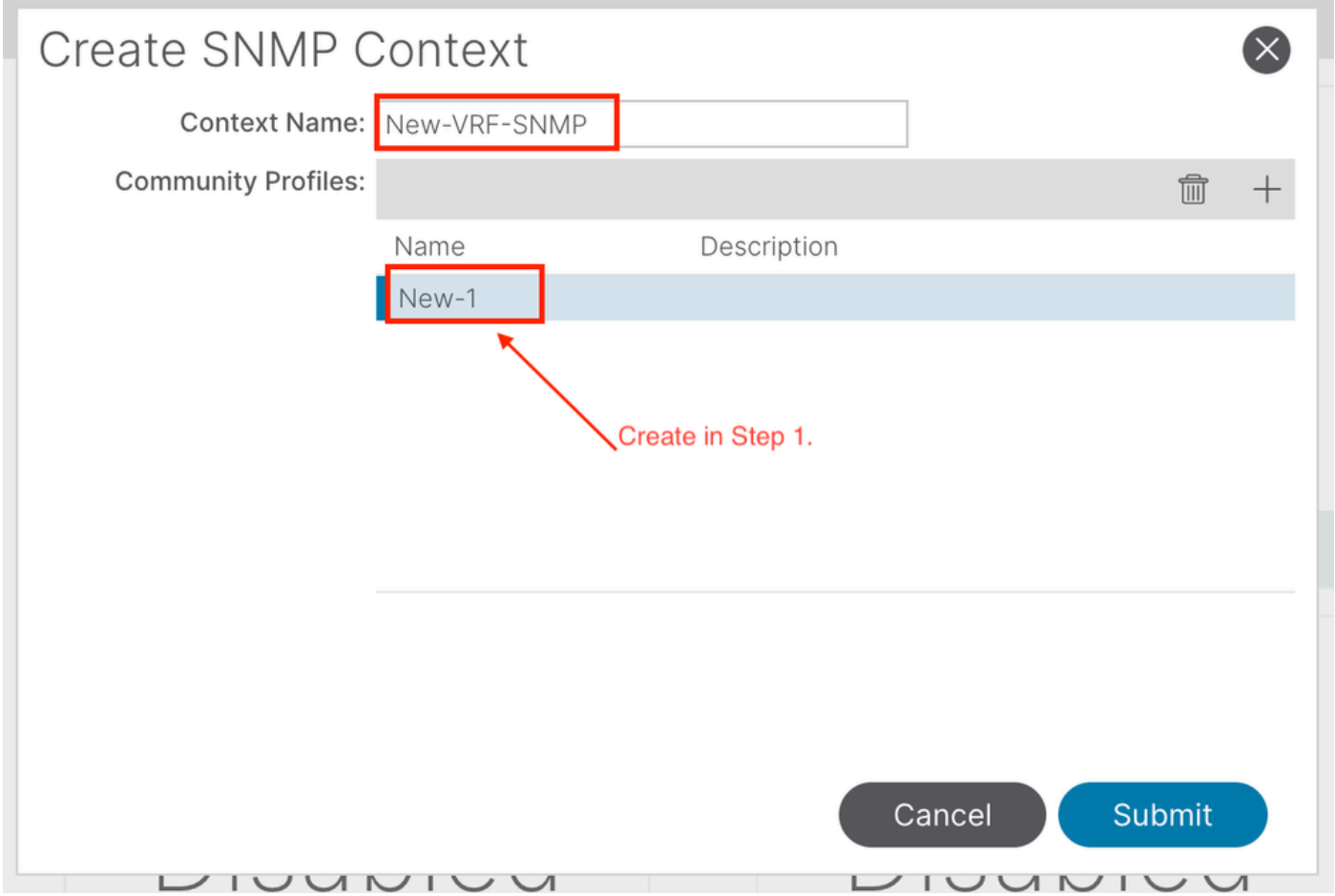
注：この時点で、SNMP設定に必要なすべての手順（ステップ1 ～ 3）が完了しており、グローバルMIBスコープが暗黙的に使用されています。 これにより、任意のACIノードまたはAPICに対してSNMPウォークを実行できます。

ステップ 4：VRFコンテキストスコープの設定

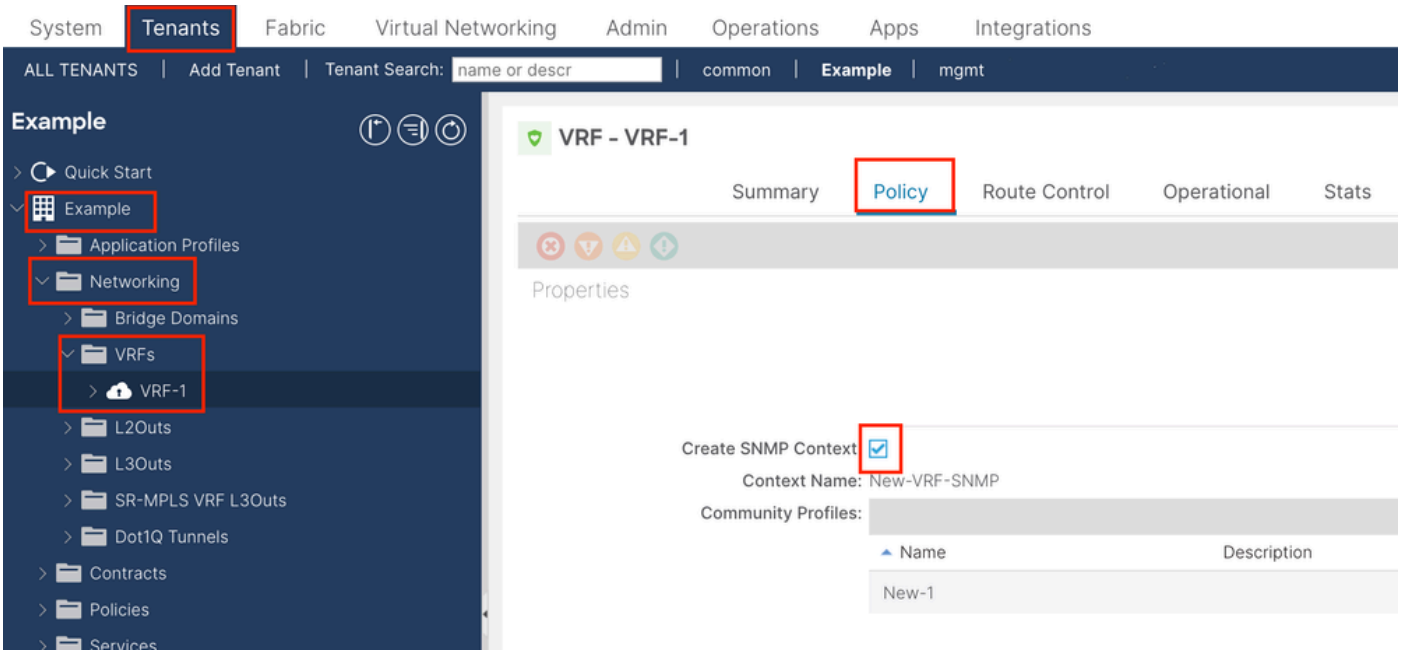
コミュニティストリングをVRFコンテキストに関連付けた後は、その特定のコミュニティストリングを使用してグローバルスコープのSNMPデータを取得することはできません。そのため、グローバルスコープとVRFコンテキストの両方のSNMPデータを取得する場合は、2つのSNMPコミュニティストリングを作成する必要があります。

この場合、以前に作成したコミュニティストリング（ステップ1.）の(**New-1**)で、VRFコンテキストスコープに**New-1** を使用し、**Example** カスタムテナントの**VRF-1** カスタムVRFを使用します。これを行うには、APIC Web GUIパス
Tenants > Example > Networking > VRFs > VRF-1 (right click) > Create SNMP Context に移動します。


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



設定を送信した後、適用したSNMPコンテキストの設定を確認するには、VRFを左クリックし、VRFのPolicyタブに移動して、ペインの一番下までスクロールします。

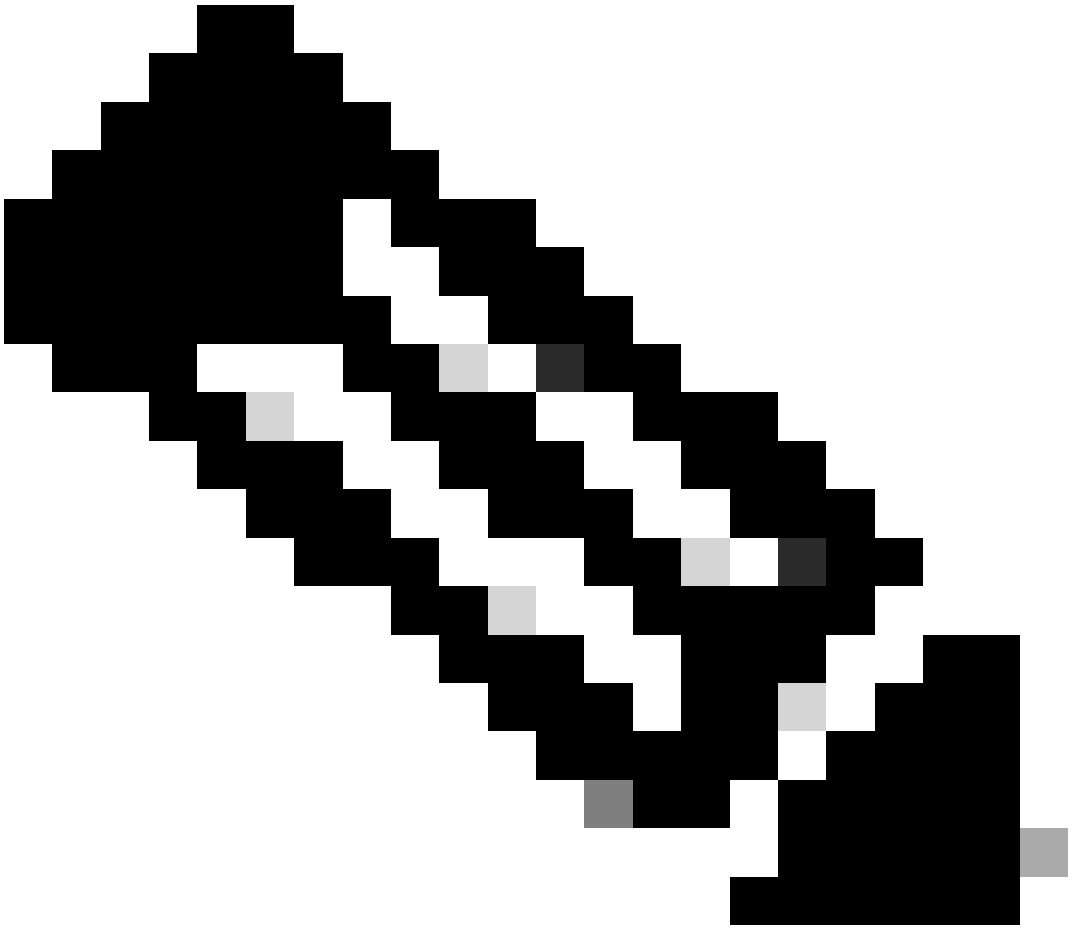


VRFでSNMPコンテキストを無効にするには、**Create SNMP Context**チェックボックスを選択解除するか（スクリーンショットを参照）、VRFを右クリックして**Delete SNMP Context**を選択します。

GUIを使用したSNMPトラップの設定

SNMP TRAPはポーリングなしでSNMPサーバ(SNMP宛先/ネットワーク管理システム(NMS))に送信され、障害/イベント（定義された条件）が発生するとACIノード/APICからSNMP TRAPが送信されます。

SNMPトラップは、アクセス/ファブリック/テナントモニタリングポリシーの下で、ポリシーのスコープに基づいて有効になります。 ACIは最大10のトラップレシーバをサポートします。

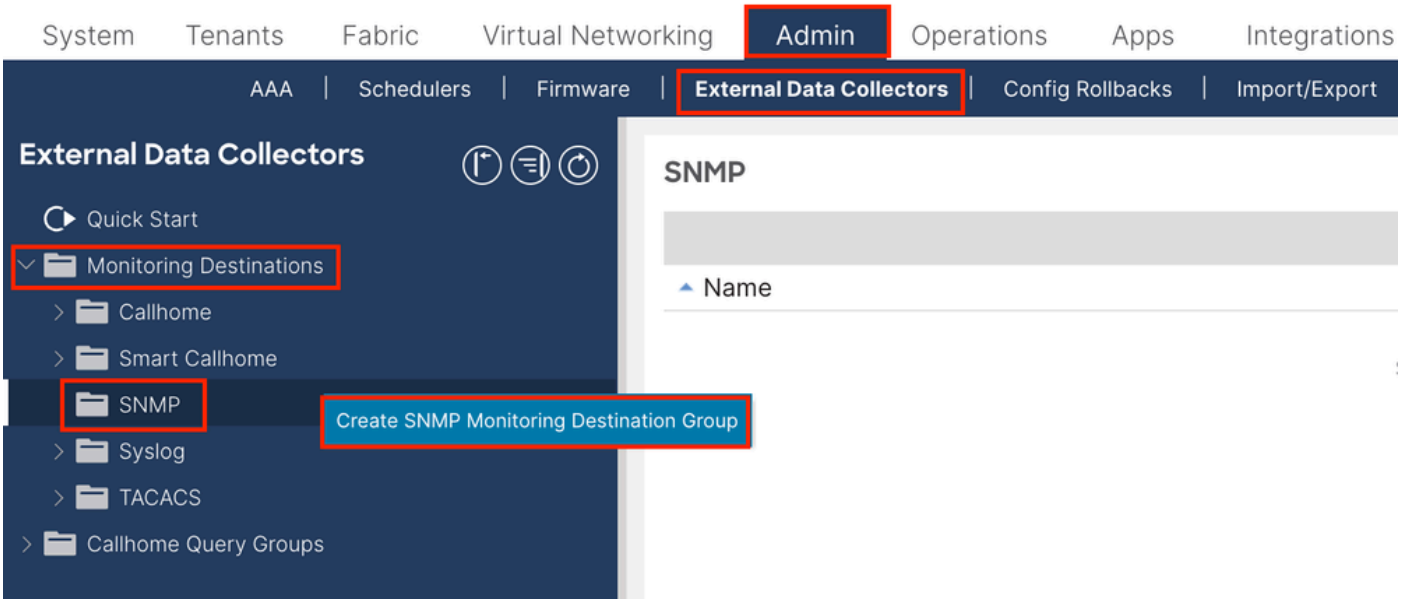


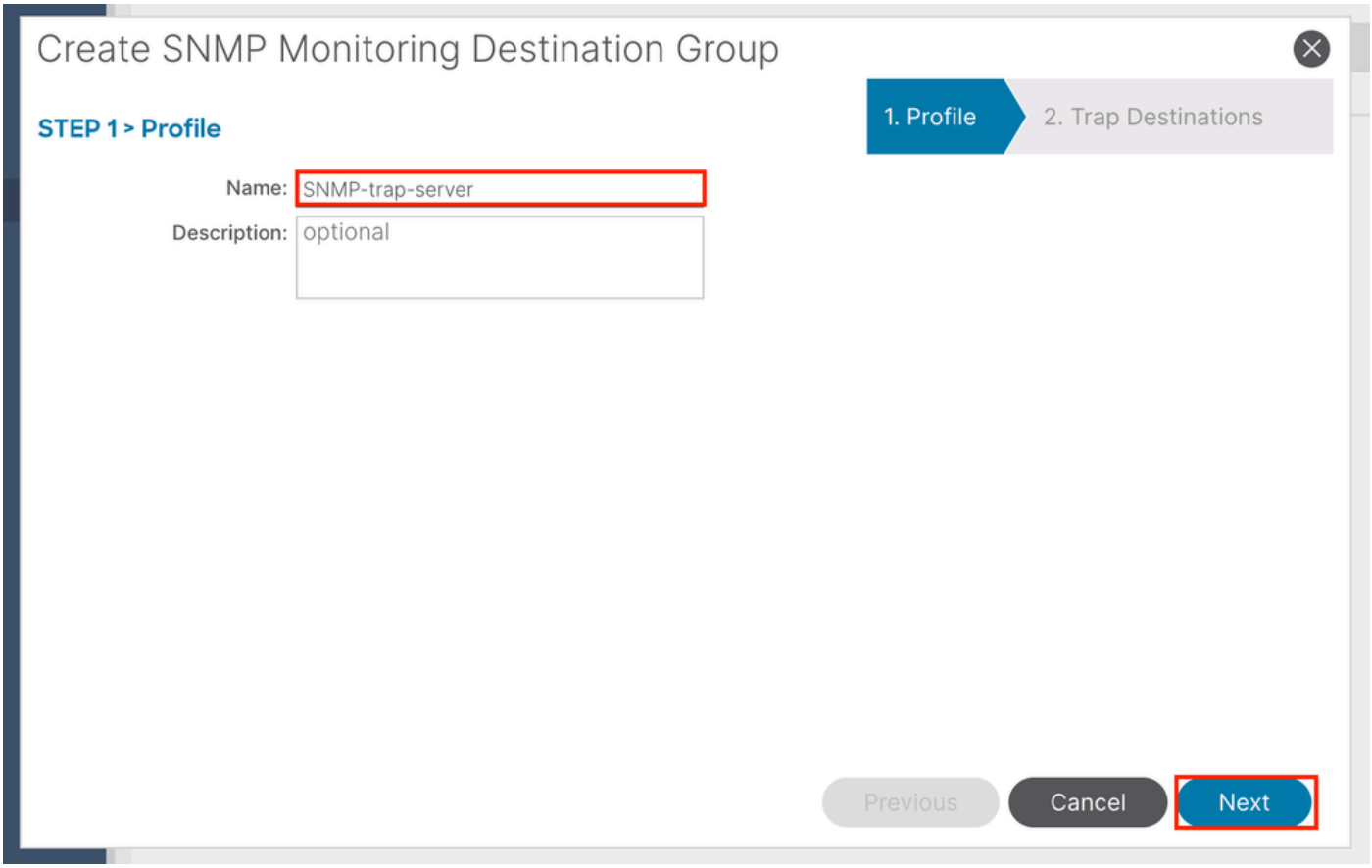
注：前のセクションのステップ1 ～ 3を実行しないと、SNMPトラップの設定では不十分です。ステップ2:SNMPトラップの設定は、（アクセス/ファブリック/テナント）のポリシーのモニタリングに関連します。

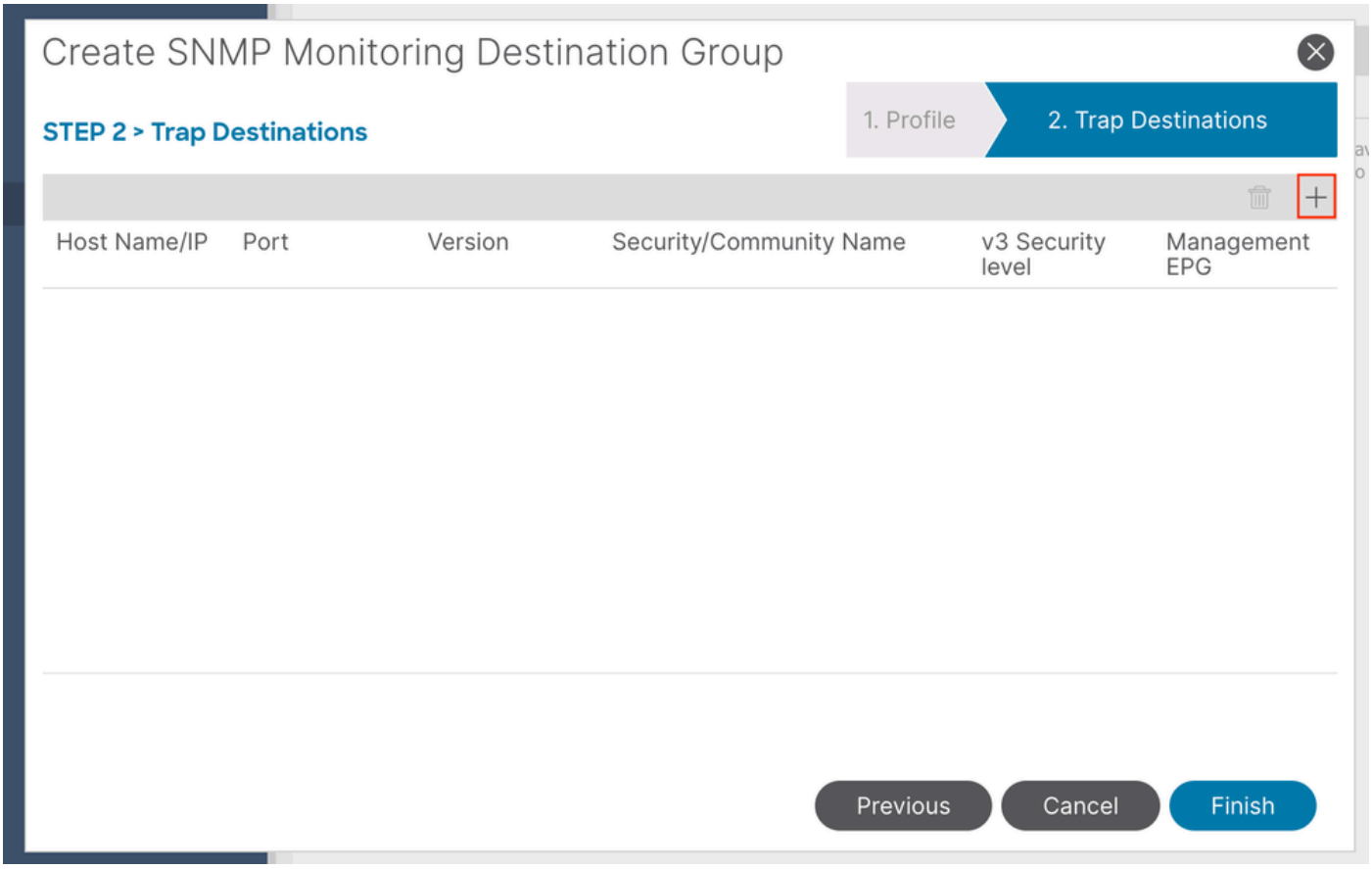
ACIでSNMPトラップを設定するには、前のセクションのステップ1、2、および3に加えて2つの手順が必要です。

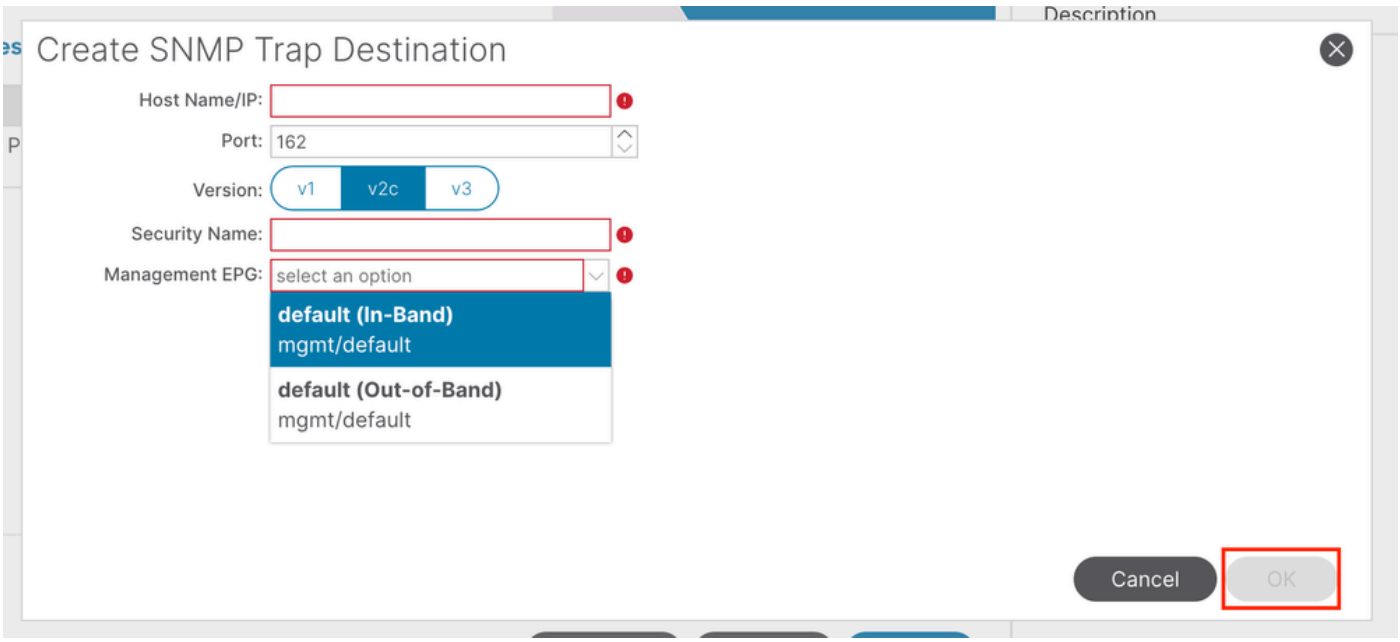
ステップ 1：SNMPトラップサーバの設定

これを行うには、APIC Web GUIパスAdmin > Eternal Data Collectors > Monitoring Destinations > SNMPに移動します。









Host Name/IP:SNMPトラップ送信先のホスト。

Port:SNMPトラップ送信先のサービスポート。範囲は0（未指定）～ 65535で、デフォルトは162です。

Version:SNMPトラップ送信先でサポートされているCDPのバージョン。バージョンは次のとおりです。

- v1:ユーザ認証にコミュニティストリングの一致を使用します。

- v2c：ユーザ認証にコミュニティストリングー致を使用します。

- v3：ネットワーク上のフレームの認証と暗号化を組み合わせてデバイスへの安全なアクセスを提供する、相互運用可能な標準ベースのネットワーク管理用プロトコル。

デフォルトは**v2c**です。

Security Name:SNMPトラップの宛先セキュリティ名（コミュニティ名）。@記号を含めることはできません。

v.3セキュリティレベル：SNMP宛先パスのSNMPv3セキュリティレベル。レベルは次のとおりです。

- auth

- noauth

- priv

デフォルトは**noauth**です。

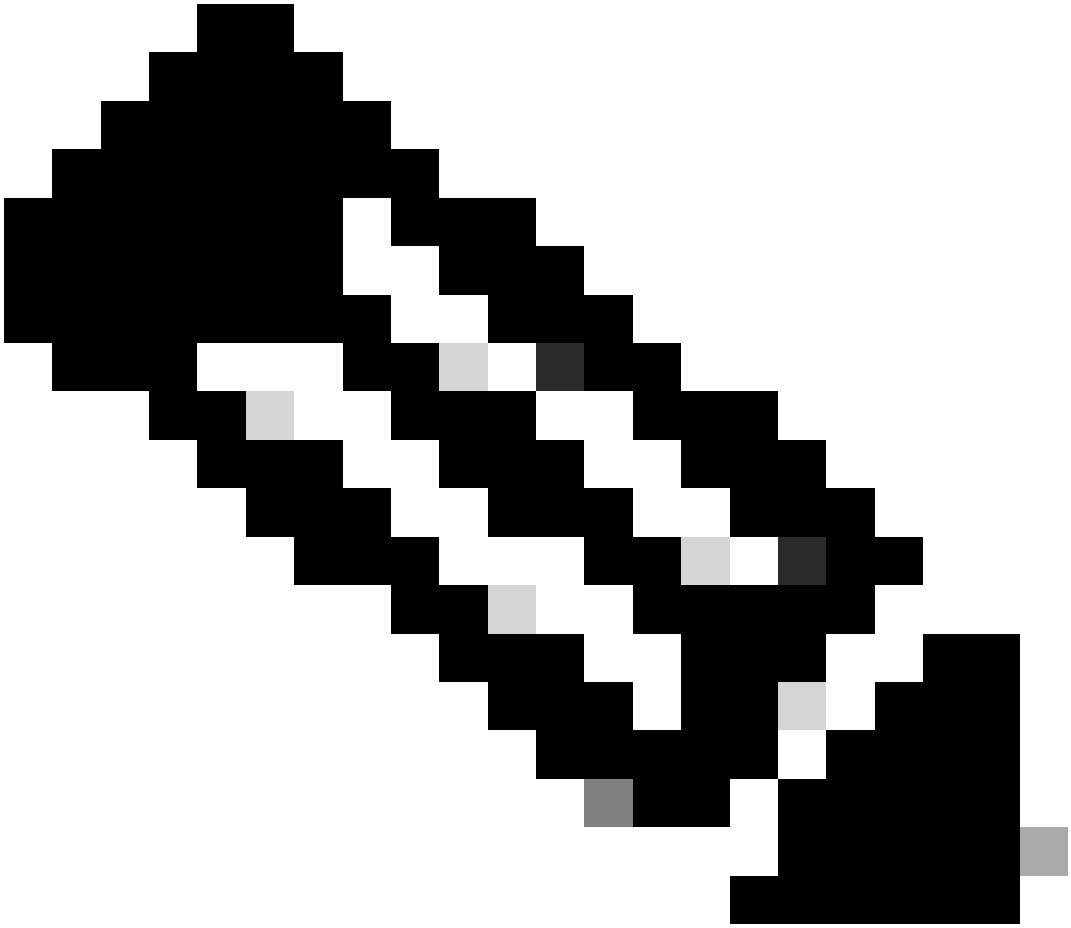
Management EPG：リモートホストに到達するために経由するSNMP宛先の管理エンドポイントグループの名前。

ステップ 2：（アクセス/ファブリック/テナント）モニタリングポリシーでのSNMPトラップソースの設定

モニタリングポリシーは、次の3つのスコープを使用して作成できます。

- アクセス：アクセスポート、FEX、VMコントローラ
- ファブリック：ファブリックポート、カード、シャーシ、ファン

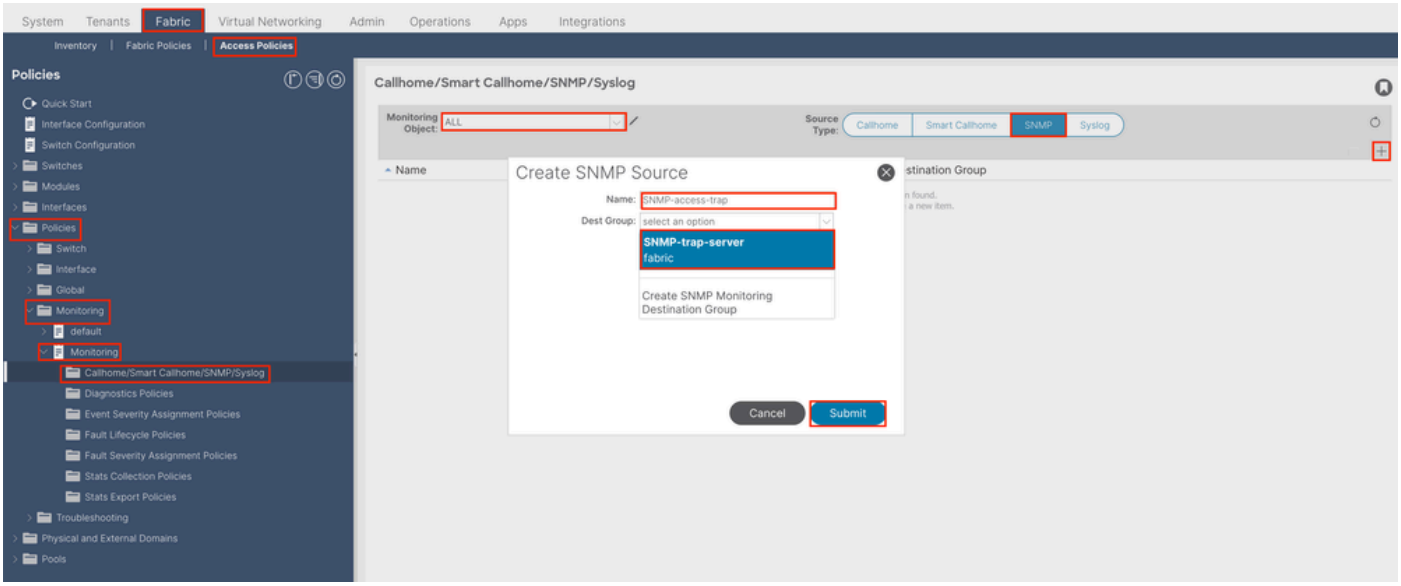
- テナント – EPG、アプリケーションプロファイル、サービス

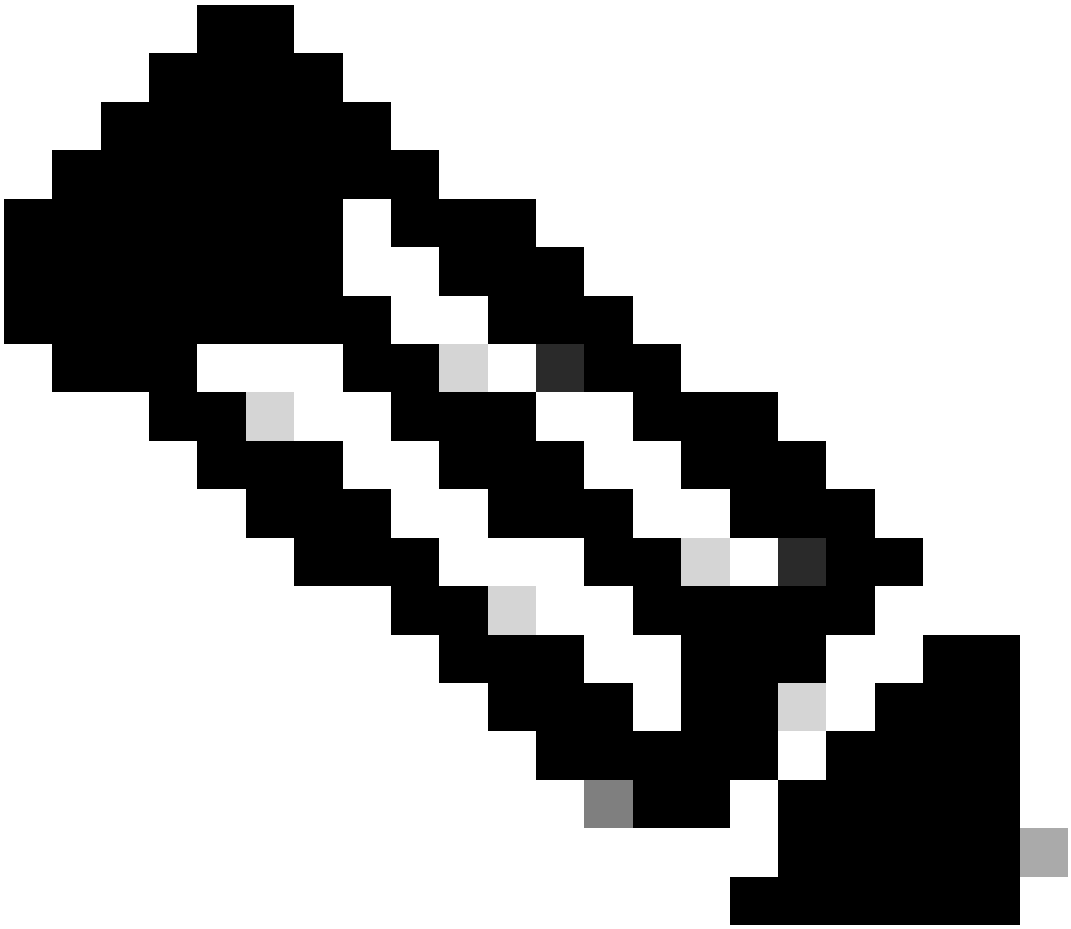


注：ニーズに応じて設定するには、任意の1つまたは任意の組み合わせを選択できます。

オプション 1アクセスポリシーでのSNMPソースの定義

これを行うには、APIC Web GUIパスFabric > Access Polices > Polices > Monitoring > Default > Callhome/Smart Callhome/SNMP/Syslog/TACACSに移動します。

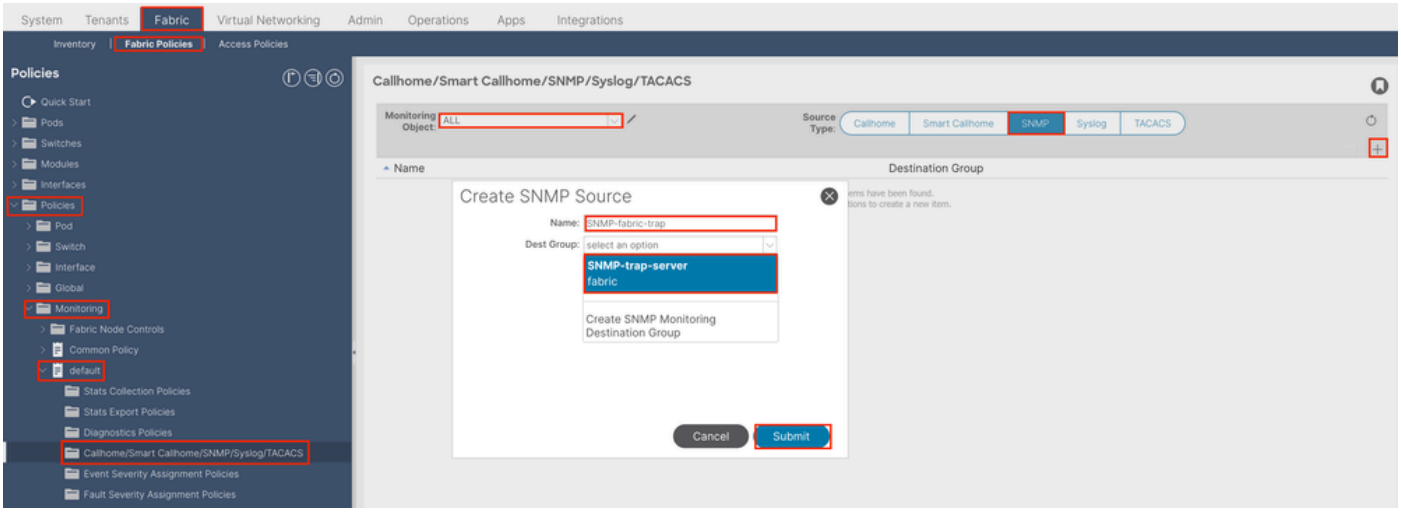

System
Tenants
Fabric
Virtual Networking
Admin
Operations
Apps
Integrations
Inventory
Fabric Policies
Access Policies
Policies
Quick Start
Interface Configuration
Switch Configuration
Switches
Modules
Interfaces
Policies
Switch
Interface
Global
Monitoring
default
Monitoring
Callhome/Smart Callhome/SNMP/Syslog
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



注：デフォルトのモニタリングポリシーの代わりにカスタム定義のモニタリングポリシー（設定されている場合）を使用できます。ここではデフォルトのモニタリングポリシーを使用します。 監視する監視オブジェクトを指定できます。ここでは、すべてが使用されています。

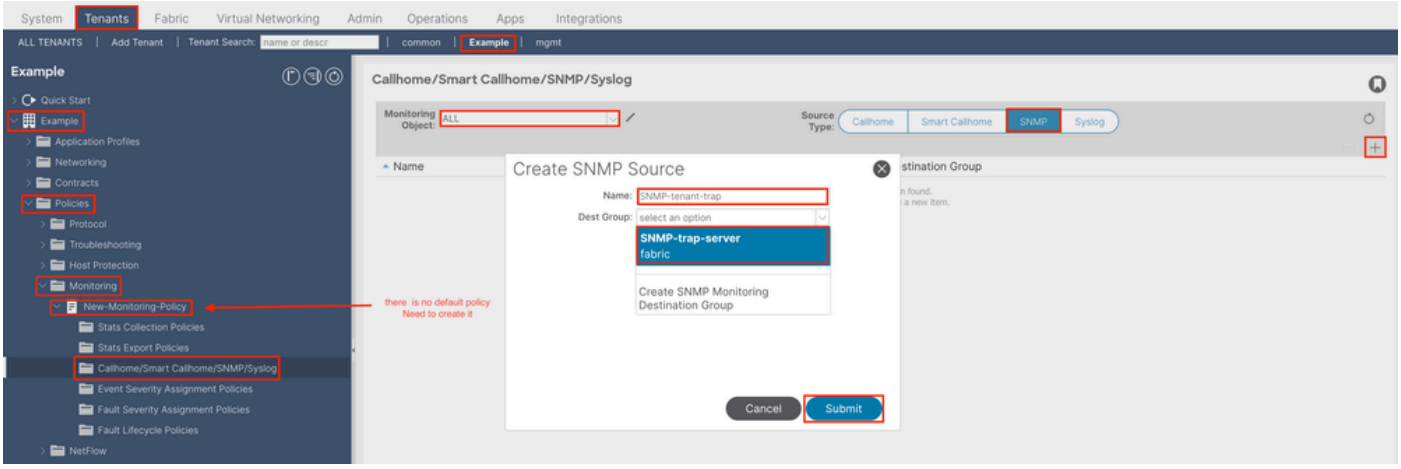
オプション 2ファブリックポリシーでのSNMPソースの定義

これを行うには、APIC Web GUIパスFabric > Fabric Polices > Polices > Monitoring > Default > Callhome/Smart Callhome/SNMP/Syslog/TACACSに移動します。



オプション 3テナントポリシーでのSNMPソースの定義

これを行うには、APIC Web GUIパスTenant > (Tenant Name) > Polices > Monitoring > (Custom monitoring policy) > Callhome/Smart Callhome/SNMP/Syslog/TACACSに移動します。



確認

snmpwalkコマンドを使用した確認

まず、リーフスイッチのグローバルスコープからSNMPデータを取得する方法を確認します。snmpwalkコマンドを使用すると、snmpwalk -v 2c -c New-1 x.x.x.xコマンドを使用するだけで実行できます。

この分割されたコマンドは、次の内容を表します。

snmpwalk = MacOS/Linux/Windowsにインストールされたsnmpwalk実行可能ファイル
-v =使用するSNMPのバージョンを指定
2c= SNMPバージョン2cを使用していることを指定します。
-c=特定のコミュニティストリングを指定します。
New-1=グローバルスコープのSNMPデータの取得にコミュニティストリングを使用

x.x.x.x=リーフスイッチのアウトオブバンド管理IPアドレス

コマンド結果：

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

省略したコマンドの出力では、snmpwalkが正常に実行され、ハードウェア固有の情報が取得されたことが確認できます。
snmpwalkを続行すると、ハードウェアインターフェイス名や説明などが表示されます。

次に、SNMPコミュニティストリング**New-1**を使用しているVRF用に作成されたVRFコンテキスト**New-VRF-SNMP**の取得に進みます。

2つの異なるSNMPコンテキストで同じコミュニティストリング**New-1**が使用されるため、SNMPデータの取得元となるSNMPコンテキストを指定する必要があります。特定のSNMPコンテキストを指定するために使用する必要があるsnmpwalk構文は、snmpwalk -v 2c -c New-1@New-VrF-SNMP 10.x.x.xです。

特定のSNMPコンテキストから取得するには、次の形式を使用します。
COMMUNITY_NAME_HERE@SNMP_CONTEXT_NAME_HERE .

CLI showコマンドの使用

APIC上：

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

スイッチ：

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

CLI Moqueryコマンドの使用

APIC/スイッチ：

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

CLI catコマンドの使用

APIC上：

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

トラブルシュート

snmpdプロセスの確認

スイッチ：

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

APIC上：

```
ps aux | grep snmp
```

プロセスが正常な場合は、Cisco TACに問い合せて指示を受けてください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。