

# ACIでのSNMPの設定

## 内容

---

### [はじめに](#)

### [前提条件](#)

#### [要件](#)

#### [使用するコンポーネント](#)

### [設定](#)

#### [SNMPスコープについて](#)

#### [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](#)

##### [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](#)

##### [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](#)

##### [ステップ 4: VRFコンテキストスコープの設定](#)

#### [GUIを使用したSNMPトラップの設定](#)

##### [ステップ 1: SNMPトラップサーバの設定](#)

##### [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](#)

##### [オプション 1アクセスポリシーでのSNMPソースの定義](#)

##### [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](#)

##### [オプション 3テナントポリシーでのSNMPソースの定義](#)

### [確認](#)

#### [snmpwalkコマンドを使用した確認](#)

#### [CLI showコマンドの使用](#)

#### [CLI Moqueryコマンドの使用](#)

#### [CLI catコマンドの使用](#)

### [トラブルシューティング](#)

#### [snmpdプロセスの確認](#)

---

## 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。

System Tenants **Fabric** Virtual Networking Admin Operations Apps Integrations

Inventory **Fabric Policies** Access Policies

**Policies**

- Quick Start
- > Pods
- > Switches
- > Modules
- > Interfaces
- > **Policies**
  - > **Pod**
  - > Date and Time
  - > **SNMP**
    - default**
    - > Management Access

**Pod - SNMP**

Name	Admin State	Location
default	Enabled	Cisco Systems,

Modify the default policy

Right Click for create New SNMP Policy

Create SNMP Policy

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。

## 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。

Create SNMP Client Group Profile

Name:

Description:

Associated Management EPG:

Client Entries:

Name	Address
Example-snmp-server	<input type="text"/>

Select Actions to create a new item

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。

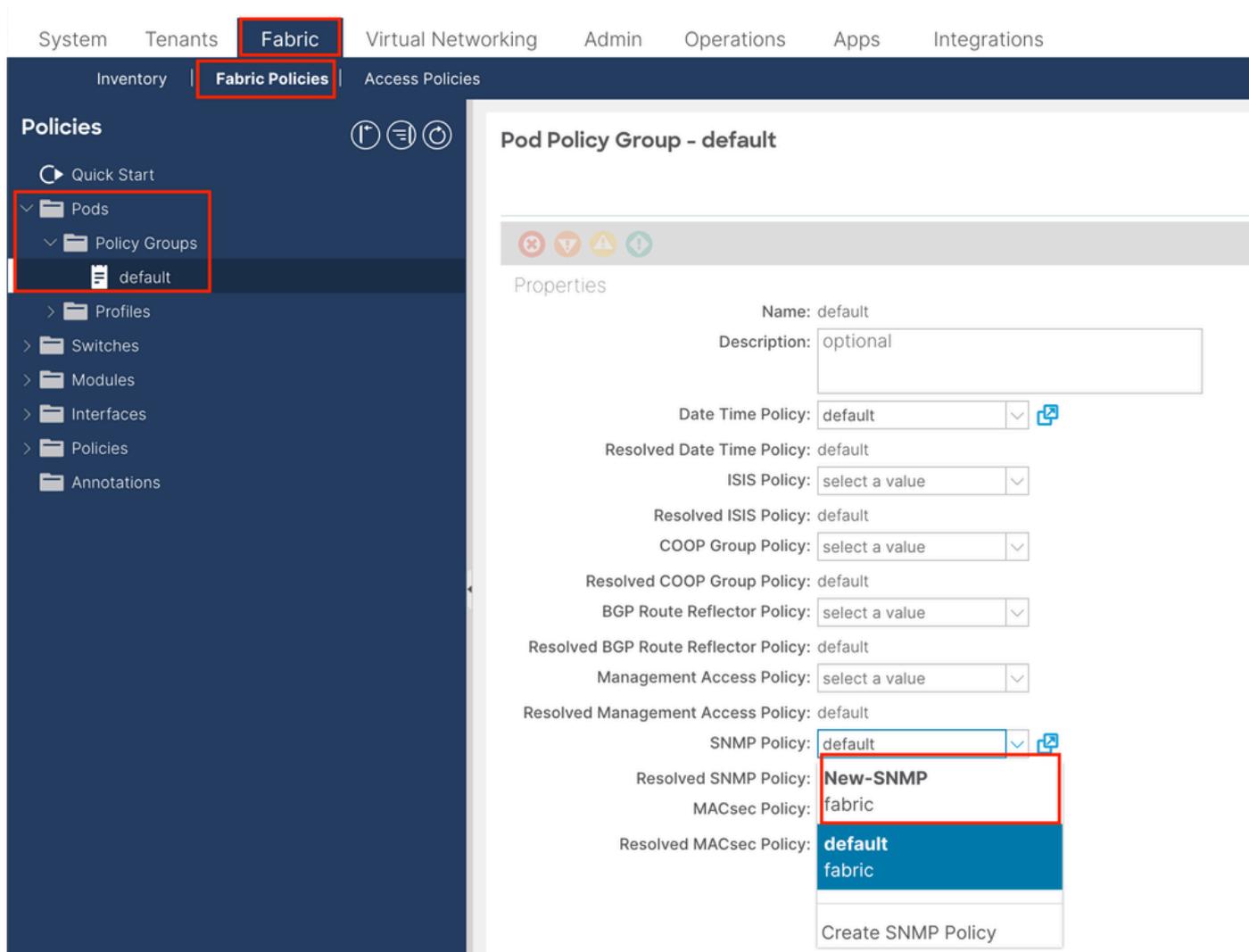
最後のステップでは、特定のIPまたはサブネット全体にアクセスしてACI SNMPデータを取得できるようにクライアントエントリを定義します。特定のIPまたはサブネット全体を定義するための構文があります。

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

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。



The screenshot displays the APIC Web GUI interface. The top navigation bar includes 'System', 'Tenants', 'Fabric', 'Virtual Networking', 'Admin', 'Operations', 'Apps', and 'Integrations'. The left sidebar shows a 'Policies' menu with 'Pods' and 'Policy Groups' expanded, and 'default' selected. The main content area is titled 'Pod Policy Group - default' and shows various configuration fields. The 'SNMP Policy' field is highlighted with a red box, and its dropdown menu is open, showing 'New-SNMP' and 'fabric' as options. The 'New-SNMP' option is selected.

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。

System Tenants **Fabric** Virtual Networking Admin Operations Apps Integrations

Inventory | **Fabric Policies** Access Policies

**Policies**

- Quick Start
- Pods
- Policy Groups
  - default**
- Profiles
- Pod Profile default
  - default**

Switches  
Modules  
Interfaces  
Policies  
Annotations

### Pod Selector - default

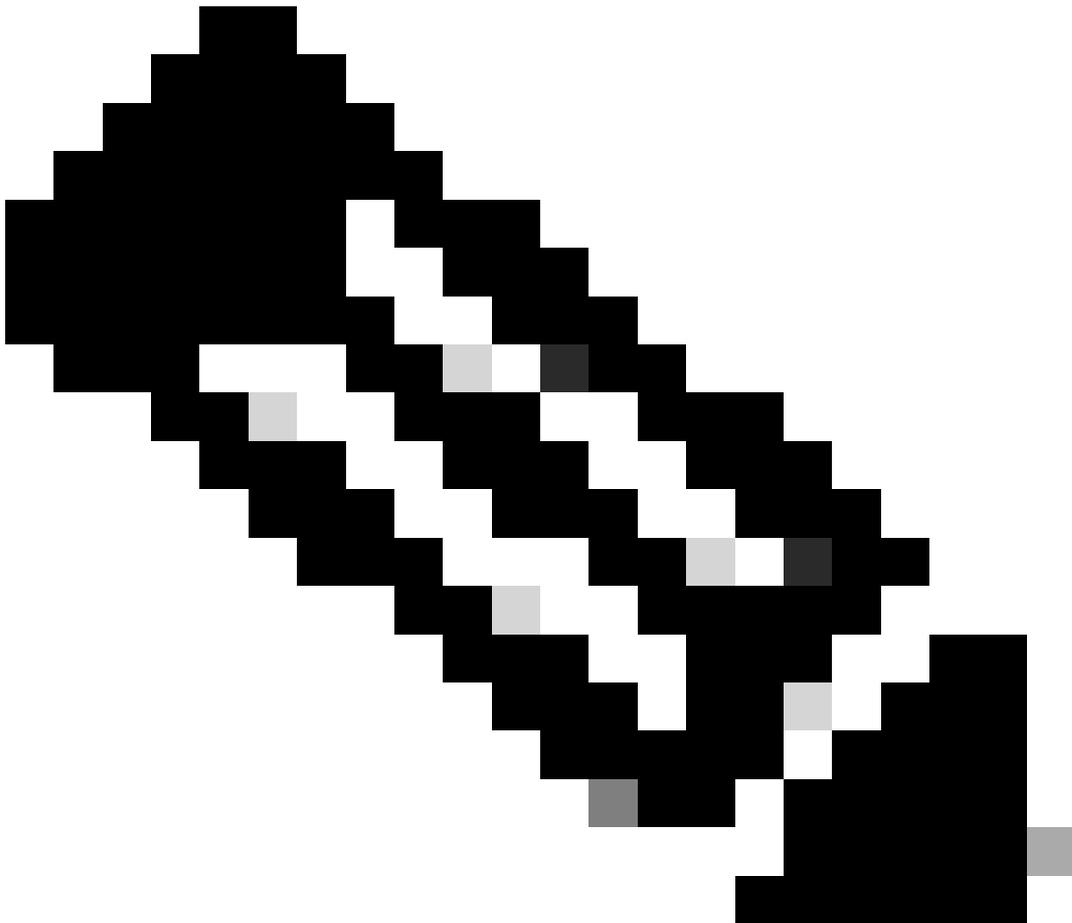
Properties

Name: default  
Description: optional

Type: ALL

Fabric Policy Group: **default**

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スコープが自動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**

> 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

## Create SNMP Context

Context Name:

Community Profiles:

Name	Description
New-1	

Create in Step 1.

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、ページの一番下までスクロールします。

System **Tenants** Fabric Virtual Networking Admin Operations Apps Integrations

ALL TENANTS | Add Tenant | Tenant Search:  | common | **Example** | mgmt

**Example**

- > Quick Start
- > **Example**
- > Application Profiles
- > **Networking**
- > Bridge Domains
- > **VRFs**
- > VRF-1
- > L2Outs
- > L3Outs
- > SR-MPLS VRF L3Outs
- > Dot1Q Tunnels
- > Contracts
- > Policies
- > Services

**VRF - VRF-1**

Summary **Policy** Route Control Operational Stats

Properties

Create SNMP Context

Context Name: New-VRF-SNMP

Community Profiles:

Name	Description
New-1	

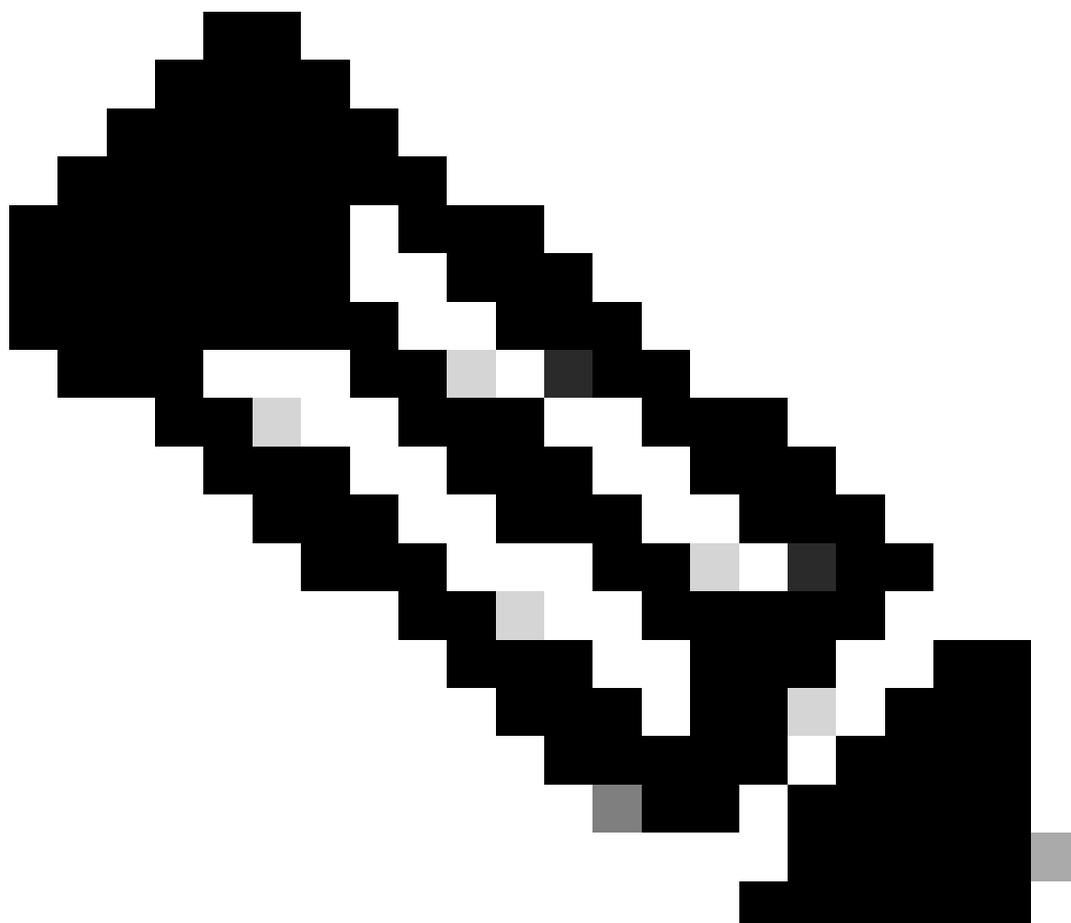
VRFでSNMPコンテキストを無効にするには、Create SNMP Contextチェックボックスを選択解除するか（スクリーンショットを参照）、VRFを右クリックしてDelete SNMP Contextを選択します。

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、ポリシーの範囲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。

---



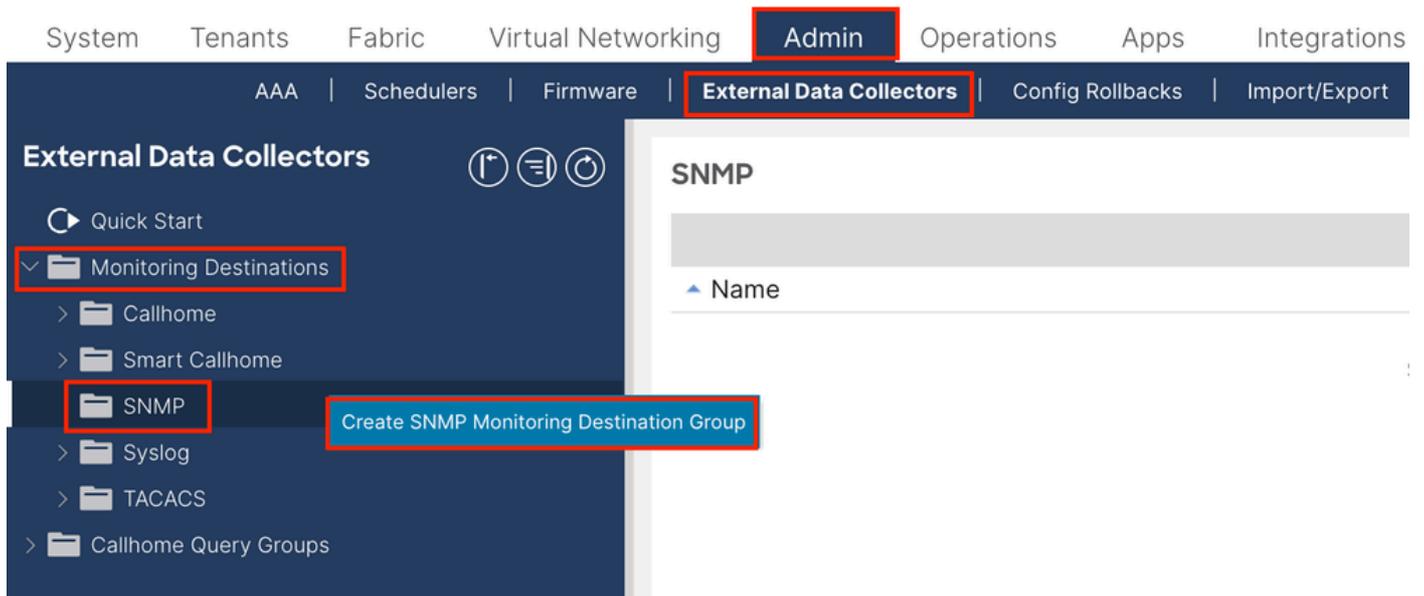
注：前のセクションのステップ1～3を実行しないと、SNMPトラップの設定では不十分です。ステップ2:SNMPトラップの設定は、(アクセス/ファブリック/テナント)のポリシーのモニタリングに関連します。

---

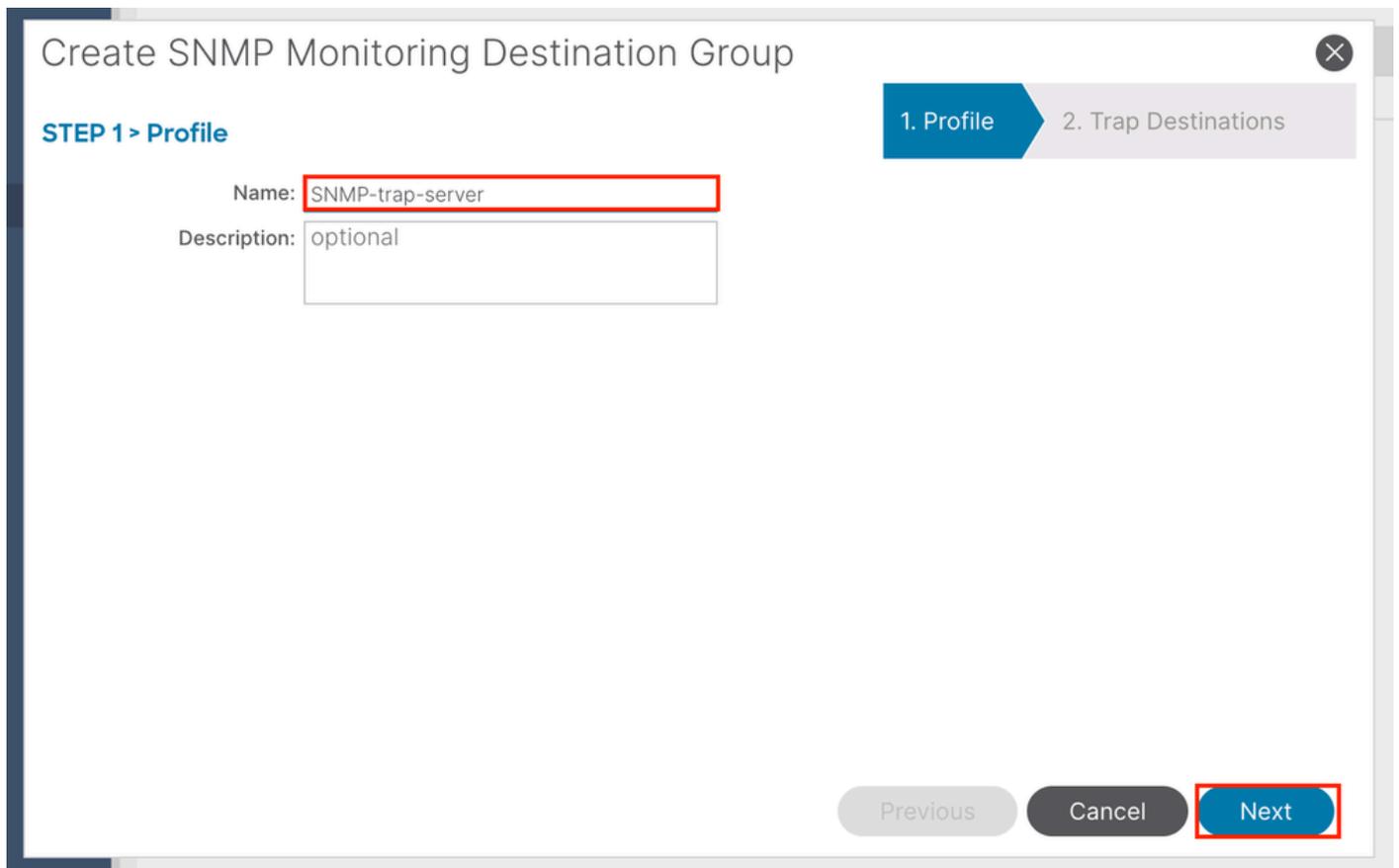
ACIでSNMPトラップを設定するには、前のセクションのステップ1、2、および3に加えて2つの手順が必要です。

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 > External Data Collectors > Monitoring Destinations > SNMPに移動します。



The screenshot shows the APIC Web GUI navigation menu. The 'Admin' tab is selected and highlighted with a red box. Under 'Admin', the 'External Data Collectors' option is highlighted with a red box. In the left sidebar, 'Monitoring Destinations' is expanded, and 'SNMP' is highlighted with a red box. A blue tooltip with the text 'Create SNMP Monitoring Destination Group' is visible over the 'SNMP' option.



The screenshot shows the 'Create SNMP Monitoring Destination Group' dialog box. The title is 'Create SNMP Monitoring Destination Group'. The dialog is divided into two steps: '1. Profile' (active) and '2. Trap Destinations'. Under 'STEP 1 > Profile', there are two input fields: 'Name' with the value 'SNMP-trap-server' and 'Description' with the value 'optional'. At the bottom right, there are three buttons: 'Previous' (disabled), 'Cancel' (disabled), and 'Next' (active and highlighted with a red box).

## 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一致を使用します。

- 

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ることで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。

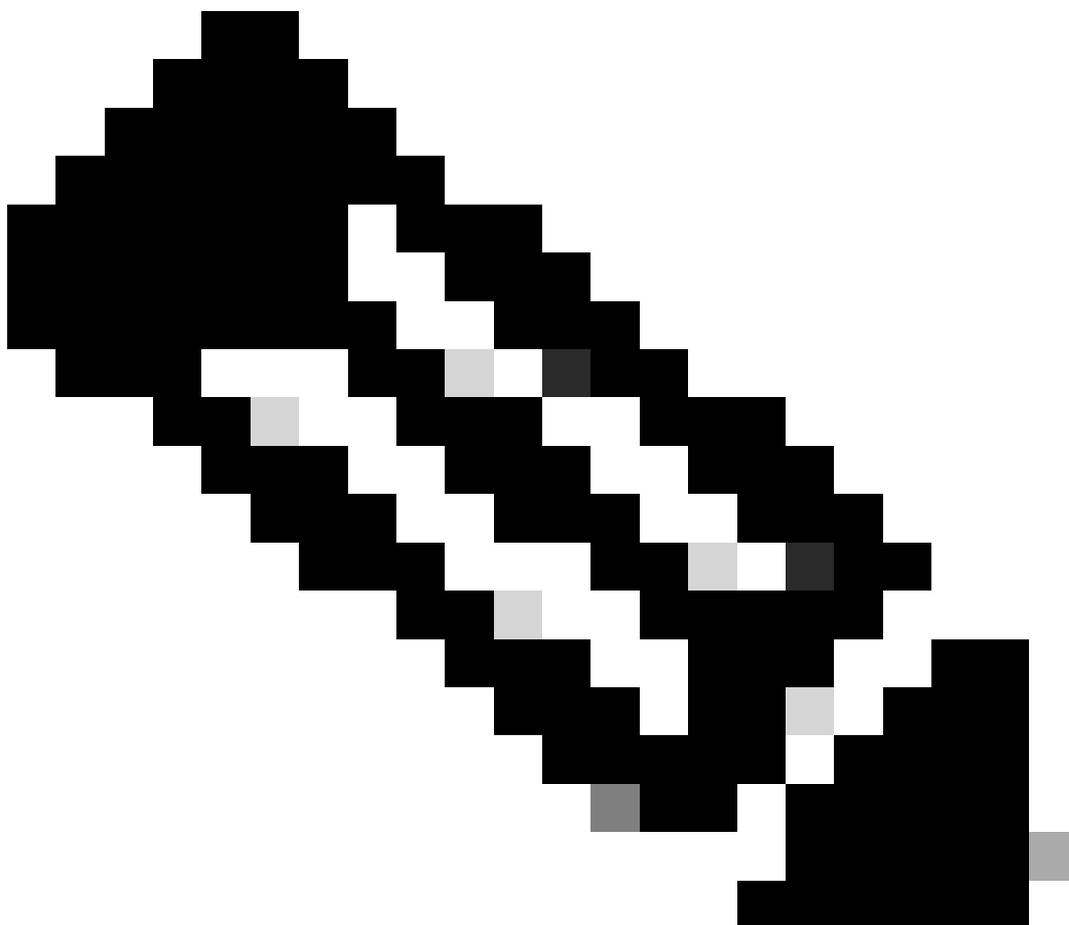
Management EPG : リモートホストに到達するために経由するSNMP宛先の管理エンドポイントグループの名前。

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
- 

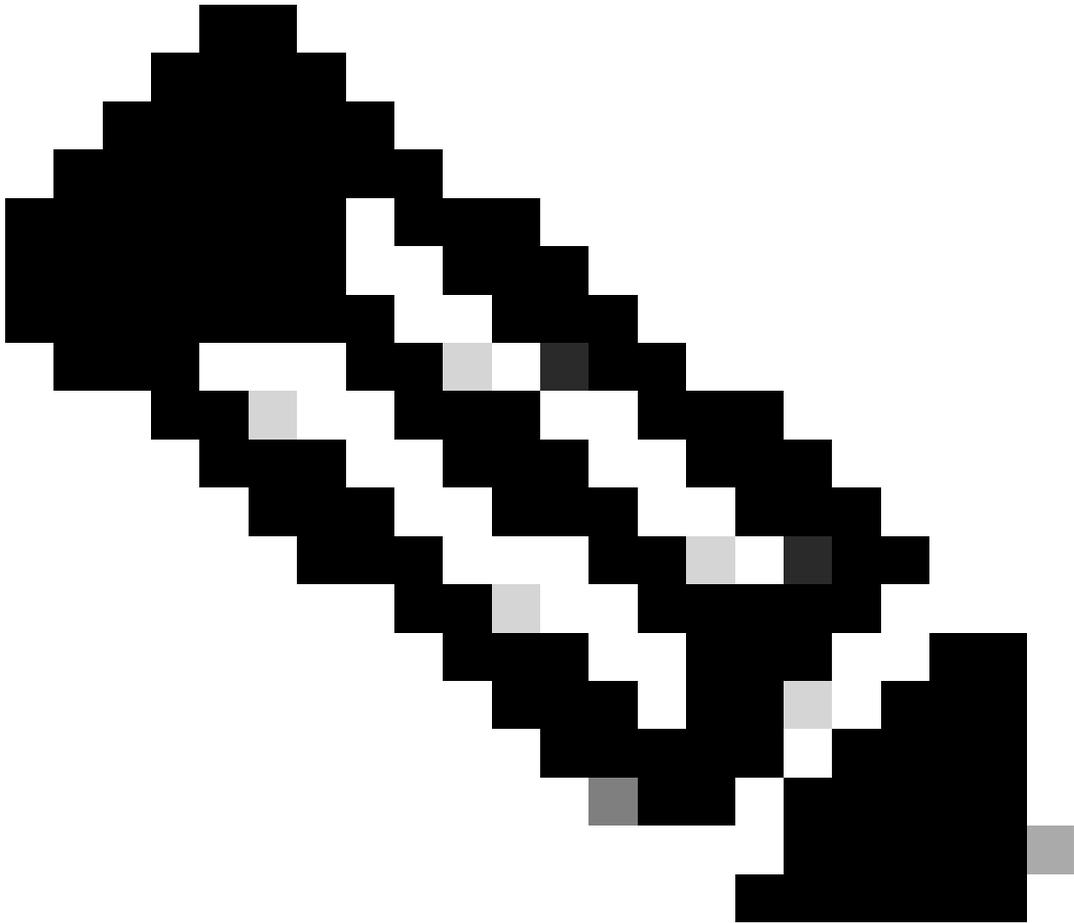
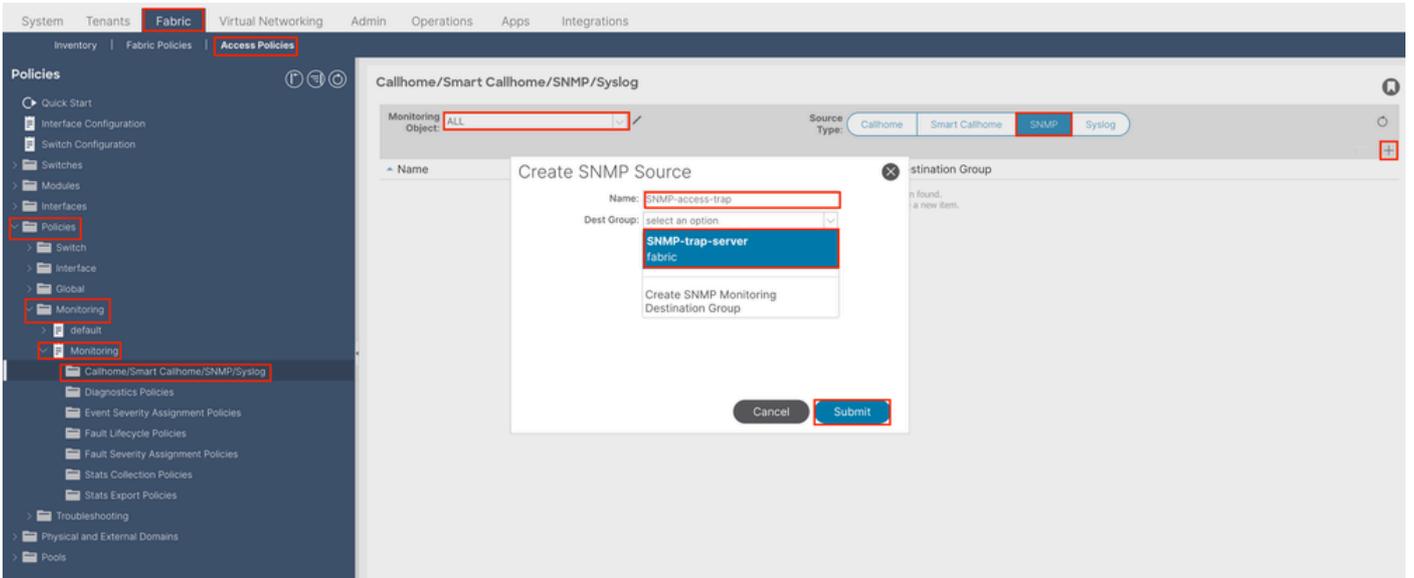


注：ニーズに応じて設定するには、任意の1つまたは任意の組み合わせを選択できます。

---

#### オプション 1アクセスポリシーでのSNMPソースの定義

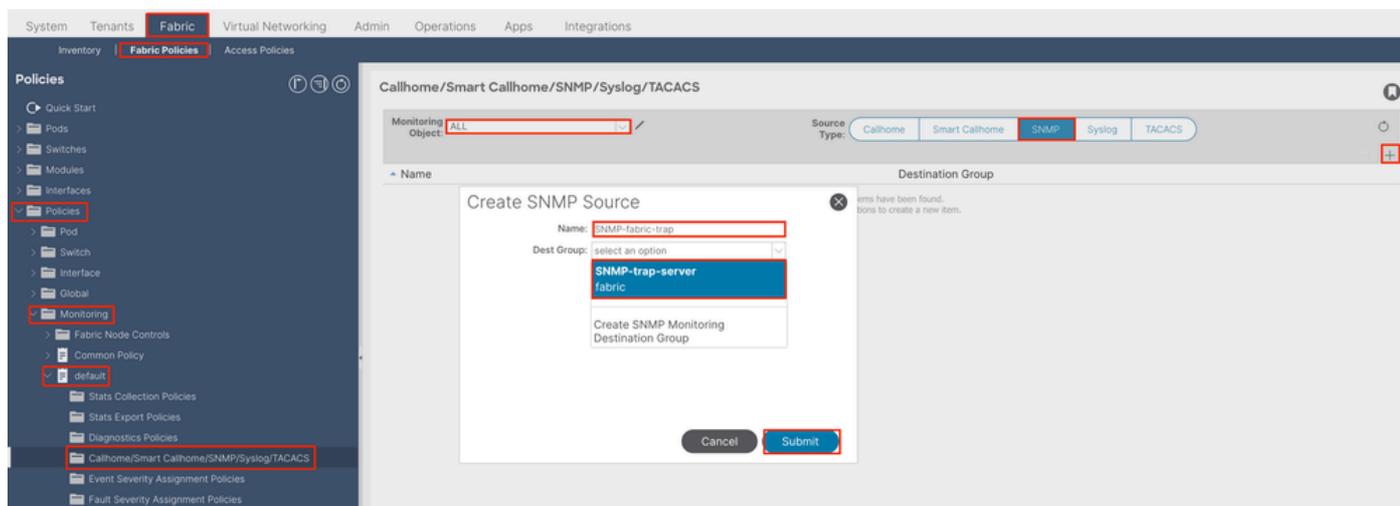
これを行うには、APIC Web GUIパスFabric > Access Polices > Polices > Monitoring > Default > Callhome/Smart Callhome/SNMP/Syslog/TACACSに移動します。



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。

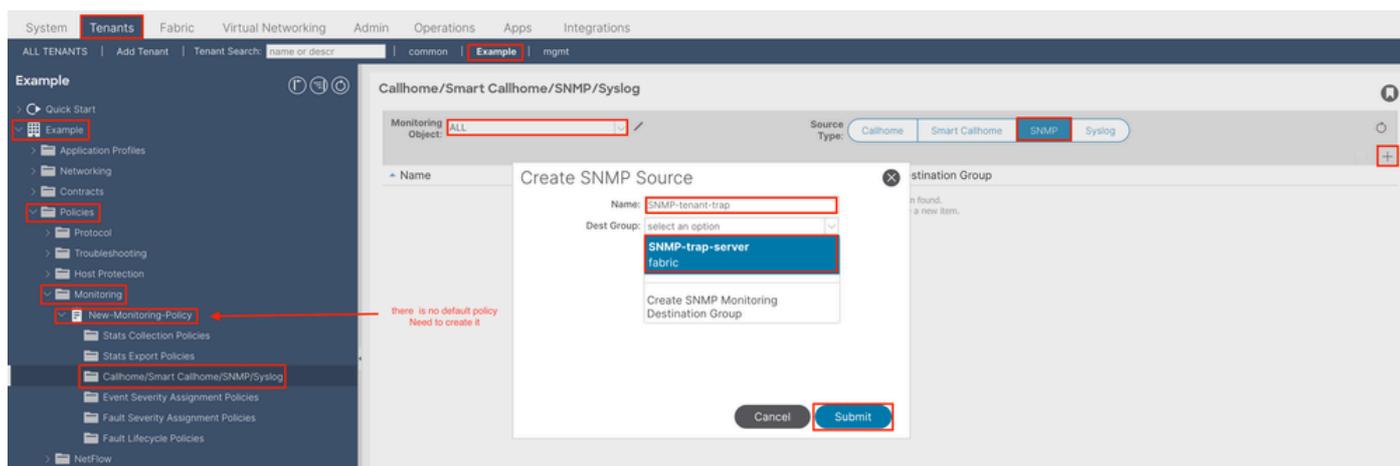
## オプション 2 ファブリックポリシーでのSNMPソースの定義

これを行うには、APIC Web GUIパスFabric > Fabric Policies > Policies > 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) > Policies > 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 snmp
```

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に問い合わ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。