

Configurer SNMP dans l'ACI

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Présentation des étendues SNMP](#)

[Étapes de configuration \(pour les étendues globales et de contexte VRF\)](#)

[Étape 1 : configuration de la politique de fabric SNMP](#)

[Étape 2 : application de la stratégie SNMP au groupe de stratégies Pod \(Fabric Policy Group\)](#)

[Étape 3. Associer le groupe de stratégies Pod au profil Pod](#)

[Étape 4 : configuration des étendues de contexte VRF](#)

[Configuration des dérouterments SNMP via l'interface utilisateur graphique](#)

[Étape 1 : configuration du serveur TRAP SNMP](#)

[Étape 2 : configuration de la source TRAP SNMP sous la politique de surveillance \(accès/fabric/locataire\)](#)

[Option 1. Définir la source SNMP sous Politiques d'accès](#)

[Option 2. Définir la source SNMP sous Politiques de fabric](#)

[Option 3. Définir la source SNMP sous Politiques de locataire](#)

[Vérifier](#)

[Utiliser la commande snmpwalk pour vérifier](#)

[Utilisation des commandes show CLI](#)

[Utilisation des commandes Moquery CLI](#)

[Utilisation des commandes cat CLI](#)

[Dépannage](#)

[Vérifiez le processus snmpd](#)

Introduction

Ce document décrit la configuration du protocole SNMP (Simple Network Management Protocol) et des dérouterments SNMP dans l'ACI.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Détection de fabric terminée
- Connectivité intra-bande/hors-bande à votre contrôleur APIC (Application Policy Infrastructure Controller) et à vos commutateurs de fabric

- Contrats intrabande/hors bande configurés pour autoriser le trafic SNMP (ports UDP 161 et 162)
- Adresses de gestion des noeuds statiques configurées pour vos APIC et vos commutateurs de fabric sous le locataire de gestion par défaut (sans cela, l'extraction des informations SNMP d'un APIC échoue)
- Comprendre le workflow du protocole SNMP

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- APIC
- Navigateur
- Infrastructure axée sur les applications (ACI) 5.2 (8e)
- `Snmpwalk` commande

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

L'ACI Cisco prend en charge les protocoles SNMPv1, v2c et v3, y compris les bases d'informations de gestion (MIB) et les notifications (déroutements). La norme SNMP permet à toutes les applications tierces qui prennent en charge les différentes MIB de gérer et de surveiller les commutateurs Leaf & Spine ACI et les contrôleurs APIC.

Cependant, les commandes d'écriture SNMP (Set) ne sont pas prises en charge dans l'ACI.

La politique SNMP est appliquée et s'exécute indépendamment sur les commutateurs Leaf et Spine et sur les contrôleurs APIC. Étant donné que chaque périphérique ACI possède sa propre entité SNMP, c'est-à-dire que plusieurs APIC dans un cluster APIC doivent être surveillés séparément, ainsi que les commutateurs. Cependant, la source de la politique SNMP est créée en tant que politique de surveillance pour l'ensemble du fabric ACI.

Par défaut, SNMP utilise le port UDP 161 pour l'interrogation et le port 162 pour les TRAP.

Présentation des étendues SNMP

Un concept fondamental du protocole SNMP dans l'ACI est qu'il existe deux étendues à partir desquelles les informations SNMP peuvent être extraites :

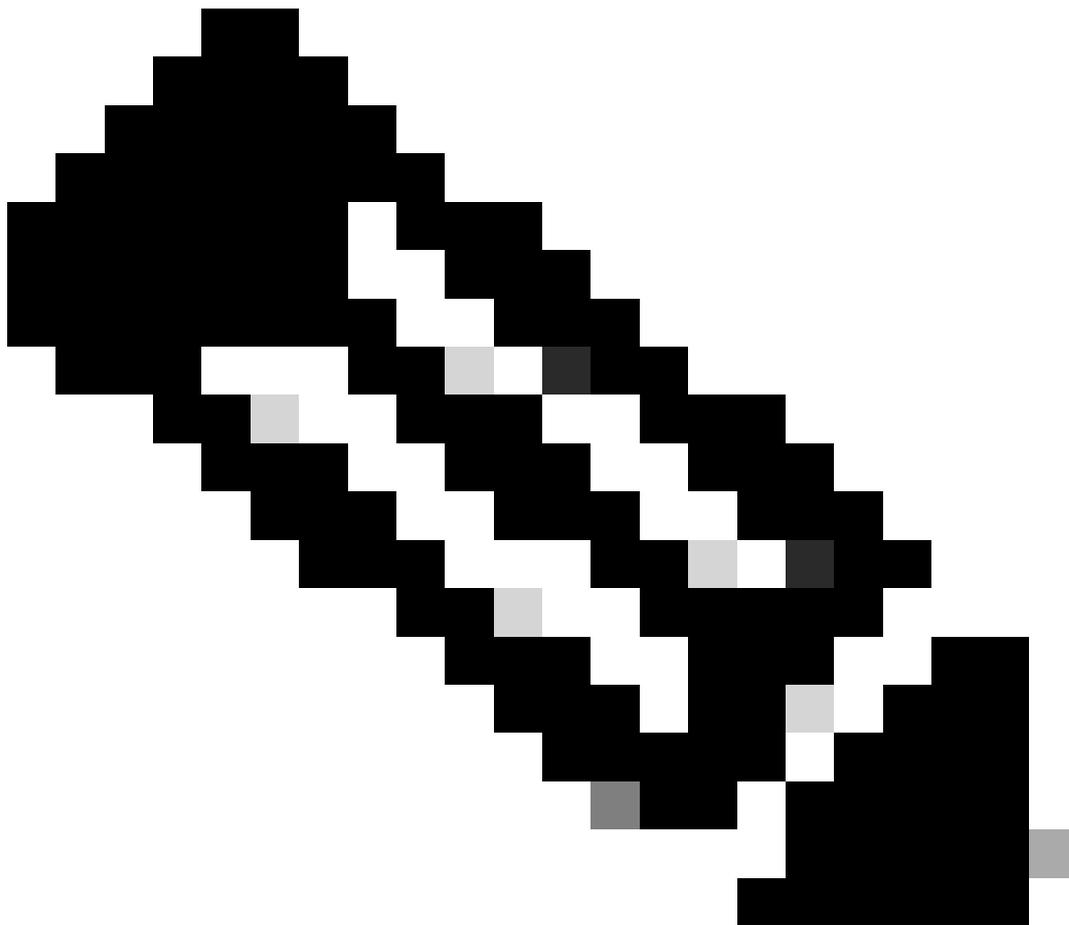
1. Mondial
2. Contexte du routage et du transfert virtuels (VRF)

L'étendue globale consiste à extraire les MIB du châssis, tels que le nombre d'interfaces, les index

d'interface, les noms d'interface, l'état de l'interface, etc. d'un noeud leaf/spine.

Les MIB spécifiques à VRF Context Scope extraient des informations spécifiques à VRF telles que des adresses IP et des informations de protocole de routage.

La liste de prise en charge des MIB de contexte VRF et global de commutateur de fabric et APIC pris en charge est [exhaustive](#) dans [Cisco ACI MIB Support List](#).

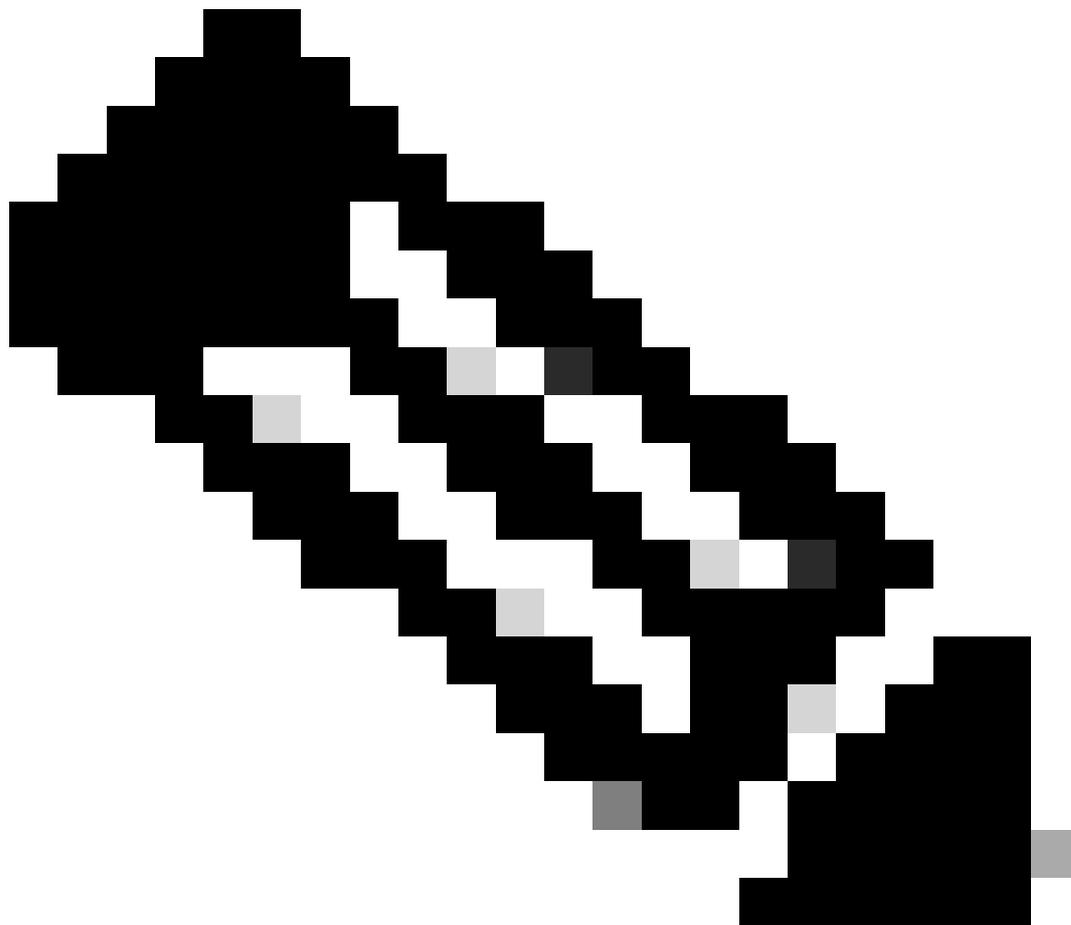


Remarque : Une MIB avec une étendue globale n'a qu'une seule instance dans le système. Les données d'une base MIB globale concernent l'ensemble du système.

Une MIB avec une étendue spécifique VRF peut avoir des instances par VRF dans le système. Les données d'une base MIB spécifique au VRF concernent uniquement ce VRF.

Étapes de configuration (pour les étendues globales et de contexte VRF)

Étape 1 : configuration de la politique de fabric SNMP



Remarque : Ici, les paramètres SNMP sont spécifiés, tels que les stratégies de communauté SNMP et les stratégies de groupe de clients SNMP.

La première étape de la configuration du protocole SNMP consiste à créer les politiques de fabric SNMP nécessaires. Afin de créer les politiques de fabric SNMP, naviguez jusqu'au chemin de l'interface utilisateur graphique Web APIC ; Fabric > Fabric Policies > Policies > Pod > SNMP.

The screenshot shows a network management interface with a top navigation bar containing 'System', 'Tenants', 'Fabric', 'Virtual Networking', 'Admin', 'Operations', 'Apps', and 'Integrations'. Below this, there are tabs for 'Inventory', 'Fabric Policies', and 'Access Policies'. The left sidebar is titled 'Policies' and contains a tree view with folders for 'Pods', 'Switches', 'Modules', 'Interfaces', 'Policies', 'Date and Time', 'SNMP', and 'Management Access'. The 'Policies' folder is expanded, showing 'Pod' and 'SNMP' sub-folders. The 'SNMP' folder is further expanded, showing a 'default' policy. A 'Create SNMP Policy' button is visible in the 'SNMP' folder. The main content area is titled 'Pod - SNMP' and displays a table with the following data:

Name	Admin State	Location
default	Enabled	Cisco Systems,

Red arrows point from the 'default' policy in the left sidebar to the text 'Modify the default policy'. Another red arrow points from the 'Create SNMP Policy' button to the text 'Right Click for create New SNMP Policy'.

Vous pouvez créer une nouvelle stratégie SNMP ou modifier la stratégie SNMP par défaut.

Dans le document, la politique SNMP est appelée New-SNMP et utilise la version v2c de SNMP de sorte que les seuls champs nécessaires ici sont les politiques de communauté et les politiques de groupe de clients.

Le champ Community Policy Name définit la chaîne de communauté SNMP à utiliser. Dans notre cas, New-1. Vous voyez où ces deux chaînes de communauté viennent plus tard.

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

Cancel
Submit

Name : nom de la stratégie SNMP. Ce nom peut contenir entre 1 et 64 caractères alphanumériques.

Description : description de la stratégie SNMP. La description peut comporter entre 0 et 128 caractères alphanumériques.

Admin State : état administratif de la stratégie SNMP. L'état peut être activé ou désactivé. Les états sont les suivants :

- enabled : l'état admin est activé
- disabled : l'état admin est désactivé.

La valeur par défaut est disabled.

Contact : informations de contact pour la stratégie SNMP.

Emplacement : emplacement de la stratégie SNMP.

Utilisateurs SNMP v3 : le profil utilisateur SNMP permet d'associer des utilisateurs à des politiques SNMP pour la surveillance des périphériques d'un réseau.

Stratégies de communauté : le profil de communauté SNMP permet d'accéder aux statistiques du routeur ou du commutateur à des fins de surveillance.

Stratégies de groupe client :

L'étape suivante consiste à ajouter la stratégie/le profil de groupe du client. L'objectif de la stratégie/du profil de groupe client est de définir quels IP/sous-réseaux sont capables d'extraire des données SNMP des APIC et des commutateurs de fabric :

The screenshot shows a web form titled "Create SNMP Client Group Profile". The form has the following fields and elements:

- Name:** A text input field containing "New-Client".
- Description:** A text input field containing "optional".
- Associated Management EPG:** A dropdown menu showing "default (Out-of-Band)".
- Client Entries:** A table with two columns: "Name" and "Address". The "Name" column contains "Example-snmp-server" and the "Address" column is empty. There is a "+" button to add new entries and a trash icon to delete existing ones.
- Buttons:** "Update" and "Cancel" buttons are located below the table. "Cancel" and "Submit" buttons are located at the bottom right of the form.

Nom : nom du profil du groupe de clients. Ce nom peut contenir entre 1 et 64 caractères alphanumériques.

Description : description du profil du groupe de clients. La description peut comporter entre 0 et 128 caractères alphanumériques.

Groupe de terminaux de gestion associé (EPG) : nom distinctif d'un groupe de terminaux via lequel le VRF est accessible. La longueur de chaîne maximale prise en charge est de 255 caractères ASCII. La valeur par défaut est l'EPG d'accès à la gestion hors bande du locataire de gestion.

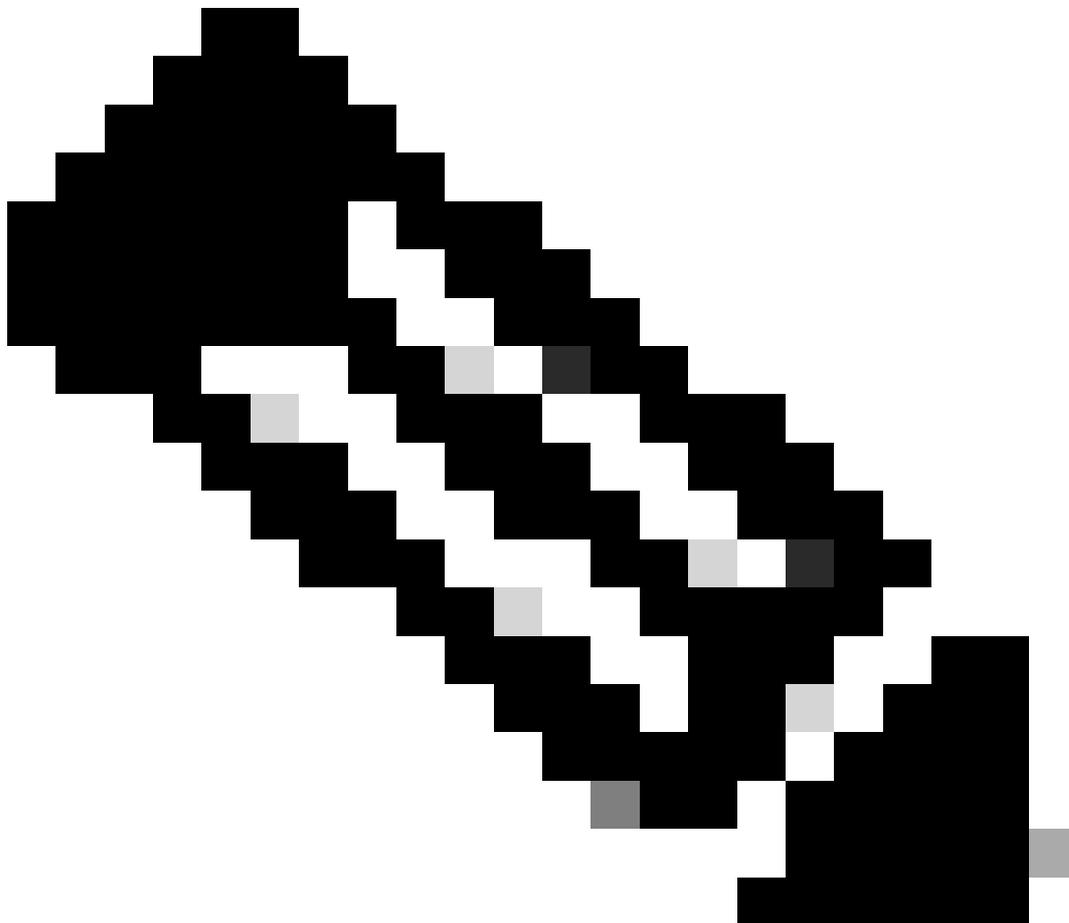
Client Entries : adresse IP du profil client SNMP.

Dans le document, la stratégie/profil de groupe du client est appelée New-Client.

Dans le profil/stratégie de groupe client, vous devez associer le groupe de gestion préféré. Vous devez vous assurer que l'EPG de gestion que vous choisissez a les contrats nécessaires pour autoriser le trafic SNMP (ports UDP 161 et 162). L'EPG de gestion hors bande par défaut est utilisé dans le document à des fins de démonstration.

La dernière étape consiste à définir vos entrées client afin d'autoriser des adresses IP spécifiques ou l'accès à des sous-réseaux entiers pour extraire les données SNMP de l'ACI. Il existe une syntaxe permettant de définir une adresse IP spécifique ou un sous-réseau entier :

- Adresse IP hôte spécifique : 192.168.1.5
- Sous-réseau entier : 192.168.1.0/24



Remarque : Vous ne pouvez pas utiliser 0.0.0.0 dans l'entrée client pour autoriser tous les sous-réseaux (si vous voulez autoriser tous les sous-réseaux à accéder à la base MIB SNMP, laissez les entrées client vides).

Étape 2 : application de la stratégie SNMP au groupe de stratégies Pod (Fabric Policy Group)

Afin d'appliquer cette configuration, naviguez jusqu'au chemin de l'interface utilisateur graphique Web APIC ;Fabric > Fabric Policies > Pods > Policy Groups > POD_POLICY_GROUP(par défaut dans le document).

The screenshot shows the Cisco APIC Web UI. The top navigation bar includes 'System', 'Tenants', 'Fabric', 'Virtual Networking', 'Admin', 'Operations', 'Apps', and 'Integrations'. The left sidebar is titled 'Policies' and contains a 'Quick Start' button and a list of folders: 'Pods', 'Policy Groups', 'default', 'Profiles', 'Switches', 'Modules', 'Interfaces', 'Policies', and 'Annotations'. The 'Fabric Policies' tab is active, and the 'Pods' folder is expanded. The main content area is titled 'Pod Policy Group - default' and shows a 'Properties' section with various policy settings. The 'SNMP Policy' dropdown menu is open, showing 'default' as the current selection and 'New-SNMP' and 'fabric' as available options. The 'New-SNMP' option is highlighted in blue, indicating it is the selected option. Below the dropdown menu is a 'Create SNMP Policy' button.

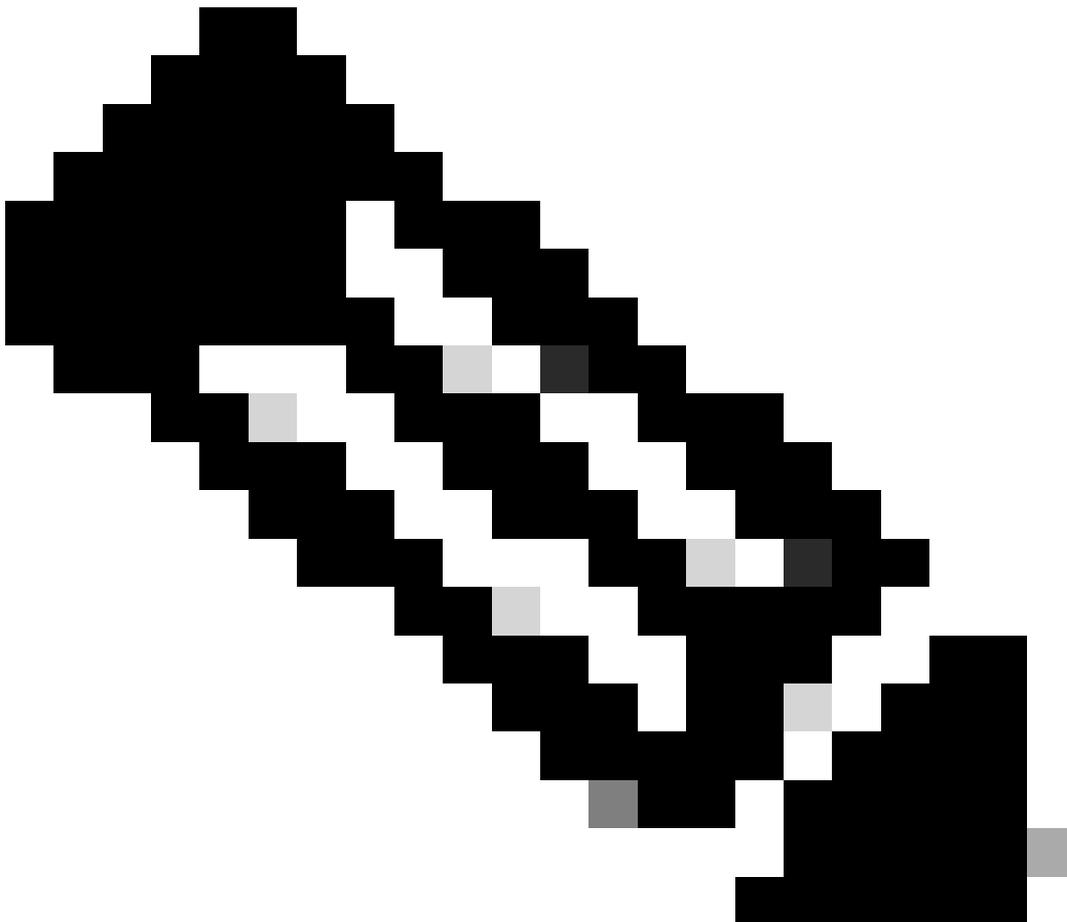
Dans le volet de droite, vous voyez un champ pour la politique SNMP. Dans la liste déroulante, sélectionnez la nouvelle politique SNMP que vous venez de créer et envoyez vos modifications.

Étape 3. Associer le groupe de stratégies Pod au profil Pod

Dans le document, utilisez le profil pod par défaut pour plus de simplicité. Pour ce faire, accédez au chemin de l'interface graphique utilisateur Web APIC (parFabric > Fabric Policies > Pods > Profiles > POD_PROFILEdéfaut dans le document).

The screenshot displays a network management interface. At the top, there are navigation tabs: System, Tenants, Fabric, Virtual Networking, Admin, Operations, Apps, and Integrations. Below these, there are sub-tabs: Inventory, Fabric Policies, and Access Policies. The left sidebar, titled 'Policies', contains a tree view with the following items: Quick Start, Pods, Policy Groups, Profiles, Pod Profile default, Switches, Modules, Interfaces, Policies, and Annotations. The 'Fabric Policies' sub-tab is active, and the 'Pod Selector - default' configuration page is shown. The configuration includes a 'Name' field set to 'default', a 'Description' field set to 'optional', a 'Type' dropdown set to 'ALL', and a 'Fabric Policy Group' dropdown set to 'default'. A red arrow points from the 'default' item under 'Pod Profile default' in the sidebar to the 'Fabric Policy Group' dropdown in the configuration panel.

Au cours de cette étape, configurez le protocole SNMP de base pour les MIB globales.



Remarque : À ce stade, toutes les étapes nécessaires (étapes 1 à 3) à la configuration SNMP ont été effectuées et l'étendue MIB globale a été implicitement utilisée. Cela permet d'effectuer une visite SNMP pour n'importe quel noeud ACI ou APIC.

Étape 4 : configuration des étendues de contexte VRF

Une fois que vous associez une chaîne de communauté à un contexte VRF, cette chaîne de communauté spécifique ne peut pas être utilisée pour extraire les données SNMP d'étendue globale. Par conséquent, il est nécessaire de créer deux chaînes de communauté SNMP si vous souhaitez extraire à la fois les données de portée globale et de contexte VRF SNMP.

Dans ce cas, les chaînes de communauté précédemment créées (à l'étape 1), à savoir (New-1), utilisent New-1 pour la portée de contexte VRF et le VRF personnalisé VRF-1 dans l'exemple de client personnalisé. Pour ce faire, accédez au chemin de l'interface utilisateur graphique Web APIC ; 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

Create SNMP Context

Context Name:

Community Profiles:

Name	Description
New-1	

Create in Step 1.

Après avoir envoyé la configuration, vous pouvez vérifier la configuration du contexte SNMP que vous avez appliquée en cliquant avec le bouton gauche sur votre VRF, en naviguant jusqu'à l'onglet Policy sur le VRF, et en faisant défiler vers le bas vers le bas du volet :

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:

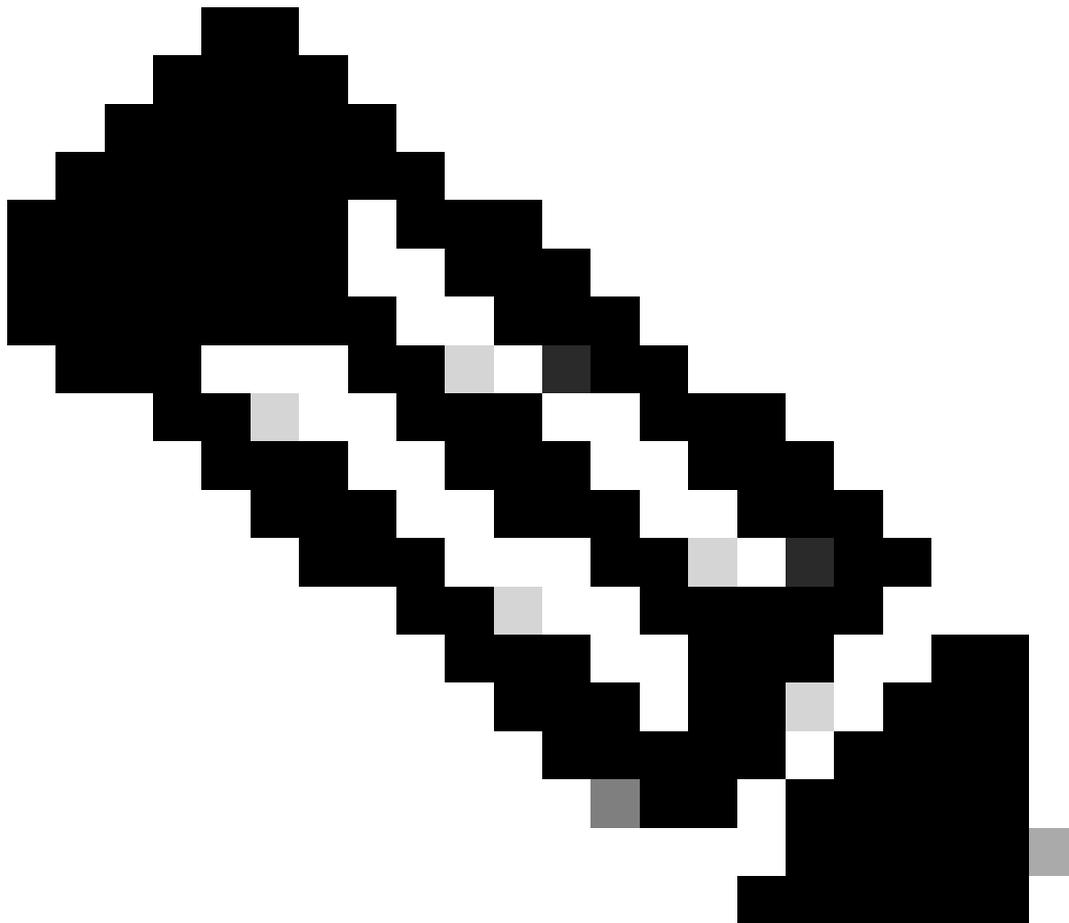
Name	Description
New-1	

Afin de désactiver un contexte SNMP sur un VRF, vous pouvez désélectionner la case à cocher Create SNMP Context (Créer un contexte SNMP) (vue dans la capture d'écran), ou cliquer avec le bouton droit sur le VRF et choisir Delete SNMP Context.

Configuration des dérouterements SNMP via l'interface utilisateur graphique

Les dérouterements SNMP sont envoyés au serveur SNMP (SNMP Destination/Network Management Systems (NMS)) sans interrogation, et le noeud ACI/APIC envoie le dérouterement SNMP une fois que la panne/l'événement (condition définie) se produit.

Les interruptions SNMP sont activées en fonction de l'étendue de la stratégie sous les stratégies de surveillance Access/Fabric/Tenant. L'ACI prend en charge un maximum de 10 récepteurs d'interruptions.



Remarque : Sans les étapes 1 à 3 de la section précédente, la configuration des dérouterements SNMP ne suffit pas. Étape 2. Dans la configuration SNMP TRAP, la fonction est liée à la surveillance des politiques pour (accès/fabric/locataire).

Pour configurer les dérouterements SNMP dans l'ACI, vous devez effectuer les deux étapes en plus des étapes 1, 2 et 3 de la section précédente.

Étape 1 : configuration du serveur TRAP SNMP

Pour ce faire, accédez au chemin de l'interface utilisateur graphique Web APIC ;Admin > External Data Collectors > Monitoring Destinations > SNMP.

The screenshot shows the Web APIC navigation menu. The 'Admin' tab is selected. Under 'External Data Collectors', the 'Monitoring Destinations' folder is expanded, and the 'SNMP' folder is selected. A tooltip 'Create SNMP Monitoring Destination Group' is visible over the 'SNMP' folder. The main content area shows the 'SNMP' configuration page with a 'Name' field.

The screenshot shows the 'Create SNMP Monitoring Destination Group' wizard. The current step is 'STEP 1 > Profile'. The 'Name' field contains 'SNMP-trap-server' and the 'Description' field contains 'optional'. The 'Next' button is highlighted in blue, indicating the next step in the process.

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 : l'hôte de la destination de déROUTement SNMP.

Port : port de service de la destination de déROUTement SNMP. La plage est comprise entre 0 (non spécifié) et 65535 ; il est défini par défaut à 162.

Version : version CDP prise en charge pour la destination de déROUTement SNMP. La version peut être :

- v1 - utilise une correspondance de chaîne de communauté pour l'authentification de l'utilisateur.

- v2c - utilise une correspondance de chaîne de communauté pour l'authentification des utilisateurs.
- v3 - protocole d'administration de réseau basé sur des normes interopérables qui fournit un accès sécurisé aux périphériques par une combinaison d'authentification et de chiffrement des trames sur le réseau.

La valeur par défaut est v2c.

Security Name : nom de sécurité de la destination du déROUTement SNMP (nom de la communauté). Il ne peut pas contenir le symbole @.

v.3 Security Level : niveau de sécurité SNMPv3 pour le chemin de destination SNMP. Le niveau peut être :

- authentication
- noauth
- priv

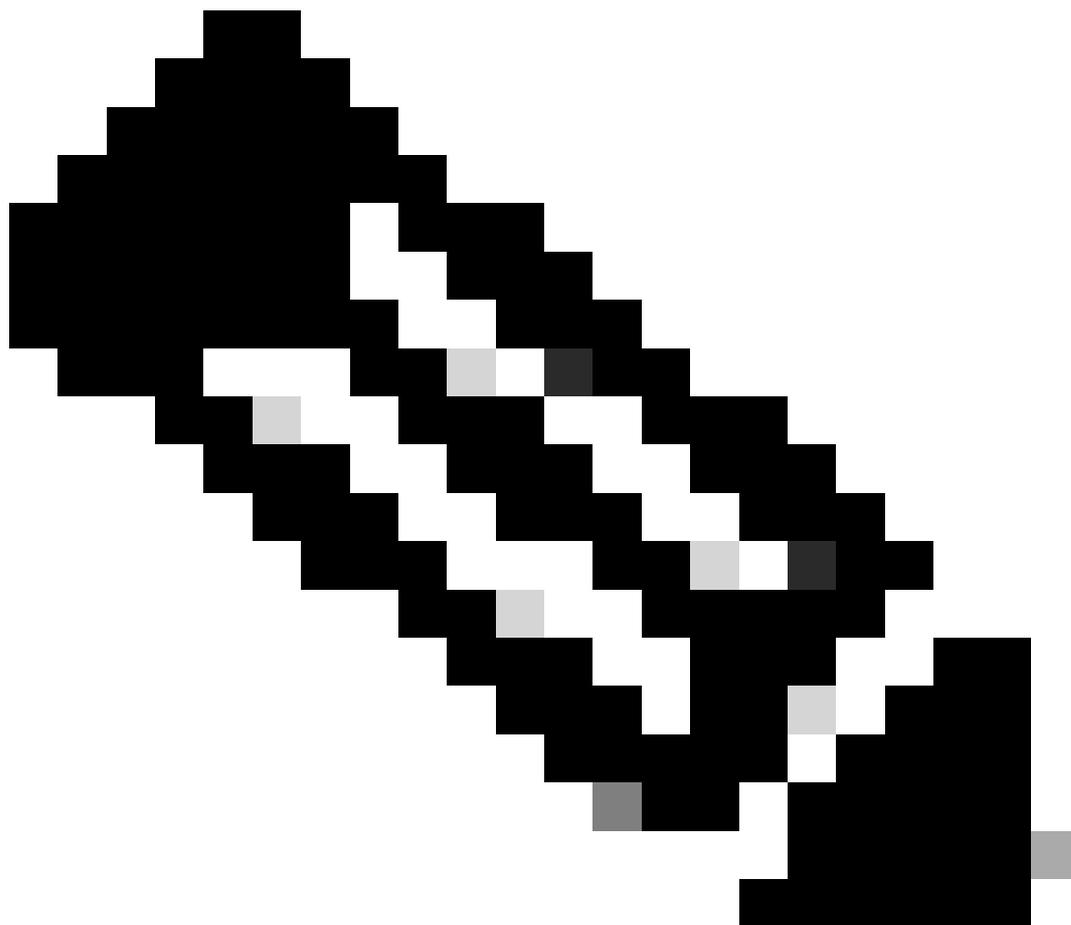
La valeur par défaut est noauth.

EPG de gestion : nom du groupe de terminaux de gestion pour la destination SNMP par laquelle l'hôte distant est accessible.

Étape 2 : configuration de la source TRAP SNMP sous la politique de surveillance (accès/fabric/locataire)

Vous pouvez créer des stratégies de surveillance avec les trois étendues suivantes :

- Accès : ports d'accès, FEX, contrôleurs de VM
- Fabric : ports de fabric, cartes, châssis, ventilateurs
- Locataire - EPG, profils d'application, services

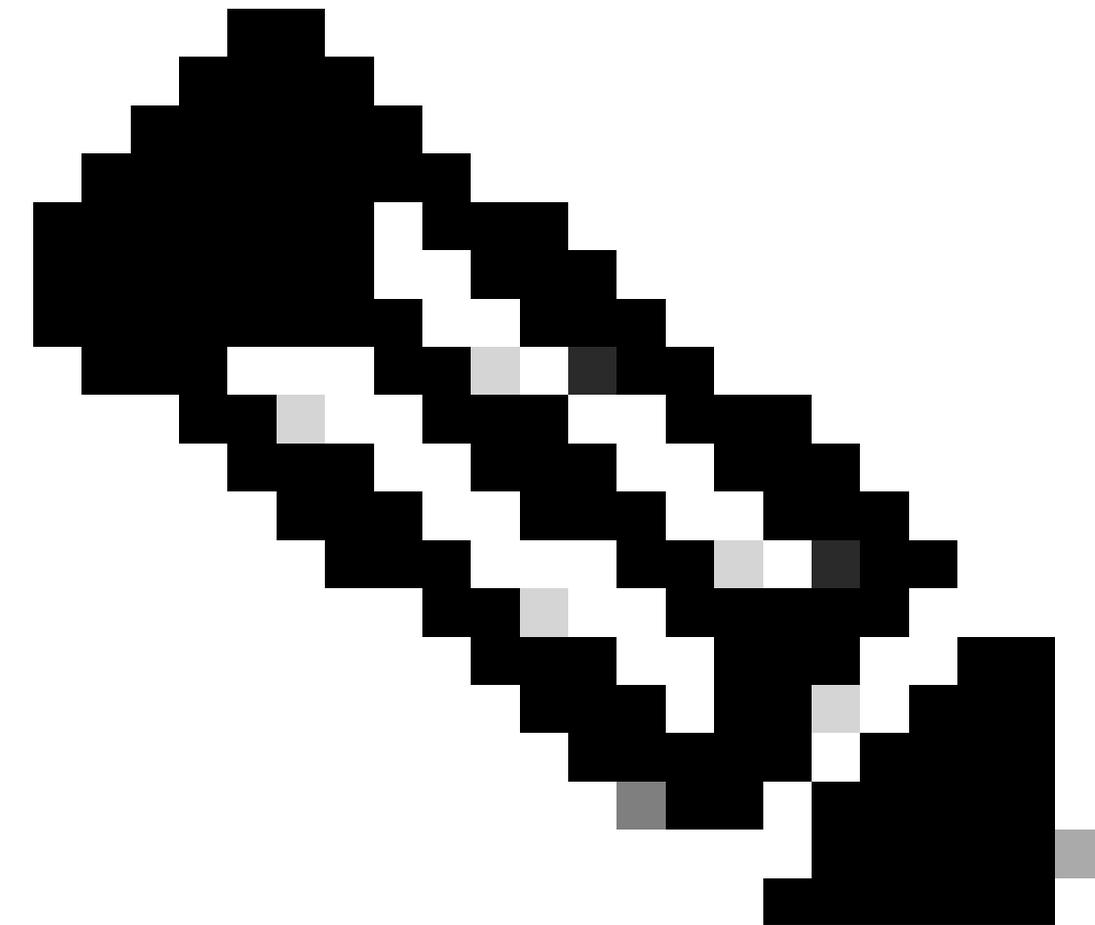
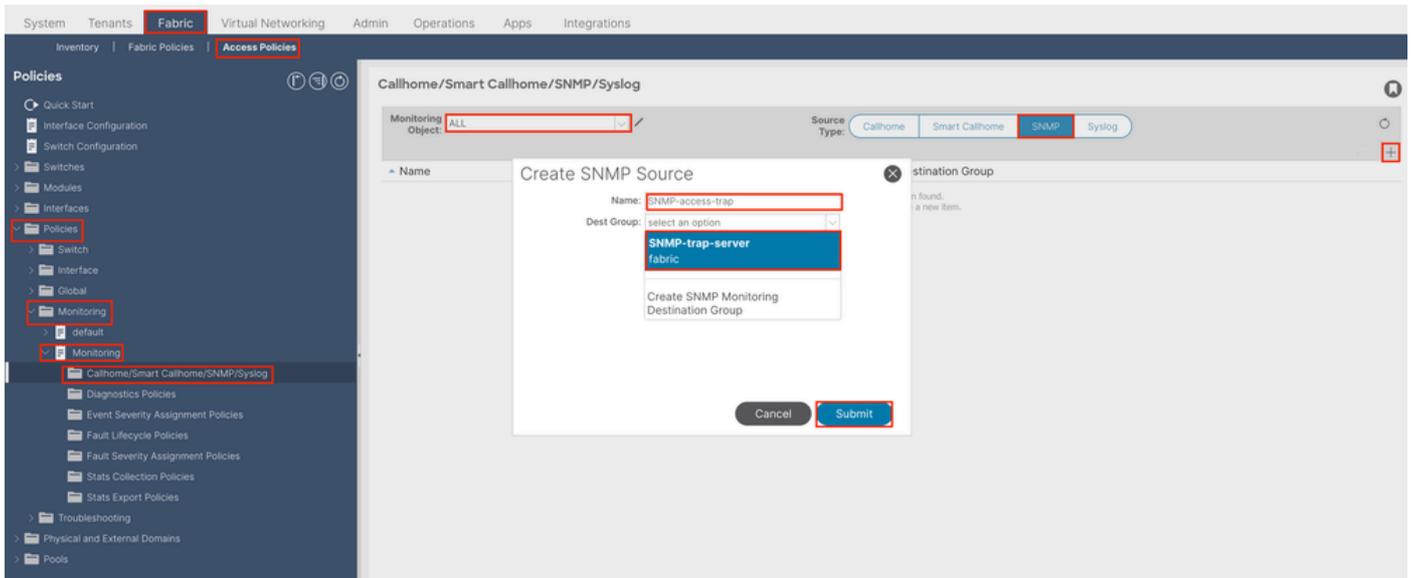


Remarque : Vous pouvez choisir n'importe laquelle ou n'importe quelle combinaison d'entre elles afin de configurer selon vos besoins.

Option 1. Définir la source SNMP sous Politiques d'accès

Pour ce faire, accédez au chemin de l'interface utilisateur graphique Web du contrôleur APIC ;

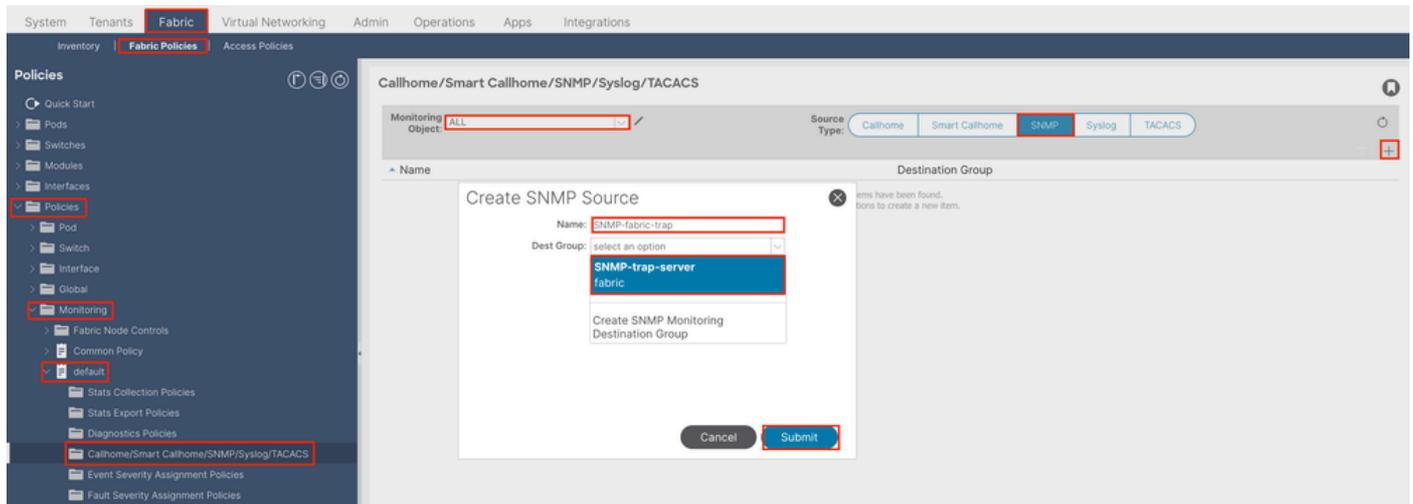
Fabric > Access Policies > Policies > Monitoring > Default > Callhome/Smart Callhome/SNMP/Syslog/TACACS.



Remarque : Vous pouvez utiliser une stratégie de surveillance personnalisée (si elle est configurée) au lieu de la stratégie par défaut, utilisez celle par défaut ici. Vous pouvez spécifier l'objet de surveillance à surveiller ; tous ont été utilisés ici.

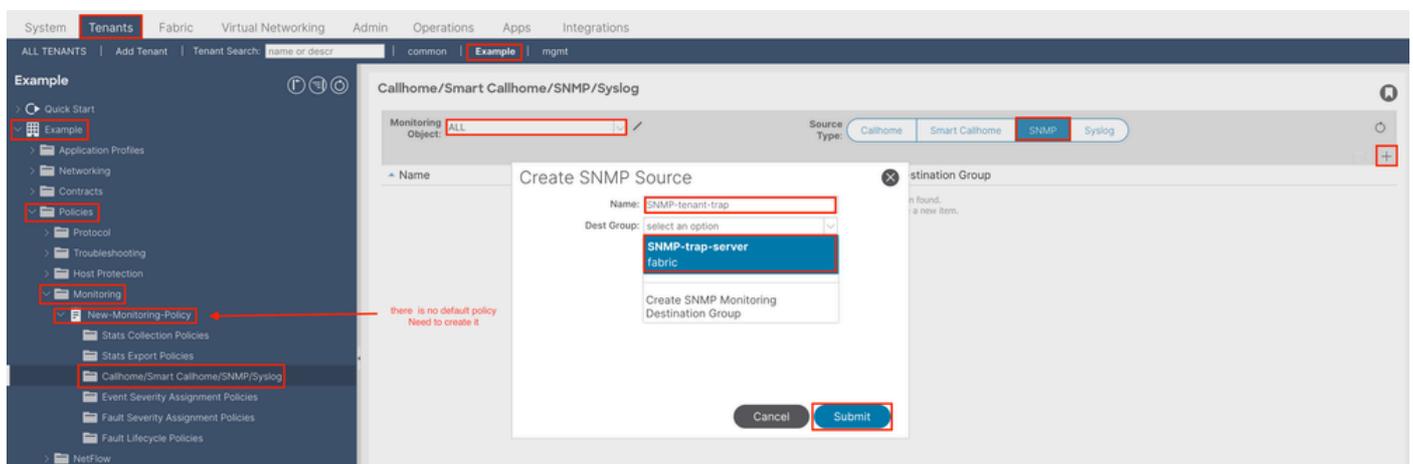
Option 2. Définir la source SNMP sous Politiques de fabric

Pour ce faire, accédez au chemin de l'interface utilisateur graphique Web du contrôleur APIC ;
Fabric > Fabric Policies > Policies > Monitoring > Default > Callhome/Smart Callhome/SNMP/Syslog/TACACS.



Option 3. Définir la source SNMP sous Politiques de locataire

Pour ce faire, accédez au chemin de l'interface utilisateur graphique Web du contrôleur APIC ;
Tenant > (Tenant Name) > Policies > Monitoring > (Custom monitoring policy) > Callhome/Smart Callhome/SNMP/Syslog/TACACS.



Vérifier

Utiliser la commande snmpwalk pour vérifier

Commencez par extraire les données SNMP de la portée globale d'un commutateur Leaf. C'est exactement ce que permet la commande snmpwalk ; snmpwalk -v 2c -c New-1 x.x.x.x.

Cette commande décomposée représente :

snmpwalk = L'exécutable snmpwalk installé sur MacOS/Linux/Windows

-v = Spécifie la version du protocole SNMP à utiliser

2c= Spécifie que utilise la version 2c du protocole SNMP

-c= Spécifie qu'une chaîne de communauté particulière

New-1= La chaîne de communauté est utilisée pour extraire les données SNMP de portée globale

x.x.x.x= Adresse IP de gestion hors bande de mon commutateur Leaf

Résultat de la commande :

```
$ 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
```

Dans le résultat de la commande capturée, vous pouvez voir que le snmpwalk a réussi et que des informations spécifiques au matériel ont été extraites. Si vous laissez le snmpwalk continuer, vous voyez les noms d'interface matérielle, les descriptions, etc.

À présent, continuez à récupérer les données SNMP de contexte VRF, contextes SNMP précédemment créés, New-VRF-SNMP pour VRF en utilisant la chaîne de communauté SNMP, New-1.

Puisque la même chaîne de communauté est utilisée, New-1, à travers deux contextes SNMP différents, vous devez spécifier le contexte SNMP dont vous voulez extraire les données SNMP. Il y a la syntaxe snmpwalk que vous devez utiliser pour spécifier un contexte SNMP particulier ;

```
snmpwalk -v 2c -c New-1@New-VrF-SNMP 10.x.x.x.
```

Vous pouvez voir que pour extraire d'un contexte SNMP spécifique, vous utilisez le format suivant :

Utilisation des commandes show CLI

Sur APIC :

```
show snmp
```

```
show snmp policy
```

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

Sur le commutateur :

```
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
```

Utilisation des commandes Moquery CLI

Sur APIC/commutateur :

```
moquery -c snmpGroup #The SNMP destination group, which contains information needed to send traps and informs.
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 information about the destination.
moquery -c snmpPol #The SNMP policy, which enables you to monitor client group, v3 user, and/ or community.
moquery -c snmpClientGrpP #A client group, which is a group of client IP addresses that allows SNMP access.
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 general information.
moquery -c snmpClientP #The client profile information.
moquery -c snmpRsEpg #A source relation to the endpoint group VRF through which the clients can access.
moquery -c snmpSrc #The SNMP source profile, which determines the fault information, severity, and other information.
moquery -c snmpCtxP #The SNMP context profile, which enables you to specify a context to monitor.
```

Utilisation des commandes cat CLI

Sur APIC :

```
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
```

Dépannage

Vérifiez le processus snmpd

Sur le commutateur :

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

Sur APIC :

```
ps aux | grep snmp
```

Si le processus est normal, contactez le TAC Cisco pour obtenir de l'aide.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.