Configurer SNMP dans l'ACI

Table des matières

Introduction

Ce document décrit la configuration du protocole SNMP (Simple Network Management Protocol) et des déroutements 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

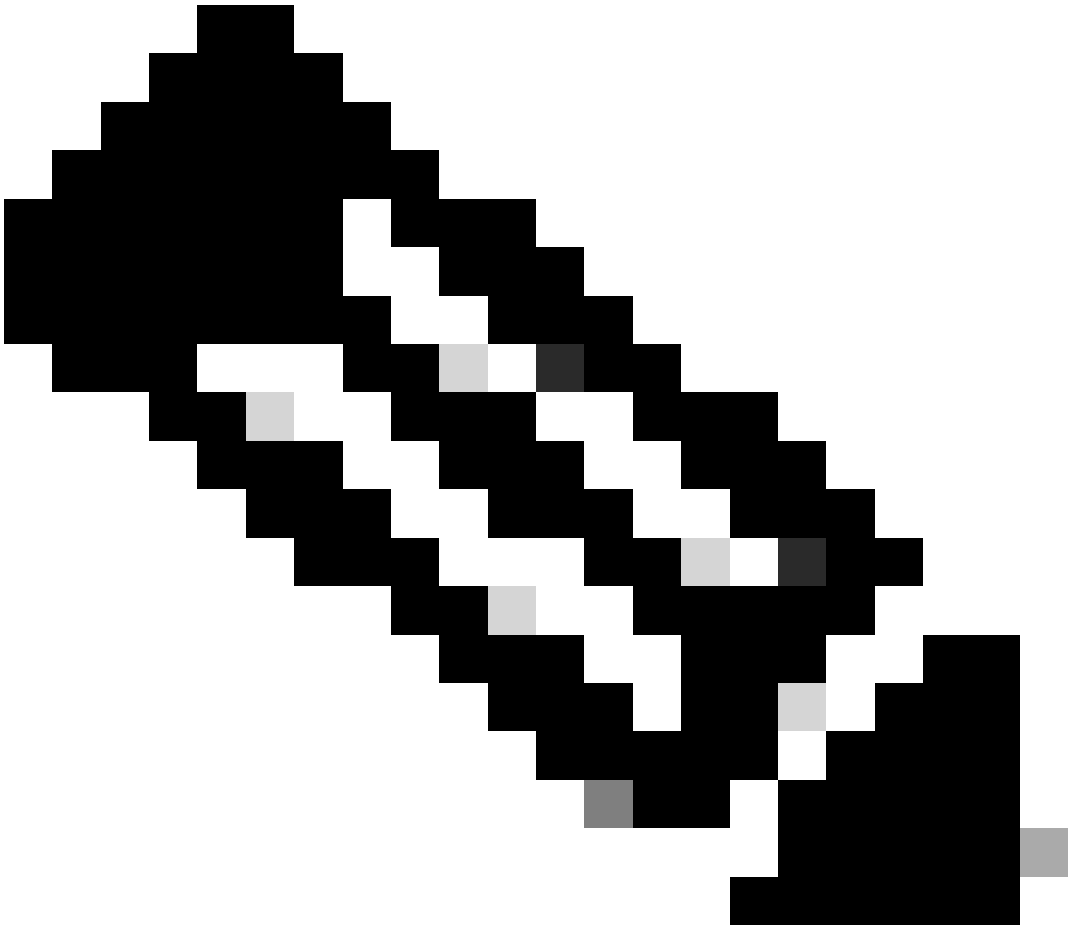
Un concept fondamental du protocole SNMP dans l'ACI est qu'il existe deux étendues à partir desquelles les informations SNMP peuvent être extraites :
1. Mondial
2. Contexte du routage et du transfert virtuels (VRF)

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 la portée du contexte VRF extraient des informations spécifiques à la VRF, telles que les adresses IP et les

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.

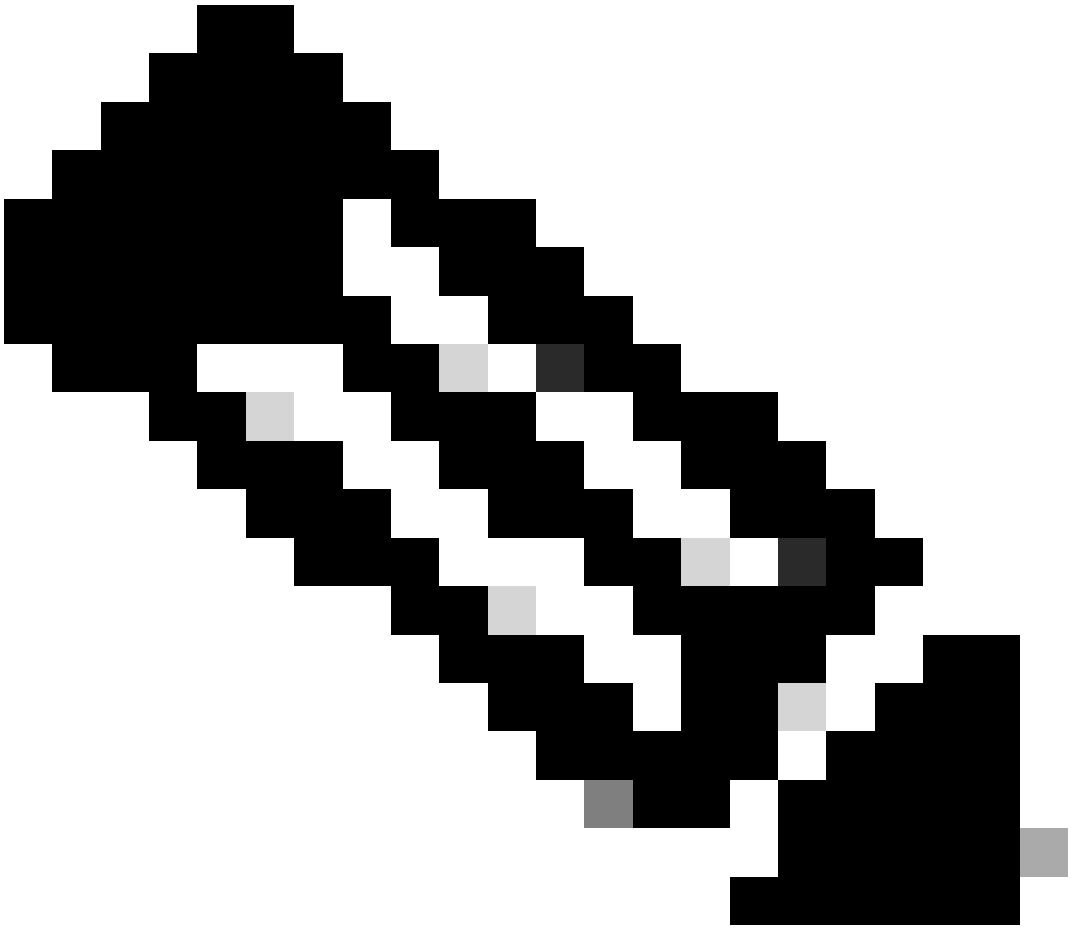


Remarque : une MIB avec une étendue globale n'a qu'une seule instance dans le système. Les données d'une base MIB globale concernent l'ensemble du système.

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.

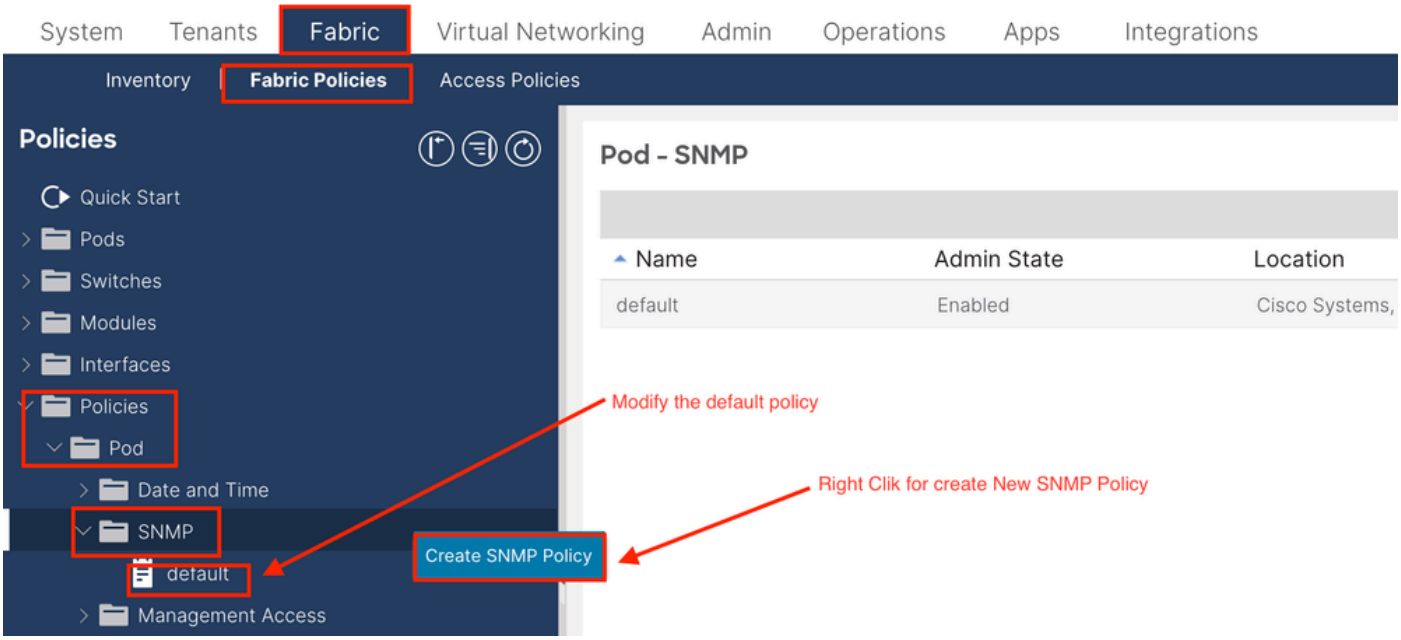
Étapes de configuration (pour les étendues globales et de contexte VRF)

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.

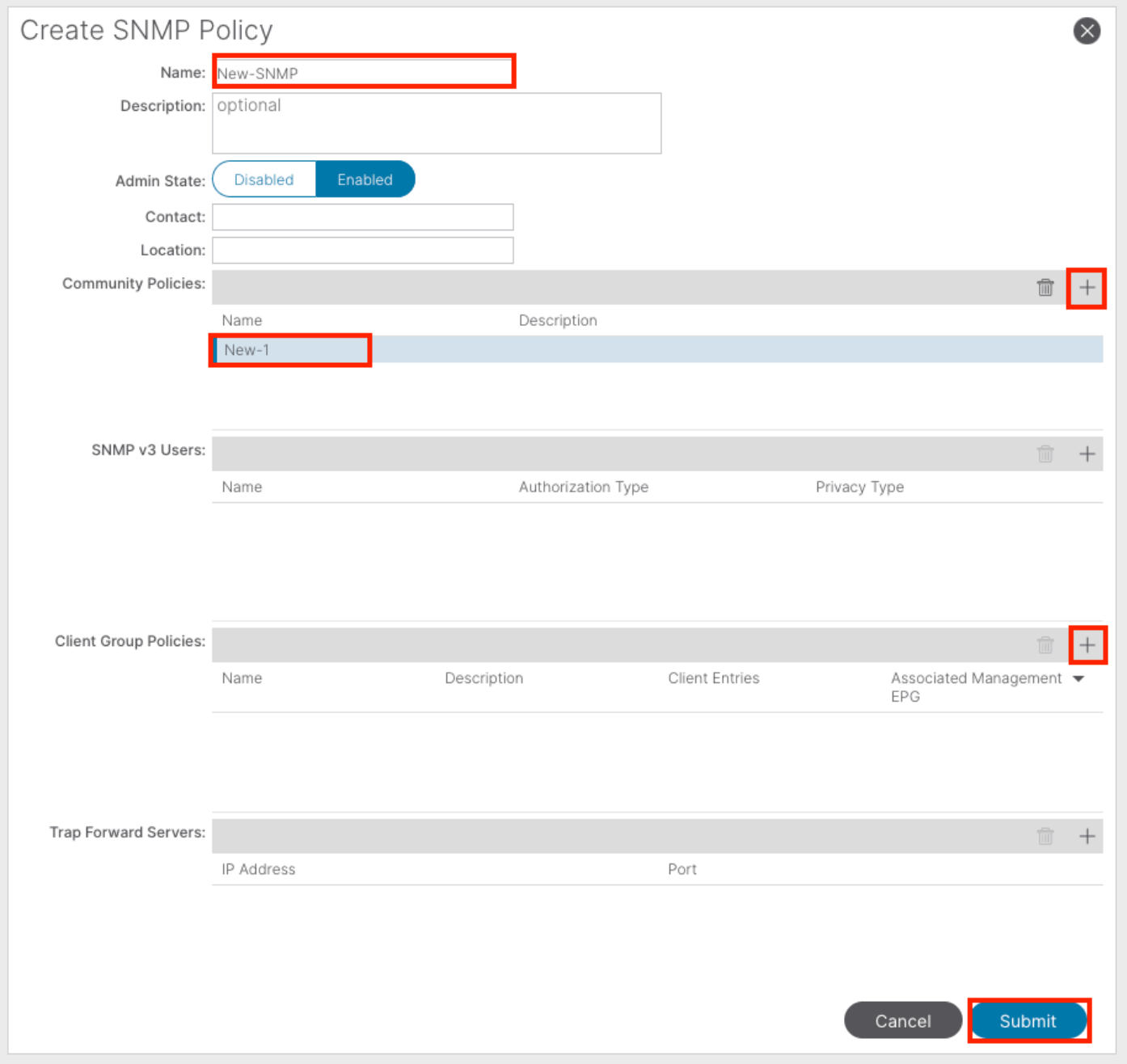
La première étape de la configuration du protocole SNMP consiste à créer les politiques de fabric SNMP nécessaires. Afin de créer les politiques de fabric SNMP, naviguez jusqu'au chemin de l'interface utilisateur graphique Web APIC ; Fabric > Fabric Policies > Policies > Pod > SNMP.



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 identités de communauté apparaissent plus tard.



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.

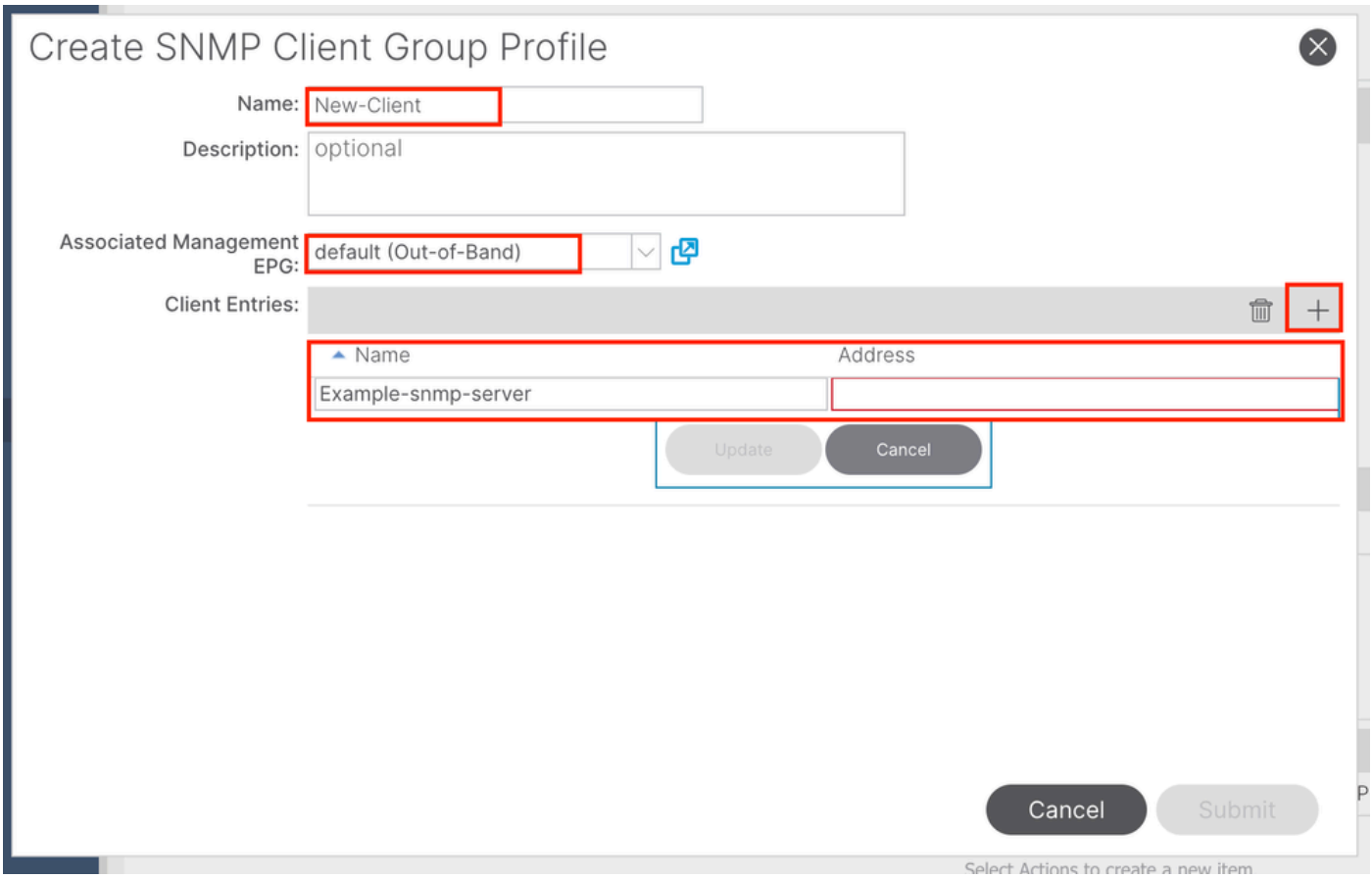
Emplacement : emplacement de la stratégie SNMP.

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 :



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.

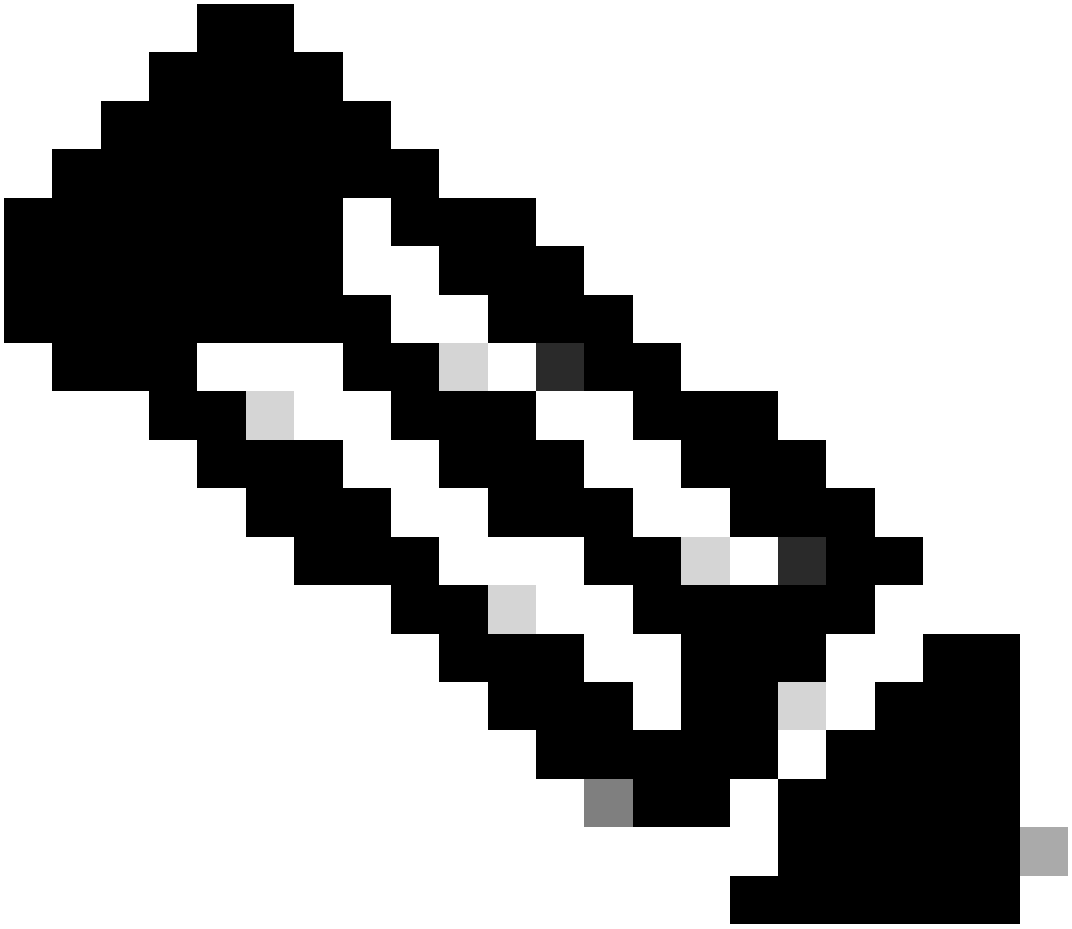
Client Entries : adresse IP du profil client SNMP.

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 :

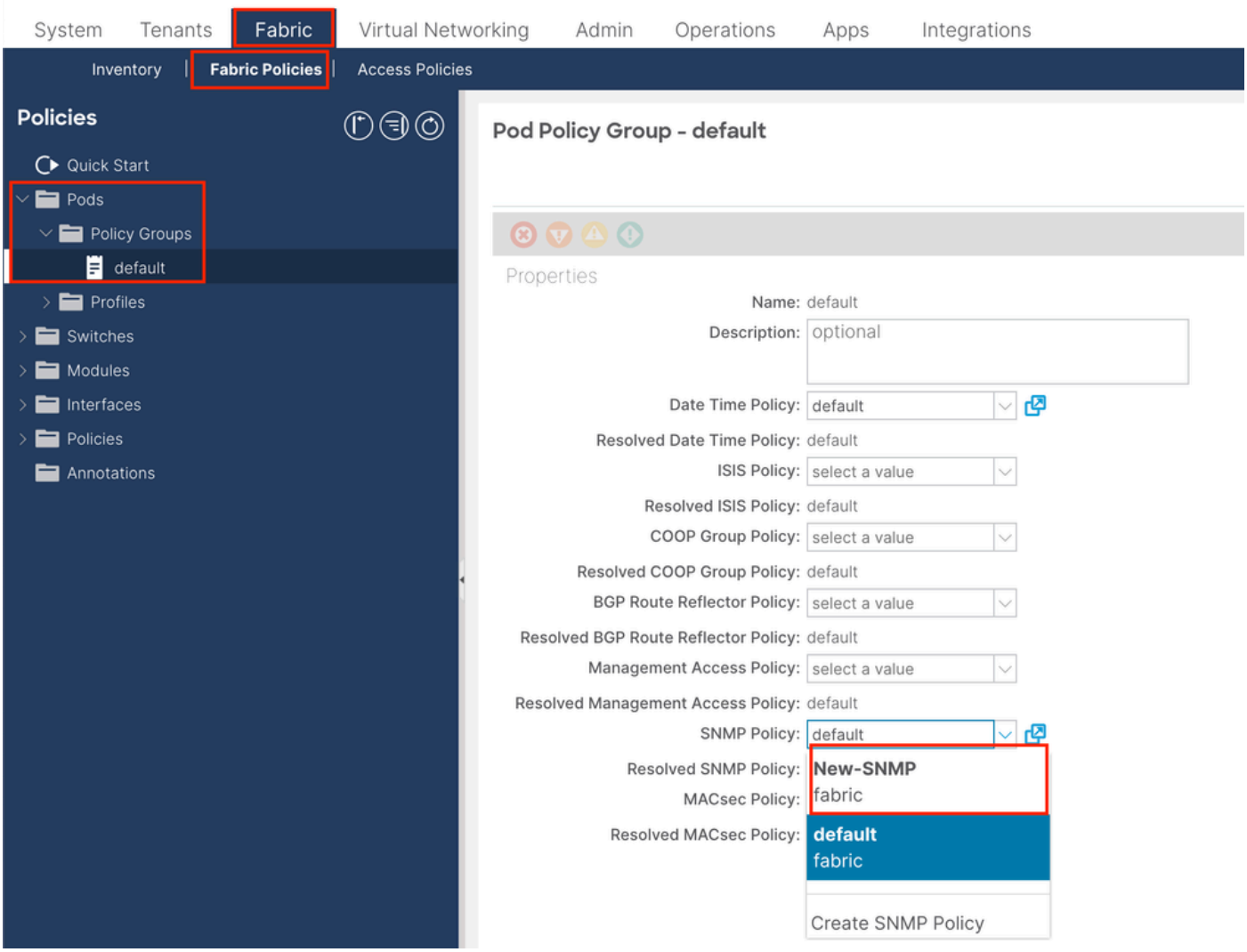
- Adresse IP hôte spécifique : 192.168.1.5
- Sous-réseau entier : 192.168.1.0/24



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 (groupe de stratégies Fabric)

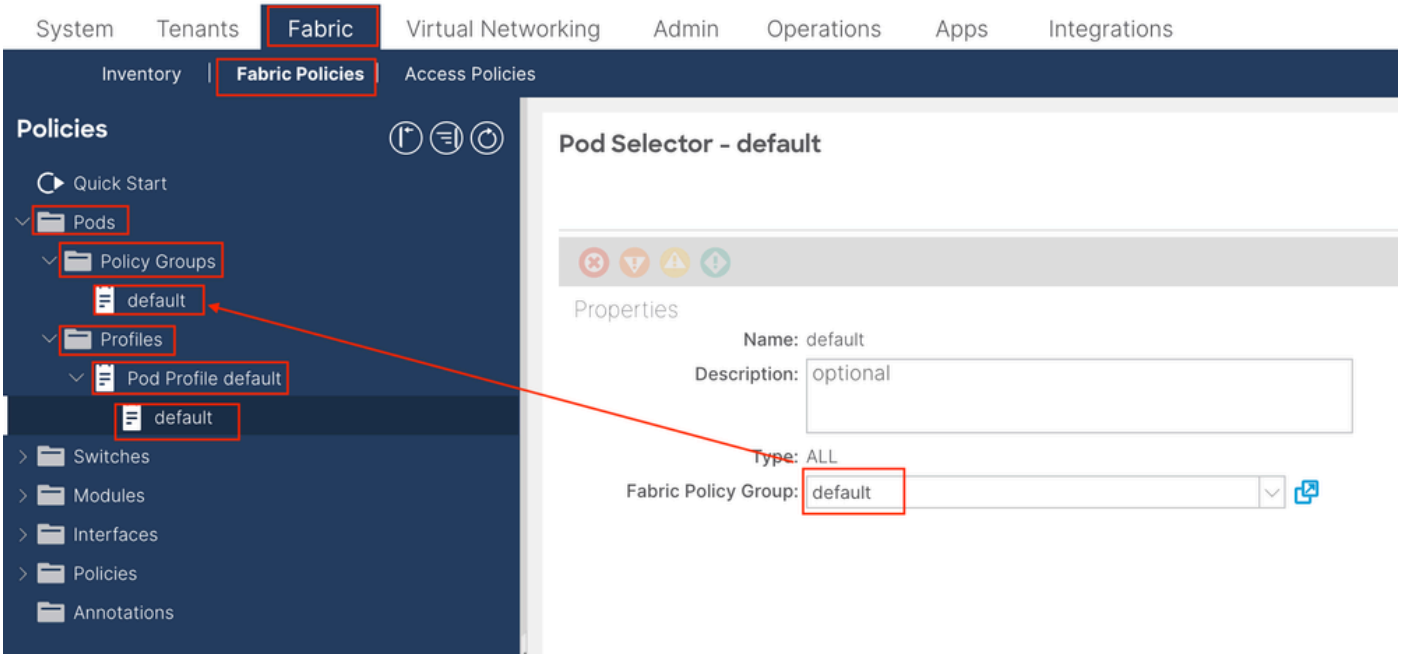
Afin d'appliquer cette configuration, naviguez jusqu'au chemin de l'interface utilisateur graphique Web APIC ; Fabric > Fabric Policies > Pods > Policy Groups > POD_POLICY_GROUP (par défaut dans le document).



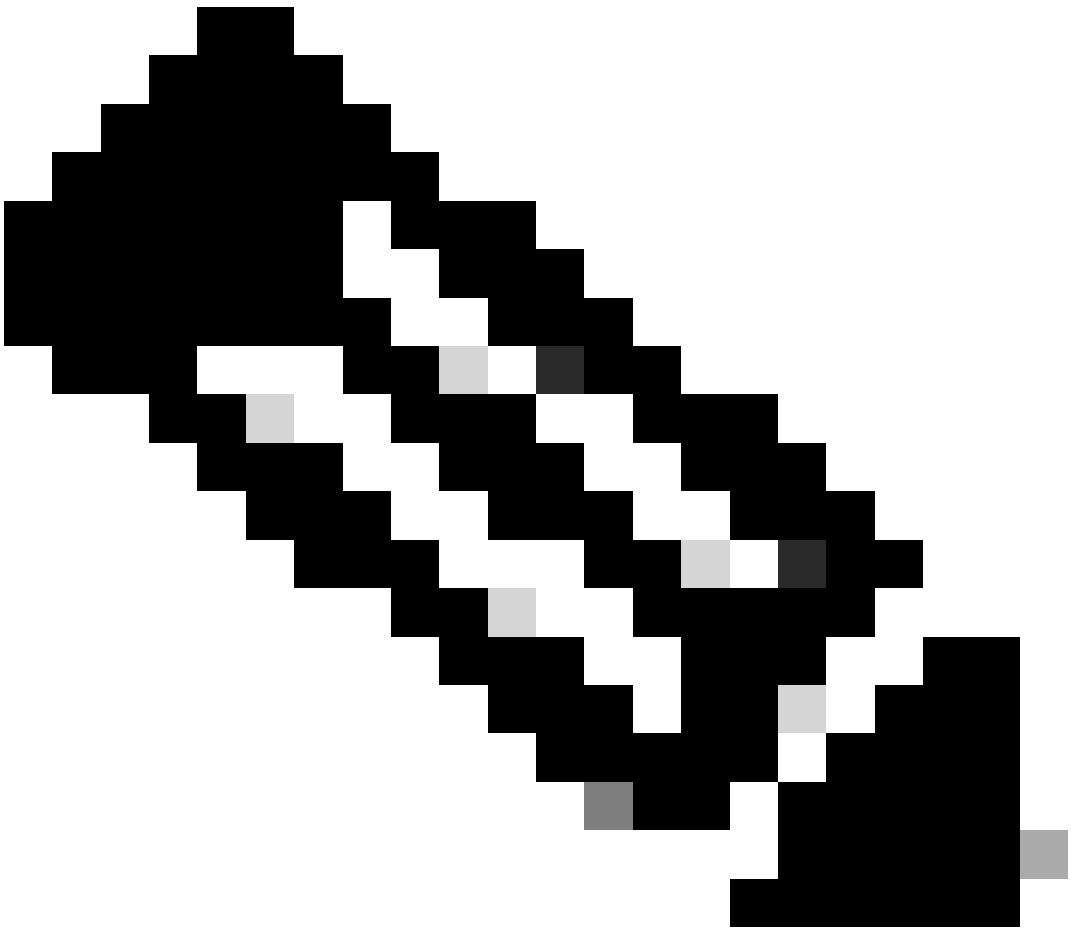
Dans le volet de droite, vous voyez un champ pour la politique SNMP. Dans la liste déroulante, sélectionnez la nouvelle politique SNMP que vous venez de créer et envoyez vos modifications.

Étape 3. Associer le groupe de politiques de pod au profil de 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_PROFILE défaut dans le document).



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

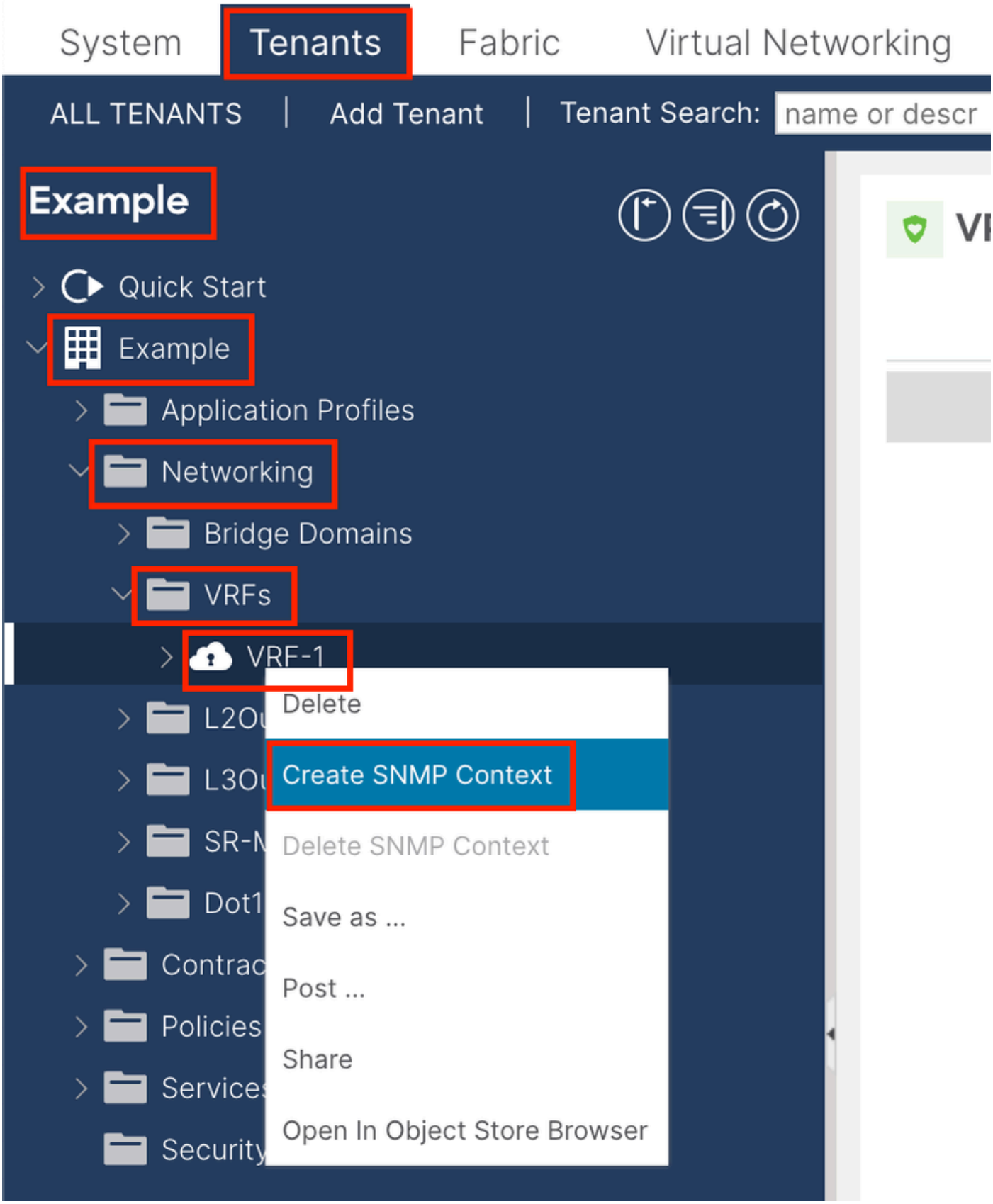


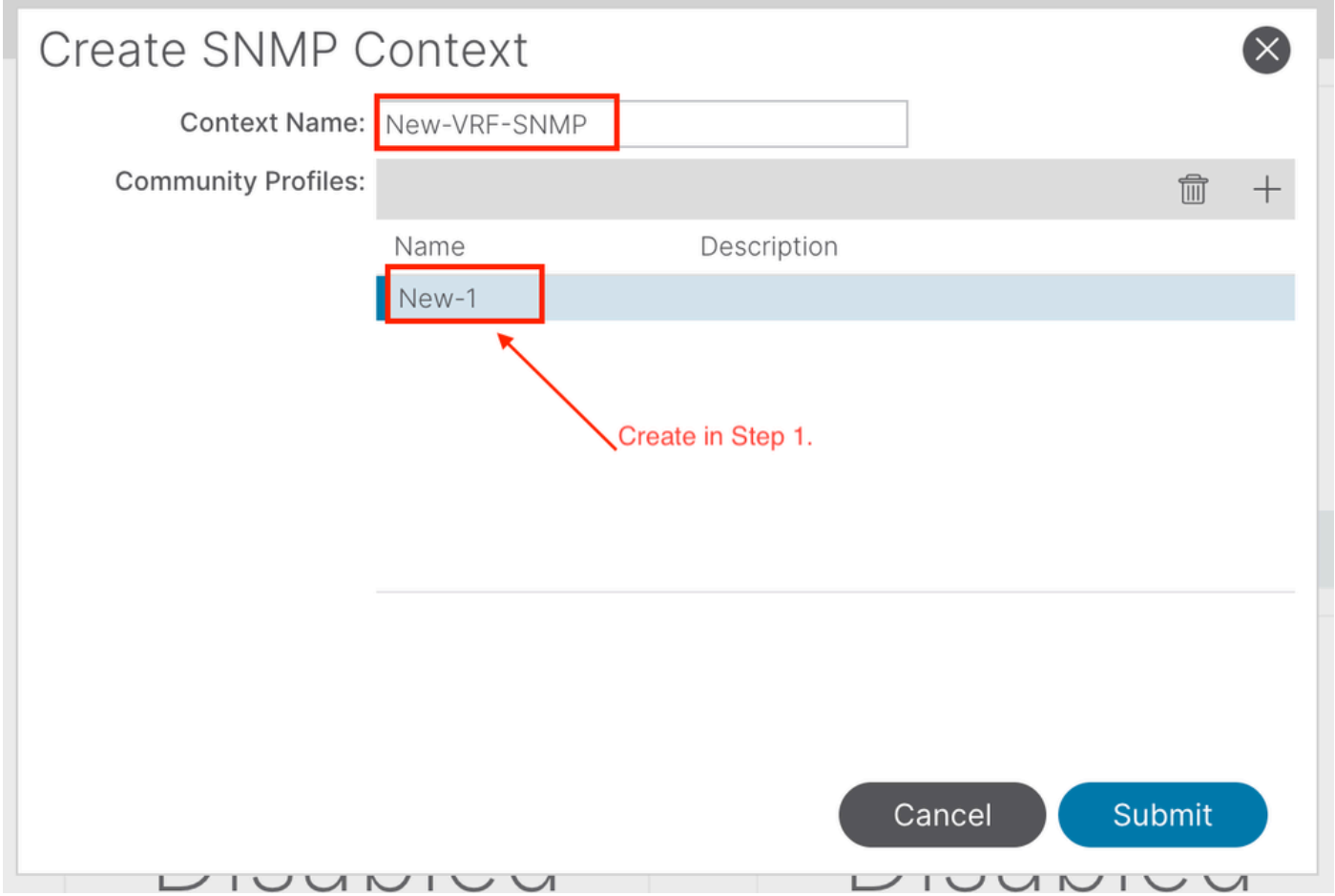
Remarque : à ce stade, toutes les étapes nécessaires (étapes 1 à 3) à la configuration SNMP ont été effectuées et l'étendue MIB globale a été implicitement utilisée. Cela permet d'effectuer un parcours SNMP pour n'importe quel noeud ACI ou APIC.

Étape 4. Configurer les étendues de contexte VRF

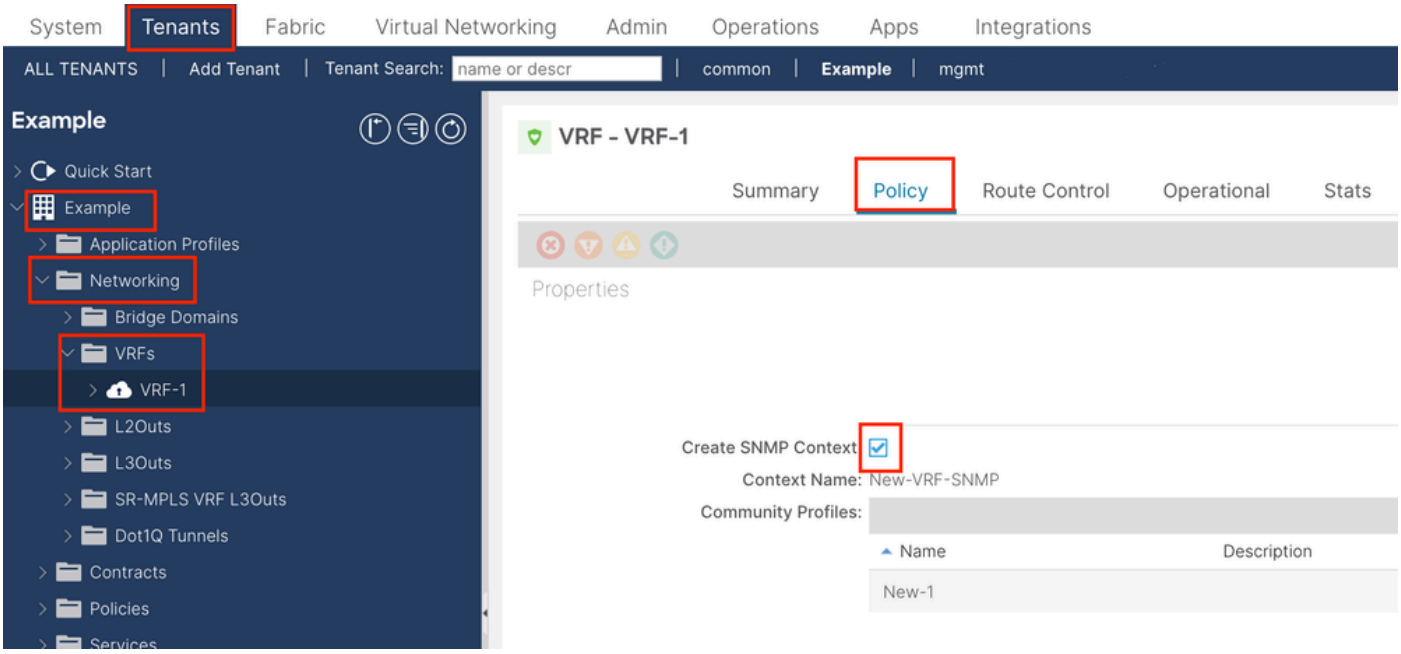
Une fois que vous associez une chaîne de communauté à un contexte VRF, cette chaîne de communauté spécifique ne peut pas être utilisée pour extraire les données SNMP d'étendue globale. Par conséquent, il est nécessaire de créer deux chaînes de communauté SNMP si vous souhaitez extraire à la fois les 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
Delete
Create SNMP Context
Delete SNMP Context
Save as ...
Post ...
Share
Open In Object Store Browser



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 :

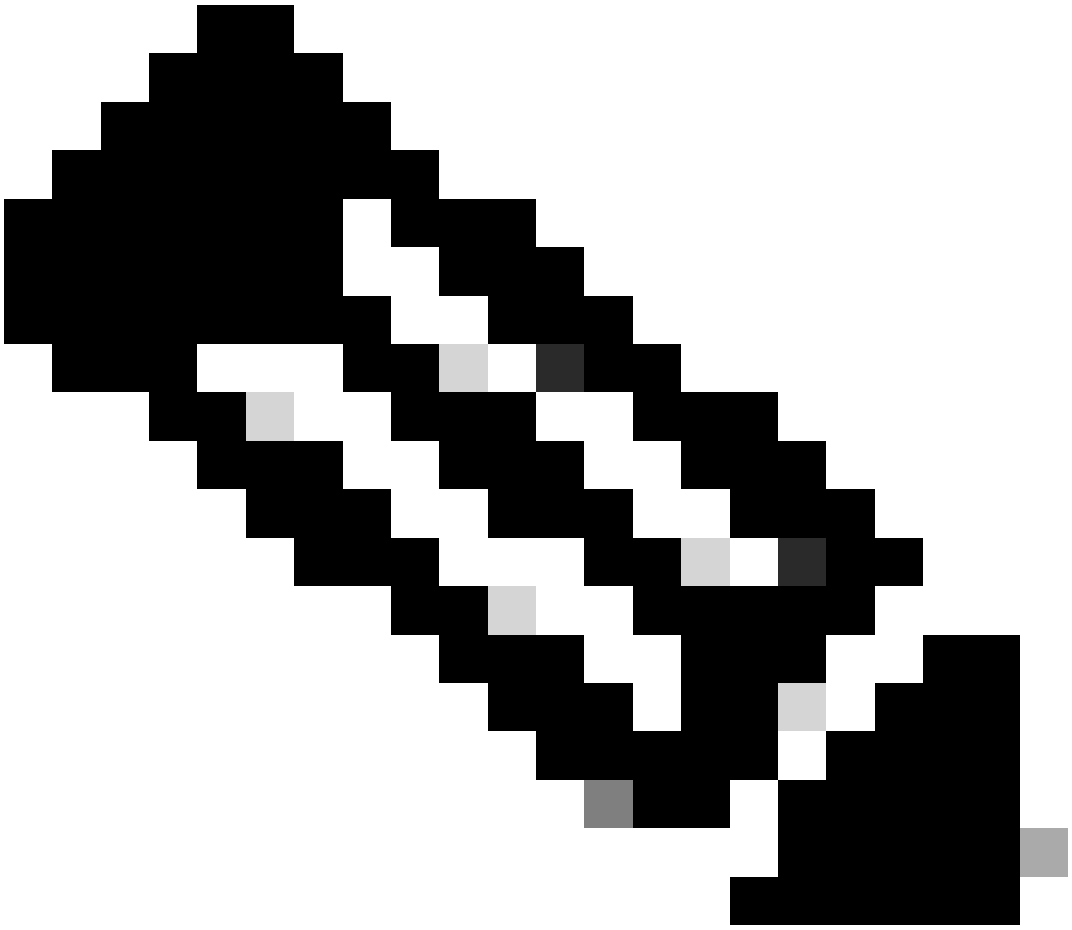


Afin de désactiver un contexte SNMP sur un VRF, vous pouvez désélectionner la case à cocher **Create SNMP Context** (**Créer un contexte SNMP**) (vue dans la capture d'écran), ou cliquer avec le bouton droit sur le VRF et choisir **Delete SNMP Context**.

Configuration des déroutements SNMP via l'interface utilisateur graphique

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

Les déroutements SNMP sont activés en fonction de l'étendue de la stratégie sous Access/Fabric/Tenant monitoring policies. L'ACI prend en charge un maximum de 10 récepteurs Trap.

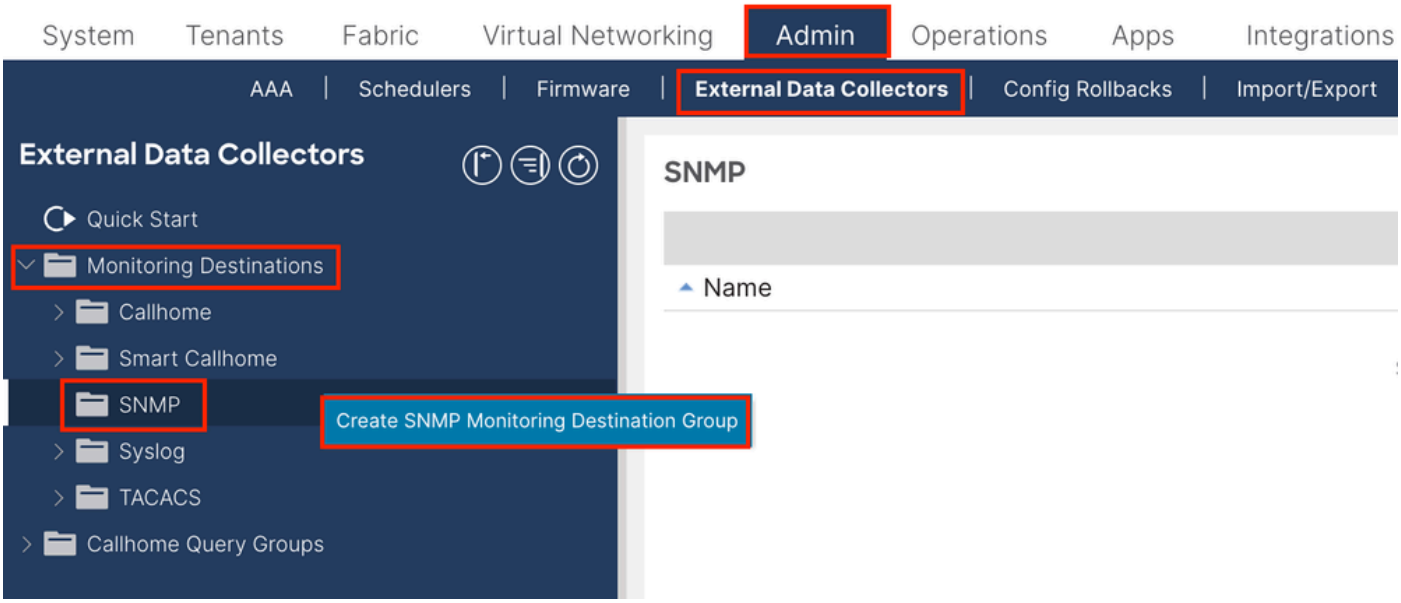


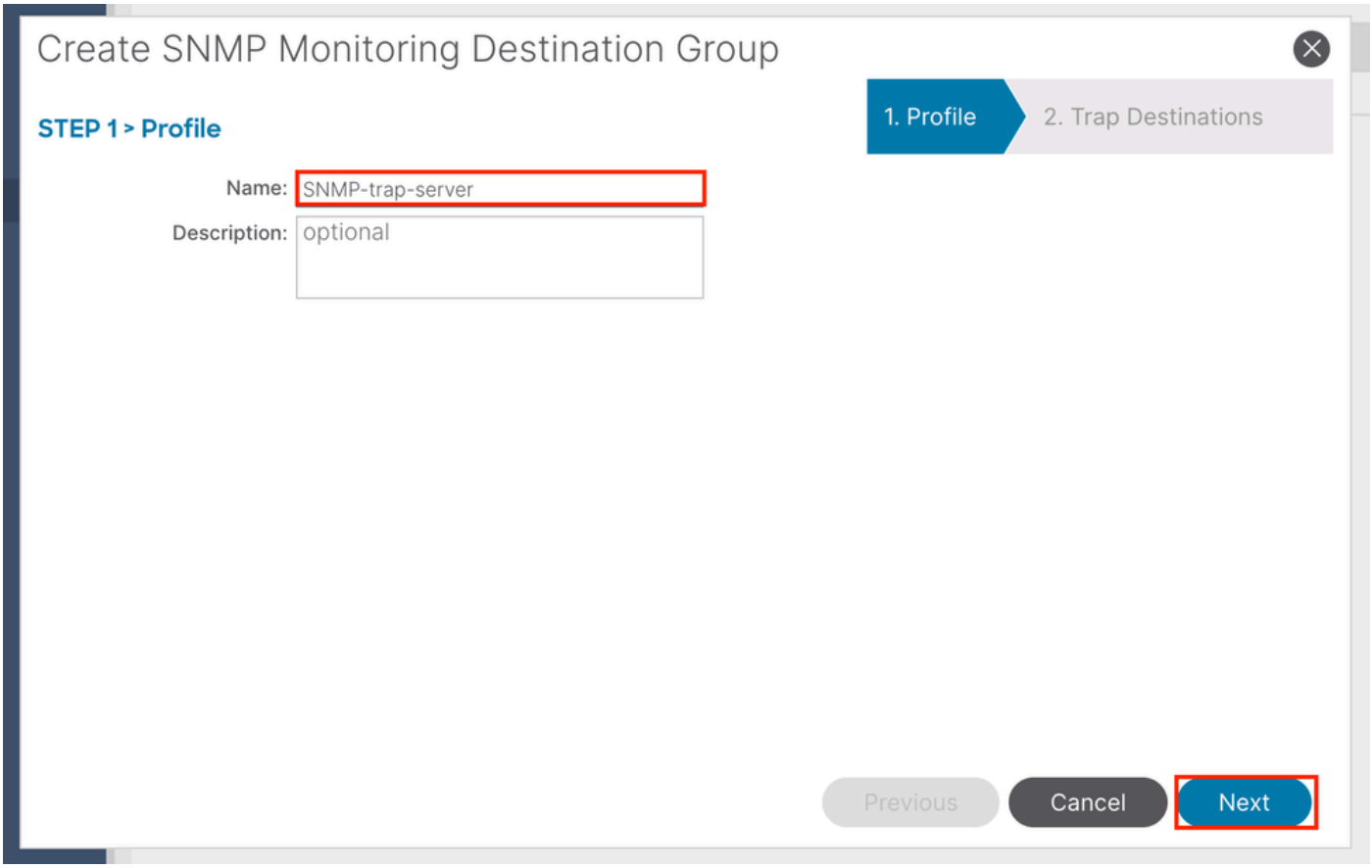
Remarque : sans les étapes 1 à 3 de la section précédente, la configuration des déroutements SNMP ne suffit pas. Étape 2. Dans la configuration SNMP TRAP, la fonction est liée à la surveillance des politiques pour (accès/fabric/locataire).

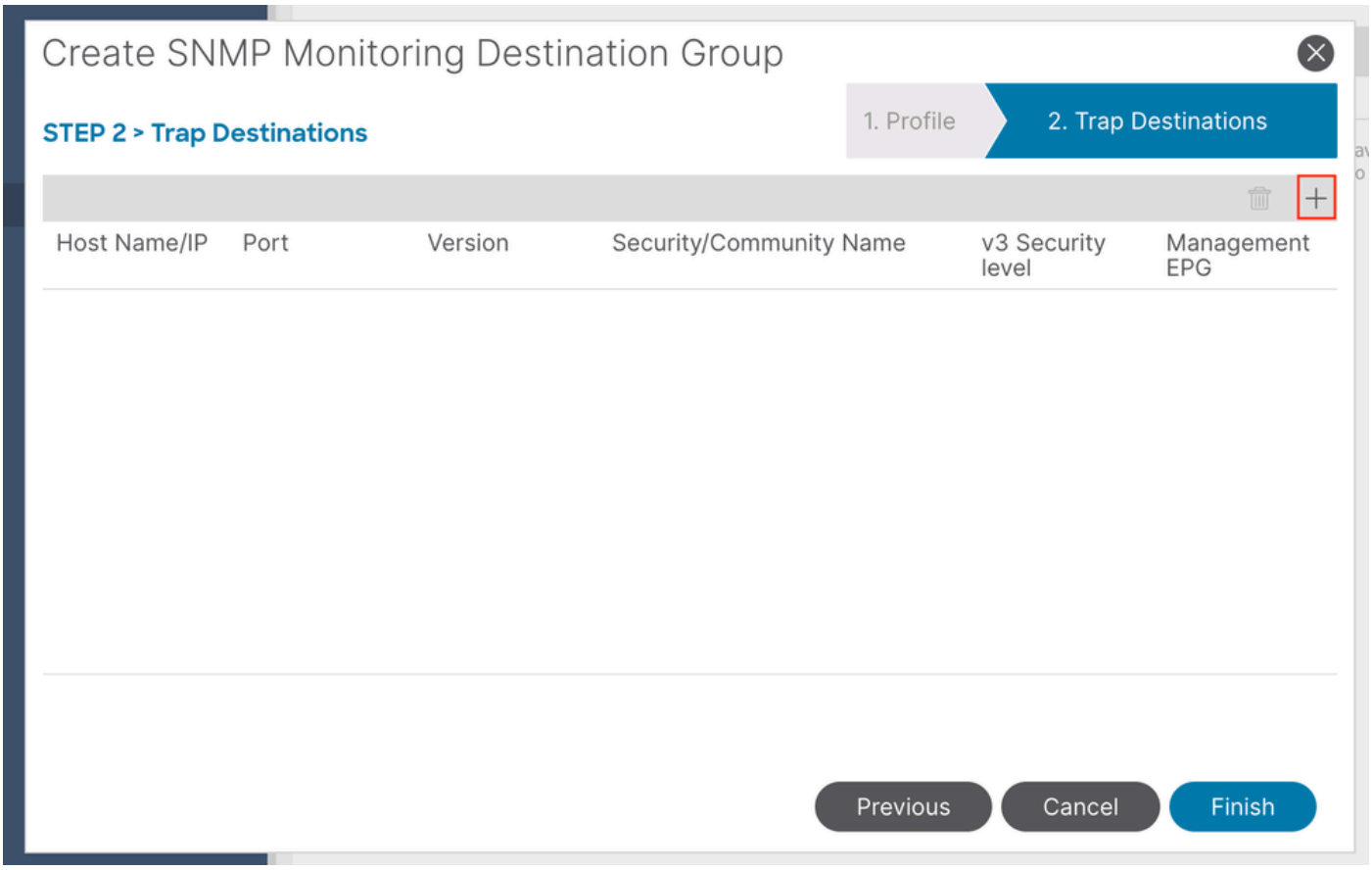
Pour configurer les déroutements SNMP dans l'ACI, vous devez effectuer les deux étapes en plus des étapes 1, 2 et 3 de la section précédente.

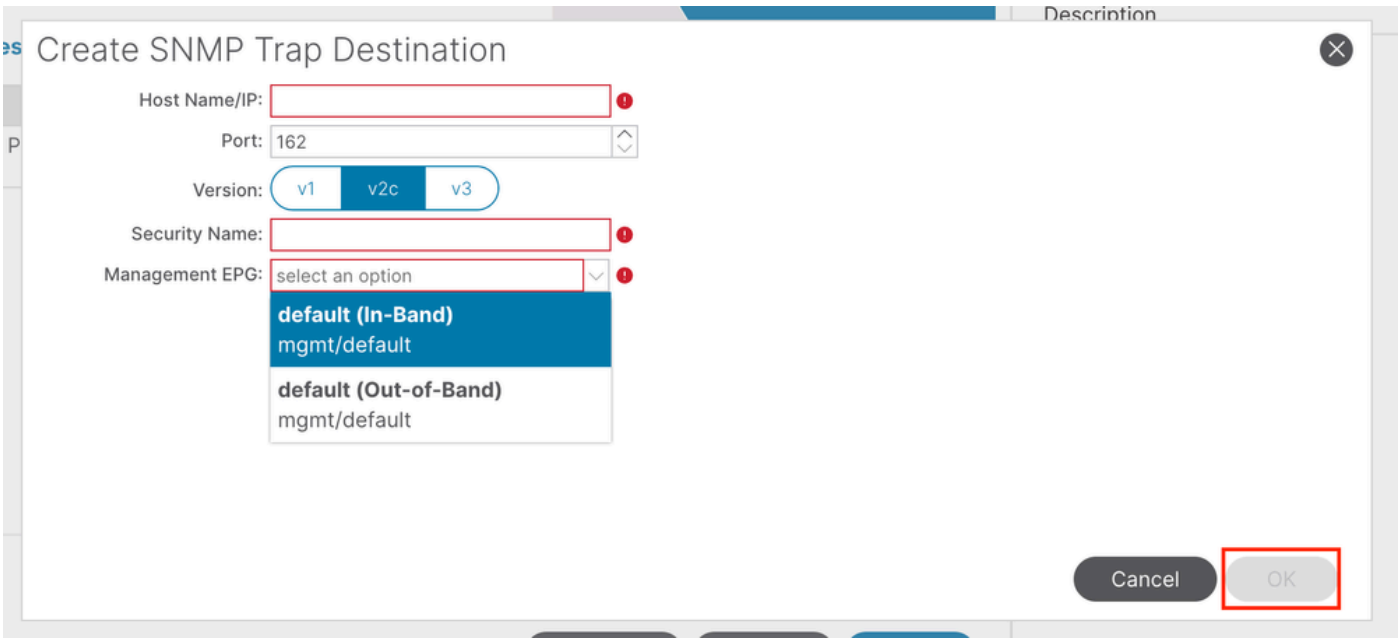
Étape 1. Configuration du serveur TRAP SNMP

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









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 ; la valeur par défaut est 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 :

- authentification

- noauth

- priv

La valeur par défaut est **noauth**.

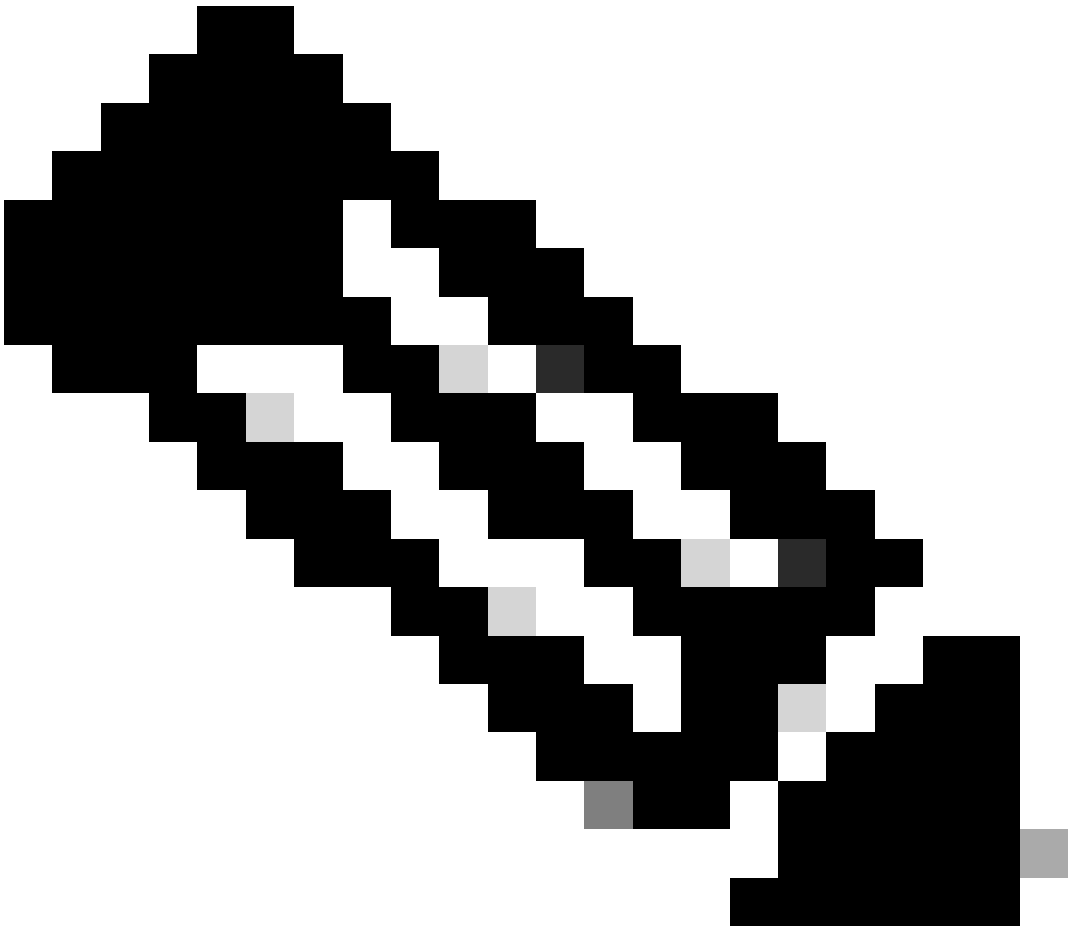
EPG de gestion : nom du groupe de terminaux de gestion pour la destination SNMP par laquelle l'hôte distant est accessible.

Étape 2. Configurez la source TRAP SNMP sous 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

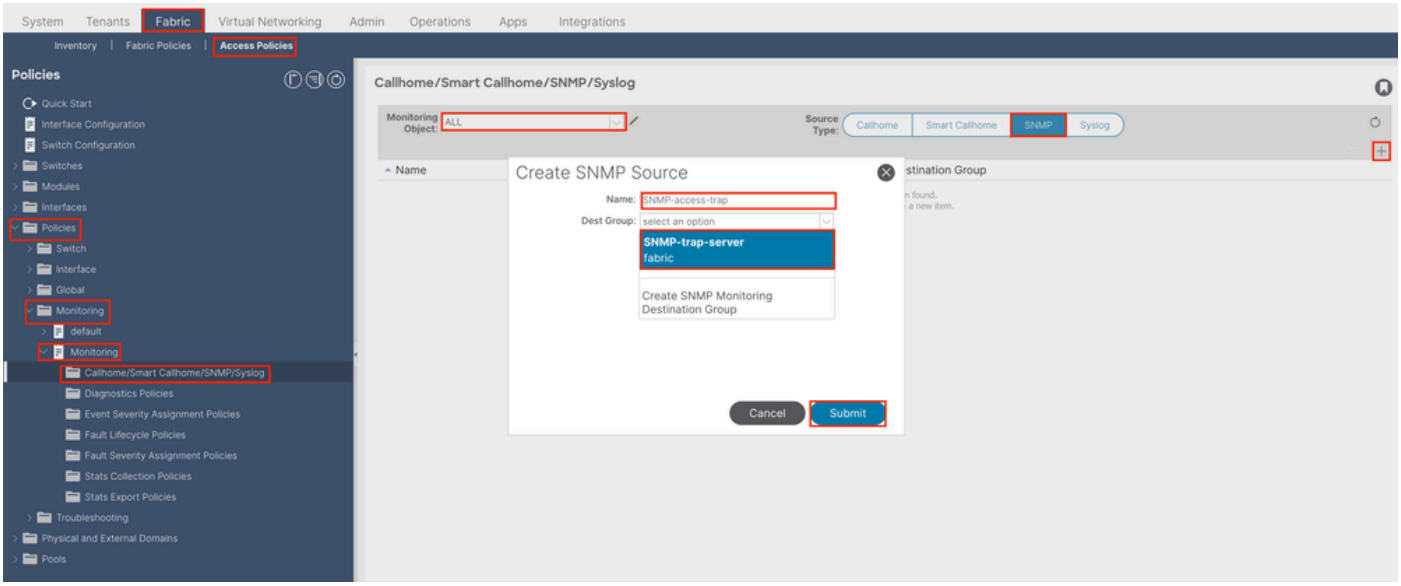


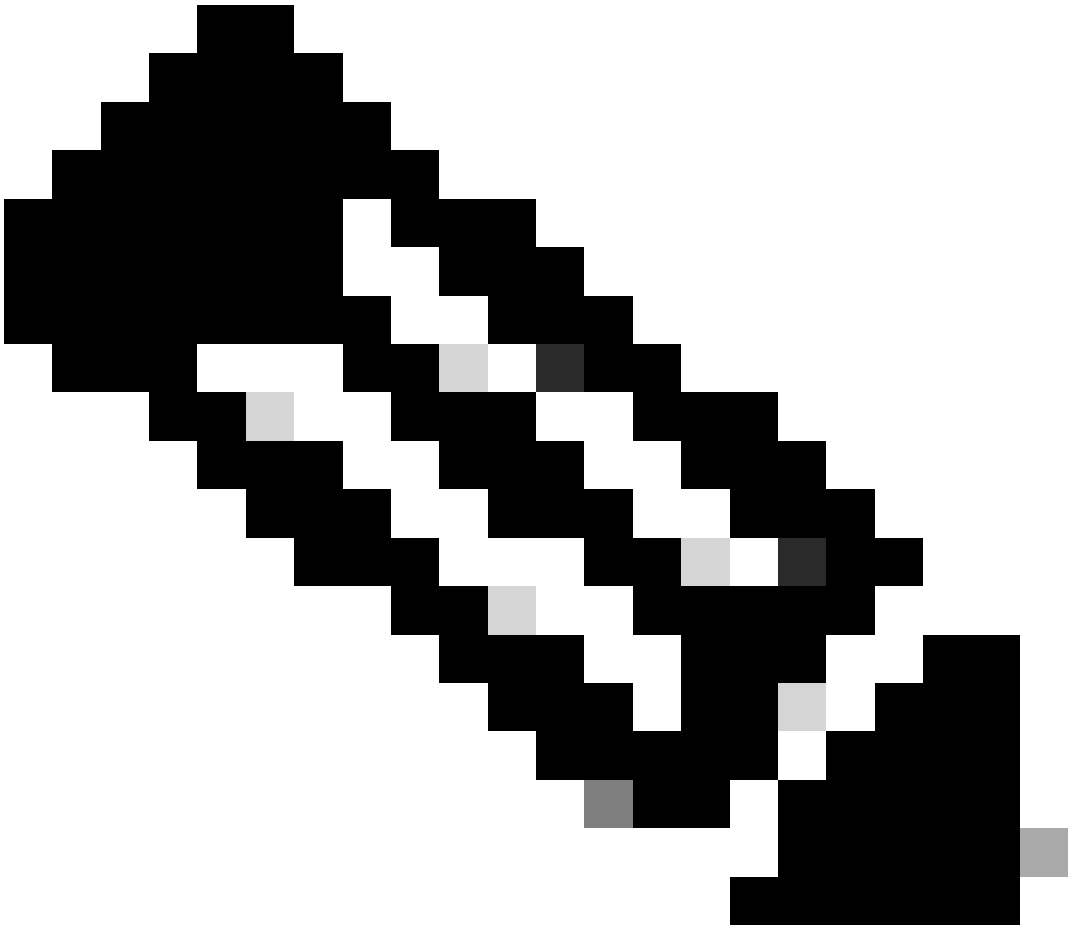
Remarque : vous pouvez choisir n'importe laquelle ou n'importe quelle combinaison d'entre elles afin de configurer en fonction de vos besoins.

Option 1. Définition de la source SNMP sous Access Policies

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

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

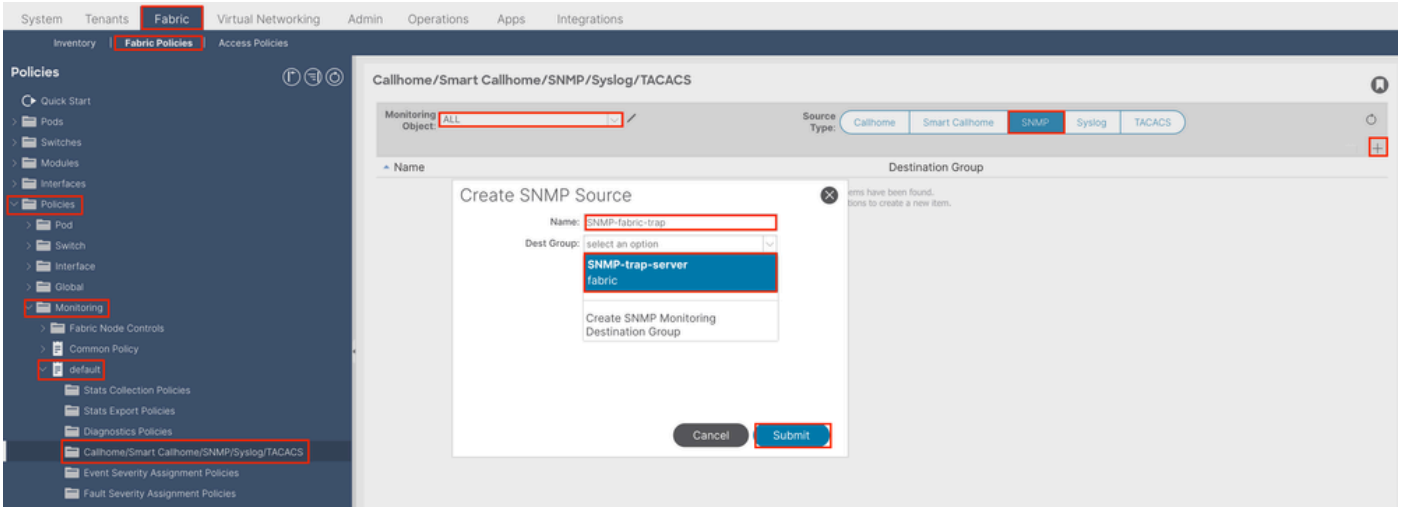

System
Tenants
Fabric
Virtual Networking
Admin
Operations
Apps
Integrations
Inventory
Fabric Policies
Access Policies
Policies
Quick Start
Interface Configuration
Switch Configuration
Switches
Modules
Interfaces
Policies
Switch
Interface
Global
Monitoring
default
Monitoring
Callhome/Smart Callhome/SNMP/Syslog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



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.

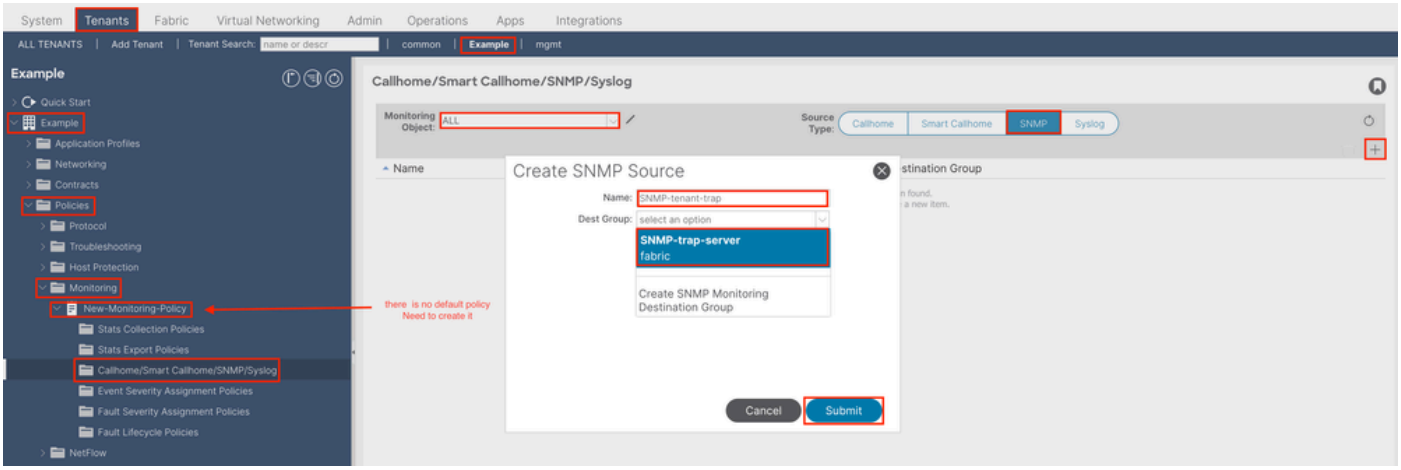
Option 2. Définition de la source SNMP sous Politiques de fabric

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



Option 3. Définition de la source SNMP sous Politiques de locataire

Pour ce faire, accédez au chemin de l'interface utilisateur graphique Web APIC ; Tenant > (Tenant Name) > Polices > 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. La commande snmpwalk permet de faire exactement

cela ; 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-n
```

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 : COMMUNITY_NAME_HERE@SNMP_CONTEXT_NAME_HERE .

Utilisation des commandes show CLI

Sur APIC :

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

Sur le commutateur :

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

Utilisation des commandes Moquery CLI

Sur APIC/commutateur :

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

Utilisation des commandes cat CLI

Sur APIC :

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

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.