Dépannage du protocole SNMP dans le fabric Cisco ACI

Introduction

Ce document décrit comment configurer, vérifier et dépanner le protocole SNMP dans l'ACI Cisco pour la version 5.x et ultérieure de l'ACI. Il couvre le modèle de politique SNMP, les contrats de gestion requis, la configuration des déroutements, la vérification opérationnelle à l'aide de requêtes d'interface de ligne de commande et d'objet géré (MO) et les workflows de dépannage structurés pour les scénarios de défaillance les plus courants sur les commutateurs Leaf/Spine et les contrôleurs APIC.

Informations générales

Le contenu de ce document est tiré de la note technique interne SNMP de l'équipe Cisco ACI Solutions Delivery Team dans ACI : Présentation, configuration, dépannage et avertissements/problèmes rédigés par Tomas de Leon, complétés par le Guide de configuration de la gestion du système Cisco APIC (version 5.x) et le Guide de référence rapide de la base de données MIB Cisco ACI.

Aperçu

Architecture SNMP dans l'ACI

SNMP (Simple Network Management Protocol) est un protocole UDP qui régit la gestion et la surveillance du réseau. Dans l'ACI, le protocole SNMP fonctionne indépendamment sur chaque entité gérée. Chaque commutateur Leaf, commutateur Spine et contrôleur APIC est son propre agent SNMP ; chacun doit être interrogé ou surveillé indépendamment.

L'ACI prend en charge les fonctionnalités SNMP suivantes :

- Opérations de lecture (Get, GetNext, BulkGet, Walk) prises en charge sur les commutateurs Leaf/Spine et les contrôleurs APIC.
- Notifications (déroutements) : déroutements SNMPv1, v2c et v3 pris en charge sur les commutateurs Leaf/Spine et les contrôleurs APIC.

- SNMPv3 — pris en charge sur les commutateurs Leaf/Spine et les contrôleurs APIC.
- Opérations d'écriture (Set) — NON prises en charge sur les périphériques ACI.
- IPv6 — SNMP est pris en charge sur IPv4 uniquement.

Remarque : Dans un cluster APIC, chaque APIC fournit des objets MIB locaux à lui-même. Vous devez interroger chaque contrôleur APIC indépendamment ; il n'y a pas d'agrégation SNMP au niveau du cluster. De même, chaque commutateur leaf et spine doit être interrogé indépendamment.

Architecture SNMPD sur le contrôleur APIC

Le contrôleur APIC exécute le processus snmpd, qui a deux composants internes :

- Agent : agent net-snmp open source (version 5.7.6 ou ultérieure) qui gère le traitement du protocole SNMP et la gestion des sessions.
- DME (Data Model Engine) : interface avec l'arborescence des informations de gestion (MIT) APIC pour lire les objets gérés (MO) et traduire les attributs MO au format d'objet SNMP. Les déroutements SNMP sont générés à partir des événements et des pannes déclenchés sur les MO.

Modèle de politique SNMP et chaîne de déploiement

L'ACI utilise un modèle basé sur des politiques pour SNMP. La configuration SNMP est abstraite en tant qu'objet géré snmpPol et doit être associée au groupe de politiques Pod du fabric avant d'être déployée sur un noeud. La chaîne de déploiement complète est la suivante :

1. SNMP Policy (`snmpPol`) : définit l'état admin, les chaînes de communauté, les politiques de groupe de clients (ACL) et les utilisateurs SNMPv3.
2. Pod Policy Group - référence la politique SNMP avec d'autres politiques au niveau des pod (BGP, ISIS, NTP, etc.).
3. Sélecteur de profil de pod — Applique le groupe de stratégies de pod aux pods de fabric.

En outre, la configuration des déroutements SNMP nécessite :

1. SNMP Monitoring Destination Group (`snmpGroup`) : définit les hôtes de destination de déroutement, le port, la version SNMP et la communauté.
2. Sources de surveillance (`snmpSrc`) — relient le groupe de destination à trois étendues de stratégie de surveillance distinctes : Fabric Default, Fabric Common Policy et Access Policy Default.

Des contrats de gestion autorisant le port UDP 161 (requêtes SNMP) et le port UDP 162 (déroutements SNMP) sont requis pour les noeuds APIC. Les noeuds Leaf et Spine nécessitent également des règles iptables correctes, qui sont automatiquement programmées lorsque les stratégies de groupe client sont configurées.

MIB prises en charge

Les bases MIB prises en charge sur le contrôleur APIC incluent :

- MIB d'entité — PhysicalTable
- MIB Cisco Entity Ext — PhysicalProcessorTable, LEDTable
- MIB de contrôle des FRU d'entité Cisco — PowerSupplyGroupTable, PowerStatusTable, FanTrayStatusTable, PhysicalTable
- MIB de capteur d'entité Cisco — SensorValueTable, SensorThresholdTable
- MIB de processus Cisco — CPUTotalTable, ProcessTable, ProcessExtRevTable, ThreadTable

Les commutateurs Leaf et Spine intègrent des MIB NX-OS standard, notamment IF-MIB, IP-MIB, CISCO-CDP-MIB, CISCO-ENTITY-QFP-MIB et la suite complète CISCO-ENTITY-FRU-CONTROL-MIB.

Les déroutements SNMP générés sur le contrôleur APIC incluent : `cefcFRUInserted`, `cefcFRURremoved`, `cefcFanTrayStatusChange`, `cefcModuleStatusChange`, `entSensorThresholdNotification`, `cefcPowerStatusChange`, `cpmCPURisingThreshold`, `cpmCPUFallingThreshold`.

Configurer SNMP dans l'ACI

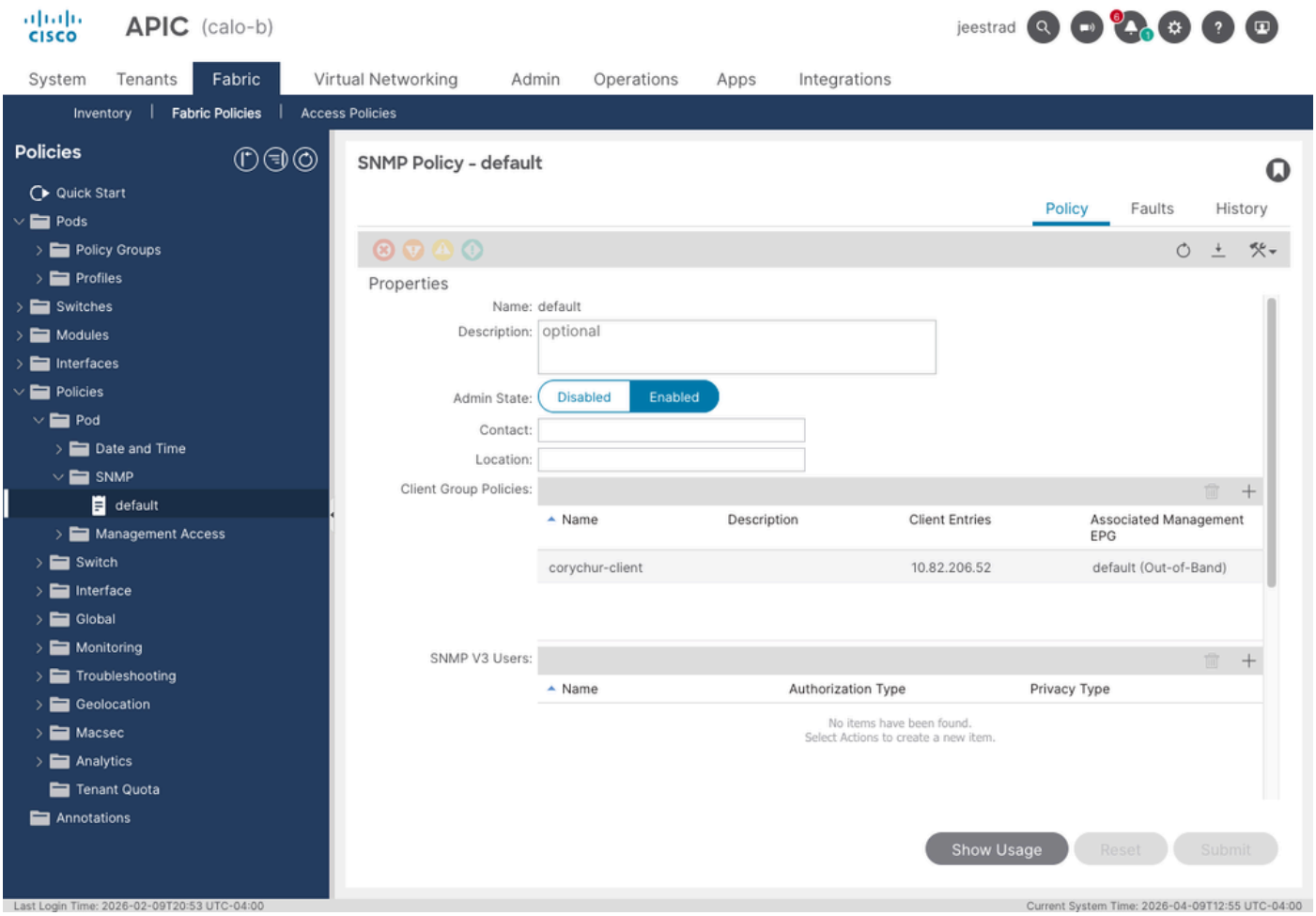
Remarque : Cette section fournit un résumé du workflow de configuration en tant que contexte pour les sections de vérification et de dépannage qui suivent. Reportez-vous au Guide de configuration de la gestion du système Cisco APIC pour des procédures de configuration complètes.

Étape 1: Configuration de la politique SNMP

Accédez à Fabric > Fabric Policies > Policies > Pod > SNMP. Sélectionnez (ou créez) la stratégie SNMP, généralement nommée default. Configurer:

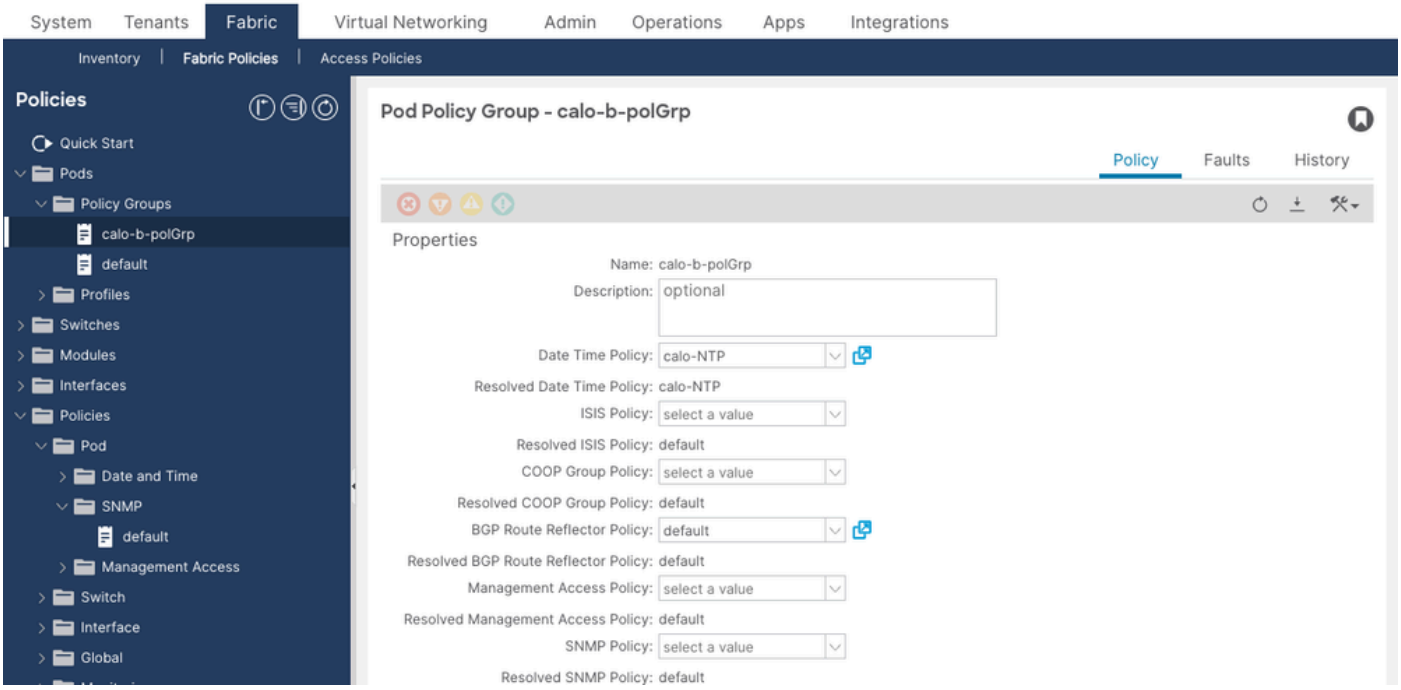
- Admin State : défini sur Enabled.

- Community Policies : ajoutez la chaîne de communauté utilisée par votre NMS.
- Stratégies de groupe de clients — Définissent un ou plusieurs profils de groupe de clients, chacun spécifiant les adresses IP de client SNMP autorisées et l'EPG de gestion associé (hors bande ou intrabande).
- SNMPv3 Users : si vous utilisez SNMPv3, ajoutez ici des utilisateurs avec des paramètres d'authentification et de confidentialité.



Étape 2: Associer la politique SNMP au groupe de politiques Pod

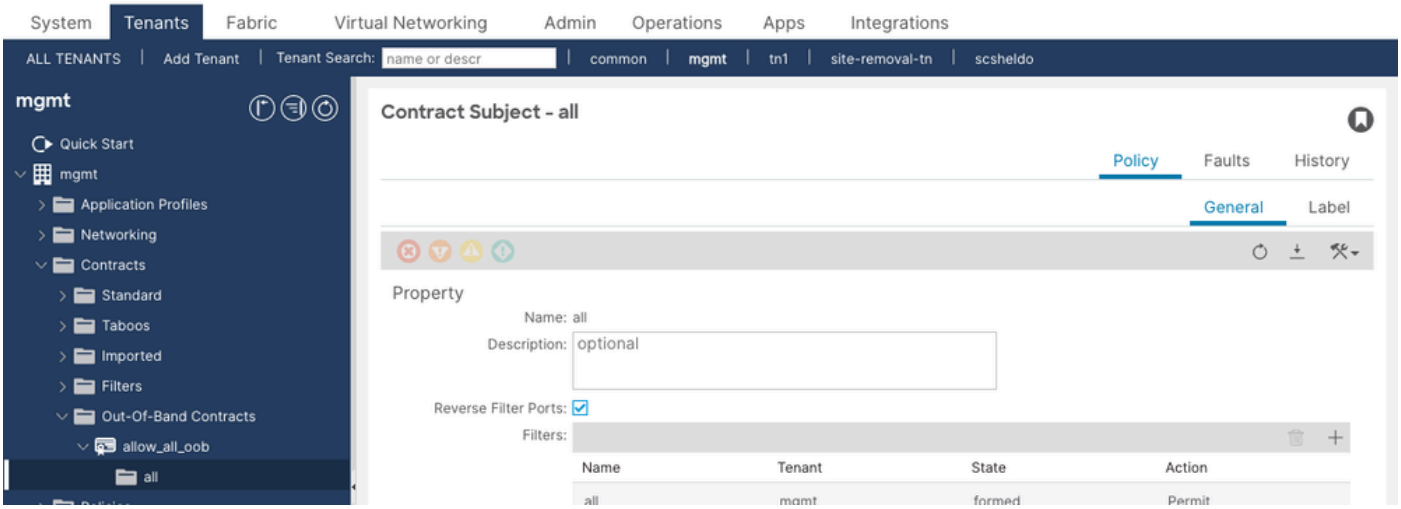
Accédez à Fabric > Fabric Policies > Pods > Policy Groups. Sélectionnez le groupe de politiques de pod actif (généralement nommé default). Définissez le champ SNMP Policy pour qu'il pointe vers la stratégie SNMP créée à l'étape 1. Vérifiez que le champ Resolved SNMP Policy affiche le nom de stratégie correct.



Accédez ensuite à Fabric > Fabric Policies > Pods > Profiles, développez le profil de pod par défaut et confirmez que le sélecteur actif référence le groupe de stratégie de pod correct.

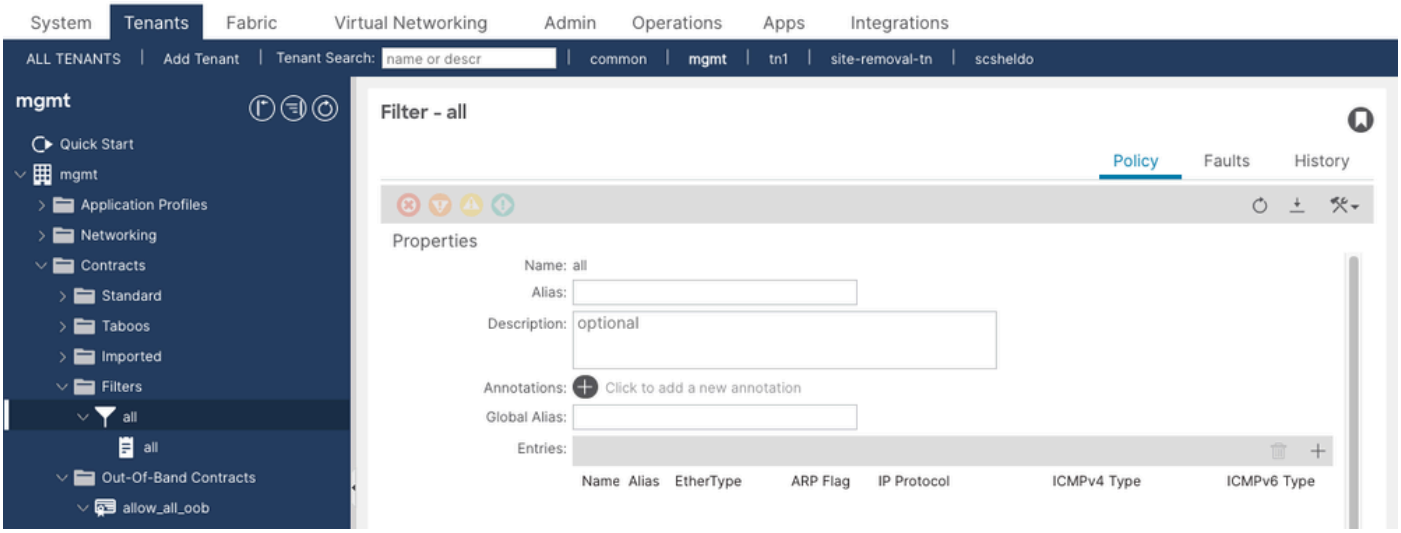
Étape 3: Configuration des contrats de gestion pour le port UDP 161

Accédez à Locants > mgmt > Contracts > Out-Of-Band Contracts. Vérifiez que l'objet du contrat OOB actif fait référence à une entrée de filtre autorisant le port UDP 161 (requêtes SNMP). Sans ce contrat sur le contrôleur APIC, tous les paquets SNMP GET/WALK seront supprimés en silence.



Les entrées de filtre associées à l'objet du contrat doivent inclure une entrée avec EtherType IP, Protocol UDP et Destination Port 161. L'exemple ci-dessus montre un filtre « allow-all » (protocole non spécifié) qui autorise le protocole SNMP mais est plus large que celui recommandé pour la

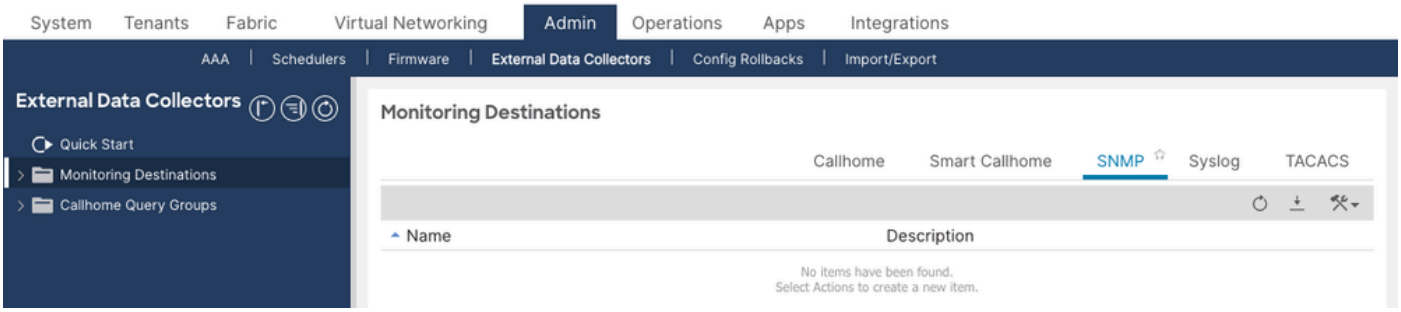
production. Une entrée de filtre SNMP dédiée avec des entrées UDP/161 et UDP/162 spécifiques est préférable.



Remarque : Dans les versions antérieures du microprogramme ACI, certains ports étaient toujours ouverts sur les noeuds Leaf et Spine et aucun contrat de gestion n'était requis pour SNMP. Dans ACI 5.x, le contrat est requis pour les noeuds APIC. Les noeuds Leaf et Spine utilisent des règles iptables dérivées des stratégies de groupe client plutôt que des contrats de gestion.

Étape 4: Configuration des destinations des déroutements SNMP

Accédez à Admin > External Data Collectors > Monitoring Destinations > SNMP. Cliquez avec le bouton droit et sélectionnez Create SNMP Monitoring Destination Group. L'onglet SNMP affiche tous les groupes de destinations configurés. Une table vide signifie qu'aucune destination de déroutement n'a encore été configurée.



Définir :

- Nom du groupe
- Destinations des déroutements : hostname/IP, port UDP (par défaut 162), version SNMP,

chaîne de communauté et EPG de gestion

Étape 5: Configurer les sources de surveillance

Les sources de surveillance relient le groupe de destinations SNMP aux politiques de surveillance qui contrôlent les événements et les défaillances générant des déroutements. Vous devez configurer une source de surveillance dans les trois emplacements suivants, sinon des déroutements de certains types de noeuds ne seront pas envoyés :

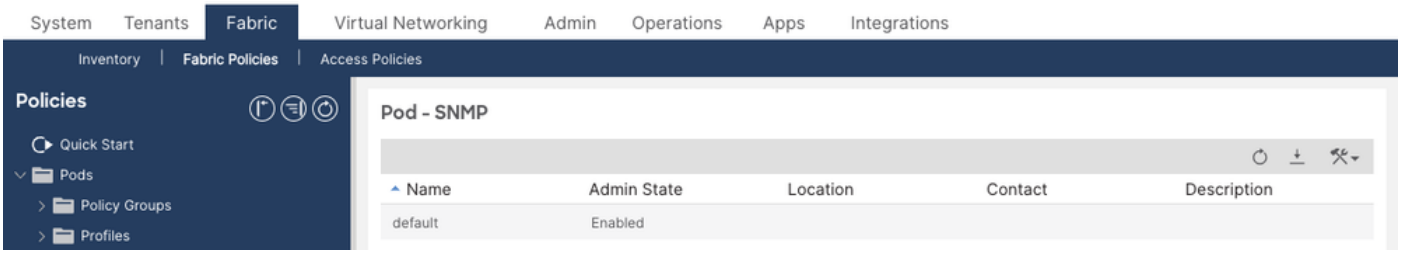
- Fabric > Politiques de fabric > Politiques > Surveillance > par défaut > Callhome/Smart Callhome/SNMP/Syslog/TACACS (couvre les événements d'infrastructure de fabric)
- Fabric > Fabric Policies > Policies > Monitoring > Common Policy > Callhome/Smart Callhome/SNMP/Syslog/TACACS (couvre les événements communs à l'échelle du fabric)
- Fabric > Access Policies > Policies > Monitoring > default > Callhome/Smart Callhome/SNMP/Syslog (couvre les événements d'accès/infrastructure)

Dans chaque emplacement, sélectionnez SNMP comme type de source et créez une nouvelle source SNMP référençant le groupe de destination créé à l'étape 4.

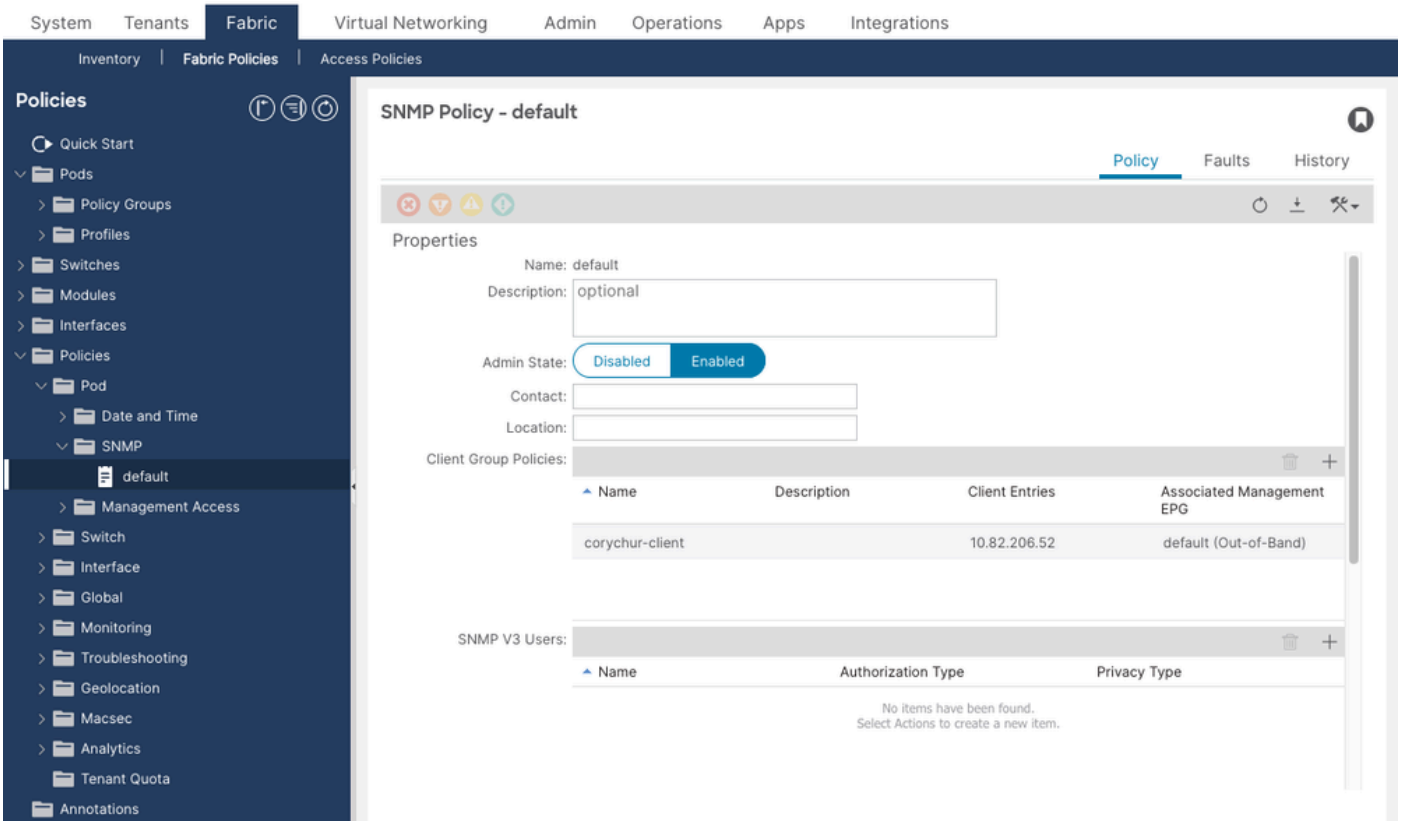
Vérifier la configuration

Vérifier le déploiement de la stratégie SNMP

Accédez à Fabric > Fabric Policies > Policies > Pod > SNMP et vérifiez que la stratégie par défaut SNMP existe et que son état Admin est défini sur Enabled. La liste Groupes de stratégies affiche toutes les stratégies SNMP configurées avec leur état d'administration en un coup d'oeil.



Pour une vérification détaillée, cliquez sur le nom de la stratégie pour l'ouvrir. Vérifiez que le bouton Admin State est défini sur Enabled, et que les stratégies de groupe client répertorient tous les hôtes NMS autorisés avec leur EPG de gestion associé.



Exécutez la requête MO suivante sur n'importe quel APIC pour confirmer que la politique SNMP est présente et activée dans le fabric :

<#root>

```
apic1#

moquery -c snmpPol

Total Objects shown: 1

# snmp.Pol
name          : default
adminSt       : enabled                    <--- must be "enabled"
contact       : NOC Team
descr         : ACI Fabric SNMP Policy
dn            : uni/fabric/snmppol-default
loc           : DC1 ACI Fabric
monPolDn      : uni/fabric/monfab-default
```

Si `adminSet` est `désactivé`, SNMP ne fonctionnera sur aucun noeud. Activez-le dans l'interface graphique APIC sous Fabric > Fabric Policies > Policies > Pod > SNMP > default.

Vérifier la configuration de la chaîne de communauté

```
<#root>

apic1#

moquery -c snmpCommunityP

Total Objects shown: 1

# snmp.CommunityP
name         : public                      <--- confirm this matches your NMS community string
dn           : uni/fabric/snmppol-default/community-public
descr        : SNMP Community String
```

Si aucune communauté n'est retournée ou si le nom ne correspond pas à ce que le NMS utilise, ajoutez ou corrigez la chaîne de communauté sous la politique SNMP.

Vérification des stratégies de groupe client (contrôle d'accès SNMP)

Les stratégies de groupe client fonctionnent comme une ACL pour l'accès SNMP GET/WALK. Chaque stratégie spécifie les adresses IP client autorisées à interroger les noeuds Leaf/Spine sur quel VRF de gestion. Sur les noeuds Leaf/Spine, ces politiques sont traduites en règles iptables.

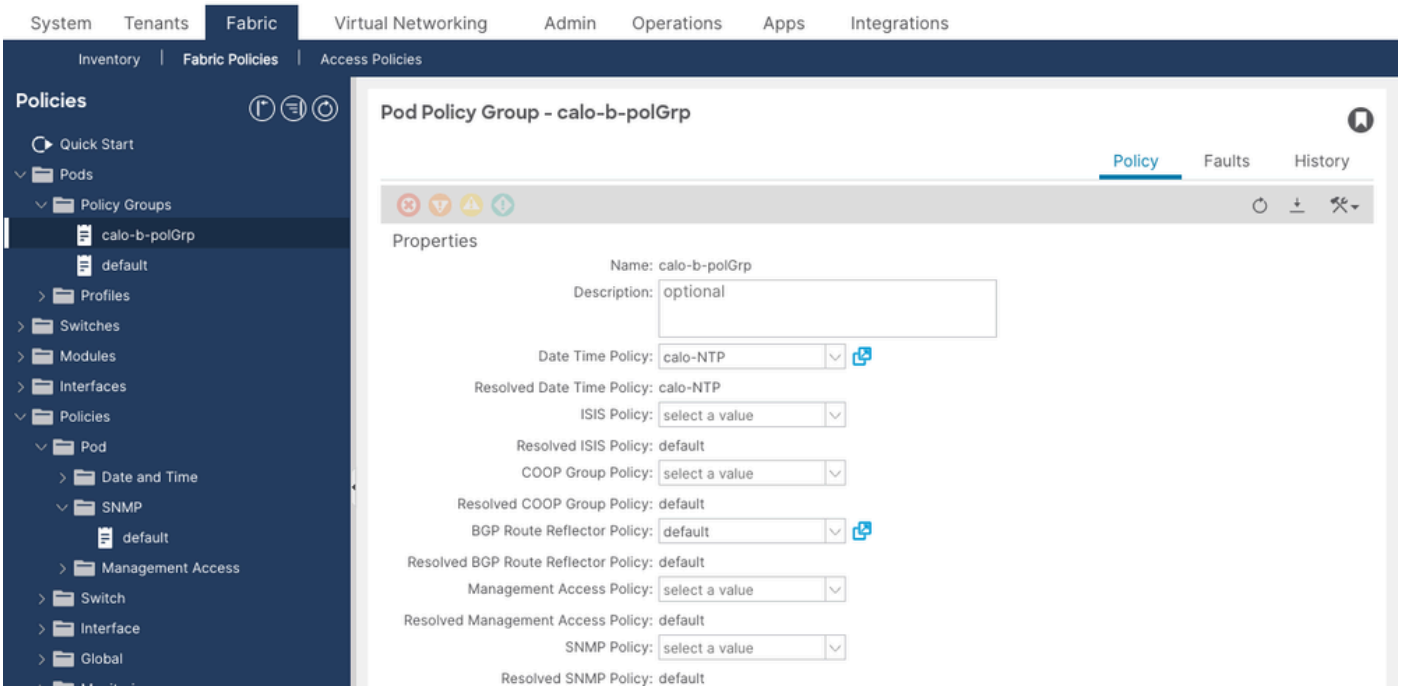
```
<#root>

apic1#

moquery -c snmpClientGrpP -x query-target=children

Total Objects shown: 3

# snmp.ClientP
addr         : 10.1.1.50                   <--- NMS server IP
dn           : uni/fabric/snmppol-default/clgrp-NMS-Clients/client-[10.1.1.50]
name         : nms-server1

# snmp.ClientP
addr         : 10.1.1.51
dn           : uni/fabric/snmppol-default/clgrp-NMS-Clients/client-[10.1.1.51]
name         : nms-server2

# snmp.ClientGrpP
name         : NMS-Clients
dn           : uni/fabric/snmppol-default/clgrp-NMS-Clients
```

Vérifiez que l'adresse IP du serveur NMS est présente dans les entrées du client. Si une adresse IP client est manquante, les requêtes SNMP GET/WALK de cet hôte seront abandonnées par iptables sur les noeuds leaf/spine.

Remarque : Avertissement SNMPv3 - Les stratégies de groupe client ne sont pas appliquées sur le contrôleur APIC lors de l'utilisation de SNMPv3. Toute requête GET/WALK SNMPv3 vers un contrôleur APIC est autorisée, quelle que soit la configuration du groupe client. L'application de groupe de clients pour SNMPv3 sur le contrôleur APIC est une limitation connue. Sur les commutateurs Leaf et Spine, l'application de groupe de clients se comporte de la même manière pour SNMPv2c et SNMPv3.

Vérification des références de groupe de politiques Pod Politique SNMP

Accédez à Fabric > Fabric Policies > Pods > Policy Groups et ouvrez le groupe de stratégie de pod actif. Vérifiez que le champ déroulant SNMP Policy est défini sur la politique SNMP souhaitée et que le champ Resolved SNMP Policy porte le même nom. Une politique manquante ou non résolue signifie que la configuration SNMP n'est jamais transmise aux commutateurs.



Dans la capture d'écran ci-dessus, le champ SNMP Policy affiche « select a value » (vide) tandis que le champ Resolved SNMP Policy affiche « default » (par défaut). Cela signifie que la stratégie est héritée de la valeur par défaut du fabric, mais n'est pas explicitement définie. Il est recommandé de définir explicitement le champ de stratégie SNMP pour éviter toute ambiguïté.

Vérifiez via l'API REST :

<#root>

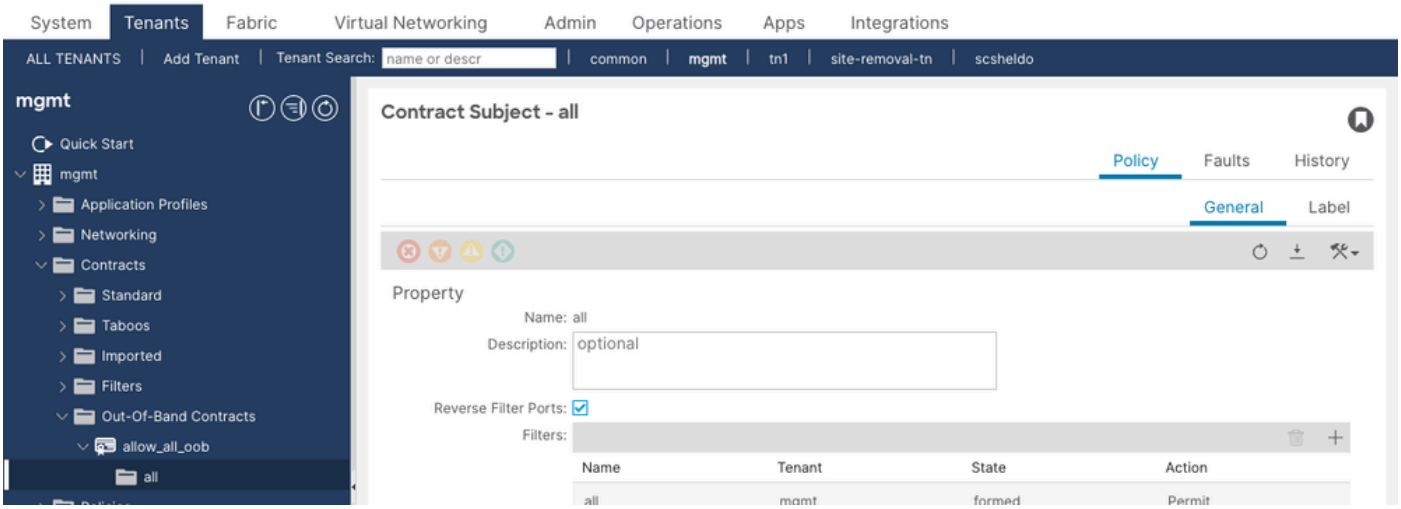
```
apic1#

moquery -c fabricPodPGrp -x rsp-subtree=full
```

```
# fabric.PodPGrp
name          : default
dn            : uni/fabric/funcprof/podpgrp-default

  # fabric.RsSnmpPol
  tnSnmpPolName : default                 <--- must reference the SNMP policy
  state         : formed                  <--- must be "formed"
```

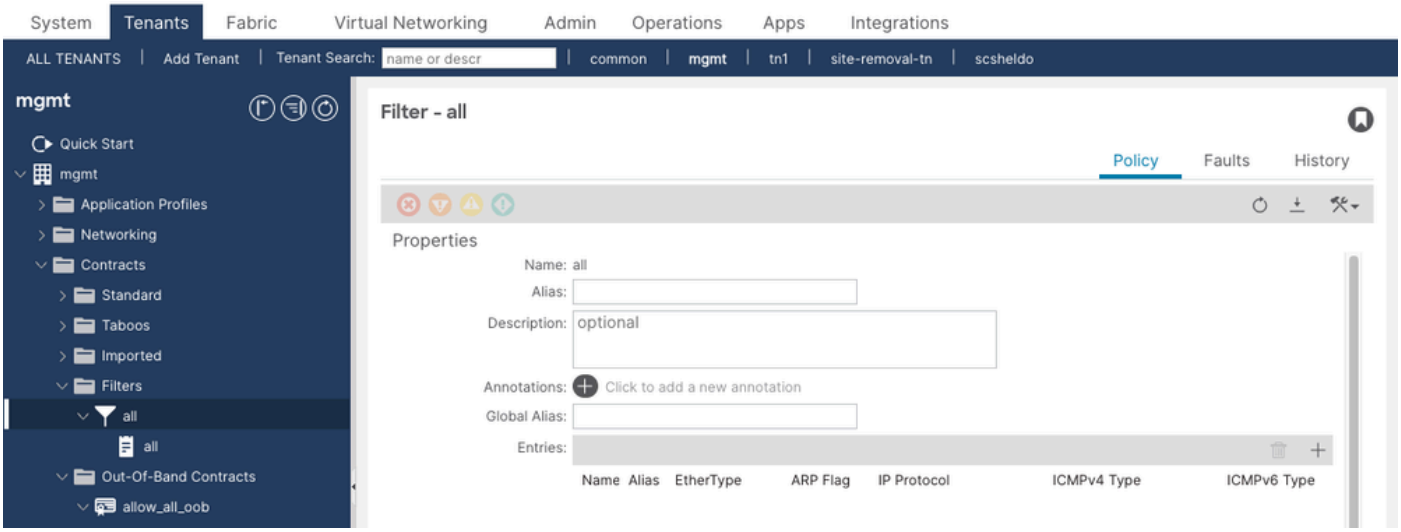
Si `l'état` n'est pas `formé`, la relation de stratégie SNMP est rompue. Sélectionnez à nouveau la stratégie SNMP dans le groupe de stratégies Pod et envoyez-la.

Vérification du contrat de gestion pour UDP 161 (noeuds APIC)

Accédez à Tenants > mgmt > Contracts > Out-Of-Band Contracts (et In-Band Contracts si vous utilisez la gestion INB). Ouvrez le contrat OOB actif et cliquez sur l'onglet Policy. Vérifiez que l'objet fait référence à un filtre qui autorise le port UDP 161.



Développez le filtre référencé par l'objet et confirmez que ses entrées incluent une entrée avec EtherType IP, Protocol UDP, Destination Port 161. Les entrées de filtre déterminent quel trafic est autorisé via le contrat de gestion OOB vers l'APIC.



Le filtre doit afficher :

- TypeEther : IP
- Protocole IP : UDP
- Port de destination - De : 161
- Port de destination vers : 161

Vérifiez également que le port UDP 162 est autorisé si vous souhaitez que le contrôleur APIC envoie des déroutements SNMP en sortie via l'interface OOB.

Vérifier via la requête MO :

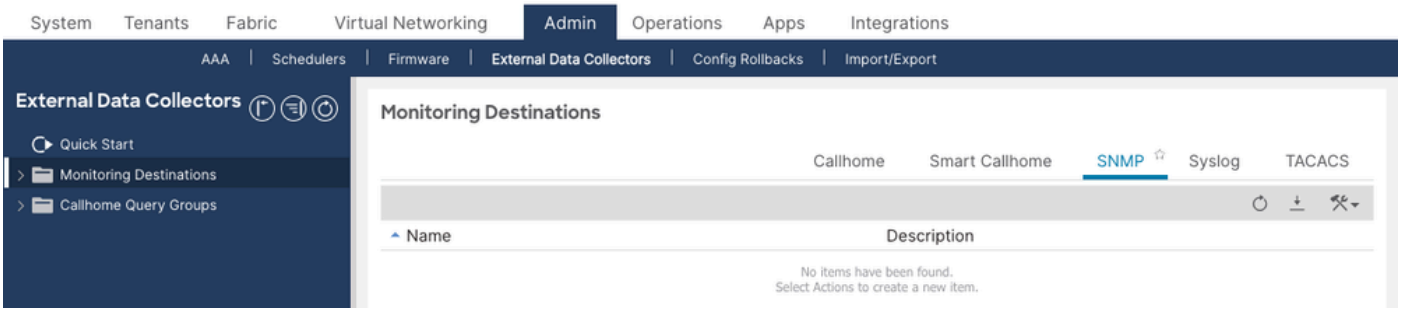
<#root>

```
apic1#

moquery -c vzEntry -x query-target-filter='and(eq(vzEntry.dFromPort,"161"),eq(vzEntry.prot,"17"))'

Total Objects shown: 2

# vz.Entry
name         : snmp-get
dn           : uni/tn-mgmt/flt-snmp-filter/e-snmp-get
dFromPort    : 161                        <--- destination port 161
dToPort      : 161
prot         : 17                         <--- UDP
stateful     : no
```

Si aucun résultat n'est renvoyé, il n'existe aucun filtre pour UDP 161. Ajoutez-en un au contrat de gestion.

Vérification de la configuration de destination des déroutements SNMP

Accédez à Admin > External Data Collectors > Monitoring Destinations > SNMP pour voir tous les groupes de destinations SNMP configurés. Une liste vide signifie qu'aucune destination de déroutement n'est configurée et qu'aucun déroutement n'est envoyé à partir d'un noeud.



<#root>

```
apic1#

moquery -c snmpTrapDest

Total Objects shown: 1

# snmp.TrapDest
host         : 10.1.1.50                  <--- NMS trap receiver IP
port         : 162                         <--- trap UDP port
ver          : v2c                         <--- SNMP version
secName      : public                      <--- community string (v2c) or username (v3)
v3SecLvl     : noauth
notifT       : traps
vrfName      : mgmt:inb                    <--- VRF used to reach the trap receiver
epgDn        : uni/tn-mgmt/mgmtp-default/inb-default
dn           : uni/fabric/snmpgroup-NMS-DestGrp/trapdest-10.1.1.50-port-162
```

Vérifiez que l'adresse IP de destination du déroutement, le port, la version, la chaîne de communauté et le VRF de gestion (`mgmt:inb` ou `management` pour OOB) correspondent à votre environnement. Le VRF doit correspondre à l'EPG de gestion attribué à la destination.

Vérifier que les sources de surveillance sont configurées dans les trois étendues

Les sources SNMP doivent exister dans les trois étendues de stratégie de surveillance. L'absence d'une source dans une étendue signifie que les déroutements d'événements associés ne seront pas transférés.

<#root>

```
apic1#

moquery -c snmpSrc | egrep "snmp.Src|name|dn|incl|minSev|monPolDn"


# snmp.Src
name          : NMS-snmpSrc
dn            : uni/fabric/monfab-default/snmpsrc-NMS-snmpSrc        <--- Fabric Default
incl          : audits,events,faults
minSev        : info
monPolDn      : uni/fabric/monfab-default

# snmp.Src
name          : NMS-snmpSrc
dn            : uni/fabric/moncommon/snmpsrc-NMS-snmpSrc              <--- Fabric Common
incl          : audits,events,faults
minSev        : info
monPolDn      : uni/fabric/moncommon

# snmp.Src
name          : NMS-snmpSrc
dn            : uni/infra/moninfra-default/snmpsrc-NMS-snmpSrc        <--- Access Default
incl          : audits,events,faults
minSev        : info
monPolDn      : uni/infra/moninfra-default
```

Si l'une des trois sources est manquante, créez la source SNMP manquante dans la politique de surveillance correspondante à l'aide de l'interface utilisateur graphique.

Vérification opérationnelle

Vérification de l'état SNMP à l'aide de show snmp summary (APIC)

Exécutez cette commande directement sur chaque contrôleur APIC pour confirmer que l'agent SNMP est en cours d'exécution et que la configuration a été appliquée :

<#root>

```
apic1#

show snmp summary


Active Policy:
default, Admin State: enabled             <--- admin state must be "enabled"

Local SNMP engineID: [Hex] 0x8000000980e2b692088976c75600000000

----------------------------------------
Community           Description
----------------------------------------
public              SNMP Community String  <--- community must be present
```

```
-------------------------------------------------------------
User                Authentication   Privacy
-------------------------------------------------------------
                                        <--- empty if using v2c only

-------------------------------------------------------------
Client-Group        Mgmt-Epg              Clients
-------------------------------------------------------------
NMS-Clients         default (In-Band)     10.1.1.50,10.1.1.51  <--- verify client IPs

-------------------------------------------------------------
Host                Port    Version   Level       SecName
-------------------------------------------------------------
10.1.1.50           162     v2c       noauth      public        <--- trap destination
```

Éléments à vérifier dans le résultat :

- L'état Admin doit être `activé`.
- La communauté doit correspondre à ce que le NMS est configuré pour utiliser.
- Client-Group doit répertorier toutes les adresses IP NMS autorisées avec un EPG de gestion correct.
- L'hôte (destination du déroutement) doit répertorier le récepteur de déroutement NMS avec le port et la version corrects.

Vérification de l'état SNMP à l'aide de show snmp summary (Leaf/Spine)

<#root>

```
leaf101#

show snmp summary

Admin State : enabled, running (pid:8192)  <--- must show "enabled, running" with a PID

Local SNMP engineID: [Hex] 80000009037C69F6105BF9

-----------------------------------------------------------------------
Community       Context         Status
-----------------------------------------------------------------------
public                          ok                                  <--- community status must be "o

-----------------------------------------------------------------------
Client          VRF             Status
-----------------------------------------------------------------------
10.1.1.50       mgmt:inb        ok                                  <--- client entry must be "ok"
10.1.1.51       mgmt:inb        ok

-------------------------------------------------------------------------------
Host            Port    Ver     Level   SecName         VRF
-------------------------------------------------------------------------------
10.1.1.50       162     v2c     noauth  public          mgmt:inb       <--- trap destination
```

Éléments à vérifier dans le résultat :

- L'état Admin doit être `activé et exécuté` avec un pid. Si elle est `désactivée`, la politique SNMP n'est pas appliquée ou la chaîne de politique pod est cassée.
- L'état de la communauté doit être `OK`. L'état d'`erreur` indique un problème de déploiement de stratégie.
- Le VRF client pour chaque hôte NMS doit correspondre au VRF de l'EPG de gestion (`mgmt:inb` pour In-Band, `management` pour OOB).
- L'hôte de déroutement doit répertorier la destination avec le contexte VRF correct.

Vérification de l'exécution du processus snmpd

Sur une feuille ou une épine :

```
<#root>

leaf101#

ps aux | grep snmp

root      5881  2.5 1907404  411444 ?    Ssl  Apr05   /isan/bin/snmpd -f -s -d udp:161 udp6:161 tcp:161

leaf101#

pidof snmpd

5881
```

Sur le contrôleur APIC :

```
<#root>

apic1#

ps aux | grep snmp

ifc   32182  1.4   0.1  641196  239716  ?   Ssl  Apr10   /mgmt//bin/snmpd.bin \
  -f -p /tmp/snmpd2.pid -a -A -LE 0-2 -c /data//snmp/snmpd.conf
```

Si aucun processus snmpd n'est trouvé sur un noeud Leaf ou Spine, SNMP n'est pas exécuté sur ce noeud. Vérifiez que l'état Admin de la stratégie SNMP est activé et que la chaîne de stratégies pod est correctement configurée.

Déflecteur (Surligner pour lire)

Vérification de l'écoute du port SNMP

<#root>

```
leaf101#
```

netstat -lutn | grep 161

```
Active Internet connections (only servers)
Proto  Recv-Q  Send-Q  Local Address    Foreign Address  State
tcp         0       0  0.0.0.0:161      0.0.0.0:*        LISTEN   <--- SNMP agent is accepting requests
udp         0       0  0.0.0.0:161      0.0.0.0:*
udp6        0       0  :::161           :::*
```

Si le port 161 n'est pas répertorié dans l'état LISTEN, le processus snmpd n'est pas en cours d'exécution ou n'a pas pu se lier au port.

Vérification des règles iptables sur Leaf/Spine

Les stratégies de groupe client sont traduites en règles iptables sur chaque noeud leaf et spine. Pour vérifier les règles, procédez comme suit :

<#root>

```
leaf101#
```

iptables -S | grep -i snmp

```
-N snmp_rules
-N vrf_2_snmp_rules
-N vrf_9_snmp_rules
-A INPUT -p udp -m udp --dport 161 -j snmp_rules    <--- SNMP port 161 redirects to snmp_rules chain
-A snmp_rules -m vrf --vrf 2 -j vrf_2_snmp_rules    <--- VRF 2 = OOB management
-A snmp_rules -m vrf --vrf 9 -j vrf_9_snmp_rules    <--- VRF 9 = In-Band management
-A snmp_rules -j DROP                                <--- default drop; only permitted clients pass
-A vrf_2_snmp_rules -s 10.1.1.50/32 -j ACCEPT       <--- permitted NMS client (OOB VRF)
-A vrf_9_snmp_rules -s 10.1.1.50/32 -j ACCEPT       <--- permitted NMS client (INB VRF)
```

Pour identifier les ID VRF corrects pour votre fabric, exécutez :

<#root>

```
leaf101#
```

show vrf

```
VRF-Name                VRF-ID  State   Reason
management              2       Up      --
mgmt:inb                9       Up      --
```

Les ID VRF dans les règles iptables doivent correspondre à ce que `show vrf` rapports. Si une adresse IP de client est absente des règles iptables, les requêtes SNMP de cet hôte seront silencieusement abandonnées même si le processus snmpd est en cours d'exécution.

Utilisez des compteurs pour vérifier si un paquet SNMP a été mis en correspondance ou abandonné :

<#root>

```
leaf101#

iptables -nvL | grep -A 20 "Chain snmp_rules"

Chain snmp_rules (1 references)
 pkts bytes target         prot opt in     out    source       destination
    1    73 vrf_9_snmp_rules all -- *      *      0.0.0.0/0    0.0.0.0/0    vrf 9
    0     0 DROP             all -- *      *      0.0.0.0/0    0.0.0.0/0    <--- if pkts>0 here, client
```

Remarque : Si SNMP est en cours d'exécution mais que iptables ne montre aucune chaîne snmp_rules, ou que les chaînes sont vides, vous pouvez redémarrer le processus snmpd pour forcer la reprogrammation de la règle iptables. L'envoi de SIGKILL au PID snmpd est sécurisé : le gestionnaire de processus ACI (`réglementé`) le redémarre automatiquement. Exécutez `pidof snmpd` pour obtenir le PID, puis `kill -9 [snmpd_pid]`. Confirmez le nouveau PID avec `pidof snmpd` après 10-15 secondes.

Vérifiez que le port SNMP écoute leaf101# netstat -lutn | grep 161 Connexions Internet actives (serveurs uniquement) Proto Recv-Q Send-Q Local Address Foreign Address State tcp 0 0 0.0.0.0:161 0.0.0.0:* LISTEN <— L'agent SNMP accepte les requêtes udp 0 0 0.0.0.0:161 0.0.0.0:* udp6 0 0 :::161 ::* Si le port 161 n'est pas répertorié dans l'état LISTEN, le processus snmpd n'est pas en cours d'exécution ou n'a pas pu se lier au port. Vérifiez que les règles iptables sur les stratégies de groupe client Leaf/Spine sont traduites en règles iptables sur chaque leaf et spine. Pour vérifier les règles, procédez comme suit : leaf101# iptables -S | grep -i snmp -N snmp_rules -N vrf_2_snmp_rules -N vrf_9_snmp_rules -A INPUT -p udp -m udp —dport 161 -j snmp_rules <— Le port SNMP 161 redirige vers la chaîne snmp_rules -A snmp_rules -m vrf —vrf 2 -j vrf_2_snmp_rules <— VRF 2 = OOB management -A snmp_rules -m vrf —vrf 9 -j vrf_9_snmp_rules <— VRF 9 = In-Band management -A snmp_rules -j DROP <— default drop ; Seuls les clients autorisés réussissent -A vrf_2_snmp_rules -s 10.1.1.50/32 -j ACCEPT <— allowed NMS client (OOB VRF) -A vrf_9_snmp_rules -s 10.1.1.50/32 -j ACCEPT <— allowed NMS client (INB VRF) Pour identifier les ID VRF corrects pour votre fabric, exécutez la commande suivante : leaf101# show vrf VRF-Name VRF-ID State Reason management 2 Up — mgmt : inb 9 Up — Les ID VRF dans les règles iptables doivent correspondre à ce qui est indiqué dans les rapports show vrf. Si une adresse IP de client est absente des règles iptables, les requêtes SNMP de cet hôte seront silencieusement abandonnées même si le processus snmpd est en cours d'exécution. Utilisez des compteurs pour vérifier si un paquet SNMP a été mis en correspondance ou abandonné : leaf101# iptables -nvL | grep -A 20 "Chain snmp_rules" Chain snmp_rules (1 references) pkts bytes target port opt in out source destination 1 73 vrf_9_snmp_rules all — * * 0.0.0.0/0 0.0.0.0/0 vrf 9 0 0 DROP all — * 0.0.0.0/0 0.0.0.0/0 <— if pkts>0 ici, les adresses IP client sont manquantes Remarque : Si SNMP est en cours d'exécution mais que iptables ne

montre aucune chaîne snmp_rules, ou que les chaînes sont vides, vous pouvez redémarrer le processus snmpd pour forcer la reprogrammation de la règle iptables. L'envoi de SIGKILL au PID snmpd est sécurisé : le gestionnaire de processus ACI (réglementé) le redémarre automatiquement. Exécutez pidof snmpd pour obtenir le PID, puis tuez -9 [snmpd_pid]. Confirmez le nouveau PID avec pidof snmpd après 10 à 15 secondes.

Vérification de la connectivité réseau aux ports SNMP

<#root>

```
leaf101#

netstat -ai | grep eth0

Iface  MTU  Met  RX-OK  RX-ERR  RX-DRP  RX-OVR  TX-OK  TX-ERR  TX-DRP  TX-OVR  Flg
eth0   1500   0  501277      0       0       0  633546      0       0       0  BMRU

leaf101#

netstat -ai | grep kpm_inb

Iface     MTU  Met    RX-OK  RX-ERR  RX-DRP  RX-OVR    TX-OK  TX-ERR  TX-DRP  TX-OVR  Flg
kpm_inb  9300   0  10361421     0       0       0   8958506      0     126       0  BMRU
```

Vérifiez que les interfaces de gestion sont actives (pas d'incréments RX-ERR) et que le trafic est acheminé. `eth0` est l'interface de gestion OOB ; `kpm_inb` est l'interface de gestion intrabande du commutateur.

Vérification de l'envoi de traps SNMP avec tcpdump

Pour confirmer que des déroutements sont générés et envoyés à partir d'un noeud leaf ou spine, capturez le trafic sur l'interface appropriée. Accédez au noeud en tant qu'administrateur et utilisez :

<#root>

```
leaf101#

tcpdump -i kpm_inb -f port 162 -vv

tcpdump: listening on kpm_inb, link-type EN10MB (Ethernet), capture size 65535 bytes
17:21:49.810052 IP (tos 0x0, ttl 64, id 63116, proto UDP, length 218)
    172.18.242.14.35582 > 10.1.1.50.snmp-trap: { SNMPv2c C=public
    { V2Trap(171) R=253 system.sysUpTime.0=5888267
      S:1.1.4.1.0=E:cisco.9.276.0.1
      interfaces.ifTable.ifEntry.ifIndex.436224000=436224000
      interfaces.ifTable.ifEntry.ifOperStatus.436224000=2 }}        <--- verify trap is being sent to N
```

Pour OOB :

<#root>

```
leaf101#

tcpdump -i eth0 -f port 162 -vv
```

Déflecteur (Surligner pour lire)

Pour les déroutements APIC (INB) :

<#root>

```
apic1#

tcpdump -i bond0.1100 -f port 162

20:01:08.453473 IP apic1-inb.cisco.com.59417 > 10.1.1.50.snmptrap: C=public V2Trap(85) S:
1.1.4.1.0=E:cisco.9.117.2.0.2 E:cisco.9.117.1.1.2.1.1.10548=1 E:cisco.9.117.1.1.2.1.2.10548=2
```

Remarque : Sur l'APIC, `bond0.1100` est la sous-interface VLAN de l'interface de gestion intrabande. Remplacez `1100` par le boîtier VLAN configuré pour votre EPG de gestion intrabande. Utilisez `oobmgmt` comme nom d'interface pour les captures OB sur le contrôleur APIC.

Pour les déroutements APIC (INB) : apic1# tcpdump -i bond0.1100 -f port 162 20:01:08.453473 IP apic1-inb.cisco.com.59417 > 10.1.1.50.snmptrap : C=public V2Trap(85) S : 1.1.4.1.0=E : cisco.9.117.2.0.2 E : cisco.9.117.1.1.2.1.1.10548=1 E : cisco.9.117.1.1.2.1.2.10548=2 Remarque : Sur le contrôleur APIC, bond0.1100 est la sous-interface VLAN de l'interface de gestion intrabande. Remplacez 1100 par le boîtier VLAN configuré pour votre EPG de gestion intrabande. Utilisez oobmgmt comme nom d'interface pour les captures OB sur le contrôleur APIC.

Vérifier les requêtes SNMP GET/WALK avec tcpdump

<#root>

```
leaf101#

tcpdump -i kpm_inb -f port 161 -vv

17:26:08.548149 IP 10.1.1.50.64245 > leaf101.cisco.com.snmp: { SNMPv2c C=public
  { GetRequest(28) R=949769396 system.sysDescr.0 }}              <--- GET request received
17:26:08.552290 IP leaf101.cisco.com.snmp > 10.1.1.50.64245: { SNMPv2c C=public
  { GetResponse(191) R=949769396
    system.sysDescr.0="Cisco NX-OS(tm) aci, Software (aci-n9000-system), \
```

```
Version 15.0(1k), RELEASE SOFTWARE" }}                    <--- response returned; SNMP working
```

Si GetRequest s'affiche mais qu'aucune GetResponse ne s'affiche, la demande est en cours de réception mais n'a pas reçu de réponse. Vérifiez le processus snmpd et la chaîne de communauté. Si vous ne voyez ni requête ni réponse, la requête est bloquée avant d'atteindre le noeud (vérifiez le routage et les tables IP).

Workflow de dépannage

Arbre de décision de triage

Utilisez cet arbre de décision lorsque les ingénieurs signalent que le protocole SNMP ne fonctionne pas. Commencez par le symptôme observé et suivez les branches jusqu'à l'isolement.

Symptôme : Aucune réponse aux requêtes SNMP GET/WALK

1. Vérifiez l'état d'administration SNMP sur APIC. Exécutez `moquery -c snmpPol`. Si `adminSet` est `désactivé`, activez-le et passez à l'étape 7.
2. Vérifiez le processus snmpd. Sur le noeud affecté, exécutez `ps aux | grep snmp` ou `pidof snmpd`. Si aucun processus n'est en cours d'exécution, la stratégie SNMP n'est pas déployée. Vérifiez la chaîne de stratégie pod (SNMP Policy → Pod Policy Group → Pod Profile).
3. Vérifiez que le port 161 écoute. Exécutez `netstat -lutn | grep 161`. Si le port 161 n'est pas à l'état LISTEN, le processus snmpd a échoué ; collectez les journaux à partir de `/var/log/dme/log/svc_ifc_dbgrelem.log*` et redémarrez le processus.
4. Vérifiez le routage. Exécutez `show ip route vrf management` et `show ip route vrf mgmt:inb`. Vérifiez qu'une route vers l'hôte NMS existe dans le VRF correct.
5. Vérifiez le contrat de gestion sur APIC. Si la cible est un APIC (et non un leaf/spine), vérifiez que le protocole UDP 161 est autorisé dans le contrat de gestion OOB ou INB.
6. Exécutez tcpdump sur le noeud. Exécutez `tcpdump -i kpm_inb -f port 161 -vv` (ou `eth0` pour OOB). Si GetRequest apparaît mais qu'aucune GetResponse ne suit, la demande atteint le noeud mais que snmpd ne répond pas — vérifiez la chaîne de communauté. Si aucune demande n'apparaît, le problème est en amont (routage ou contrat).
7. Test à partir d'un client autorisé. Exécutez `snmpget -v2c -c [community] [node-ip] SNMPv2-MIB::sysDescr.0` à partir d'un hôte NMS répertorié dans le groupe de clients. Une réponse positive confirme que le protocole SNMP est entièrement opérationnel.

Symptôme : Aucune interruption SNMP reçue au NMS

1. Vérifiez la configuration de la destination du déroutement. Exécutez `moquery -c snmpTrapDest`.

Vérifiez que l'adresse IP, le port, la version et la communauté du NMS correspondent aux valeurs attendues.
2. Vérifiez que les sources de surveillance existent dans les trois étendues. Exécutez `moquery -c snmpSrc | egrep "snmp.Src|name|dn"`. Confirmez que des entrées existent avec des valeurs `monPolDn` pour `uni/fabric/monfab-default`, `uni/fabric/moncommon` et `uni/infra/moninfra-default`. S'il en manque, ajoutez la source SNMP dans la stratégie de surveillance correspondante.
3. Vérifiez le processus snmpd. Vérifiez que snmpd est en cours d'exécution sur le noeud qui doit envoyer le déroutement.
4. Générez un événement de test et effectuez une capture avec tcpdump. Effleurez une interface ou modifiez un état pour générer un événement. Sur le noeud, exécutez `tcpdump -i kpm_inb -f port 162 -vv`. Si aucun trafic de déroutement n'apparaît sur le fil, l'événement ne génère pas de déroutement : vérifiez à nouveau l'attribut `incl de la` source de surveillance (doit inclure les `pannes` ou les `événements`).
5. Vérifiez la connectivité au récepteur de déroutement. Vérifiez que le récepteur de déroutement est accessible depuis le VRF de gestion : `show ip route vrf mgmt:inb` doit indiquer un chemin vers l'hôte NMS.
6. Si des déroutements apparaissent sur tcpdump mais pas sur le NMS, le problème est côté réseau : pare-feu, routage ou configuration NMS. Vérifiez que le NMS écoute le protocole UDP 162 à partir de l'adresse IP source de gestion du noeud ACI.

Scénarios courants

Scénario 1 : Stratégie SNMP activée mais aucune donnée retournée par Leaf/Spine

Problème : La politique SNMP sur le contrôleur APIC indique l'état Admin activé. Le NMS peut atteindre l'IP de gestion du leaf. `snmpget` expire sans réponse.

Vérification de la configuration : Vérifiez que le groupe de politiques Pod fait référence à la politique SNMP et que la politique SNMP résolue affiche le nom correct. Si le champ de stratégie SNMP du groupe de politiques de pod est vide ou si la relation n'est pas formée, le processus snmpd peut ne pas démarrer sur les commutateurs.

Contrôle opérationnel : Envoyez SSH à la feuille affectée et exécutez `show snmp summary`. Si le résultat affiche `Admin State : désactivé` même si le contrôleur APIC est activé, la stratégie n'a pas été déployée. Recherchez dans la chaîne de stratégie pod un groupe de stratégie pod manquant ou incorrectement référencé.

Cause première : La stratégie SNMP n'est pas liée au groupe de stratégies Pod ou le sélecteur de profil Pod n'applique pas le groupe de stratégies Pod correct à ce pod.

Solution :

1. Accédez à Fabric > Fabric Policies > Pods > Policy Groups > default.
2. Confirmez que le champ SNMP Policy pointe vers la politique SNMP activée.
3. Accédez à Fabric > Fabric Policies > Pods > Profiles et confirmez que le sélecteur actif référence ce groupe de stratégies de pod.
4. Après l'enregistrement, revérifiez `show snmp summary` sur le leaf dans les 2 minutes.

Scénario 2 : SNMP GET/WALK fonctionne pour certains hôtes NMS mais pas pour d'autres

Problème : Un serveur NMS peut interroger les noeuds ACI avec succès. Un deuxième serveur NMS sur un sous-réseau différent n'obtient aucune réponse.

Vérification de la configuration : Exécutez `moquery -c snmpClientGrpP -x query-target=children` sur l'APIC. Vérifiez que l'adresse IP du deuxième serveur NMS est répertoriée en tant qu'entrée client. Si elle est manquante, cette adresse IP sera bloquée par la règle DROP iptables au bas de la chaîne snmp_rules.

Contrôle opérationnel : sur le leaf concerné, vérifiez que le protocole UDP 161 est autorisé dans le contrat de gestion OOB ou INB. Si aucun contrat ou filtre n'a de ports SNMP, la requête est abandonnée.

Cause première : La deuxième adresse IP du serveur NMS ne figure pas dans la stratégie de groupe du client.

Solution : Ajoutez l'adresse IP NMS manquante en tant qu'entrée client dans la stratégie de groupe de clients SNMP sous Fabric > Fabric Policies > Policies > Pod > SNMP > default > Client Group Policies. Les règles iptables sur tous les noeuds seront mises à jour dans les minutes qui suivent l'enregistrement de la stratégie.

Scénario 3 : Déroutements SNMP non reçus — Déroutements générés mais non remis

Problème : Les défaillances sont visibles dans la table des défaillances du contrôleur APIC. `moquery -c snmpTrapDest` affiche l'adresse IP NMS correcte. Le NMS ne reçoit aucun piège.

Vérification de la configuration : Exécutez `moquery -c snmpSrc | egrep "snmp.Src|name|dn"`. Vérifiez que les sources de surveillance existent dans les trois étendues (`monfab-default`, `moncommon`, `moninfra-default`). Une surveillance courante consiste à configurer la source uniquement dans la stratégie Fabric Default, qui ne prend pas en compte les événements de stratégie d'accès.

Contrôle opérationnel : Déclenchez un événement de test (par exemple, basculez une interface dans l'état admin-down). Sur le noeud approprié, exécutez `tcpdump -i kpm_inb -f port 162`. Si des paquets déroutés apparaissent à l'interface du noeud, le côté ACI fonctionne et le problème se situe sur le chemin réseau vers le NMS (pare-feu, routage). Si aucun déroutement n'apparaît sur le fil, la source de surveillance ACI est manquante ou le type d'événement n'est pas inclus dans l'attribut `incl` de la source.

Cause première : Une ou plusieurs sources de surveillance sont absentes des étendues requises.

Cause première 2 : L'attribut `incl` source de surveillance exclut le type d'événement en cours de génération (par exemple, `incl : les événements` sans `défaillance` signifient que les déroutements basés sur des pannes ne seront pas envoyés).

Solution :

1. Ajoutez les sources de surveillance manquantes dans l'interface utilisateur graphique pour chacune des trois étendues (Fabric Default, Fabric Common, Access Default). Définissez le groupe de destinations sur votre groupe de destinations SNMP configuré.
2. Vérifiez que l'attribut `incl` inclut les `audits, les événements et les pannes` pour une couverture complète des déroutements.
3. Après les modifications, relancez l'événement de test et revérifiez tcpdump.

Déflecteur (Surligner pour lire)

Remarque : Sur le contrôleur APIC, la `commande tcpdump/code> n'est disponible que pour l'utilisateur racine. Pour APIC et les commutateurs, la commande iptables est uniquement disponible pour l'utilisateur racine.`

Scénario 4 : Application de groupe de clients SNMPv3 ne fonctionnant pas sur APIC

Problème : Un client SNMP qui n'est PAS dans la stratégie de groupe du client peut interroger le contrôleur APIC à l'aide de SNMPv3, même si la même requête échoue à partir des noeuds leaf/spine.

Cause première : C'est une **mise en garde connue**. Les stratégies de groupe client (application d'IP source basée sur iptables) ne sont pas appliquées pour les GET/Walks SNMPv3 vers les contrôleurs APIC. Tout hôte peut interroger le contrôleur APIC via SNMPv3, quelle que soit la configuration du groupe de clients. Sur les commutateurs Leaf et Spine, l'application de groupe de clients fonctionne de manière identique pour SNMPv2c et SNMPv3.

Atténuation : Utilisez des filtres de contrat de gestion sur le contrôleur APIC pour limiter l'accès SNMP par sous-réseau source. Les groupes de clients sont efficaces pour les noeuds Leaf/Spine. Pour le contrôleur APIC avec SNMPv3, utilisez le filtrage basé sur la source du contrat de gestion comme mécanisme de contrôle d'accès.

Scénario 5 : Requêtes SNMP réussies, mais les données MIB sont incomplètes ou obsolètes

Problème : SNMP GET/WALK renvoie des données, mais certains OID de MIB renvoient des valeurs vides ou périmées. En particulier, les statistiques d'interface ou les données d'état opérationnel ne reflètent pas l'état actuel du fabric.

Contrôle opérationnel : Vérifiez quel APIC est interrogé. Chaque APIC renvoie uniquement des objets MIB pour les données locales. Exécutez show snmp summary sur le contrôleur APIC interrogé et comparez le résultat avec ce que vous attendez. Pour les données au niveau du commutateur (IF-MIB, entityMIB), interrogez le commutateur directement, et non le contrôleur APIC.

Cause première : Interrogation d'un APIC pour les données MIB de niveau feuille. Chaque APIC fournit des objets MIB uniquement pour ses propres objets gérés. Les données au niveau du commutateur (états de l'interface, CPU, mémoire, capteurs environnementaux) doivent être récupérées en interrogeant directement chaque noeud leaf et spine.

Solution : Configurez votre NMS pour interroger directement les adresses IP de gestion de spine et de leaf pour les données MIB de l'interface et du matériel. Utilisez les adresses IP de gestion APIC uniquement pour les MIB natives APIC (entité, FRU, processus, capteur associé au matériel du serveur APIC).

Scénario 6 : Le protocole SNMP fonctionne sur les interfaces Leaf/Spine, mais pas sur le contrôleur APIC

Problème : SNMPv2c GET de NMS vers les noeuds leaf et spine réussit. Le même NMS ne peut pas interroger le contrôleur APIC.

Vérification de la configuration : APIC SNMP nécessite un contrat de gestion explicite autorisant UDP 161. Accédez à **Tenants > mgmt** et vérifiez le contrat OOB/INB et son filtre pour UDP 161.

Contrôle opérationnel : Sur le contrôleur APIC, exécutez iptables -S | grep 161. Si aucune règle ACCEPT pour UDP 161 n'apparaît sous la chaîne fp-137 (ou un contrat OOB équivalent), le filtre de contrat pour UDP 161 est manquant ou n'est pas déployé.

```
<#root>

apic1#

iptables -S | grep 161

-A fp-137 -s 10.0.0.0/8 -p udp -m udp --dport 161 -j ACCEPT     <--- permit SNMP from the management su
-A fp-137 -s 172.18.0.0/16 -p udp -m udp --dport 161 -j ACCEPT  <--- permit SNMP from INB management su
```

Si ces règles sont absentes, ajoutez une entrée de filtre pour UDP 161 à l'objet du contrat de gestion et revérifiez.

Cause première : Contrat de gestion manquant ou mal configuré. Dans l'ACI 5.x, les noeuds APIC appliquent strictement le contrat de gestion : les paquets SNMP sont abandonnés à moins qu'une autorisation explicite existe.

Solution :

1. Accédez à **Tenants > mgmt > Security Policies > Out-Of-Band Contracts**.
2. Développez le contrat OOB, sélectionnez l'objet et vérifiez/ajoutez un filtre pour le **port UDP 161**.
3. Répétez l'opération pour le contrat intrabande si le NMS atteint le contrôleur APIC sur la gestion INB.
4. Vérifier avec iptables -S | grep 161 sur le contrôleur APIC après l'enregistrement.

Scénario 7 : Les règles iptables SNMP sont absentes ou incorrectes

Problème : show snmp summary montre que la politique SNMP est appliquée mais que iptables -S | grep snmp ne renvoie aucune règle ou l'adresse IP du client NMS est absente des règles.

Contrôle opérationnel : Vérifiez que snmpd est en cours d'exécution avec pidof snmpd. Si snmpd est en cours d'exécution mais que iptables n'a pas de règles SNMP, le processus a été démarré

avant le déploiement de la stratégie de groupe du client. Redémarrez snmpd pour forcer la reprogrammation des règles si le nombre de redémarrages est inférieur à 250 :

```
<#root>

leaf101#

pidof snmpd

5881

leaf101# show system internal sysmgr service name snmpd
Service "snmpd" ("snmpd", 127):
UUID = 0x1A, PID = 5881, SAP = 1545
State: SRV_STATE_HANDSHAKED (entered at time Mon Aug 25 19:23:50 2025).

Restart count: 3


Time of last restart: Mon Aug 25 19:23:48 2025.
Previous PID: 32080
Reason of last termination: SYSMGR_DEATH_REASON_FAILURE_SIGNAL
Tag = N/A
Plugin ID: 0
leaf101#

kill -9 5881
```

Le gestionnaire de processus ACI redémarre automatiquement snmpd. Après le redémarrage, vérifiez :

```
<#root>

leaf101#

iptables -S | grep -i snmp
```

Les chaînes snmp_rules et les règles ACCEPT par client VRF doivent maintenant apparaître.

Cause première : Le processus snmpd a été redémarré avant le déploiement complet de la stratégie de groupe du client sur le noeud, laissant iptables sans les règles d'accès SNMP.

Remarque : Sur le contrôleur APIC, la commande tcpdump/code> n'est disponible que pour l'utilisateur racine. Pour APIC et les commutateurs, la commande iptables est disponible uniquement pour l'utilisateur racine. Scénario 4 : Application de groupe de clients SNMPv3 ne fonctionnant pas sur le problème APIC : Un client SNMP qui n'est PAS dans la stratégie de groupe du client peut interroger le contrôleur APIC à l'aide de SNMPv3, même si la même requête échoue à partir des noeuds leaf/spine. Cause première : C'est une mise en garde connue. Les stratégies de groupe client (application d'IP source basée sur iptables) ne sont pas appliquées pour les GET/Walks SNMPv3 vers les contrôleurs APIC. Tout hôte peut interroger le contrôleur APIC via SNMPv3, quelle que soit la configuration du groupe de clients. Sur les commutateurs Leaf et Spine, l'application de groupe de clients fonctionne de manière identique pour SNMPv2c et SNMPv3. Atténuation : Utilisez des filtres de contrat de gestion sur le contrôleur APIC pour limiter l'accès SNMP par sous-réseau source. Les groupes de clients sont efficaces pour les noeuds Leaf/Spine. Pour le contrôleur APIC avec SNMPv3, utilisez le filtrage basé sur la source du contrat de gestion comme mécanisme de contrôle d'accès. Scénario 5 : Requêtes SNMP réussies mais les données MIB sont incomplètes ou périmées Problème : SNMP GET/WALK renvoie des données, mais certains OID de MIB renvoient des valeurs vides ou périmées. En particulier, les statistiques d'interface ou les données d'état opérationnel ne reflètent pas l'état actuel du

fabric. Contrôle opérationnel : Vérifiez quel APIC est interrogé. Chaque APIC renvoie uniquement des objets MIB pour les données locales. Exécutez la commande show snmp summary sur le contrôleur APIC interrogé et comparez le résultat avec ce que vous attendez. Pour les données au niveau du commutateur (IF-MIB, entityMIB), interrogez le commutateur directement, et non le contrôleur APIC. Cause première : Interrogation d'un APIC pour les données MIB de niveau feuille. Chaque APIC fournit des objets MIB uniquement pour ses propres objets gérés. Les données au niveau du commutateur (états de l'interface, CPU, mémoire, capteurs environnementaux) doivent être récupérées en interrogeant directement chaque noeud leaf et spine. Solution : Configurez votre NMS pour interroger directement les adresses IP de gestion de spine et de leaf pour les données MIB de l'interface et du matériel. Utilisez les adresses IP de gestion APIC uniquement pour les MIB natives APIC (entité, FRU, processus, capteur associé au matériel du serveur APIC). Scénario 6 : Le protocole SNMP fonctionne sur les noeuds Leaf/Spine, mais pas sur le problème APIC : SNMPv2c GET de NMS vers les noeuds leaf et spine réussit. Le même NMS ne peut pas interroger le contrôleur APIC. Vérification de la configuration : APIC SNMP nécessite un contrat de gestion explicite autorisant UDP 161. Accédez à Tenants > mgmt et vérifiez le contrat OOB/INB et son filtre pour UDP 161. Contrôle opérationnel : Sur le contrôleur APIC, exécutez iptables -S | grep 161. Si aucune règle ACCEPT pour UDP 161 n'apparaît sous la chaîne fp-137 (ou contrat OOB équivalent), le filtre de contrat pour UDP 161 est manquant ou n'est pas déployé. apic1# iptables -S | grep 161 -A fp-137 -s 10.0.0.0/8 -p udp -m udp –dport 161 -j ACCEPT <– permit SNMP from the management subnet -A fp-137 -s 172.18.0.0/16 -p udp -m udp –dport 161 -j ACCEPT <– permit SNMP from INB management subnet Si ces règles sont absentes, ajoutez une entrée de filtre pour UDP 161 à l'objet du contrat de gestion et vérifiez à nouveau. Cause première : Contrat de gestion manquant ou mal configuré. Dans l'ACI 5.x, les noeuds APIC appliquent strictement le contrat de gestion : les paquets SNMP sont abandonnés à moins qu'une autorisation explicite existe. Solution : Accédez à Tenants > mgmt > Security Policies > Out-Of-Band Contracts. Développez le contrat OOB, sélectionnez l'objet et vérifiez/ajoutez un filtre pour le port UDP 161. Répétez l'opération pour le contrat intrabande si le NMS atteint le contrôleur APIC sur la gestion INB. Vérifier avec iptables -S | grep 161 sur le contrôleur APIC après l'enregistrement. Scénario 7 : Les règles iptables SNMP sont absentes ou incorrectes Problème : show snmp summary montre que la politique SNMP est appliquée mais iptables -S | grep snmp ne renvoie aucune règle ou l'adresse IP du client NMS est absente des règles. Contrôle opérationnel : Vérifiez que snmpd est en cours d'exécution avec pidof snmpd. Si snmpd est en cours d'exécution mais que iptables n'a pas de règles SNMP, le processus a été démarré avant le déploiement de la stratégie de groupe du client. Redémarrez snmpd pour forcer la reprogrammation des règles si le nombre de redémarrages est inférieur à 250 : leaf101# pidof snmpd 5881leaf101# show system internal sysmgr service name snmpdService "snmpd" ("snmpd", 127):UUID = 0x1A, PID = 5881, SAP = 1545État : SRV_STATE_HANDSHAKED (entré à l'heure lun août 25 19:23:50 2025).Nombre de redémarrages : 3Heure du dernier redémarrage : Lun Aug 25 19:23:48 2025.PID précédent : 32080Motif de la dernière résiliation : SYSMGR_DEATH_REASON_FAILURE_SIGNALTag = N/APlugin ID : 0 leaf101# kill -9 5881 Le gestionnaire de processus ACI redémarre automatiquement snmpd. Après le redémarrage, vérifiez : leaf101# iptables -S | grep -i snmp Les chaînes snmp_rules et les règles ACCEPT par client VRF doivent maintenant apparaître. Cause première : Le processus snmpd a été redémarré avant le déploiement complet de la stratégie de groupe du client sur le noeud, laissant iptables sans les règles d'accès SNMP.

Fichiers journaux pour le dépannage étendu

Lorsque les étapes de vérification ci-dessus ne résolvent pas le problème, les fichiers journaux suivants sur les noeuds leaf, spine et APIC contiennent des informations de diagnostic relatives au protocole SNMP :

<#root>

leaf101#

zgrep "snmp" /var/log/dme/log/svc_ifc_dbgrelem.log*

leaf101#

zgrep "snmpd" /var/log/dme/log/svc_ifc_dbgrelem.log*

```
leaf101#
```

```
zgrep "snmpd_log" /var/log/dme/log/*
```

Ces journaux contiennent des événements de redémarrage snmpd, des événements de déploiement de stratégie et des erreurs de configuration de communauté/client qui ne sont pas visibles via show snmp summary.

Références

- Guide de configuration de la gestion du système Cisco APIC, version 5.x – Gestion du protocole SNMP
- Guide de référence rapide de la base MIB Cisco ACI

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.