

Dépannage de la gestion ACI et des services principaux - Politiques de pod

Contenu

[Introduction](#)

[Informations générales](#)

[Présentation des politiques Pod](#)

[Politiques de pod](#)

[Politique de date et heure](#)

[Workflow de dépannage](#)

[Stratégie de réflecteur de route BGP](#)

[Workflow de dépannage](#)

[SNMP](#)

[Workflow de dépannage](#)

Introduction

Ce document décrit les étapes à suivre pour comprendre et dépanner les politiques Pod ACI.

Informations générales

Le matériel de ce document a été extrait de la [Dépannage de l'infrastructure axée sur les applications Cisco, deuxième édition](#), en particulier les services de gestion et de base - **Politiques POD - BGP RR/ Date&Time / SNMP** chapitre.

Présentation des politiques Pod

Les services de gestion tels que BGP RR, Date & Time et SNMP sont appliqués au système à l'aide d'un groupe de politiques Pod. Un groupe de politiques de pod régit un groupe de politiques de pod liées aux fonctions essentielles d'un fabric ACI. Ces politiques de pod concernent les composants suivants, dont beaucoup sont provisionnés dans un fabric ACI par défaut.

Politiques de pod

Politique de pod	Configuration manuelle requis
Date et heure	Oui
Réflecteur de route BGP	Oui
SNMP (Server Network Management Protocol)	Oui
ISIS	Non
COOP	Non
Accès de gestion	Non
Sec MAC	Oui

Même dans un fabric ACI unique, le groupe de politiques et le profil de pods doivent être configurés. Cela n'est pas spécifique à un déploiement multipod ou même multisite. Cette exigence s'applique à **tous les** types de déploiement ACI.

Ce chapitre se concentre sur ces politiques Pod essentielles et sur la façon de vérifier qu'elles sont appliquées correctement.

Politique de date et heure

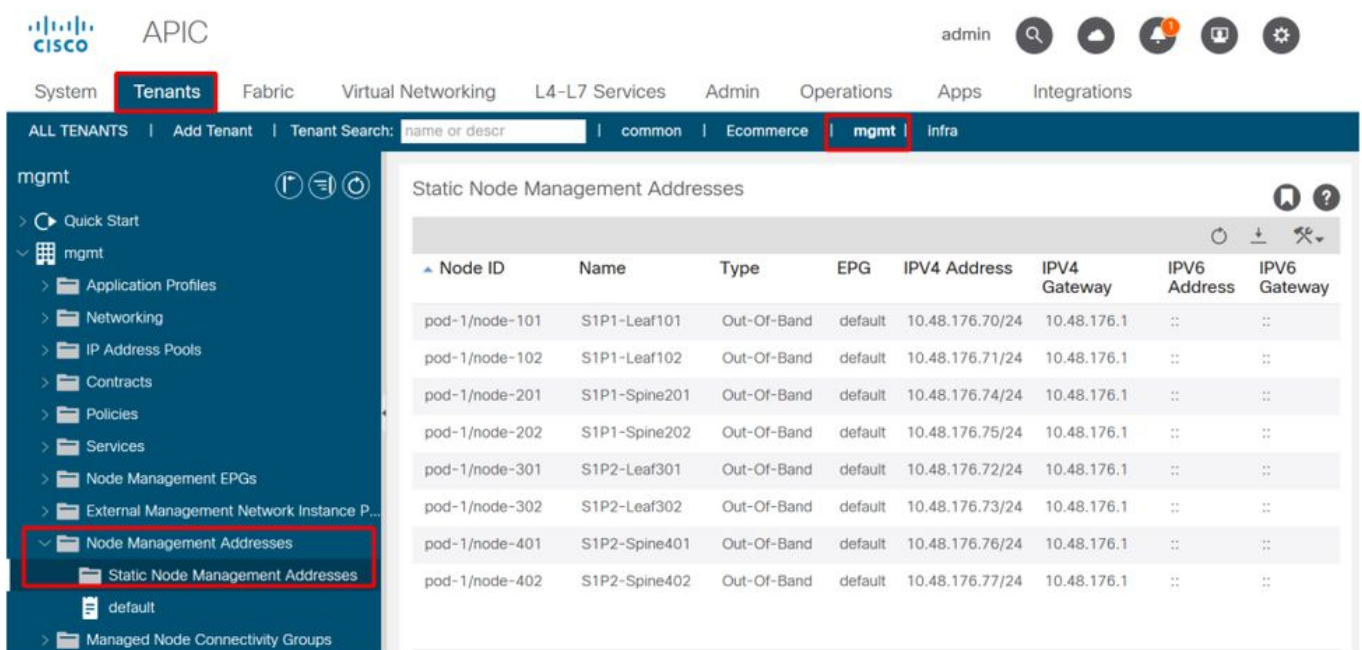
La synchronisation temporelle joue un rôle essentiel dans le fabric ACI. De la validation des certificats au maintien de la cohérence des horodatages des journaux dans les APIC et les commutateurs, il est recommandé de synchroniser les noeuds du fabric ACI avec une ou plusieurs sources temporelles fiables à l'aide du protocole NTP.

Pour que les noeuds soient correctement synchronisés avec un fournisseur de serveur NTP, il existe une dépendance pour attribuer des noeuds avec des adresses de gestion. Cela peut être effectué sous le locataire de gestion à l'aide d'adresses de gestion de noeud statiques ou de groupes de connectivité de noeud de gestion.

Workflow de dépannage

1. Vérifiez si les adresses de gestion des noeuds sont attribuées à tous les noeuds

Client de gestion - Adresses de gestion de noeud



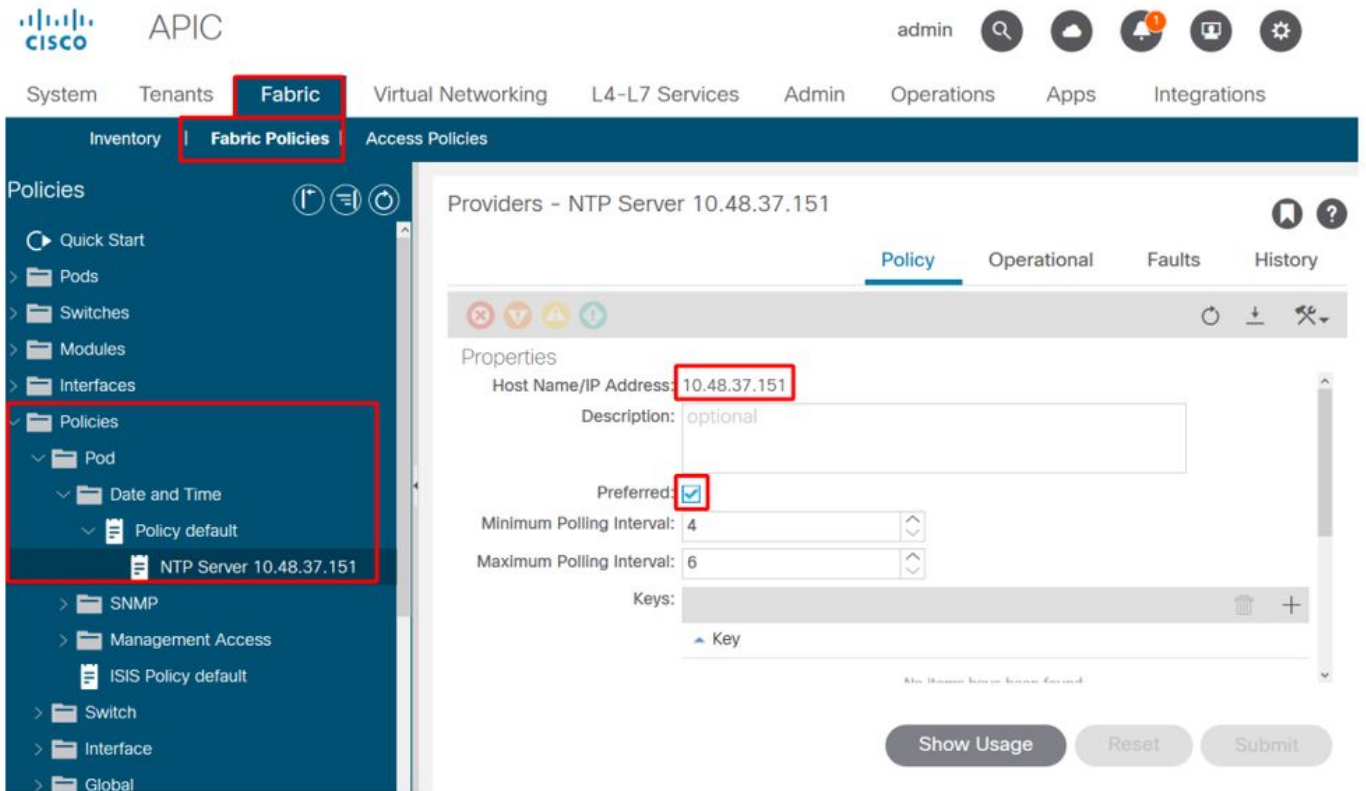
The screenshot shows the APIC management interface. The 'mgmt' tenant is selected in the top navigation bar. The left sidebar shows the 'mgmt' tenant structure, with 'Node Management Addresses' and 'Static Node Management Addresses' highlighted. The main content area displays a table of 'Static Node Management Addresses'.

Node ID	Name	Type	EPG	IPv4 Address	IPv4 Gateway	IPv6 Address	IPv6 Gateway
pod-1/node-101	S1P1-Leaf101	Out-Of-Band	default	10.48.176.70/24	10.48.176.1	::	::
pod-1/node-102	S1P1-Leaf102	Out-Of-Band	default	10.48.176.71/24	10.48.176.1	::	::
pod-1/node-201	S1P1-Spine201	Out-Of-Band	default	10.48.176.74/24	10.48.176.1	::	::
pod-1/node-202	S1P1-Spine202	Out-Of-Band	default	10.48.176.75/24	10.48.176.1	::	::
pod-1/node-301	S1P2-Leaf301	Out-Of-Band	default	10.48.176.72/24	10.48.176.1	::	::
pod-1/node-302	S1P2-Leaf302	Out-Of-Band	default	10.48.176.73/24	10.48.176.1	::	::
pod-1/node-401	S1P2-Spine401	Out-Of-Band	default	10.48.176.76/24	10.48.176.1	::	::
pod-1/node-402	S1P2-Spine402	Out-Of-Band	default	10.48.176.77/24	10.48.176.1	::	::

2. Vérifiez si un serveur NTP a été configuré en tant que fournisseur NTP

S'il y a plusieurs fournisseurs NTP, marquez au moins l'un d'entre eux comme source de temps préférée en utilisant la case à cocher « Préféré » comme dans la figure ci-dessous.

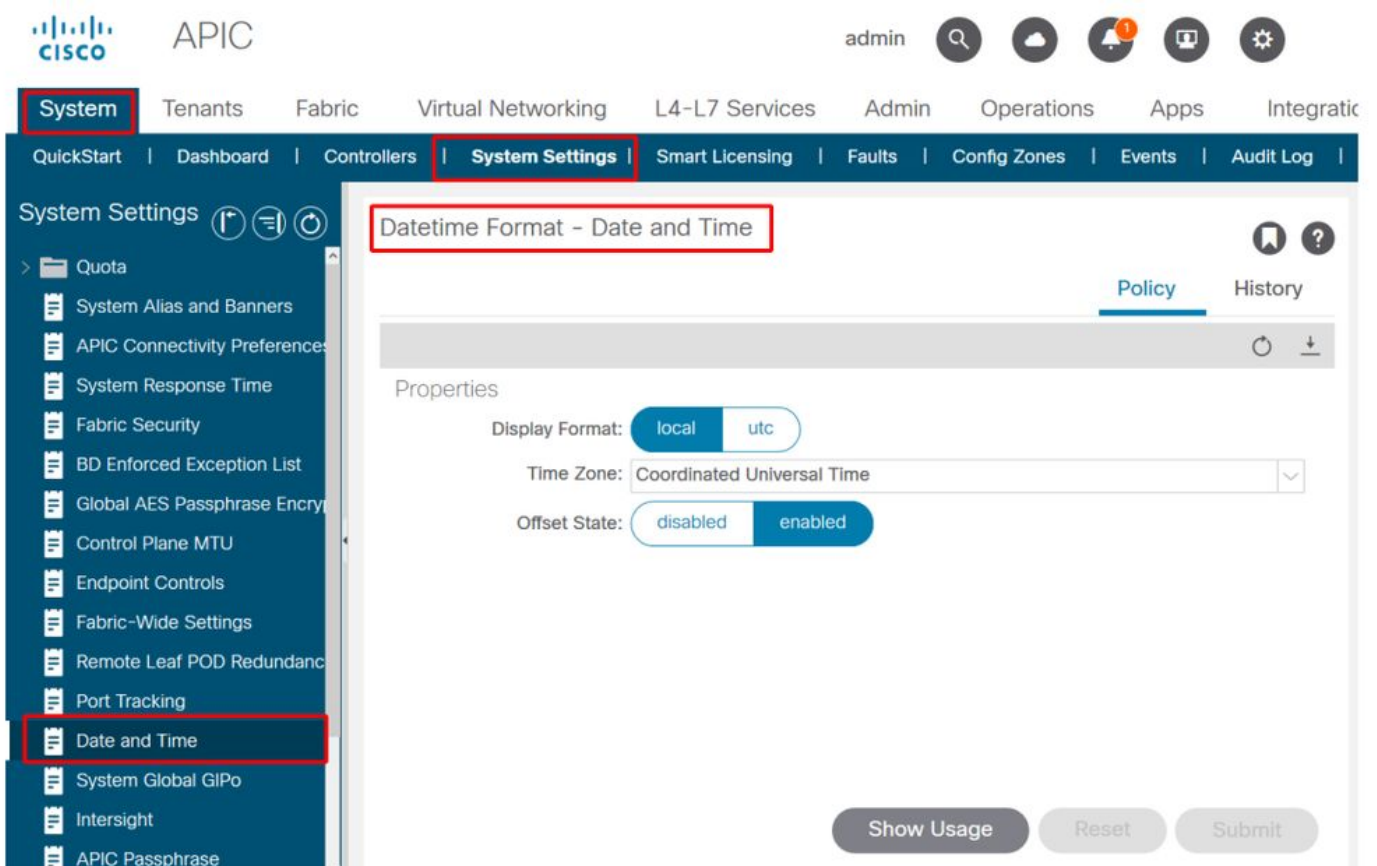
Fournisseur/serveur NTP sous Date and Time Pod Policy



3. Vérifiez le format de date et d'heure sous Paramètres système

La figure ci-dessous présente un exemple dans lequel le format Date et heure a été défini sur UTC.

Paramètres de date et d'heure sous Paramètres système



4. Vérifiez l'état de synchronisation opérationnel du fournisseur NTP pour tous les noeuds

Comme le montre la figure ci-dessous, la colonne État de synchronisation doit indiquer « Synchronisé avec le serveur NTP distant ». Sachez qu'il peut s'écouler plusieurs minutes avant que l'état de synchronisation converge correctement vers le serveur NTP distant .Synchronized. état.

État de synchronisation fournisseur NTP/serveur

The screenshot shows the APIC interface with the following elements highlighted:

- Top navigation: **Fabric** tab.
- Left sidebar: **Policies** > **Pod** > **NTP Server 10.48.37.151**.
- Main content: **Providers - NTP Server 10.48.37.151** page with **Operational** and **Deployed Servers** tabs.
- Table columns: **Sync Status**.
- Table data:

Name	Switch	VRF	Preferred	Sync Status
10.48.37.151	Node-101	management	True	Synced to Remote NTP Server
10.48.37.151	Node-103	management	True	Synced to Remote NTP Server
10.48.37.151	Node-104	management	True	Synced to Remote NTP Server
10.48.37.151	Node-105	management	True	Synced to Remote NTP Server
10.48.37.151	Node-102	management	True	Synced to Remote NTP Server
10.48.37.151	Node-201	management	True	Synced to Remote NTP Server
10.48.37.151	Node-106	management	True	Synced to Remote NTP Server
10.48.37.151	Node-202	management	True	Synced to Remote NTP Server

Vous pouvez également utiliser les méthodes CLI sur les cartes APIC et les commutateurs pour vérifier la synchronisation temporelle correcte avec le serveur NTP.

APIC - CLI NX-OS

La colonne « refld » ci-dessous indique la prochaine source de serveur NTP en fonction de la strate.

```
apic1# show ntpq
nodeid  remote          refid          st      t   when
poll   reach    auth  delay    offset  jitter
-----
1      * 10.48.37.151          192.168.1.115  2      u   25
64     377     none  0.214   -0.118  0.025
2      * 10.48.37.151          192.168.1.115  2      u   62
64     377     none  0.207   -0.085  0.043
3      * 10.48.37.151          192.168.1.115  2      u   43
64     377     none  0.109   -0.072  0.030
```

```
apic1# show clock
Time : 17:38:05.814 UTC Wed Oct 02 2019
```

APIC - Bash

```
apic1# bash
admin@apic1:~> date
Wed Oct 2 17:38:45 UTC 2019
```

Commutateur

Utilisez la commande « show ntp peers » pour vous assurer que la configuration du fournisseur NTP a été correctement transmise au commutateur.

```
leaf1# show ntp peers
-----
Peer IP Address                Serv/Peer Prefer KeyId  Vrf
-----
10.48.37.151                   Server   yes   None  management
```

```
leaf1# show ntp peer-status
Total peers : 1
* - selected for sync, + - peer mode(active),
- - peer mode(passive), = - polled in client mode
remote                local                st poll reach delay vrf
-----
*10.48.37.151        0.0.0.0              2 64 377 0.000 management
```

Le caractère '*' est essentiel ici car il détermine si le serveur NTP est réellement utilisé pour la synchronisation.

Vérifiez le nombre de paquets envoyés/reçus dans la commande suivante pour vous assurer que les noeuds ACI sont accessibles au serveur NTP.

```
leaf1# show ntp statistics peer ipaddr 10.48.37.151
...
packets sent:          256
packets received:     256
...
```

Stratégie de réflecteur de route BGP

Un fabric ACI utilise le protocole BGP multiprotocole (MP-BGP) et, plus précisément, le VPNv4 iBGP entre les noeuds Leaf et Spine pour échanger les routes locales reçues des routeurs externes (connectés sur des L3Out). Pour éviter une topologie d'homologue iBGP à maillage global, les noeuds spine reflètent les préfixes VPNv4 reçus d'un noeud terminal vers d'autres noeuds terminaux dans le fabric.

Sans la stratégie BGP Route Reflector (BGP RR), aucune instance BGP ne sera créée sur les commutateurs et les sessions BGP VPNv4 ne seront pas établies. Dans un déploiement multipod, chaque pod nécessite au moins un spine configuré en tant que RR BGP et essentiellement plus d'un pour la redondance.

Par conséquent, la politique BGP RR est un élément essentiel de la configuration dans chaque fabric ACI. La politique BGP RR contient également l'ASN que le fabric ACI utilise pour le

processus BGP sur chaque commutateur.

Workflow de dépannage

1. Vérifiez si la stratégie BGP RR a un ASN et au moins un spine configuré

L'exemple ci-dessous fait référence à un seul déploiement de pod.

Stratégie de réflecteur de route BGP sous Paramètres système

The screenshot shows the Cisco APIC System Settings page for BGP Route Reflector configuration. The 'System' tab is selected in the top navigation bar. The 'System Settings' menu on the left has 'BGP Route Reflector' highlighted. The main content area is titled 'BGP Route Reflector Policy - BGP Route Reflector' and shows the 'Policy' tab. The 'Autonomous System Number' is set to 65001. The 'Route Reflector Nodes' table lists two nodes: bdsol-aci12-spine1 and bdsol-aci12-spine2.

Pod ID	Node ID	Node Name	Description
1	201	bdsol-aci12-spine1	
1	202	bdsol-aci12-spine2	

2. Vérifiez si la stratégie BGP RR est appliquée sous le groupe de stratégie Pod

Appliquez une stratégie BGP RR par défaut sous le groupe de stratégie Pod. Même si l'entrée est vide, la stratégie BGP RR par défaut sera appliquée dans le cadre du groupe de stratégie Pod.

Stratégie de réflecteur de route BGP appliquée sous Groupe de stratégie Pod

Properties

Name: All

Description: optional

Date Time Policy: default

Resolved Date Time Policy: default

ISIS Policy: select a value

Resolved ISIS Policy: default

COOP Group Policy: select a value

Resolved COOP Group Policy: default

BGP Route Reflector Policy: default

Show Usage

Reset

Submit

3. Vérifiez si le groupe de stratégies Pod est appliqué sous le profil Pod

Groupe de stratégies Pod appliqué sous le profil Pod

The screenshot displays the Cisco APIC interface for configuring a Pod Profile. The 'Fabric' tab is selected in the top navigation bar. In the left-hand 'Policies' menu, 'Pod Profile default' is highlighted. The main content area shows the 'Pod Profile - default' configuration page with the 'Policy' tab active. The 'Properties' section shows 'Name: default' and 'Description: optional'. Below, the 'Pod Selectors' table lists a selector named 'default' with 'Type: ALL', 'Blocks: ALL', and 'Policy Group: All'. At the bottom, there are buttons for 'Show Usage', 'Reset', and 'Submit'.

4. Connectez-vous à un spine et vérifiez si le processus BGP s'exécute avec des sessions homologues VPN4 établies

```
spine1# show bgp process vrf overlay-1
```

```
BGP Process Information
BGP Process ID           : 26660
BGP Protocol Started, reason: : configuration
BGP Protocol Tag         : 65001
BGP Protocol State       : Running
BGP Memory State         : OK
BGP asformat             : asplain
Fabric SOO               : SOO:65001:33554415
Multisite SOO            : SOO:65001:16777199
Pod SOO                  : SOO:1:1
...
Information for address family VPNv4 Unicast in VRF overlay-1
Table Id                 : 4
Table state              : UP
Table refcount           : 9
Peers      Active-peers  Routes    Paths    Networks  Aggregates
  7         6            0         0         0         0

Redistribution
  None
```

```
Wait for IGP convergence is not configured
Additional Paths Selection route-map interleaf_rtmap_golf_rtmap_path_advertise_all
Is a Route-reflector
```



```
Nexthop trigger-delay
  critical 500 ms
  non-critical 5000 ms
```

Information for address family VPNv6 Unicast in VRF overlay-1

```
Table Id           : 80000004
Table state        : UP
Table refcount     : 9
Peers      Active-peers  Routes   Paths   Networks  Aggregates
7           6             0        0         0         0
```

```
Redistribution
  None
```

```
Wait for IGP convergence is not configured
Additional Paths Selection route-map interleaf_rtmap_golf_rtmap_path_advertise_all
Is a Route-reflector
```

```
Nexthop trigger-delay
  critical 500 ms
  non-critical 5000 ms
```

...

```
Wait for IGP convergence is not configured
Is a Route-reflector
```

```
Nexthop trigger-delay
  critical 500 ms
  non-critical 5000 ms
```

Comme indiqué ci-dessus, MP-BGP entre les noeuds Leaf et Spine transporte uniquement les familles d'adresses VPNv4 et VPNv6. La famille d'adresses IPv4 est utilisée dans MP-BGP uniquement sur les noeuds leaf.

Les sessions BGP VPNv4 et VPNv6 entre les noeuds spine et leaf peuvent également être facilement observées à l'aide de la commande suivante.

```
spine1# show bgp vpnv4 unicast summary vrf overlay-1
```

```
BGP summary information for VRF overlay-1, address family VPNv4 Unicast
BGP router identifier 10.0.136.65, local AS number 65001
BGP table version is 15, VPNv4 Unicast config peers 7, capable peers 6
0 network entries and 0 paths using 0 bytes of memory
BGP attribute entries [0/0], BGP AS path entries [0/0]
BGP community entries [0/0], BGP clusterlist entries [0/0]
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.0.136.64	4	65001	162	156	15	0	0	02:26:00	0
10.0.136.67	4	65001	154	154	15	0	0	02:26:01	0
10.0.136.68	4	65001	152	154	15	0	0	02:26:00	0
10.0.136.69	4	65001	154	154	15	0	0	02:26:01	0
10.0.136.70	4	65001	154	154	15	0	0	02:26:00	0
10.0.136.71	4	65001	154	154	15	0	0	02:26:01	0

```
spine1# show bgp vpnv6 unicast summary vrf overlay-1
```

```
BGP summary information for VRF overlay-1, address family VPNv6 Unicast
BGP router identifier 10.0.136.65, local AS number 65001
BGP table version is 15, VPNv6 Unicast config peers 7, capable peers 6
0 network entries and 0 paths using 0 bytes of memory
BGP attribute entries [0/0], BGP AS path entries [0/0]
BGP community entries [0/0], BGP clusterlist entries [0/0]
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
----------	---	----	---------	---------	--------	-----	------	---------	--------------

10.0.136.64	4	65001	162	156	15	0	0	02:26:11	0
10.0.136.67	4	65001	155	155	15	0	0	02:26:12	0
10.0.136.68	4	65001	153	155	15	0	0	02:26:11	0
10.0.136.69	4	65001	155	155	15	0	0	02:26:12	0
10.0.136.70	4	65001	155	155	15	0	0	02:26:11	0
10.0.136.71	4	65001	155	155	15	0	0	02:26:12	0

Notez la colonne « Up/Down » du résultat ci-dessus. Il doit indiquer une durée qui indique l'heure à laquelle la session BGP a été établie. Notez également que dans l'exemple, la colonne « PfxRcd » affiche 0 pour chaque homologue BGP VPNv4/VPNv6, car ce fabric ACI n'a pas encore de sorties L3 configurées et, en tant que tel, aucune route/préfixe externe ne correspond à des échanges entre des noeuds Leaf et Spine.

5. Connectez-vous à un leaf et vérifiez si le processus BGP s'exécute avec des sessions homologues VPN4 établies

```
leaf1# show bgp process vrf overlay-1
```

```
BGP Process Information
BGP Process ID           : 43242
BGP Protocol Started, reason: : configuration
BGP Protocol Tag         : 65001
BGP Protocol State       : Running
...
```

```
leaf1# show bgp vpnv4 unicast summary vrf overlay-1
```

```
BGP summary information for VRF overlay-1, address family VPNv4 Unicast
BGP router identifier 10.0.136.64, local AS number 65001
BGP table version is 7, VPNv4 Unicast config peers 2, capable peers 2
0 network entries and 0 paths using 0 bytes of memory
BGP attribute entries [0/0], BGP AS path entries [0/0]
BGP community entries [0/0], BGP clusterlist entries [0/0]
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.0.136.65	4	65001	165	171	7	0	0	02:35:52	0
10.0.136.66	4	65001	167	171	7	0	0	02:35:53	0

Les résultats de la commande ci-dessus indiquent un nombre de sessions BGP VPNv4 égal au nombre de noeuds spine présents dans le fabric ACI. Cela diffère des noeuds spine car ils établissent des sessions vers chaque noeud leaf et l'autre noeud spine de réflecteur de route.

SNMP

Il est important de clarifier dès le départ quel sous-ensemble spécifique de fonctions SNMP cette section couvre. Les fonctions SNMP d'un fabric ACI sont liées à la fonction SNMP Walk ou à la fonction SNMP Trap. La distinction importante ici est que SNMP Walk gouverne les flux de trafic **entrant** SNMP sur le port UDP 161 tandis que SNMP Trap gouverne les flux de trafic **sortant** SNMP avec un serveur de dé routement SNMP écoutant sur le port UDP 162.

Le trafic de gestion en entrée sur les noeuds ACI nécessite que les EPG de gestion des noeuds (intranche ou hors bande) fournissent les contrats nécessaires pour permettre au trafic de circuler. Cela s'applique également aux flux de trafic SNMP en entrée.

Cette section traite des flux de trafic SNMP entrants (SNMP Walks) dans les noeuds ACI (APIC et commutateurs). Il ne couvrira pas les flux de trafic SNMP de sortie (déroulements SNMP), car cela élargirait la portée de cette section en Politiques de surveillance et dépendances de la Politique de surveillance (par exemple, portée de la Politique de surveillance, Paquets de surveillance, etc.).

Cette section ne traite pas non plus des MIB SNMP pris en charge par l'ACI. Ces informations sont disponibles sur le site Web de Cisco CCO à l'adresse suivante :

<https://www.cisco.com/c/dam/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/mib/list/mib-support.html>

Workflow de dépannage

1. SNMP Pod Policy — Vérifier si une stratégie de groupe client est configurée

Assurez-vous qu'au moins un client SNMP unique est configuré dans le cadre de la stratégie de groupe du client, comme indiqué dans les captures d'écran ci-dessous.

Politiques Pod — Politique SNMP — Politiques de groupe client

The screenshot displays the Cisco ACI GUI configuration for an SNMP Policy. The navigation menu on the left shows the path: Fabric Policies > Pod > SNMP > default. The main configuration area is titled 'SNMP Policy - default' and includes the following fields:

- Name: default
- Description: optional
- Admin State: Disabled (selected), Enabled
- Contact: [empty field]
- Location: [empty field]

Below these fields is a table for 'Client Group Policies':

Name	Description	Client Entries	Associated Management EPG
snmpClientGrpProf		10.155.0.153	default (Out-of-Band)

Buttons at the bottom include 'Show Usage', 'Reset', and 'Submit'.

Politiques Pod — Politique SNMP — Politiques de groupe client

SNMP Client Group Profile - snmpClientGrpProf



Policy

History



Properties

Name: snmpClientGrpProf

Description: optional

Associated Management EPG: default (Out-of-Band)

Client Entries:  

Name	Address
Server01	10.155.0.153

2. SNMP Pod Policy : vérifiez si au moins une stratégie de communauté est configurée

Politiques Pod — Politique SNMP — Politiques de communauté

The screenshot shows the network management interface with the following elements:

- Navigation Menu:** System, Tenants, **Fabric** (highlighted), Virtual Networking, L4-L7 Services, Admin, Operations, Apps, Integration.
- Sub-menu:** Inventory, **Fabric Policies** (highlighted), Access Policies.
- Left Panel (Policies):** Quick Start, Pods, Switches, Modules, Interfaces, Policies (expanded), Pod (expanded), Date and Time, SNMP (expanded), default (highlighted), Management Access, ISIS Policy default, Switch, Interface, Global, Monitoring, Troubleshooting.
- Main Content Area:** SNMP Policy - default (Policy tab selected).
 - Community Policies:** A table with columns Name and Description. One entry is highlighted: my-secret-SNMP-community.
 - Trap Forward Servers:** A table with columns IP Address and Port. A message below states: "No items have been found. Click Actions to create a new item."
- Buttons:** Show Usage, Reset, Submit.

3. SNMP Pod Policy — Vérifiez si l'état Admin est défini sur 'Enabled'

The screenshot shows the Cisco DNA Center interface. The top navigation bar includes 'System', 'Tenants', 'Fabric', 'Virtual Networking', 'L4-L7 Services', 'Admin', 'Operations', 'Apps', and 'Integration'. The 'Fabric' tab is selected, and the 'Fabric Policies' section is expanded. The 'SNMP' folder is selected, and the 'default' policy is highlighted. The 'Admin State' is set to 'Enabled'.

The main content area shows the configuration for the 'SNMP Policy - default'. The 'Admin State' is set to 'Enabled'. The 'Client Group Policies' table is as follows:

Name	Description	Client Entries	Associated Management EPG
snmpClientGrpProf		10.155.0.153	default (Out-of-Ban...

4. Management tenant : vérifiez si l'EPG OOB fournit un contrat OOB autorisant le port UDP 161

L'EPG OOB régit la connectivité dans les ports de gestion APIC et OOB du commutateur. Elle affecte donc tous les flux de trafic entrant dans les ports OOB.

Assurez-vous que le contrat fourni ici inclut tous les services de gestion nécessaires au lieu du protocole SNMP. Exemple : il doit également inclure au moins SSH (port TCP 22). Sans cela, il n'est pas possible de se connecter aux commutateurs à l'aide de SSH. Veuillez noter que cela ne s'applique pas aux APIC car ils disposent d'un mécanisme permettant SSH, HTTP, HTTPS pour empêcher les utilisateurs d'être complètement verrouillés.

APIC Tenants

System **Tenants** Fabric Virtual Networking L4-L7 Services Admin Operations Apps Integrations

ALL TENANTS | Add Tenant | Tenant Search: name or descr | common **mgmt** | Ecommerce | infra

mgmt

Quick Start

mgmt

- Application Profiles
- Networking
- IP Address Pools
- Contracts
- Policies
- Services
- Node Management EPGs**
 - Out-of-Band EPG - default**
- External Management Network Insta...
- Node Management Addresses
- Managed Node Connectivity Groups

Out-of-Band EPG - default

Policy Faults History

Properties

Name: default

Tags:

Configuration Issues:

Configuration State: applied

Class ID: 32770

QoS Class: Unspecified

Provided Out-of-Band Contracts:

OOB Contract	Tenant	Type	QoS Class	State
snmp-walk-oob-contract	mgmt	oobbrc-snmp-walk-oob-contract	Unspecified	formed

Show Usage Reset Submit

5. Management tenant : vérifiez que le contrat OOB est présent et qu'il comporte un filtre autorisant le port UDP 161

Locataire de gestion — OOB EPG — Contrat OOB fourni

APIC Tenants

System **Tenants** Fabric Virtual Networking L4-L7 Services Admin Operations Apps Integrations

ALL TENANTS | Add Tenant | Tenant Search: name or descr | common **mgmt** | Ecommerce | infra

mgmt

Quick Start

mgmt

- Application Profiles
- Networking
- IP Address Pools
- Contracts**
 - Standard
 - Taboos
 - Imported
 - Filters
 - Out-Of-Band Contracts**
 - snmp-walk-oob-contract**
 - snmp-walk-oob-subject**
 - Policies
 - Services
 - Node Management EPGs
 - External Management Network Insta...

Contract Subject - snmp-walk-oob-subject

Policy Faults History

General Label

Property

Name: snmp-walk-oob-subject

Description: optional

Reverse Filter Ports:

Filters:

Name	Tenant	State	Action
snmp-walk-filter	mgmt	formed	Permit

Show Usage Reset Submit

Dans la figure ci-dessous, il n'est pas obligatoire d'autoriser uniquement le port UDP 161. Un contrat comportant un filtre autorisant le port UDP 161 de quelque manière que ce soit est correct. Il peut même s'agir d'un objet de contrat avec le filtre par défaut du locataire commun. Dans notre exemple, pour des raisons de clarté, un filtre spécifique a été configuré uniquement pour le port

UDP 161.

The screenshot shows the Cisco APIC interface. The top navigation bar includes 'System', 'Tenants', 'Fabric', 'Virtual Networking', 'L4-L7 Services', 'Admin', 'Operations', 'Apps', and 'Integrations'. The 'Tenants' tab is active, and the 'mgmt' tenant is selected. The left sidebar shows a tree view with 'Contracts' and 'Filters' expanded, and 'snmp-walk-filter' selected. The main content area displays the configuration for the 'Filter - snmp-walk-filter'. The 'Properties' section includes fields for Name, Alias, Description, Tags, and Global Alias. The 'Entries' section contains a table with the following data:

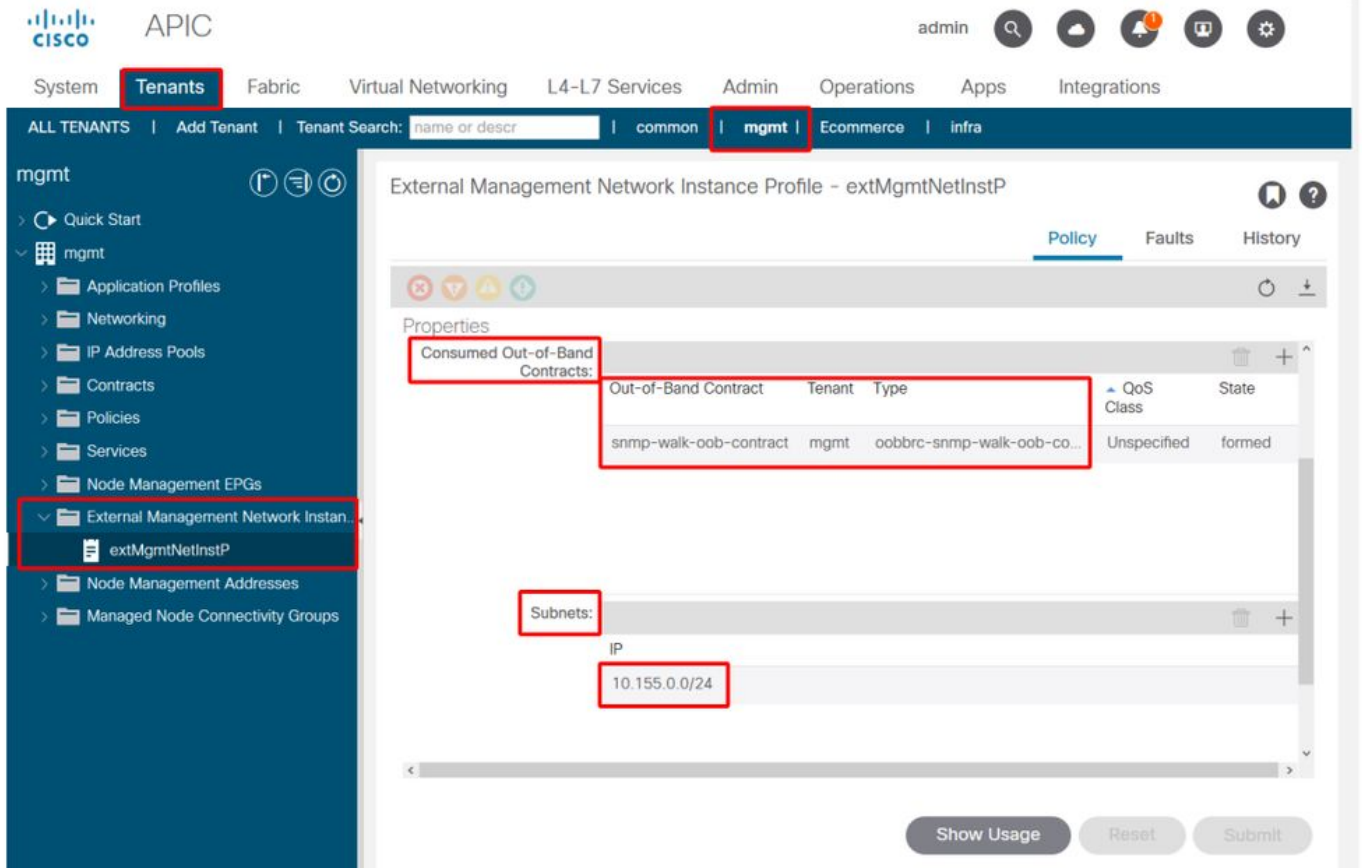
Name	Alias	EtherType	ARF Flag	IP Protocol	Match Only	Stateful	Source Port / Range		Destination Port / Range	
					Frage		From	To	From	To
sn...		IP		udp	False	False	unspecified	unspecified	161	161

Buttons at the bottom include 'Show Usage', 'Reset', and 'Submit'.

6. Client de gestion : vérifiez si un profil d'instance de réseau de gestion externe est présent avec un sous-réseau valide utilisant le contrat OOB

Le profil d'instance de réseau de gestion externe (ExtMgmtNetInstP) représente les sources externes définies par les « sous-réseaux » qui doivent consommer les services accessibles via l'EPG OOB. Ainsi, ExtMgmtNetInstP utilise le même contrat OOB fourni par l'EPG OOB. Il s'agit du contrat autorisant le port UDP 161. En outre, ExtMgmtNetInstP spécifie également les plages de sous-réseaux autorisées qui peuvent consommer les services fournis par l'EPG OOB.

Client de gestion - ExtMgmtNetInstP avec contrat OOB et sous-réseau consommés



Comme le montre la figure ci-dessus, une notation de sous-réseau basée sur CIDR est requise. La figure illustre un sous-réseau /24 spécifique. Les entrées de sous-réseau doivent couvrir les entrées de client SNMP telles que configurées dans la politique Pod SNMP (reportez-vous à la figure Politiques Pod SNMP — Politique SNMP — Politiques de groupe client).

Comme mentionné précédemment, veuillez à inclure tous les sous-réseaux externes requis pour empêcher le verrouillage d'autres services de gestion nécessaires.

7. Connectez-vous à un commutateur et exécutez une commande tcpdump pour vérifier si les paquets de marche SNMP (port UDP 161) sont observés

Si des paquets SNMP Walk entrent dans un commutateur par le port OOB, cela signifie que toutes les politiques/paramètres SNMP et OOB nécessaires ont été correctement configurés. C'est donc une méthode de vérification appropriée.

Tcpdump sur les noeuds leaf exploite leur shell Linux et leurs netdevices Linux. Par conséquent, il est nécessaire de capturer les paquets sur l'interface 'eth0' comme dans l'exemple ci-dessous. Dans l'exemple, un client SNMP exécute une requête SNMP Get sur l'OID .1.0.802.1.1.2.1.1.0.

```
leaf1# ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether f4:cf:e2:28:fc:ac brd ff:ff:ff:ff:ff:ff
    inet 10.48.22.77/24 brd 10.48.22.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::f6cf:e2ff:fe28:fcac/64 scope link
        valid_lft forever preferred_lft forever
```

```
leaf1# tcpdump -i eth0 udp port 161
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
```



```
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
22:18:10.204011 IP 10.155.0.153.63392 > 10.48.22.77.snmp: C=my-snmp-community
GetNextRequest(28) .iso.0.8802.1.1.2.1.1.1.0
22:18:10.204558 IP 10.48.22.77.snmp > 10.155.0.153.63392: C=my-snmp-community GetResponse(29)
.iso.0.8802.1.1.2.1.1.2.0=4
```

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.