

# Probleemoplossing voor ACI-beheer en kernservices - Pod-beleid

## Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[POD-beleidsverzicht](#)

[POD-beleid](#)

[Datum- en tijdbeleid](#)

[Werkstroom voor probleemoplossing](#)

[BGP-routeweergavebeleid](#)

[Werkstroom voor probleemoplossing](#)

[SNMP](#)

[Werkstroom voor probleemoplossing](#)

## Inleiding

Dit document beschrijft stappen om ACI Pod-beleid te begrijpen en problemen op te lossen.

## Achtergrondinformatie

Het materiaal van dit document is [Problemen oplossen met Cisco Application Centric Infrastructure, tweede editie](#) Meer specifiek de Management en Core Services - POD-beleid - BGP RR/datum&tijd/SNMP hoofdstuk.

## POD-beleidsverzicht

Beheerservices zoals BGP RR, Date & Time en SNMP worden toegepast op het systeem met behulp van een Pod Policy Group. Een Pod Policy Group regelt een groep pod beleid met betrekking tot essentiële functies van een ACI Fabric. Dit beleid van de Peul heeft op de volgende componenten betrekking, veel waarvan voorzien in een stof ACI door gebrek zijn.

## POD-beleid

|                                           |                                 |
|-------------------------------------------|---------------------------------|
| POD-beleid                                | Vereist handmatige configuratie |
| Datum en tijd                             | Ja                              |
| BGP-routereflector                        | Ja                              |
| SNMP (server network management protocol) | Ja                              |
| ISIS                                      | Nee                             |
| COOP                                      | Nee                             |
| Beheertoegang                             | Nee                             |
| MAC Sec                                   | Ja                              |

Zelfs in een enkele ACI-stof moeten de Pod Policy Group en Pod Profile worden geconfigureerd. Dit is niet specifiek voor een Multi-Pod of zelfs een Multi-Site-implementatie. Deze eis geldt voor **alle** uitroltypes van ACI.

Dit hoofdstuk concentreert zich op deze essentiële Pod-beleid en hoe te verifiëren ze correct worden toegepast.

## Datum- en tijdbeleid

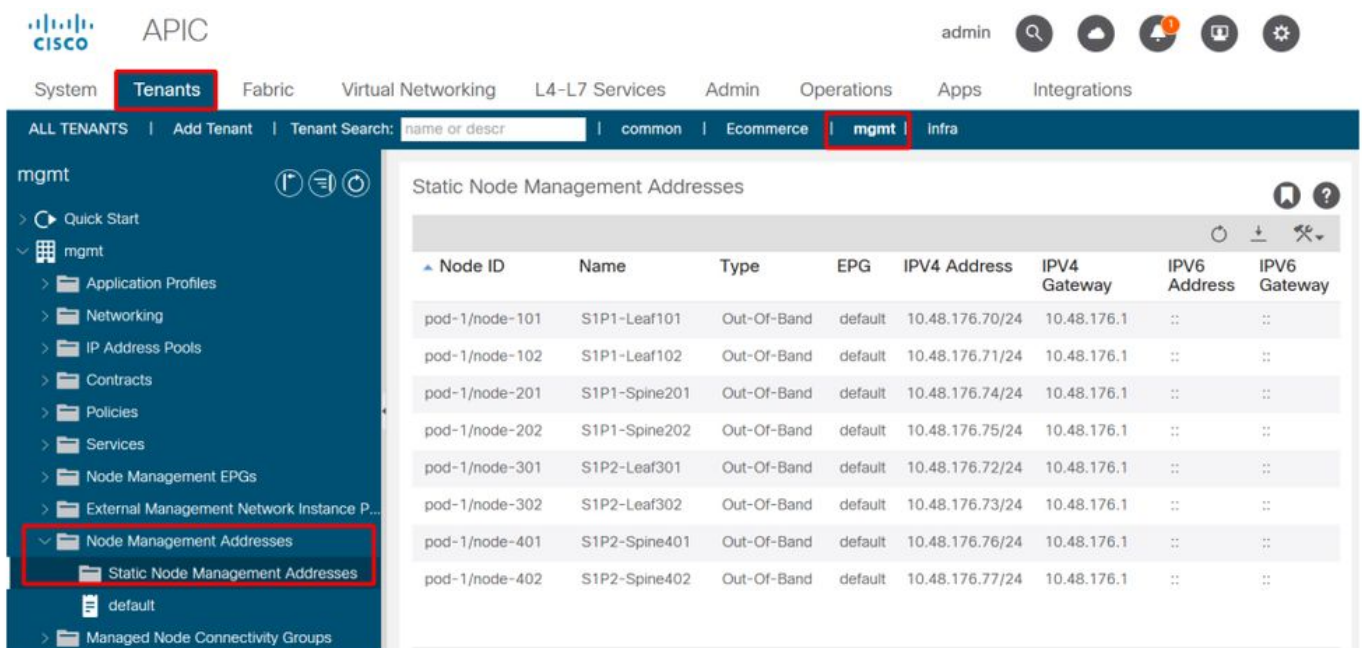
Tijdsynchronisatie speelt een cruciale rol in de ACI-structuur. Van het valideren van certificaten tot het consistent houden van logtijdstempels in APIC's en switches, het is best practice om de knooppunten in de ACI-structuur te synchroniseren met een of meer betrouwbare tijdbronnen met NTP.

Om de knooppunten goed te laten synchroniseren met een NTP-serverprovider, is er een afhankelijkheid om knooppunten met beheeradressen toe te wijzen. Dit kan onder de management tenant worden gedaan met behulp van statische knooppuntbeheeradressen of Management Node Connectivity-groepen.

## Werkstroom voor probleemoplossing

### 1. Controleer of Nodebeheeradressen aan alle knooppunten worden toegewezen

#### Beheerder - Nodebeheeradressen



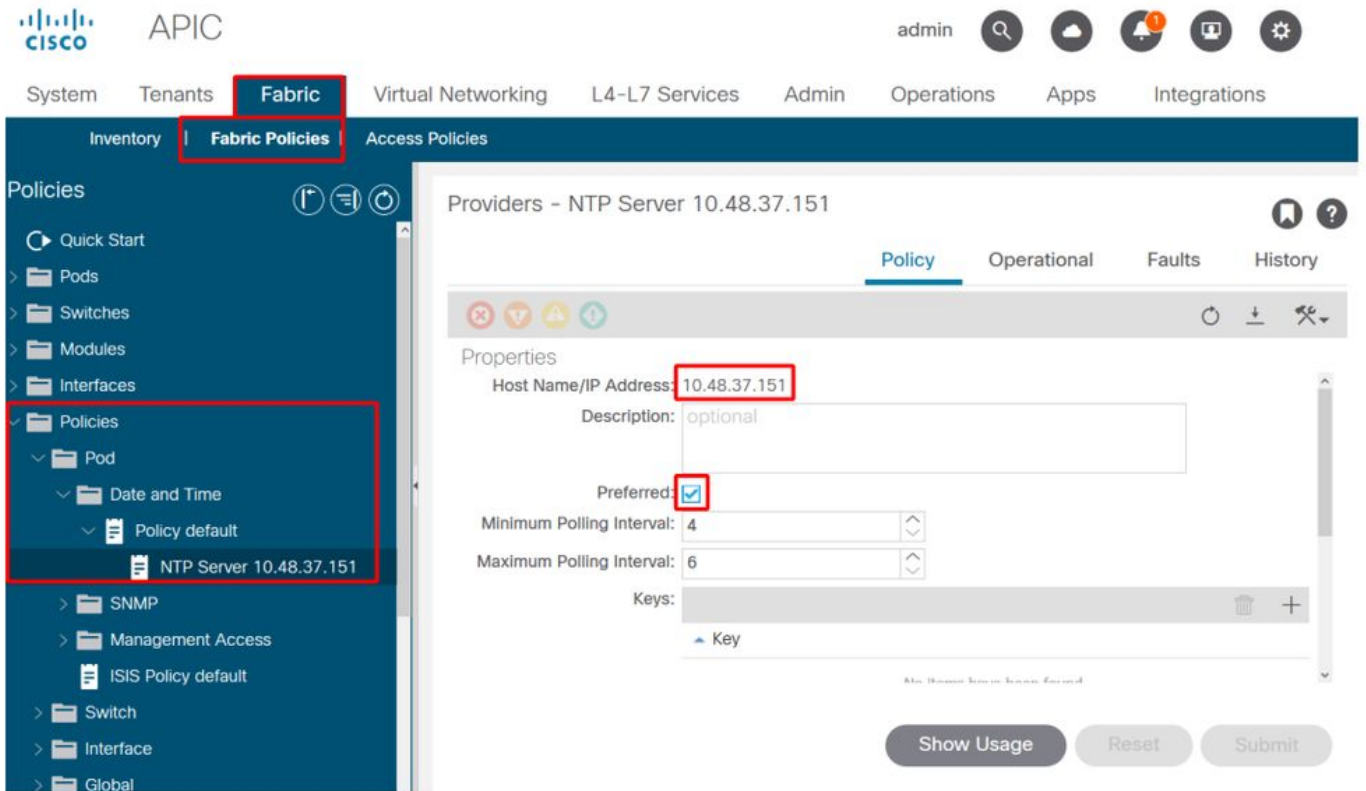
The screenshot shows the APIC interface with the 'mgmt' tenant selected. The 'Static Node Management Addresses' table is displayed, listing various nodes and their associated IP addresses and gateways.

| 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. Controleer of een NTP-server als NTP-provider is geconfigureerd

Als er meerdere NTP-providers zijn, markeer dan ten minste een van hen als de voorkeursbron met behulp van het 'Voorkeursvakje' zoals in de onderstaande afbeelding.

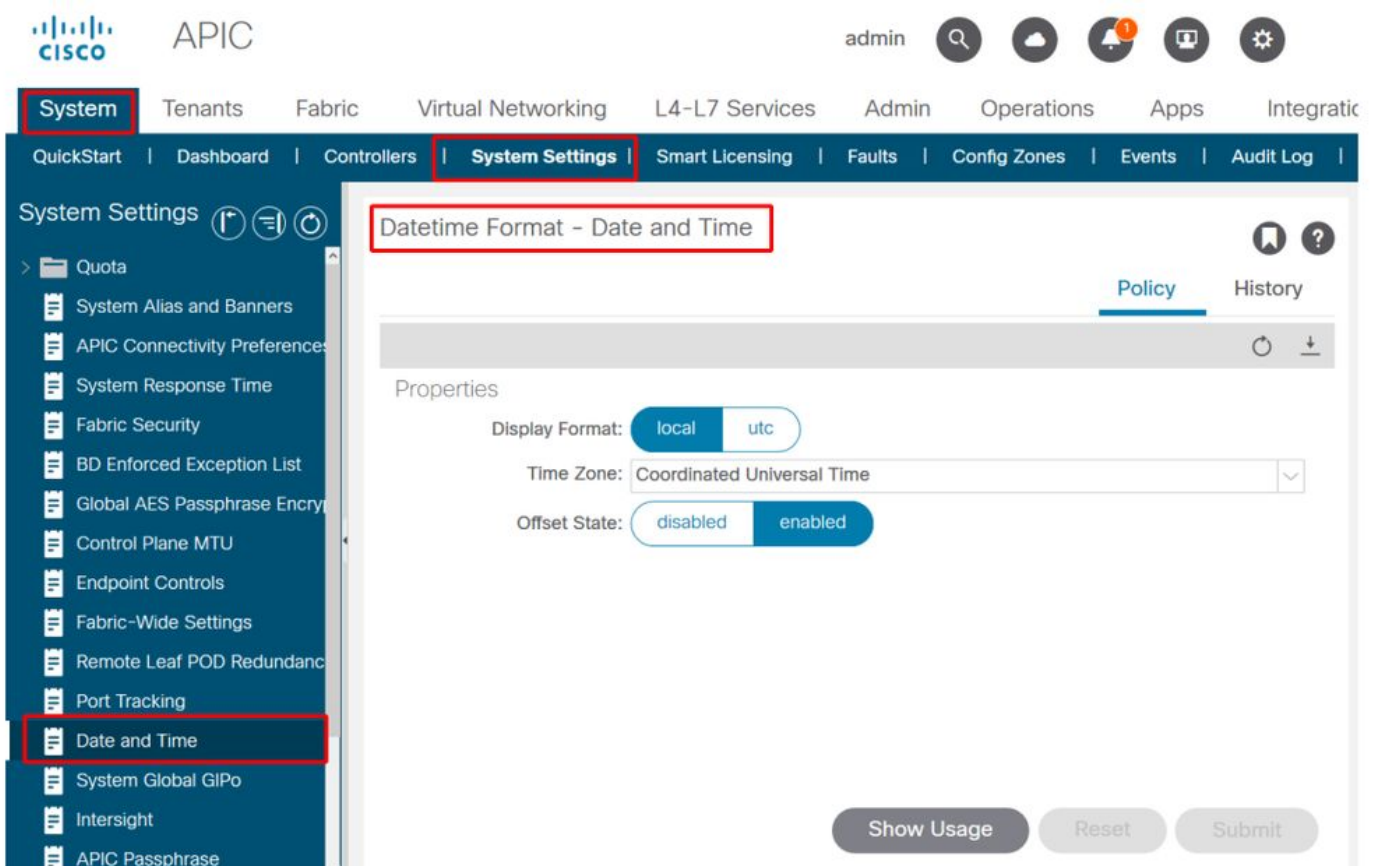
#### NTP-provider/server onder datum- en tijdpootbeleid



### 3. Controleer de datum- en tijdnnotatie onder Systeeminstellingen

In de onderstaande figuur is een voorbeeld weergegeven waarbij het datum- en tijdformaat is ingesteld op UTC.

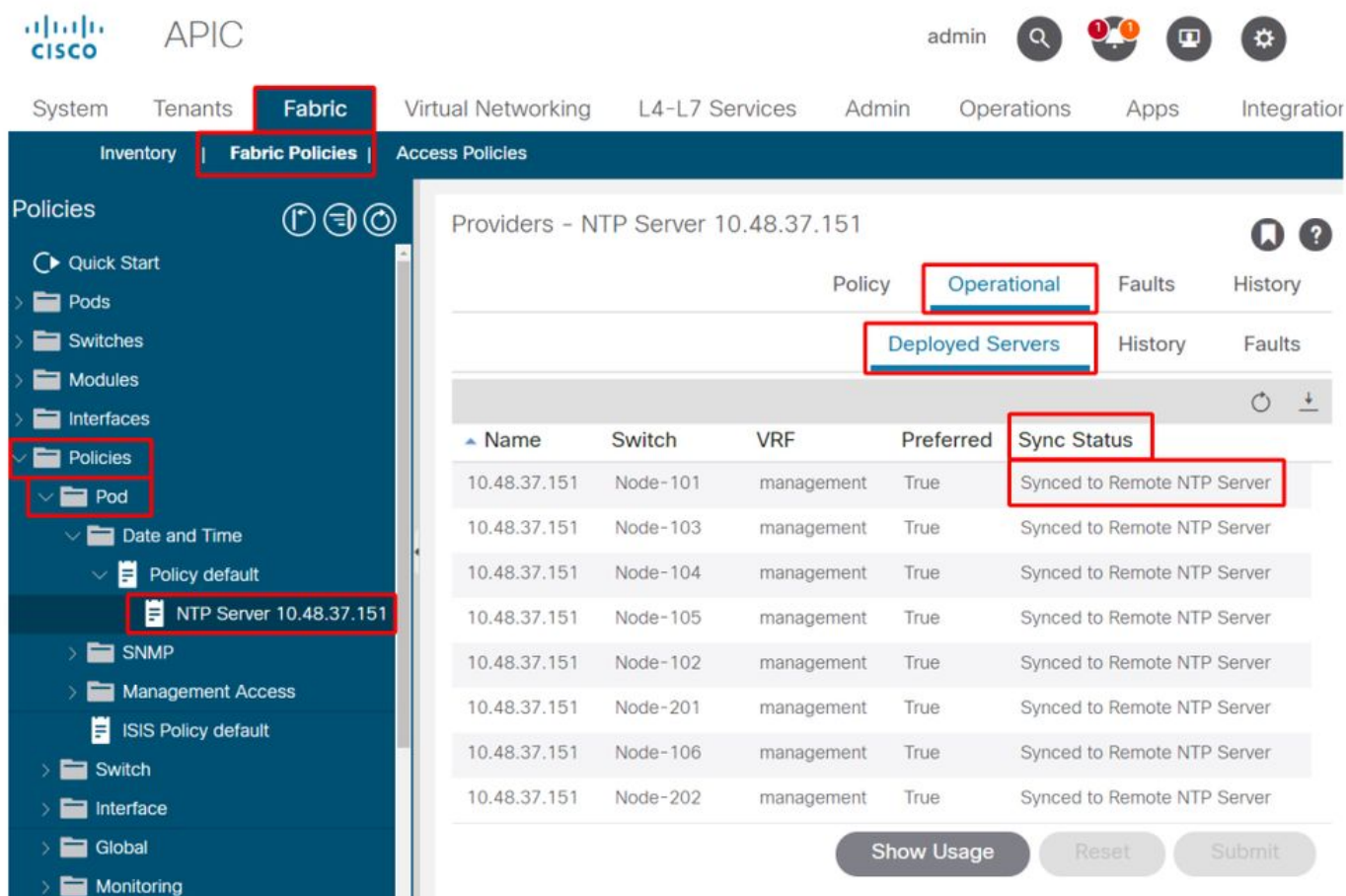
#### Datum en tijd instellen onder Systeeminstellingen



#### 4. Controleer de operationele sync-status van de NTP-provider voor alle knooppunten

Zoals in de afbeelding hieronder wordt getoond, moet in de kolom Sync Status 'Synced to Remote NTP Server' worden weergegeven. Houd er rekening mee dat het enkele minuten kan duren voordat de Sync Status op de juiste manier naar de .Synced to Remote NTP-server convergeert. status.

#### NTP-provider/server synchronisatiestatus



U kunt ook CLI-methoden gebruiken op de APIC's en de switches om te controleren of de juiste tijd sync is ten opzichte van de NTP-server.

#### APIC - NX-OS CLI

De kolom 'refId' hieronder toont de volgende tijdbron NTP-servers afhankelijk van het stratum.

```
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
```

## Switch

Gebruik het 'show ntp peers' commando om er zeker van te zijn dat de NTP provider configuratie goed naar de switch is geduwd.

```
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
```

Het '\*' teken is hier essentieel omdat het bepaalt of de NTP server daadwerkelijk voor sync wordt gebruikt.

Controleer het aantal verzonden/ontvangen pakketten in de volgende opdracht om ervoor te zorgen dat ACI-knooppunten bereikbaar zijn voor de NTP-server.

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

## BGP-routeweergavebeleid

Een ACI-fabric maakt gebruik van multi-protocol BGP (MP-BGP) en, meer specifiek, iBGP VPNv4 tussen blad- en spineknooppunten om huiroutes te ruilen die van externe routers worden ontvangen (aangesloten op L3Outs). Om een volledige mesh iBGP peer topologie te vermijden, weerspiegelen de wervelknooppunten VPNv4 prefixes ontvangen van een blad naar andere bladknooppunten in de stof.

Zonder het BGP Route Reflector-beleid (BGP RF) wordt er op de switches geen BGP-instantie gemaakt en worden BGP VPNv4-sessies niet ingesteld. In een Multi-Pod plaatsing, vereist elke Pod minstens één wervelkolom die als BGP RR wordt gevormd en hoofdzakelijk meer dan één voor overtuigendheid.

Hierdoor is het BGP RF-beleid een essentieel onderdeel van de configuratie in elke ACI Fabric. Het BGP RF-beleid bevat ook de ASN die de ACI Fabric gebruikt voor het BGP-proces op elke switch.



## Werkstroom voor probleemoplossing

### 1. Controleer of het BGP RF-beleid een ASN en ten minste één geconfigureerde wervelkolom heeft

Het voorbeeld hieronder verwijst naar een enkele podinzet.

#### BGP-routeweergavebeleid onder systeeminstellingen

The screenshot shows the APIC System Settings page for BGP Route Reflector configuration. The 'System' menu is highlighted in the top navigation bar. The 'System Settings' menu is also highlighted, and the 'BGP Route Reflector' option is selected in the left sidebar. The main content area displays the 'BGP Route Reflector Policy - BGP Route Reflector' configuration page. The 'Policy' tab is active, showing the following configuration details:

- Name: default
- Description: optional
- Autonomous System Number: 65001
- Route Reflector Nodes:

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

At the bottom of the configuration page, there are three buttons: 'Show Usage', 'Reset', and 'Submit'.

### 2. Controleer of het BGP RF-beleid wordt toegepast in het kader van de Pod Policy Group

Pas een standaard BGP RF-beleid toe onder de Pod Policy Group. Zelfs als het bericht leeg is, wordt het standaard BGP RF-beleid toegepast als onderdeel van de Pod Policy Group.

#### BGP-routeweergavebeleid toegepast onder Pod Policy Group

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. Controleer of de Pod Policy Group wordt toegepast onder het Podprofiel

Pod Policy Group toegepast onder het pod-profiel

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 this is a 'Pod Selectors' table with one entry: 'default' with 'Type: ALL', 'Blocks: ALL', and 'Policy Group: All'. At the bottom of the configuration page are buttons for 'Show Usage', 'Reset', and 'Submit'.

#### 4. Log in een spine en controleer of het BGP-proces wordt uitgevoerd met bestaande VPN4-peer sessies

```
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 interleak_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
```

Zoals hierboven is aangetoond, kan MP-BGP tussen blad- en ruggengraatknooppunten alleen VPNv4- en VPNv6-adresfamilies bevatten. De IPv4-adresfamilie wordt alleen op bladknooppunten in MP-BGP gebruikt.

De BGP VPNv4- en VPNv6-sessies tussen wervelkolom- en bladknooppunten kunnen ook gemakkelijk worden waargenomen met de volgende opdracht.

```
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 |

Noteer de 'Up/Down'-kolom uit de bovenstaande uitvoer. Er moet een tijdsduur staan die het tijdstip aangeeft waarop de BGP-sessie is ingesteld. Let ook in het voorbeeld op de 'PfxRcd' kolom 0 voor elke BGP VPNv4/VPNv6 peer als deze ACI Fabric nog geen L3Outs geconfigureerd heeft en als zodanig geen externe routes / prefixes zijn uitwisselingen tussen blad en wervelkolom knooppunten.

## 5. Log in een blad en controleer of het BGP-proces wordt uitgevoerd met gevestigde VPN4-peer sessies

```
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            |

De bovenstaande opdrachtoutput laat een hoeveelheid BGP VPNv4-sessies zien die gelijk is aan het aantal wervelkolomknooppunten in de ACI Fabric. Dit verschilt van de wervelkolomknooppunten omdat zij sessies aan elk blad en de andere route reflector wervelknooppunten instellen.

## SNMP

Het is belangrijk om vanaf het begin duidelijk te maken welke specifieke subset van SNMP-functies deze sectie bestrijkt. SNMP-functies in een ACI-fabric hebben betrekking op de SNMP-functie lopen of de SNMP-functie trap. Het belangrijke onderscheid hier is dat SNMP Walk **toegang tot** SNMP-verkeer regelt op UDP-poort 161, terwijl SNMP Trap **uitgaande** SNMP-verkeer regelt met een SNMP Trap-server die luistert op UDP-poort 162.

Het toegangsbeheerverkeer op ACI-knooppunten vereist dat de EPG's voor knooppunten (in-band of out-of-band) de benodigde contracten leveren om het verkeer te laten stromen. Als zodanig is dit ook van toepassing op de toegang tot SNMP-verkeersstromen.

In dit gedeelte worden de SNMP-verkeersstromen (SNMP-wandelingen) naar ACI-knooppunten (APIC's en switches) besproken. Het zal niet de uitgaande SNMP-verkeersstromen (SNMP-traps) bestrijken aangezien dat het toepassingsgebied van deze sectie zou uitbreiden tot bewakingsbeleid en afhankelijkheden van bewakingsbeleid (d.w.z. reikwijdte van

bewakingsbeleid, bewakingspakketten, enz.).

Deze sectie zal ook niet behandelen welke SNMP MIBs door ACI worden ondersteund. Die informatie is beschikbaar op de Cisco CCO-website via de volgende link:

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

## Werkstroom voor probleemoplossing

### 1. SNMP Pod-beleid — Controleer of een clientgroepbeleid is geconfigureerd

Zorg ervoor dat ten minste één SNMP-client is geconfigureerd als deel van het clientgroepsbeleid volgens de onderstaande screenshots.

#### POD-beleid — SNMP-beleid — clientgroepbeleid

The screenshot displays the Cisco ACI GUI configuration page for an SNMP Policy. The navigation menu on the left shows the path: Fabric > 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]

The 'Client Group Policies' section contains a table with the following data:

| 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'.

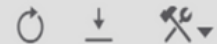
#### POD-beleid — SNMP-beleid — clientgroepbeleid

# 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-poortbeleid — Controleer of ten minste één communautair beleid is geconfigureerd

POD-beleid — SNMP-beleid — Gemeenschapsbeleid

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. It shows "No items have been found. Click Actions to create a new item."
  - Buttons:** Show Usage, Reset, Submit.

### 3. SNMP Pod Policy — Controleer of de Admin State is ingesteld op 'Enabled'

The screenshot displays the Cisco DNA Center interface for configuring an SNMP Policy. The 'Fabric' tab is active in the top navigation bar. The left-hand navigation pane shows the following structure:

- Inventory
  - Fabric Policies
  - Access Policies
- Policies
  - Quick Start
  - Pods
  - Switches
  - Modules
  - Interfaces
  - Policies
    - Pod
      - Date and Time
      - SNMP
        - default
      - Management Access
        - ISIS Policy default
      - Switch
      - Interface
      - Global
      - Monitoring
      - Troubleshooting

The main configuration area for 'SNMP Policy - default' shows the following details:

- Name: default
- Description: optional
- Admin State: **Enabled** (highlighted with a red box)
- Contact: [Empty field]
- Location: [Empty field]

The 'Client Group Policies' table is as follows:

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

Buttons at the bottom: Show Usage, Reset, Submit.

### 4. Beheerder — controleer of de OOB EPG een OOB-contract verstrekt dat UDP-poort toestaat 161

De OOB EPG regelt de connectiviteit in de APIC- en switch OOB-beheerpoorten. Als zodanig beïnvloedt het alle verkeersstromen die de OOB-havens binnenkomen.

Zorg ervoor dat het contract dat hier wordt geleverd alle nodige beheerservices bevat in plaats van alleen SNMP. Voorbeeld: het moet ook ten minste SSH (TCP poort 22). Zonder dit is het niet mogelijk om in te loggen op de switches met SSH. Let op: dit is niet van toepassing op APIC's, aangezien deze een mechanisme hebben waarmee SSH, HTTP en HTTPS kunnen voorkomen dat gebruikers volledig worden vergrendeld.

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. Beheerder — controleer of het OOB-contract aanwezig is en een filter heeft dat UDP-poort toestaat 161

Managementhuurder — OOB EPG — Voorzien OOB-contract

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

In de onderstaande afbeelding is het niet verplicht om alleen UDP-poort 161 toe te staan. Een contract met een filter dat UDP-poort 161 op welke manier dan ook toestaat, is correct. Dit kan zelfs een contractonderwerp zijn met het standaardfilter van de gemeenschappelijke huurder. In ons voorbeeld is voor de duidelijkheid een specifiek filter ingesteld voor UDP-poort 161.



The screenshot shows the Cisco APIC interface for the 'mgmt' tenant. The left navigation menu is expanded to show 'Filters' and 'snmp-walk-filter'. The main configuration area displays the properties of the 'snmp-walk-filter' filter. The 'Entries' table is as follows:

| Name  | Alias | EtherType | ARP Flag | IP Protocol | Match Only | Stateful | Source Port / Range     | Destination Port / Range |
|-------|-------|-----------|----------|-------------|------------|----------|-------------------------|--------------------------|
|       |       |           |          |             | Fragment   |          | From To                 | From To                  |
| sn... |       | IP        |          | udp         | False      | False    | unspecified unspecified | 161 161                  |

## 6. Management tenant — controleer of er een extern beheernetwerk aanwezig is met een geldig subnet dat het OOB-contract gebruikt

Het externe beheernetwerk-instantieprofiel (ExtMgmtNetInstP) is een externe bron die wordt gedefinieerd door de 'subnetten' in het profiel die diensten moeten gebruiken die via de OOB EPG bereikbaar zijn. Dus de ExtMgmtNetInstP gebruikt hetzelfde OOB-contract dat door de OOB EPG wordt geleverd. Dit is het contract dat UDP-poort 161 toestaat. Daarnaast specificeert ExtMgmtNetInstP ook de toegestane subnetbereiken die de services van de OOB EPG kunnen gebruiken.

**Beheerder — ExtMgmtNetInstP met verbruikt OOB-contract en subnet**

The screenshot shows the Cisco APIC interface for configuring an External Management Network Instance Profile. The 'mgmt' tenant is selected. The configuration page for 'extMgmtNetInstP' is displayed, showing the 'Policy' tab. The 'Consumed Out-of-Band Contracts' table lists the following contract:

| Out-of-Band Contract   | Tenant | Type                      | QoS Class   | State  |
|------------------------|--------|---------------------------|-------------|--------|
| snmp-walk-oob-contract | mgmt   | oobrc-snmp-walk-oob-co... | Unspecified | formed |

The 'Subnets' section shows a single subnet with the IP address 10.155.0.0/24.

Zoals in de bovenstaande afbeelding is aangegeven, is een op CIDR gebaseerde subnetnotatie vereist. Het cijfer toont een specifieke /24 subnetverbinding. Het vereiste is dat de subnetvermeldingen de SNMP-clientvermeldingen dekken zoals geconfigureerd in het SNMP-podbeleid (zie afbeelding podbeleid — SNMP-beleid — clientgroepbeleid).

Zoals eerder vermeld, dient u ervoor te zorgen dat alle vereiste externe subnetten zijn opgenomen om te voorkomen dat andere noodzakelijke beheerservices worden uitgesloten.

## 7. Log in een switch en voer een tcpdump uit om te observeren of SNMP-looppakketten — UDP-poort 161 — worden waargenomen

Als SNMP Walk-pakketten een switch via de OOB-poort invoeren, betekent dit dat alle benodigde op SNMP en OOB gebaseerde beleid/parameters correct zijn geconfigureerd. Het is dus een goede verificatiemethode.

Tcpdump op de bladknooppunten maakt gebruik van hun Linux-shell en Linux-netwerkapparaten. Daarom is het noodzakelijk om de pakketten op interface 'eth0' zoals hieronder voorbeeld te vangen. In het voorbeeld voert een SNMP-client een SNMP-aanvraag uit tegen OID .1.0.802.1.1.2.1.1.1.0.

```
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
```

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.