

Fehlerbehebung bei ACI Management und Core Services - POD-Richtlinien

Inhalt

[Einleitung](#)

[Hintergrundinformationen](#)

[Pod-Richtlinien im Überblick](#)

[POD-Richtlinien](#)

[Datums- und Uhrzeitrichtlinie](#)

[Fehlerbehebung-Workflow](#)

[BGP-Route-Reflector-Richtlinie](#)

[Fehlerbehebung-Workflow](#)

[SNMP](#)

[Fehlerbehebung-Workflow](#)

Einleitung

In diesem Dokument werden die Schritte zum Verständnis der ACI-POD-Richtlinien und zur Fehlerbehebung beschrieben.

Hintergrundinformationen

Das Material aus diesem Dokument wurde aus dem [Fehlerbehebung: Cisco Application Centric Infrastructure, Second Edition](#) Buch, insbesondere die Management- und Core-Services - **POD-Richtlinien - BGP-RR/Datum&Uhrzeit/SNMP** Kapitel.

Pod-Richtlinien im Überblick

Verwaltungsdienste wie BGP RR, Datum und Uhrzeit und SNMP werden mithilfe einer Pod Policy Group auf das System angewendet. Eine Pod-Richtliniengruppe regelt eine Gruppe von Pod-Richtlinien, die sich auf wesentliche Funktionen einer ACI-Fabric beziehen. Diese Pod-Richtlinien beziehen sich auf die folgenden Komponenten, von denen viele standardmäßig in einer ACI-Fabric bereitgestellt werden.

POD-Richtlinien

Pod-Richtlinie	Manuelle Konfiguration erforderlich
Datum und Uhrzeit	Ja
BGP-Routen-Reflektor	Ja
SNMP (Server Network Management Protocol)	Ja
ISIS	Nein
COOP	Nein

Managementzugriff
MAC-Sekunde

Nein
Ja

Selbst in einer einzigen ACI-Fabric müssen die Pod-Richtliniengruppe und das Pod-Profil konfiguriert werden. Dies gilt nicht nur für Multi-Pod- oder Multi-Site-Bereitstellungen. Diese Anforderung gilt für **alle** ACI-Bereitstellungsarten.

Dieses Kapitel konzentriert sich auf diese grundlegenden Richtlinien für PODs und darauf, wie diese korrekt angewendet werden.

Datums- und Uhrzeitrichtlinie

Die Zeitsynchronisierung spielt in der ACI-Fabric eine wichtige Rolle. Von der Validierung von Zertifikaten bis hin zur Konsistenz der Protokoll-Zeitstempel in APICs und Switches ist es Best Practice, die Knoten in der ACI-Fabric mithilfe von NTP mit einer oder mehreren zuverlässigen Zeitquellen zu synchronisieren.

Um eine ordnungsgemäße Synchronisierung der Knoten mit einem NTP-Serveranbieter zu ermöglichen, müssen Knoten mit Verwaltungsadressen zugewiesen werden. Dies kann über den Management-Tenant mithilfe von statischen Knotenmanagement-Adressen oder Management-Knotenverbindungen erfolgen.

Fehlerbehebung-Workflow

1. Überprüfen Sie, ob Node-Management-Adressen allen Knoten zugewiesen sind.

Management-Tenant - Knotenmanagement-Adressen

The screenshot shows the APIC GUI interface. The 'mgmt' tenant is selected in the top navigation bar. The left sidebar shows the 'Node Management Addresses' folder expanded. The main content area displays a table of 'Static Node Management Addresses' for various nodes in the 'pod-1' group.

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. Überprüfen Sie, ob ein NTP-Server als NTP-Anbieter konfiguriert wurde.

Wenn es mehrere NTP-Anbieter gibt, markieren Sie mindestens einen dieser Anbieter mithilfe des Kontrollkästchens "Bevorzugt" wie in der folgenden Abbildung dargestellt als bevorzugte Zeitquelle.

NTP-Anbieter/Server unter Pod-Richtlinie für Datum und Uhrzeit

The screenshot displays the Cisco APIC web interface. At the top, the 'Fabric' tab is selected in the main navigation bar. Below it, the 'Fabric Policies' sub-tab is active. The left-hand navigation pane shows a tree structure where 'Policies' is expanded, and 'Pod' is further expanded to show 'Date and Time' and 'Policy default'. The 'NTP Server 10.48.37.151' entry is highlighted. The main content area shows the configuration for this NTP server. The 'Host Name/IP Address' field is set to '10.48.37.151'. The 'Description' field contains the text 'optional'. The 'Preferred' checkbox is checked. The 'Minimum Polling Interval' is set to 4, and the 'Maximum Polling Interval' is set to 6. At the bottom of the configuration area, there are three buttons: 'Show Usage', 'Reset', and 'Submit'.

3. Überprüfen Sie unter Systemeinstellungen das Datums- und Uhrzeitformat.

Die folgende Abbildung zeigt ein Beispiel, bei dem das Datums- und Uhrzeitformat auf UTC eingestellt wurde.

Datums- und Uhrzeiteinstellungen unter Systemeinstellungen

The screenshot shows the Cisco APIC interface. At the top, the Cisco logo and 'APIC' are visible. The user is logged in as 'admin'. The navigation bar includes 'System', 'Tenants', 'Fabric', 'Virtual Networking', 'L4-L7 Services', 'Admin', 'Operations', 'Apps', and 'Integrations'. The 'System' tab is selected, and the 'System Settings' sub-tab is active. The left sidebar lists various settings, with 'Date and Time' highlighted. The main content area is titled 'Datetime Format - Date and Time' and shows the following configuration:

- Display Format: local (selected) / utc
- Time Zone: Coordinated Universal Time
- Offset State: disabled (selected) / enabled

Buttons for 'Show Usage', 'Reset', and 'Submit' are located at the bottom right of the configuration area.

4. Überprüfen Sie den betriebsbereiten Synchronisierungsstatus des NTP-Anbieters für alle Knoten.

Wie in der Abbildung unten gezeigt, sollte in der Spalte "Synchronisierungsstatus" "Mit Remote-NTP-Server synchronisiert" angezeigt werden. Beachten Sie, dass es einige Minuten dauern kann, bis der Synchronisierungsstatus ordnungsgemäß mit dem NTP-Remote-Server mit der Synchronisierung konvergiert. status.

Synchronisierungsstatus für NTP-Anbieter/Server

Inventory **Fabric Policies** Access Policies

Policies

- Quick Start
- Pods
- Switches
- Modules
- Interfaces
- Policies**
 - Pod
 - Date and Time
 - Policy default
 - NTP Server 10.48.37.151**
 - SNMP
 - Management Access
 - ISIS Policy default
 - Switch
 - Interface
 - Global
 - Monitoring

Providers - NTP Server 10.48.37.151

Policy **Operational** Faults History

Deployed Servers History Faults

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

Show Usage Reset Submit

Alternativ können CLI-Methoden auf den APICs und Switches verwendet werden, um die korrekte Zeitsynchronisierung mit dem NTP-Server zu überprüfen.

APIC = NX-OS-CLI

In der Spalte "refld" unten werden die NTP-Server je nach Schicht als nächste Quelle angezeigt.

```

apicl# 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
  
```

```

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

APIC - Bash

```

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

Switch

Verwenden Sie den Befehl "show ntp peers", um sicherzustellen, dass die NTP-Anbieterkonfiguration ordnungsgemäß an den Switch übertragen wurde.

```
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
```

Das Zeichen '*' ist hier von entscheidender Bedeutung, da es bestimmt, ob der NTP-Server tatsächlich für die Synchronisierung verwendet wird.

Überprüfen Sie die Anzahl der über den folgenden Befehl gesendeten/empfangenen Pakete, um sicherzustellen, dass die ACI-Knoten auf den NTP-Server zugreifen können.

```
leaf1# show ntp statistics peer ipaddr 10.48.37.151
```

```
...  
packets sent:           256  
packets received:      256  
...
```

BGP-Route-Reflector-Richtlinie

Eine ACI-Fabric verwendet Multiprotokoll-BGP (MP-BGP) und insbesondere iBGP-VPNv4 zwischen Leaf- und Spine-Knoten, um Tenant-Routen auszutauschen, die von externen Routern (die über L3Outs verbunden sind) empfangen werden. Zur Vermeidung einer Full-Mesh-iBGP-Peer-Topologie reflektieren die Spine-Knoten VPNv4-Präfixe, die von einem Leaf an andere Leaf-Knoten im Fabric empfangen werden.

Ohne die BGP Route Reflector (BGP RR)-Richtlinie wird auf den Switches keine BGP-Instanz erstellt, und es werden keine BGP-VPNv4-Sitzungen eingerichtet. In einer Multi-Pod-Bereitstellung benötigt jeder Pod mindestens einen Spine, der als BGP RR konfiguriert ist, und im Wesentlichen mehr als einen Spine, um die Redundanz sicherzustellen.

Daher ist die BGP RR-Richtlinie ein wesentlicher Konfigurationsbestandteil in jeder ACI-Fabric. Die BGP-RR-Richtlinie enthält außerdem das ASN, das die ACI-Fabric für den BGP-Prozess auf jedem Switch verwendet.

Fehlerbehebung-Workflow

1. Überprüfen Sie, ob die BGP-RR-Richtlinie über ein ASN und mindestens ein konfiguriertes Spine verfügt.

Das nachfolgende Beispiel bezieht sich auf eine einzelne Pod-Bereitstellung.

BGP-Routen-Reflektorrichtlinie unter "Systemeinstellungen"

System Settings

- Quota
- APIC Connectivity Preferences
- System Alias and Banners
- System Response Time
- Global AES Passphrase Encrypt
- BD Enforced Exception List
- Fabric Security
- Control Plane MTU
- Endpoint Controls
- Fabric-Wide Settings
- Port Tracking
- System Global GIPo
- Date and Time
- Intersight
- APIC Passphrase
- BGP Route Reflector**
- COOP Group

BGP Route Reflector Policy - BGP Route Reflector

Policy | Faults | History

Properties

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	

Show Usage | Reset | Submit

2. Überprüfen Sie, ob die BGP RR-Richtlinie unter der Pod-Richtliniengruppe angewendet wird.

Wenden Sie unter der Pod Policy Group (PoD-Richtliniengruppe) eine Standard-BGP-RR-Richtlinie an. Auch wenn der Eintrag leer ist, wird die BGP RR-Standardrichtlinie als Teil der Pod Policy Group angewendet.

Anwendung der BGP-Routen-Reflektorrichtlinie unter der Pod-Richtliniengruppe

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. Überprüfen Sie, ob die Pod-Richtliniengruppe unter dem Pod-Profil angewendet wird.

Pod-Richtliniengruppe angewendet unter Pod-Profil

4. Melden Sie sich bei einem Spine an, und überprüfen Sie, ob der BGP-Prozess mit den bestehenden VPN4-Peer-Sitzungen ausgeführt wird.

```
spinel# 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
```

Wie oben gezeigt, überträgt das MP-BGP zwischen Leaf- und Spine-Knoten nur VPNv4- und VPNv6-Adressfamilien. Die IPv4-Adressfamilie wird im MP-BGP nur auf Leaf-Knoten verwendet.

Die BGP-VPNv4- und VPNv6-Sitzungen zwischen Spine- und Leaf-Knoten können ebenfalls mit dem folgenden Befehl überwacht werden.

```
spinel# 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

```
spinel# 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

Beachten Sie die Spalte 'Nach oben/Nach unten' aus der obigen Ausgabe. Dieser sollte eine Zeitdauer angeben, die den Zeitpunkt bezeichnet, zu dem die BGP-Sitzung eingerichtet wurde. Beachten Sie im Beispiel auch, dass in der Spalte "PfxRcd" für jeden BGP-VPNv4/VPNv6-Peer 0 angezeigt wird, da für diese ACI-Fabric noch keine L3Outs konfiguriert sind und als solche keine externen Routen/Präfixe Tauschvorgänge zwischen Leaf- und Spine-Knoten sind.

5. Melden Sie sich bei einem Leaf an, und überprüfen Sie, ob der BGP-Prozess mit den etablierten VPN4-Peer-Sitzungen ausgeführt wird.

```
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

Die obigen Befehlsausgaben zeigen die Anzahl der BGP VPNv4-Sitzungen an, die der Anzahl der in der ACI-Fabric vorhandenen Spine-Knoten entspricht. Dies unterscheidet sich von den Spine-Knoten, da sie Sitzungen mit jedem Leaf und den anderen Routen-Reflektor-Spine-Knoten herstellen.

SNMP

Es ist wichtig, von Anfang an klarzustellen, welche spezifischen SNMP-Funktionen in diesem Abschnitt behandelt werden. SNMP-Funktionen in einer ACI-Fabric beziehen sich entweder auf die SNMP-Trap- oder die SNMP-Trap-Funktion. Der wichtige Unterschied besteht darin, dass SNMP Walk den **eingehenden** SNMP-Datenverkehr auf UDP-Port 161 steuert, während SNMP-Trap den **ausgehenden** SNMP-Datenverkehr über einen SNMP-Trap-Server steuert, der auf UDP-Port 162 wartet.

Für den eingehenden Management-Datenverkehr an ACI-Knoten müssen die Node Management-EPGs (In-Band oder Out-of-Band) die erforderlichen Verträge für den Datenfluss bereitstellen. Dies gilt auch für eingehenden SNMP-Datenverkehr.

In diesem Abschnitt werden die eingehenden SNMP-Datenverkehrsflüsse (SNMP Walks) in ACI-Knoten (APICs und Switches) behandelt. Er deckt nicht die ausgehenden SNMP-Datenverkehrsflüsse (SNMP-Traps) ab, da der Umfang dieses Abschnitts in

Überwachungsrichtlinien und Überwachungsrichtlinienabhängigkeiten (d. h. Überwachungsrichtlinienbereich, Überwachungspakete usw.) erweitert würde.

In diesem Abschnitt wird auch nicht behandelt, welche SNMP MIBs von der ACI unterstützt werden. Diese Informationen finden Sie auf der Cisco CCO-Website unter folgendem Link: <https://www.cisco.com/c/dam/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/mib/list/mib-support.html>

Fehlerbehebung-Workflow

1. SNMP Pod-Richtlinie - Überprüfen der Konfiguration einer Client-Gruppenrichtlinie

Stellen Sie sicher, dass mindestens ein SNMP-Client als Teil der Client-Gruppenrichtlinie konfiguriert ist (siehe Screenshots unten).

POD-Richtlinien - SNMP-Richtlinie - Client-Gruppen-Richtlinien

The screenshot shows the Cisco ACI GUI with the 'Fabric Policies' menu open. The 'SNMP Policy - default' configuration page is displayed. The 'Client Group Policies' table is visible, showing a policy named 'snmpClientGrpProf' with client entries '10.155.0.153' and an associated management EPG 'default (Out-of-Band)'. The 'Admin State' is set to 'Enabled'.

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

POD-Richtlinien - SNMP-Richtlinie - Client-Gruppen-Richtlinien

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-Richtlinie - Überprüfen der Konfiguration von mindestens einer Community-Richtlinie

Pod-Richtlinien - SNMP-Richtlinie - Community-Richtlinien

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

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

SNMP Policy - default

Policy Faults History

Properties

Community Policies:

Name	Description
my-secret-SNMP-community	

Trap Forward Servers:

IP Address	Port
No items have been found. Select Actions to create a new item	

Show Usage Reset Submit

3. SNMP Pod-Richtlinie - Überprüfen Sie, ob der Admin-Status auf "Aktiviert" eingestellt ist.

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

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

SNMP Policy - default

Policy Faults History

Properties

Name: default
Description: optional

Admin State: Disabled Enabled

Contact:
Location:

Client Group Policies:

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

Show Usage Reset Submit

4. Management-Tenant: Überprüfen, ob die OOB-EPG einen OOB-Vertrag bereitstellt, der den UDP-Port 161 zulässt

Die OOB-EPG steuert die Verbindungen zu den APIC- und Switch-OOB-Management-Ports. Dies wirkt sich auf den gesamten Datenverkehr aus, der in die OOB-Ports eingeht.

Stellen Sie sicher, dass der hier bereitgestellte Vertrag alle erforderlichen Management-Services enthält, nicht nur SNMP. Beispiele: muss mindestens SSH (TCP-Port 22) enthalten sein. Andernfalls ist eine Anmeldung bei den Switches über SSH nicht möglich. Bitte beachten Sie, dass dies nicht für APICs gilt, da diese über einen Mechanismus verfügen, der SSH, HTTP und HTTPS erlaubt, um zu verhindern, dass Benutzer vollständig gesperrt werden.

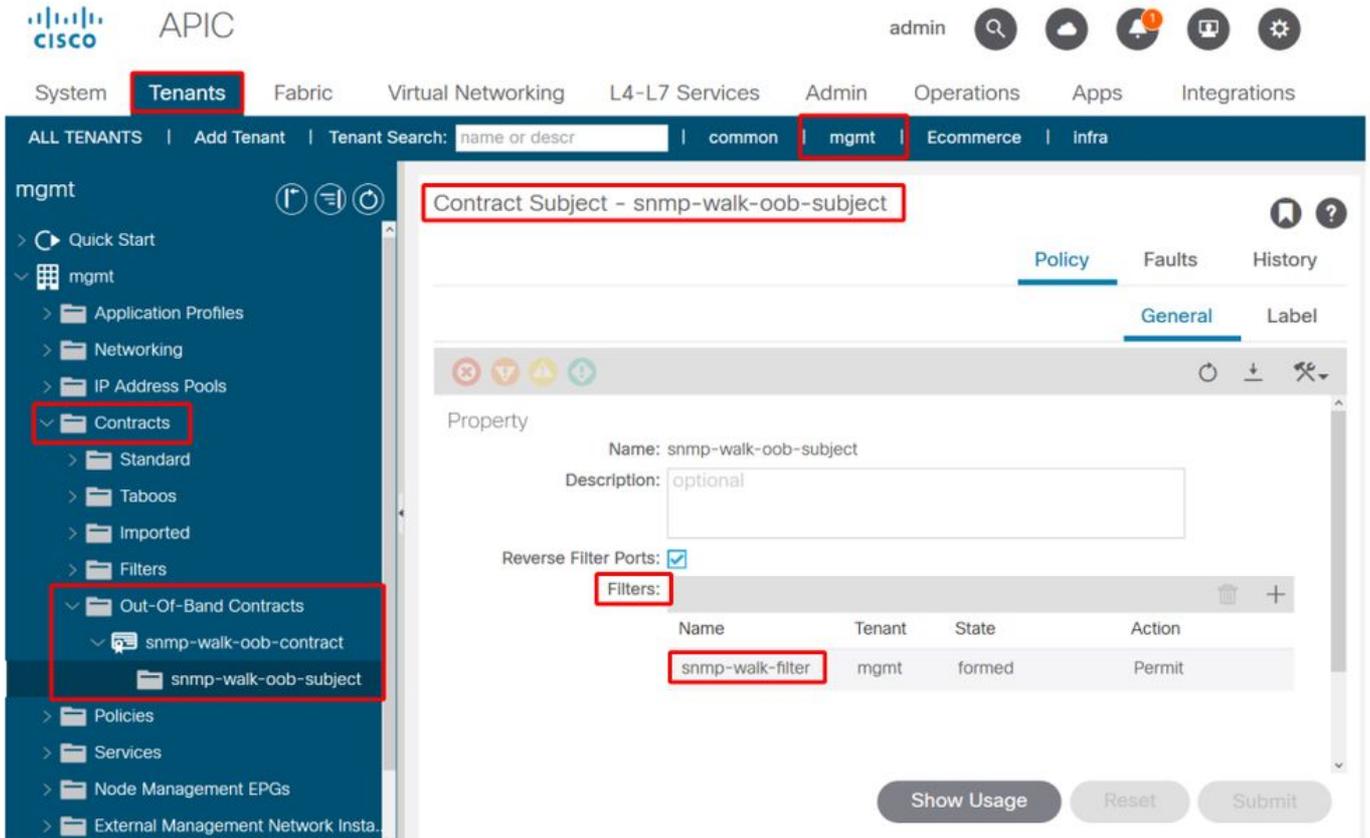
The screenshot shows the Cisco APIC interface for managing tenants. The 'mgmt' tenant is selected, and the 'Out-of-Band EPG - default' is highlighted. The configuration details for this EPG are as follows:

Property	Value
Name	default
Tags	
Configuration State	applied
Class ID	32770
QoS Class	Unspecified

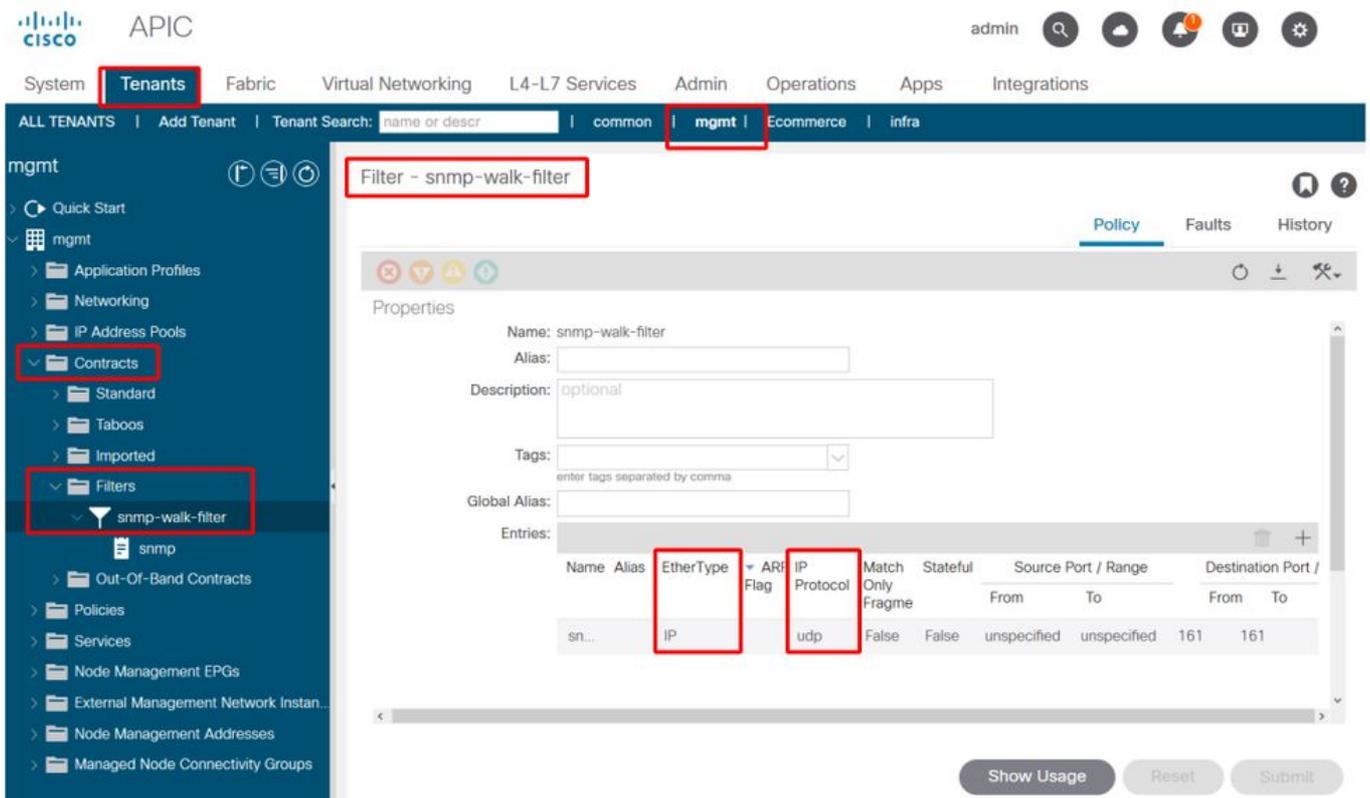
OOB Contract	Tenant	Type	QoS Class	State
snmp-walk-oob-contract	mgmt	oobrc-snmp-walk-oob-contract	Unspecified	formed

5. Management-Tenant: Überprüfen, ob der OOB-Vertrag vorhanden ist und über einen Filter verfügt, der den UDP-Port 161 zulässt

Management-Tenant - OOB-EPG - bereitgestellter OOB-Vertrag



In der Abbildung unten ist es nicht zwingend erforderlich, nur den UDP-Port 161 zuzulassen. Ein Vertrag, der über einen Filter verfügt, der den UDP-Port 161 in irgendeiner Weise zulässt, ist richtig. Dies kann sogar ein Vertragsgegenstand mit dem Standardfilter des gemeinsamen Tenants sein. Im vorliegenden Beispiel wurde zur besseren Übersicht ein spezifischer Filter nur für den UDP-Port 161 konfiguriert.



6. Management-Tenant: Überprüfen, ob ein externes Management-Netzwerk-Instanzprofil mit

einem gültigen Subnetz vorhanden ist, das den OOB-Vertrag belegt

Das externe Managementnetzwerk-Instanzprofil (ExtMgmtNetInstP) stellt externe Quellen dar, die durch die darin enthaltenen "Subnetze" definiert sind und Services nutzen müssen, die über die OOB-EPG erreichbar sind. Daher verwendet ExtMgmtNetInstP denselben OOB-Vertrag, der von der OOB-EPG bereitgestellt wird. Dies ist der Vertrag, der den UDP-Port 161 zulässt. Darüber hinaus gibt ExtMgmtNetInstP die zulässigen Subnetzbereiche an, die die von der OOB-EPG bereitgestellten Services nutzen können.

Management-Tenant - ExtMgmtNetInstP mit genutztem OOB-Vertrag und Subnetz

The screenshot shows the Cisco APIC interface for the 'mgmt' tenant. The 'External Management Network Instance Profile - extMgmtNetInstP' is configured under the 'Policy' tab. The 'Consumed Out-of-Band Contracts' table is as follows:

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

The 'Subnets' section contains one entry:

IP
10.155.0.0/24

Wie in der Abbildung oben gezeigt, ist eine CIDR-basierte Subnetznotation erforderlich. Die Abbildung zeigt ein bestimmtes /24-Subnetz. Die Subnetzeinträge müssen die SNMP-Clienteinträge abdecken, die in der SNMP Pod-Richtlinie konfiguriert sind (siehe Abbildung Pod-Richtlinien - SNMP-Richtlinie - Clientgruppenrichtlinien).

Wie bereits erwähnt, achten Sie darauf, alle erforderlichen externen Subnetze einzubeziehen, um zu verhindern, dass andere erforderliche Management-Services gesperrt werden.

7. Melden Sie sich bei einem Switch an, und führen Sie einen tcpdump aus, um festzustellen, ob SNMP-Walk-Pakete - UDP-Port 161 - beobachtet werden.

Wenn SNMP-Walk-Pakete über den OOB-Port auf einen Switch gelangen, bedeutet dies, dass alle erforderlichen SNMP- und OOB-basierten Richtlinien/Parameter ordnungsgemäß konfiguriert wurden. Daher ist es eine geeignete Überprüfungs-methode.

Tcpdump auf den Endknoten nutzt ihre Linux-Shell und Linux-Netzwerkgeräte. Daher ist es notwendig, die Pakete auf Schnittstelle 'eth0' wie im folgenden Beispiel zu erfassen. In diesem Beispiel führt ein SNMP-Client eine SNMP Get-Anforderung für die OID .1.0.8802.1.1.2.1.1.1.0

durch.

```
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
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.