

Risoluzione dei problemi relativi alla gestione ACI e ai servizi di base - Pod Policies

Sommario

[Introduzione](#)

[Premesse](#)

[Panoramica dei criteri POD](#)

[Criteri POD](#)

[Criteri data e ora](#)

[Flusso di lavoro di risoluzione dei problemi](#)

[criterio BGP Route Reflector](#)

[Flusso di lavoro di risoluzione dei problemi](#)

[SNMP](#)

[Flusso di lavoro di risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come comprendere e risolvere i problemi relativi ai criteri ACI Pod.

Premesse

Il materiale tratto da questo documento è stato [Risoluzione dei problemi di Cisco Application Centric Infrastructure, Second Edition](#) , in particolare i servizi di gestione e di base - **Criteri POD - BGP RR/ Data e ora / SNMP** capitolo.

Panoramica dei criteri POD

I servizi di gestione come BGP RR, Date & Time e SNMP vengono applicati sul sistema utilizzando un Pod Policy Group. Un Gruppo di criteri dei pod gestisce un gruppo di criteri dei pod relativi alle funzioni essenziali di un fabric ACI. Queste policy relative ai pod si riferiscono ai seguenti componenti, molti dei quali sono forniti in un fabric ACI per impostazione predefinita.

Criteri POD

Criteri POD	Richiede configurazione manuale
Data e ora	Sì
BGP Route Reflector	Sì
SNMP (server network management protocol)	Sì
ISIS	No
COOP	No
Accesso alla gestione	No

Anche in un singolo fabric ACI, è necessario configurare il Pod Policy Group e il Pod Profile. Ciò non riguarda solo i dispositivi multi-pod o le installazioni multisito. Il requisito si applica a **tutti** i tipi di distribuzione ACI.

Questo capitolo si concentra su queste politiche essenziali del POD e su come verificare che siano applicate correttamente.

Criteri data e ora

La sincronizzazione dell'ora svolge un ruolo critico nell'infrastruttura ACI. Dalla convalida dei certificati al mantenimento della coerenza dei timestamp dei log in APIC e switch, è buona norma sincronizzare i nodi nella struttura ACI con una o più origini dell'ora affidabili utilizzando NTP.

Per sincronizzare correttamente i nodi con un provider di server NTP, esiste una dipendenza da assegnare nodi con indirizzi di gestione. Questa operazione può essere eseguita nel tenant di gestione utilizzando indirizzi di gestione dei nodi statici o gruppi di connettività dei nodi di gestione.

Flusso di lavoro di risoluzione dei problemi

1. Verificare che gli indirizzi di gestione dei nodi siano assegnati a tutti i nodi

Tenant di gestione - Indirizzi di gestione dei nodi

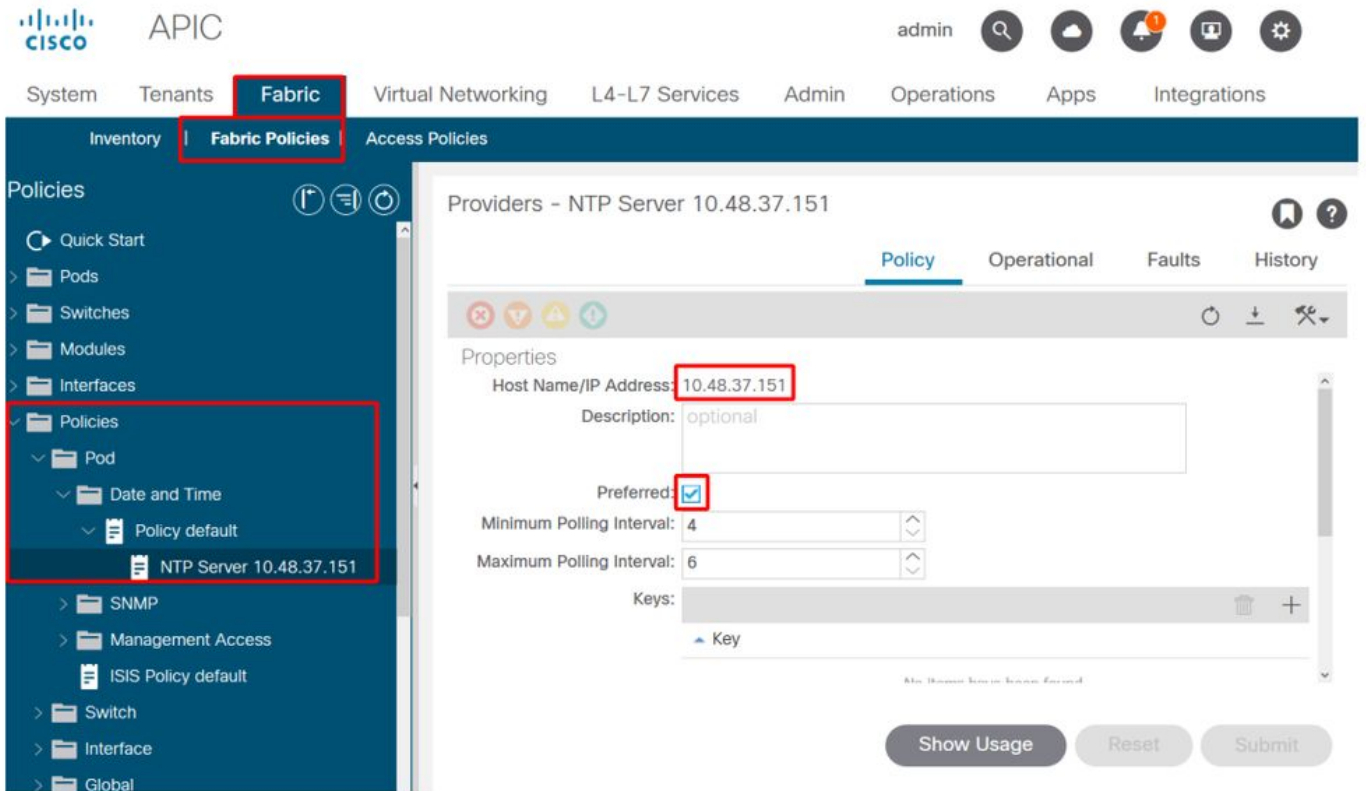
The screenshot shows the APIC interface with the 'mgmt' tenant selected. The 'Static Node Management Addresses' table is displayed, listing various nodes and their associated IP addresses and gateways.

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. Verificare se un server NTP è stato configurato come provider NTP

Se sono presenti più provider NTP, contrassegnare almeno uno di essi come origine preferita dell'ora utilizzando la casella di controllo 'Preferito' come illustrato nella figura seguente.

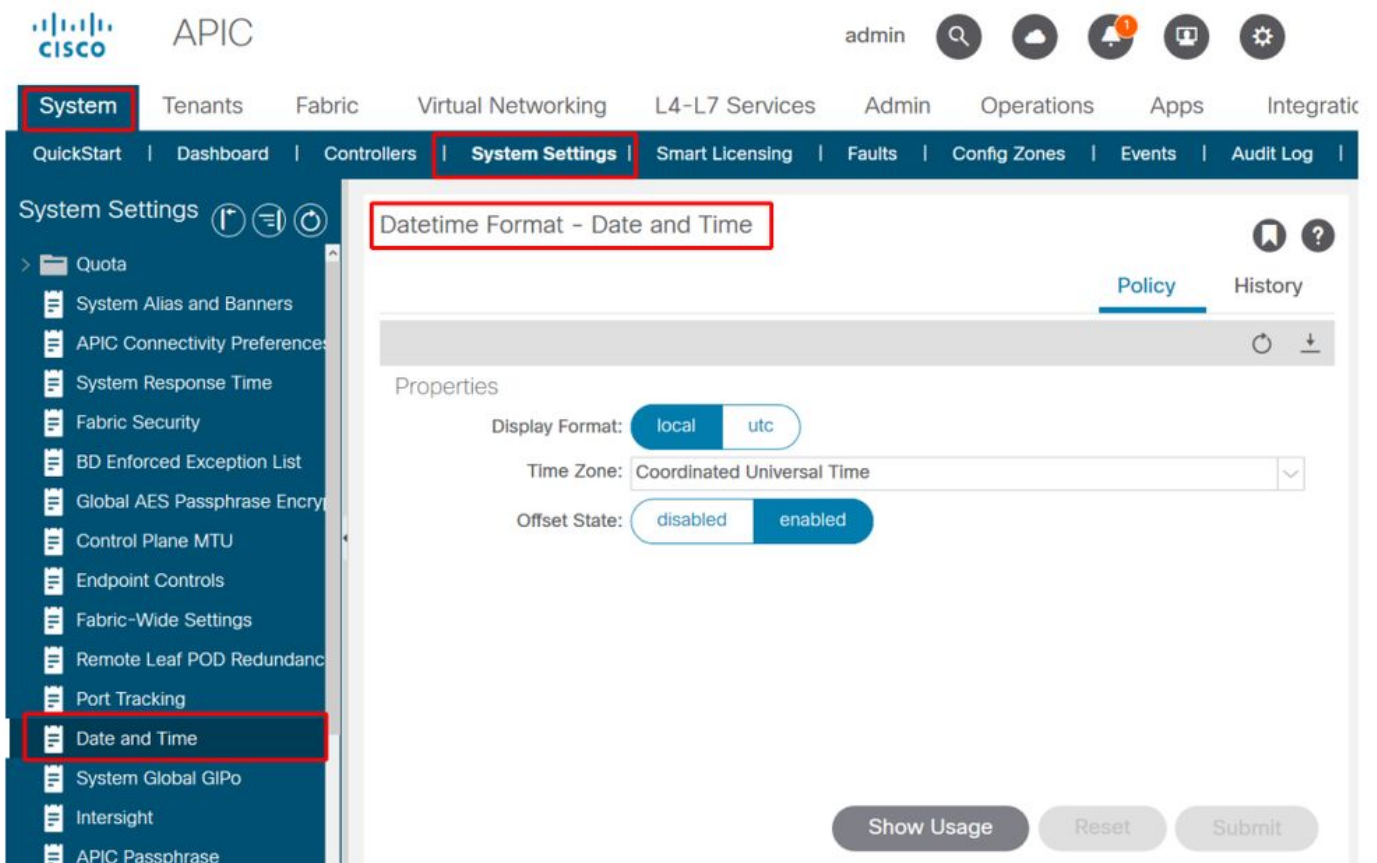
Provider/server NTP in Criteri POD per data e ora



3. Verificare il formato di data e ora in Impostazioni di sistema

La figura seguente mostra un esempio in cui il formato di data e ora è stato impostato su UTC.

Impostazione di data e ora in Impostazioni di sistema



4. Verificare lo stato di sincronizzazione operativo del provider NTP per tutti i nodi

Come illustrato nella figura seguente, nella colonna Stato sincronizzazione dovrebbe essere visualizzato 'Sincronizzato con server NTP remoto'. Tenere presente che la corretta convergenza dello stato di sincronizzazione con il server NTP remoto può richiedere alcuni minuti. stato.

Stato sincronizzazione provider/server NTP

The screenshot shows the Cisco APIC interface. The 'Fabric' tab is selected, and the 'NTP Server 10.48.37.151' is highlighted in the left sidebar. The main content area shows a table of providers for the NTP server 10.48.37.151. The 'Operational' and 'Sync Status' columns are highlighted. The 'Sync Status' column shows 'Synced to Remote NTP Server' for all listed providers.

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

In alternativa, è possibile usare i metodi CLI sugli APIC e sugli switch per verificare la corretta sincronizzazione dell'ora sul server NTP.

APIC - CLI NX-OS

La colonna 'refld' seguente mostra i server NTP la prossima volta che avranno origine, a seconda dello strato.

```

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

Utilizzare il comando 'show ntp peers' per verificare che la configurazione del provider NTP sia stata inserita correttamente nello switch.

```
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
```

Il carattere '*' è essenziale in quanto determina se il server NTP viene effettivamente utilizzato per la sincronizzazione.

Verificare il numero di pacchetti inviati/ricevuti nel comando seguente per assicurarsi che i nodi ACI siano raggiungibili dal server NTP.

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

criterio BGP Route Reflector

Una struttura ACI utilizza BGP (MP-BGP) multiprotocollo e, più specificamente, VPNv4 iBGP tra nodi foglia e spine per scambiare le route dei tenant ricevute dai router esterni (connessi su L3Out). Per evitare una topologia peer iBGP con rete completa, i nodi della spine riflettono i prefissi VPNv4 ricevuti da una foglia ad altri nodi foglia nella struttura.

Senza la policy BGP Route Reflector (BGP RR), non verrà creata alcuna istanza BGP sugli switch e le sessioni BGP VPNv4 non verranno stabilite. In un'installazione multi-pod, ogni pod richiede almeno una spine configurata come RR BGP e sostanzialmente più di una per la ridondanza.

Di conseguenza, la policy BGP RR è un elemento essenziale di configurazione in ogni fabric ACI. La policy BGP RR contiene anche l'ASN che ACI Fabric utilizza per il processo BGP su ciascuno switch.

Flusso di lavoro di risoluzione dei problemi

1. Verificare se per il criterio RR BGP è configurato un ASN e almeno un dorso

L'esempio che segue si riferisce a un'installazione di un singolo Pod.

Criterio BGP Route Reflector in Impostazioni di sistema

The screenshot shows the Cisco APIC System Settings interface. 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'. The 'Policy' tab is active, showing the following configuration:

- 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	

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

2. Verificare se la policy BGP RR è applicata nel gruppo Pod Policy

Applicare un criterio BGP RR predefinito nel gruppo Pod Policy. Anche se la voce è vuota, la policy BGP RR predefinita verrà applicata come parte del Pod Policy Group.

Policy BGP Route Reflector applicata nel gruppo di criteri 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. Verificare se il gruppo di criteri POD viene applicato sotto il profilo POD

Gruppo di criteri POD applicato sotto il profilo POD

4. Accedere a un dorso e verificare se il processo BGP è in esecuzione con le sessioni peer VPN4 stabilite

```
spinel1# 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
```

Come mostrato sopra, MP-BGP tra nodi foglia e spine trasporta solo le famiglie di indirizzi VPNv4 e VPNv6. La famiglia di indirizzi IPv4 viene utilizzata in MP-BGP solo sui nodi foglia.

Le sessioni VPNv4 e VPNv6 BGP tra i nodi spine e foglia possono essere osservate facilmente utilizzando il comando seguente.

```
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

Osservare la colonna Su/Giù dell'output precedente. Deve elencare una durata che indica l'ora in cui è stata stabilita la sessione BGP. Si noti inoltre che nella colonna 'PfxRcd' dell'esempio viene visualizzato 0 per ogni peer BGP VPNv4/VPNv6, in quanto per questo fabric ACI non sono ancora configurati L3Out e pertanto non esistono route/prefissi esterni che siano scambi tra nodi foglia e dorso.

5. Accedere a una foglia e verificare se il processo BGP è in esecuzione con le sessioni peer VPN4 stabilite

```
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

Gli output del comando sopra riportati mostrano una quantità di sessioni BGP VPNv4 uguale al numero di nodi spine presenti nell'infrastruttura ACI. Questo differisce dai nodi della spine perché stabiliscono sessioni per ogni foglia e gli altri nodi della spine riflettore di instradamento.

SNMP

È importante chiarire fin dall'inizio quale sottoinsieme specifico di funzioni SNMP viene trattato in questa sezione. Le funzioni SNMP in un fabric ACI si riferiscono alla funzione SNMP Walk o alla funzione SNMP Trap. La distinzione importante qui è che SNMP Walk gestisce i flussi di traffico SNMP **in entrata** sulla porta UDP 161, mentre SNMP Trap gestisce i flussi di traffico SNMP **in uscita** con un server Trap SNMP in ascolto sulla porta UDP 162.

Il traffico di gestione in ingresso sui nodi ACI richiede che gli EPG di gestione dei nodi (in-band o out-of-band) forniscano i contratti necessari per consentire il flusso del traffico. Pertanto, ciò si applica anche ai flussi di traffico SNMP in entrata.

In questa sezione verranno descritti i flussi di traffico SNMP in entrata (SNMP Walk) nei nodi ACI (APIC e switch). Non includerà i flussi di traffico SNMP in uscita (trap SNMP), in quanto amplierebbe l'ambito di questa sezione in Criteri di monitoraggio e dipendenze dei criteri di monitoraggio (ad esempio ambito dei criteri di monitoraggio, pacchetti di monitoraggio e così via).

Questa sezione non illustra inoltre quali MIB SNMP sono supportati da ACI. Tali informazioni sono disponibili sul sito Web Cisco CCO al seguente collegamento:

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

Flusso di lavoro di risoluzione dei problemi

1. Criterio POD SNMP — Verifica della configurazione di Criteri di gruppo client

Verificare che almeno un singolo client SNMP sia configurato come parte dei Criteri di gruppo del client come indicato nelle schermate seguenti.

Criteri POD — Criteri SNMP — Criteri di gruppo client

The screenshot displays the Cisco ACI GUI configuration page 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)

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

Criteri POD — Criteri SNMP — Criteri di gruppo 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 — Verifica della configurazione di almeno un criterio comunitario

Pod Policies — SNMP Policy — Community Policies

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. Under Fabric, the path is Inventory > **Fabric Policies** > Access Policies.
- Left Panel:** Policies > Pod > SNMP > default (highlighted).
- Main Content Area:** SNMP Policy - default. The 'Policy' tab is active. The 'Community Policies' section contains a table with one entry: my-secret-SNMP-community.

Name	Description
my-secret-SNMP-community	

Trap Forward Servers:

IP Address	Port
No items have been found. <small>Click Actions to create a new item</small>	

Buttons: Show Usage, Reset, Submit

3. SNMP Pod Policy — Verifica che lo stato dell'amministratore sia impostato su 'Enabled'

The screenshot shows the Cisco APIC interface for configuring an SNMP Policy. The navigation menu on the left is expanded to 'Policies' > 'Pod' > 'SNMP' > 'default'. The main content area displays the configuration for 'SNMP Policy - default'. The 'Admin State' is set to 'Enabled'. Below the configuration, a table lists the Client Group Policies:

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

4. Tenant di gestione: verificare se l'OOB EPG fornisce un contratto OOB che consente l'accesso alla porta UDP 161

L'EPG OOB controlla la connettività nell'APIC e le porte di gestione OOB dello switch. Influisce quindi su tutti i flussi di traffico in entrata nelle porte OOB.

Accertarsi che il contratto fornito includa tutti i servizi di gestione necessari invece di SNMP. Ad esempio: deve includere almeno SSH (porta TCP 22). Senza questa opzione, non è possibile accedere agli switch con SSH. Si noti che questo non si applica agli APIC poiché dispongono di un meccanismo che consente di bloccare completamente gli utenti SSH, HTTP e HTTPS.

APIC

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. Tenant di gestione: verificare se il contratto OOB è presente e dispone di un filtro che consente la porta UDP 161

Tenant di gestione — OOB EPG — Contratto OOB fornito

APIC

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

Nella figura seguente, non è obbligatorio consentire solo la porta 161 UDP. Un contratto che dispone di un filtro che consente in qualsiasi modo la porta 161 UDP è corretto. Può anche essere un oggetto del contratto con il filtro predefinito del tenant comune. Nell'esempio riportato, per motivi di chiarezza, è stato configurato un filtro specifico solo per la porta UDP 161.

The screenshot shows the Cisco APIC interface for configuring a filter. The navigation menu on the left is expanded to show the 'Filters' section under 'Contracts'. The filter configuration page is titled 'Filter - snmp-walk-filter'. The configuration details are as follows:

- Name: snmp-walk-filter
- Alias: (empty)
- Description: optional
- Tags: (empty)
- Global Alias: (empty)
- Entries:

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. Tenant di gestione: verificare se è presente un profilo di istanza della rete di gestione esterna con una subnet valida che utilizza il contratto OOB

Il profilo dell'istanza della rete di gestione esterna (ExtMgmtNetInstP) rappresenta le origini esterne definite dalle 'Subnet' in essa contenute che devono utilizzare i servizi raggiungibili tramite l'EPG OOB. Pertanto, ExtMgmtNetInstP utilizza lo stesso contratto OOB fornito dall'EPG OOB. Questo è il contratto che consente la porta UDP 161. Inoltre, ExtMgmtNetInstP specifica anche gli intervalli di subnet consentiti che possono utilizzare i servizi forniti da OOB EPG.

Tenant di gestione: ExtMgmtNetInstP con contratto OOB e subnet utilizzati

Come illustrato nella figura precedente, è necessaria una notazione di subnet basata su CIDR. Nella figura viene illustrata una subnet /24 specifica. Il requisito è che le voci della subnet coprano le voci del client SNMP come configurato in SNMP Pod Policy (fare riferimento alla figura Pod Policies — SNMP Policy — Client Group Policies).

Come accennato in precedenza, fare attenzione a includere tutte le subnet esterne necessarie per evitare che altri servizi di gestione necessari vengano bloccati.

7. Accedere a uno switch ed eseguire un dump tcp per verificare se i pacchetti SNMP Walk — porta UDP 161 — sono rispettati

Se i pacchetti SNMP Walk entrano in uno switch attraverso la porta OOB, significa che tutti i criteri/parametri SNMP e OOB necessari sono stati configurati correttamente. È un metodo di verifica appropriato.

Tcpdump sui nodi foglia sfrutta la shell Linux e i dispositivi di rete Linux. Pertanto, è necessario acquisire i pacchetti sull'interfaccia 'eth0' come mostrato nell'esempio che segue. Nell'esempio, un client SNMP sta eseguendo una richiesta Get SNMP su 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
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).