Risoluzione dei problemi relativi all'NTP in un'infrastruttura Cisco ACI

Introduzione

In questo documento viene descritto come verificare, risolvere e risolvere i problemi relativi al protocollo NTP (Network Time Protocol) in un'infrastruttura Cisco ACI. Vengono descritti il modello di policy NTP, la verifica della configurazione, i comandi di verifica operativa, un flusso di lavoro di valutazione per i sintomi NTP comuni e gli scenari dettagliati di risoluzione dei problemi.

Premesse

Il materiale di questo documento è stato estratto dalla guida alla risoluzione dei problemi di ACI Management and Core Services — Pod Policies, dalla guida alla configurazione di base di Cisco APIC, versione 6.1(x) — Provisioning Core ACI Fabric Services e dalla guida alla progettazione di Cisco ACI.

Panoramica

La sincronizzazione dell'ora è una funzionalità cruciale in un fabric ACI da cui dipendono le attività di monitoraggio, operative e risoluzione dei problemi. La sincronizzazione dell'orologio garantisce la corretta analisi dei flussi di traffico, la correlazione dei timestamp di debug e di errore su più nodi di fabric e l'utilizzo completo della funzionalità del contatore atomico da cui dipendono i punteggi di integrità dell'applicazione. Una configurazione NTP inesistente o non corretta non attiva necessariamente un errore o un livello di integrità basso, pertanto è importante configurare la sincronizzazione dell'ora nelle prime fasi dell'implementazione dell'infrastruttura.

Modello di criteri NTP in ACI

L'NTP in ACI è gestito attraverso una catena di quattro oggetti di policy:

1. Criterio data e ora (`datetimePol`): definisce la configurazione NTP, inclusi lo stato amministrativo, lo stato di autenticazione, lo stato del server e la modalità master. Disponibile in Fabric > Fabric Policies > Policies > Pod > Date and Time (Fabric > Criteri fabric > Criteri > Pod > Data e ora).

2. Provider NTP (`datetimeNtpProv`): definisce le singole voci del server NTP (provider) all'interno di una policy di data e ora, inclusi l'IP/FQDN del server, la selezione EPG di gestione (fuori banda o in banda), il flag preferito e gli intervalli di polling.
3. Pod Policy Group (`fabricPodPGrp`): fa riferimento alla policy su data e ora insieme ad altre policy a livello di pod (BGP RR, SNMP, ecc.). Disponibile in Fabric > Fabric Policies > Pods > Policy Groups (Infrastruttura > Criteri fabric > Bacchetti > Gruppi di criteri).
4. Pod Profile (`fabricPodP`) - associa un Pod Policy Group a un selettore di pod. Disponibile in Fabric > Fabric Policies > Pods > Profiles.

Tutti e quattro i collegamenti in questa catena devono essere configurati per NTP da applicare ai nodi fabric. Se un collegamento è interrotto, la configurazione del provider NTP non verrà trasferita sugli switch.

Prerequisiti

- È necessario completare l'individuazione dell'infrastruttura.
- Gli indirizzi di gestione dei nodi (OOB o in banda) devono essere assegnati a tutti gli APIC e gli switch sotto il tenant mgmt.
- Per l'NTP fuori banda, l'EPG di gestione OOB deve consentire la porta UDP 123.
- Per il NTP in banda, è necessario configurare un EPG di gestione in banda con contratti appropriati e raggiungibilità al server NTP. Gli indirizzi IP in-band non sono raggiungibili dall'esterno dell'infrastruttura senza criteri aggiuntivi.

Autenticazione NTP

ACI supporta tre schemi di autenticazione NTP: MD5, SHA-1 e AES128-CMAC. AES128-CMAC è stato introdotto nella versione APIC 6.1(1) ed è lo schema consigliato, in quanto MD5 è considerato debole e non sicuro. Quando la modalità FIPS è abilitata, sono supportati solo AES128-CMAC e SHA-1.

Funzionalità server NTP

Gli switch foglia ACI possono fungere da server NTP per i client downstream (ad esempio, server collegati al fabric). Questa funzionalità è disabilitata per impostazione predefinita e deve essere abilitata in modo esplicito tramite l'opzione Stato server nei criteri di data e ora. Se abilitato, i client possono utilizzare l'indirizzo IP dello switch foglia in banda, fuori banda, SVI di dominio bridge o L3Out come indirizzo del server NTP.

Nota: Gli switch fabric non devono essere sincronizzati con altri switch dello stesso fabric. Gli switch fabric devono sempre essere sincronizzati con i server NTP esterni.

Verifica della configurazione

Prima di risolvere i problemi relativi allo stato operativo NTP, verificare che la catena di configurazione sia stata completata. La configurazione errata è la causa principale più comune dei problemi NTP in ACI.

Passaggio 1: Verifica indirizzi di gestione dei nodi

Passare a Tenant > mgmt > Indirizzi di gestione dei nodi (per l'assegnazione statica) o EPG di gestione dei nodi (per i gruppi di connettività).

Confermare che a ogni APIC e nodo dello switch sia assegnato un indirizzo IP di gestione. I nodi senza indirizzi di gestione non possono comunicare con il server NTP.

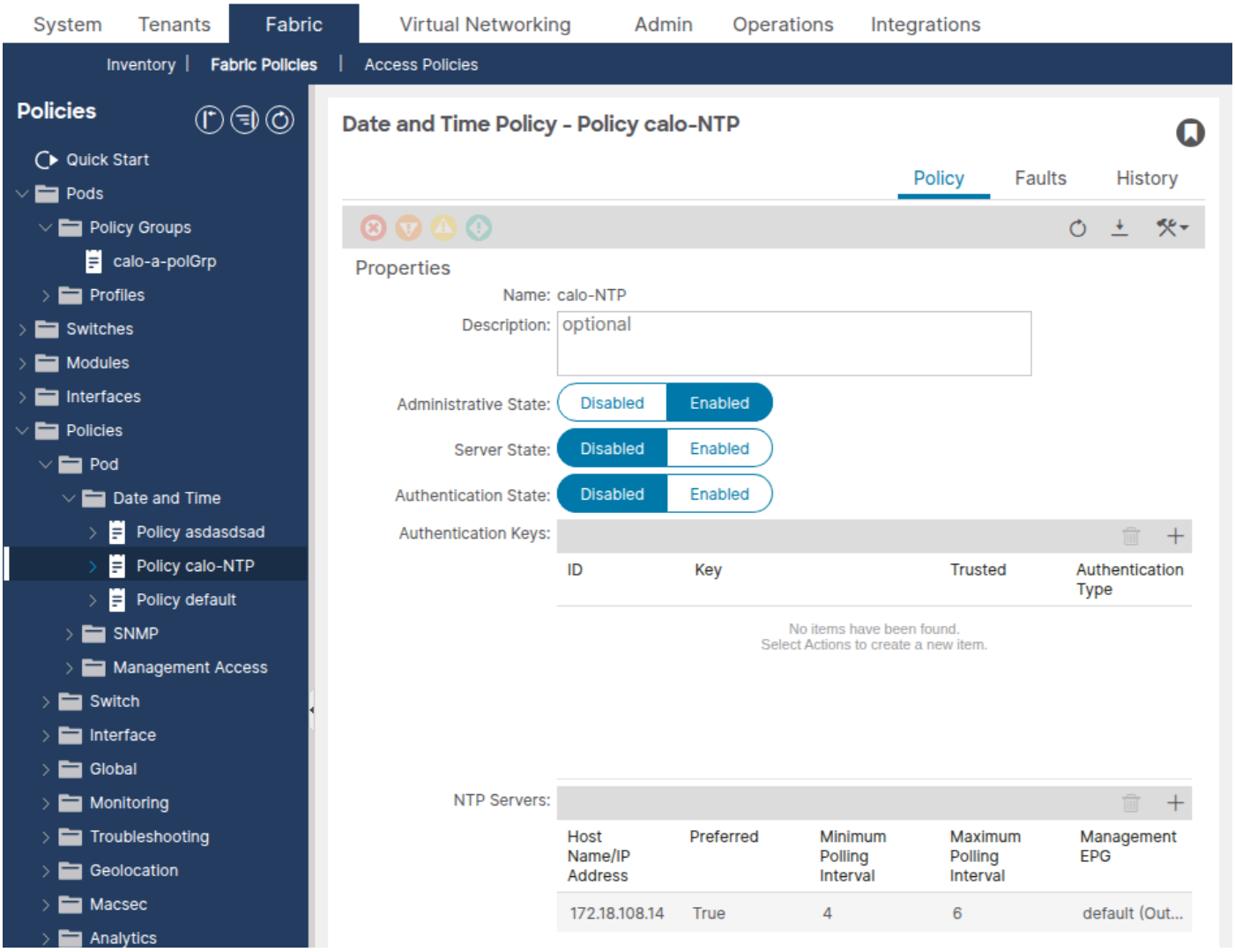
In alternativa, eseguire una query sull'API:

<#root>

```
apic1#

moquery -c mgmtRsOoBStNode
```

Passaggio 2: Verificare che i criteri di data e ora dispongano di un provider NTP

Selezionare Fabric > Fabric Policies > Policies > Pod > Date and Time > [Your Policy].



Verificare che sia configurato almeno un provider NTP (server). Se esistono più provider, contrassegnarne almeno uno come Preferito.

Verificare il provider NTP tramite l'API:

<#root>

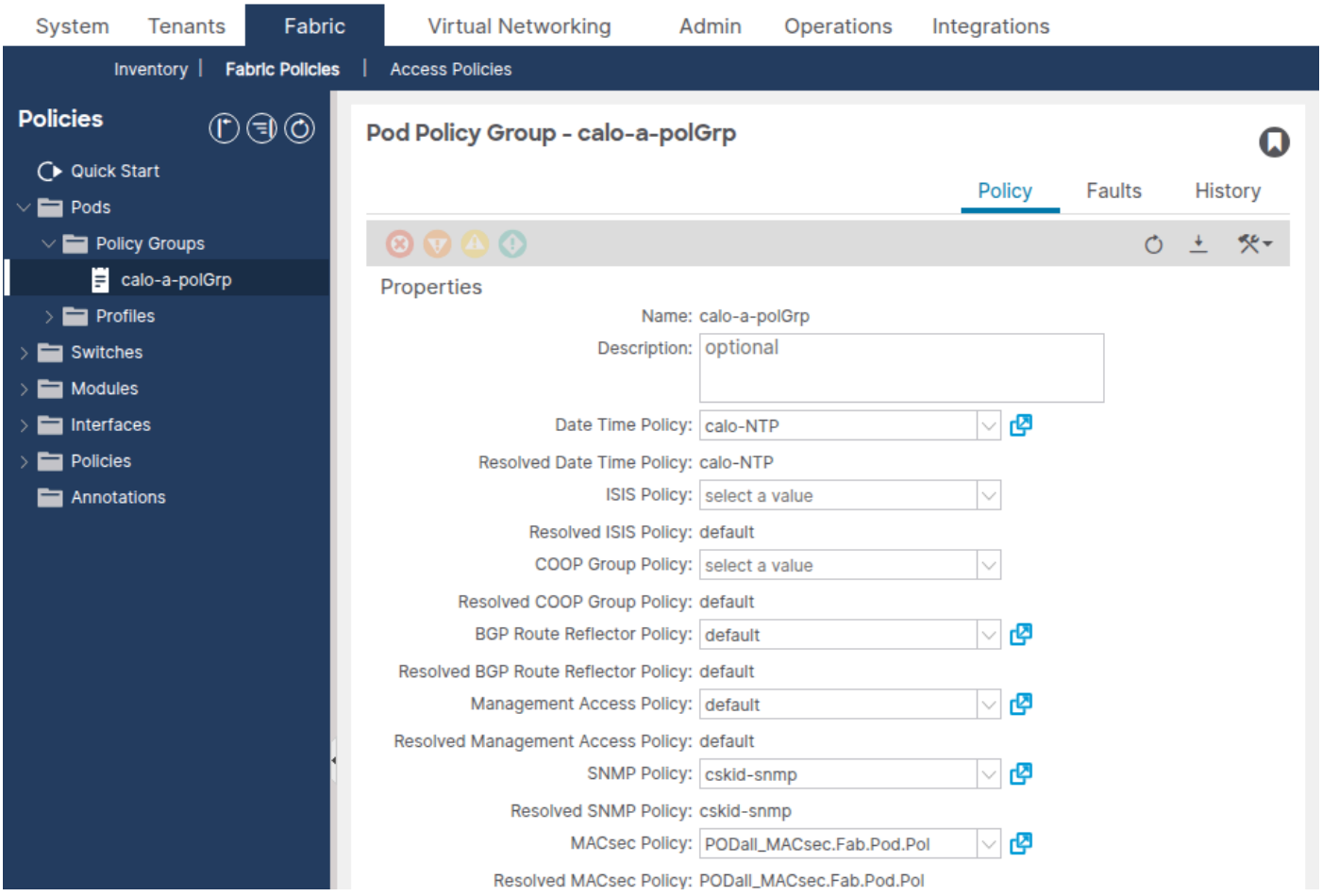
```
apic1#

moquery -c datetimeNtpProv

# datetimeNtpProv
dn           : uni/fabric/time-NTP-Policy/ntpprov-10.1.1.100
name         : 10.1.1.100
preferred    : yes                    <--- at least one should be "yes"
epgDn        : uni/tn-mgmt/mgmtp-default/oob-default   <--- management EPG
minPoll      : 4
maxPoll      : 6
keyId        : 0
```

Configurazioni errate comuni

- Nessun provider NTP configurato. I criteri di data e ora esistono ma non hanno provider. Il criterio verrà applicato ma i nodi non avranno alcun server NTP da sincronizzare.
- EPG di gestione errato selezionato: il provider NTP fa riferimento all'EPG fuori banda, ma il server NTP è raggiungibile solo tramite in banda (o viceversa). Verificare quale gestione EPG fornisce raggiungibilità al server NTP.
- FQDN e IP dello stesso server aggiunti come provider separati: genera un errore IP duplicato. Eliminare la voce duplicata.
- Provider basato su FQDN senza criteri DNS: se si utilizza un nome host per il provider NTP, verificare che siano configurati criteri del servizio DNS e che l'etichetta DNS appropriata sia applicata al VRF di gestione.

Passaggio 3: Verificare che il gruppo di criteri POD faccia riferimento ai criteri di data e ora

Selezionare Fabric > Fabric Policies > Pods > Policy Groups > [Gruppo di criteri del pod].



Verificare che il campo Criterio data/ora faccia riferimento al criterio di data e ora corretto.

<#root>

apic1#

moquery -c fabricPodPGrp -f 'fabricPodPGrp.name=="default"'

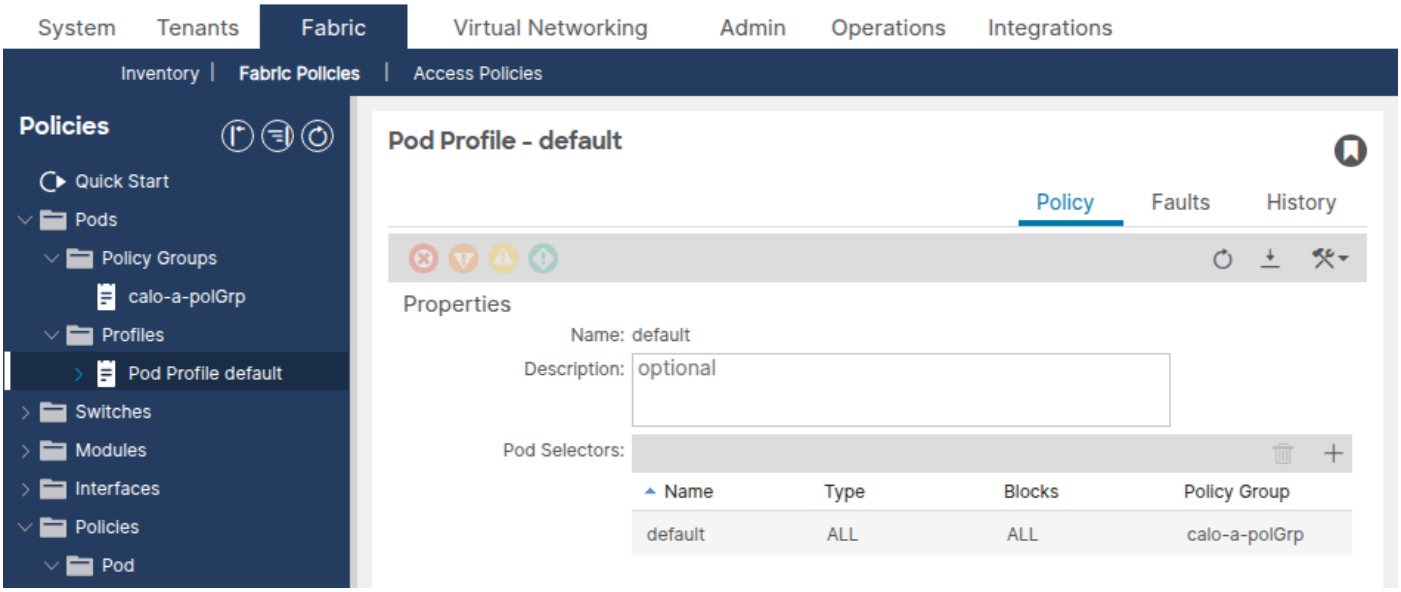
Cercare l'attributo `datetimePolName` o la relazione `fabricRsTimePol` associata.

Configurazioni errate comuni

- Il gruppo di criteri POD fa riferimento al criterio di data e ora errato. Se esistono più criteri di data e ora (ad esempio, "predefinito" e uno personalizzato), verificare che il gruppo di criteri POD faccia riferimento al criterio desiderato.
- Gruppo di criteri POD non creato: al gruppo di criteri POD predefinito potrebbero non essere associati i criteri di data e ora. Verifica sempre.

Passaggio 4: Verifica dei riferimenti del profilo del dispositivo di scorrimento nel gruppo di criteri del dispositivo di scorrimento

Passare a Fabric > Fabric Policies > Pods > Profiles > [Profilo del tuo dispositivo] (Fabric > Fabric Policies > Pods > Profiles > [Profilo del tuo dispositivo].



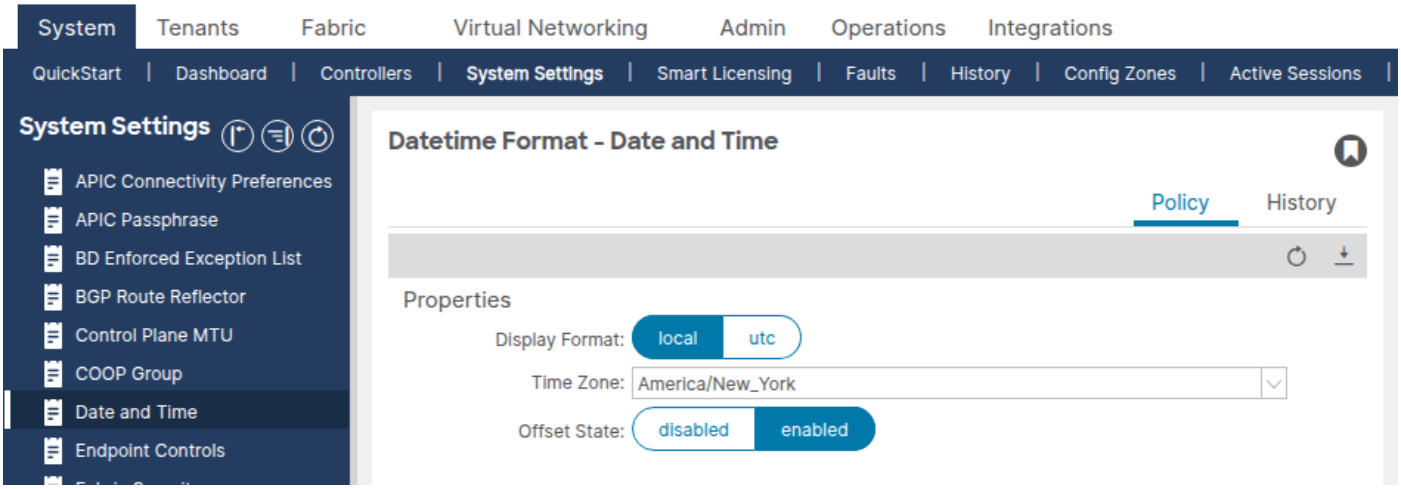
Verificare che il campo Gruppo di criteri infrastruttura faccia riferimento al gruppo di criteri POD corretto.

Configurazioni errate comuni

- Il profilo del pod fa riferimento al gruppo di criteri del pod sbagliato — specialmente in ambienti con più pod, ciascun profilo del pod deve fare riferimento al gruppo di criteri del pod corretto.

Passaggio 5: Verifica formato data e ora

Selezionare Sistema > Impostazioni di sistema > Data e ora.



Verificare che il formato di visualizzazione (locale o UTC) e il fuso orario siano impostati come previsto. Questa impostazione è un criterio di formattazione data/ora predefinito distinto che non può essere eliminato o duplicato.

Verifica operativa

Dopo aver verificato che la catena di configurazione sia corretta, utilizzare i comandi seguenti per verificare il funzionamento di NTP in fase di esecuzione.

Verifica APIC

mostra ntpq

Questo comando mostra lo stato di sincronizzazione NTP su tutti gli APIC. Il simbolo * indica che il server è selezionato per la sincronizzazione.

<#root>

```
apic1#

show ntpq

 nodeid     remote                          refid                           st        t   when      pol
 ------  -  ------------------------------  ------------------------------  --------  --  --------  ---
 1       *  ntp.example.com                 .GPS.                           1         u   20        64
 2       *  ntp.example.com                 .GPS.                           1         u   6         64
 3       *  ntp.example.com                 .GPS.                           1         u   27        64
```

Aspetto positivo:

- Tutti gli APIC vengono visualizzati con `*` (selezionati per la sincronizzazione) accanto al server remoto.
- `reach` è `377` (ottale), il che indica che gli ultimi 8 sondaggi hanno avuto successo.
- `st` (strato) è compreso tra 1 e 15. Strato 16 indica che il server non è sincronizzato.
- `l'offset` è basso (generalmente meno di 100 ms in ambienti sani).

Aspetto negativo:

- No `*` accanto a qualsiasi server - nessun server è selezionato per la sincronizzazione.
- `reach` è `0` — non è stata ricevuta alcuna risposta NTP.
- `st` è `16`: il server NTP non è sincronizzato con la relativa origine del tempo upstream.
- `offset` è estremamente grande (migliaia di millisecondi) — l'orologio viene spostato in modo significativo.

show clock

<#root>

```
apic1#

show clock

Time : 11:24:18.391 UTC-04:00 Tue Apr 07 2026
```

Verificare che l'ora sia corretta. Confrontare con il tempo previsto per rilevare la deviazione dell'orologio.

APIC Bash (alternativa)

<#root>

apic1#

bash

admin@apic1:~>

date

Tue Apr 7 11:24:45 EDT 2026

Verifica commutatore (foglia/dorso)

mostra peer ntp

Verificare che il provider NTP sia stato inserito nello switch.

<#root>

leaf1#

show ntp peers

```
-------------------------------------------------------------------------------
  Peer IP Address                 Serv/Peer Prefer KeyId   Vrf
-------------------------------------------------------------------------------
  10.1.1.100                      Server    yes    None    management
```

Aspetto positivo: L'indirizzo IP o il nome host del server NTP viene visualizzato con `Serv/Peer` = `Server` e il VRF corretto (in genere `gestione` per OOB).

Aspetto negativo: Nessun peer elencato oppure l'indirizzo IP del server NTP non corrisponde al provider configurato. In genere indica che i criteri di data e ora non sono stati applicati tramite la catena di profili del gruppo di criteri POD/POD.

show ntp peer-status

Verificare che il server NTP sia selezionato per la sincronizzazione.

<#root>

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
-------------------------------------------------------------------------------
*10.1.1.100                               0.0.0.0         1  64   377   0.000  management
```

Il carattere `*` è essenziale: conferma che il server NTP è utilizzato per la sincronizzazione.

Aspetto negativo:

- No `*` accanto al server — lo switch non è sincronizzato con il server.
- `reach` è `0` — non è stata ricevuta alcuna risposta NTP. Ciò indica un problema di raggiungibilità.
- `st` è `16`: il server NTP non è sincronizzato e non può fornire un'ora valida.

show ntp statistics peer ipaddr

Verificare lo scambio di pacchetti NTP per confermare la raggiungibilità. Sostituire l'indirizzo IP con l'indirizzo del provider NTP dello switch interessato.

<#root>

```
leaf1#

show ntp statistics peer ipaddr 10.1.1.100


...
packets sent:     9256
packets received:   9256
...
```

Aspetto positivo: `i pacchetti inviati` e `i pacchetti ricevuti` sono all'incirca uguali e in aumento.

Aspetto negativo: `i pacchetti inviati` aumentano, ma `i pacchetti ricevuti` sono pari a `0` o aumentano a malapena — le risposte NTP non raggiungono lo switch.

show clock

<#root>

```
leaf1#

show clock

11:24:24.121066 EDT Tue Apr 07 2026
```

Verifica GUI

Selezionare Fabric > Fabric Policies > Policies > Pod > Date and Time > [Your Policy] > [Provider NTP].

Nella colonna Stato sincronizzazione dovrebbe essere visualizzato Sincronizzato con il server NTP remoto per tutti i nodi. La convergenza dello stato di sincronizzazione dopo la distribuzione iniziale può richiedere alcuni minuti.

Verifica API

Eseguire una query sulla classe `datetimeNtpq` per controllare la sincronizzazione NTP tra tutti gli APIC:

<#root>

```
apic1#

moquery -c datetimeNtpq

# datetimeNtpq
dn        : topology/pod-1/node-1/sys/ntpq-ntp.example.com
remote    : ntp.example.com
tally     : *                           <--- selected for sync
stratum   : 1
reach     : 377                         <--- all recent polls successful
offset    : +0.102
delay     : 0.213
jitter    : 0.005
refid     : .GPS.
```

Flusso di lavoro di risoluzione dei problemi

Utilizzare questa struttura decisionale quando viene segnalato un problema NTP su un nodo ACI.

Passaggio 1: I peer NTP sono configurati sullo switch?

Accedere allo switch interessato ed eseguire:

<#root>

leaf1#

show ntp peers

- Nessun peer elencato → il criterio di data e ora non è stato applicato a questo nodo. Andare allo scenario 1: Provider NTP non inserito nello switch.
- Peer elencati → passare al punto 2.

Passaggio 2: Il server NTP è selezionato per la sincronizzazione?

<#root>

leaf1#

show ntp peer-status

- `*` presente → NTP sta sincronizzando. Se l'ora non è corretta, passare allo scenario 5: Offset grande/deriva orologio.
- No `*` presente → passare al punto 3.

Passaggio 3: Il valore di portata è zero?

Controllare la colonna `reach` in `show ntp peer-status`.

- **`reach` = `0`** → nessuna risposta dal server NTP. Andare allo scenario 2: Server NTP non raggiungibile.
- **`reach` > `0`** ma non `*` → sono in arrivo risposte ma la sincronizzazione non è stabilita. Controllare lo strato — andare al passo 4.

Passaggio 4: Il valore dello strato è 16?

- Stratum = 16 → il server NTP non è sincronizzato con la propria origine upstream. Andare allo scenario 3: Server NTP non sincronizzato (Stratum 16).
- Stratum 1-15 ma nessuna sincronizzazione → andare allo Scenario 4: Autenticazione NTP non corrispondente.

Scenari comuni di risoluzione dei problemi

Scenario 1: Provider NTP non inserito nello switch

Sintomo: `show ntp peers` on the switch non restituisce voci.

Controllo configurazione:

1. Verificare che per i criteri di data e ora sia configurato almeno un provider NTP.
2. Verificare che il gruppo di criteri POD faccia riferimento al criterio di data e ora corretto.
3. Verificare che il Profilo del Pod faccia riferimento al Gruppo di criteri del Pod corretto.
4. Verificare che al nodo sia assegnato un indirizzo IP di gestione nel tenant mgmt.

Causa principale: Uno dei quattro link nella catena di policy (Date and Time Policy → NTP Provider → Pod Policy Group → Pod Profile) è rotto. La causa più comune è la mancata associazione del gruppo di criteri per i pod al profilo dei pod o la mancata selezione dei criteri di data e ora nel gruppo di criteri per i pod.

Soluzione: Completare il collegamento mancante nella catena di criteri. Verificare che il profilo del pod per il pod interessato faccia riferimento a un gruppo di criteri del pod contenente i criteri di data e ora corretti. Dopo l'applicazione, la configurazione del provider NTP verrà inviata agli switch entro pochi minuti.

Scenario 2: Server NTP non raggiungibile

Sintomo: `show ntp peer-status` mostra `reach = 0`. `show ntp statistics peer ipaddr 10.1.1.100` mostra `i pacchetti ricevuti = 0`.

Controllo configurazione: Verificare che il provider NTP sia associato all'EPG (OOB o in-band) di gestione corretto. Se si utilizza OOB, verificare che i contratti OOB consentano l'uso della porta UDP 123.

Controllo operativo:

1. Eseguire il ping tra il server NTP e lo switch interessato utilizzando il VRF di gestione:
   <#root>

   ```
   leaf1#
   ```

   ping 10.1.1.100 vrf management

2. Eseguire un dump TCP sullo switch per verificare se i pacchetti NTP stanno arrivando e partendo:
   <#root>

   ```
   leaf1#
   ```

   tcpdump -n -i eth0 dst port 123

   ```
   tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
   listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
   16:49:01.431624 IP 10.1.20.23.123 > 10.1.1.100.123: NTPv4, Client, length 48
   16:49:01.440303 IP 10.1.1.100.123 > 10.1.20.23.123: NTPv4, Server, length 48
   ```

Causa principale: In genere, una delle seguenti opzioni:

- Allo switch non è assegnato un indirizzo IP di gestione.
- Il gateway predefinito per il VRF di gestione è mancante o non corretto.
- Un firewall blocca la porta UDP 123 tra lo switch e il server NTP.
- Il contratto OOB non consente l'uso della porta UDP 123.
- Il provider NTP fa riferimento all'EPG di gestione errato (ad esempio, OOB selezionato ma raggiungibile solo in banda).

Soluzione: Risolvere il problema relativo alla raggiungibilità. Assegnare un indirizzo di gestione se mancante, correggere il gateway predefinito, aggiornare le regole del firewall o correggere la selezione EPG di gestione sul provider NTP.

Scenario 3: Server NTP non sincronizzato (Stratum 16)

Sintomo: `show ntp peer-status` mostra lo strato (`st`) = `16`. Lo switch non verrà sincronizzato con un server dello strato 16.

Controllo operativo: Accedere al server NTP o eseguire una query su di esso da un host esterno per verificare che sia sincronizzato con la propria origine temporale upstream.

Causa principale: Il server NTP stesso ha perso la sincronizzazione con il proprio orologio di riferimento upstream. Un server con strato 16 indica che non dispone di un'origine tempo affidabile.

Soluzione: Correggere il server NTP. Si trova all'esterno dell'infrastruttura ACI: controllare la configurazione del server NTP e la relativa origine del tempo upstream. Se il server NTP non può essere corretto immediatamente, configurare un provider NTP alternativo nei criteri di data e ora.

Scenario 4: Autenticazione NTP non corrispondente

Sintomo: `show ntp peer-status` mostra `reach` > `0` e lo strato è valido, ma non `*` viene visualizzato. Il server NTP risponde, ma lo switch non accetta la risposta.

Controllo configurazione:

1. Verificare se il server NTP richiede l'autenticazione.
2. Se è necessaria l'autenticazione, verificare che lo stato di autenticazione dei criteri di data e ora sia impostato su Abilitato.
3. Verificare l'ID della chiave di autenticazione, il valore della chiave e l'algoritmo (MD5, SHA-1 o AES128-CMAC) corrispondenti tra l'infrastruttura ACI e il server NTP.
4. Verificare che la chiave sia contrassegnata come attendibile nella tabella Chiavi di autenticazione client NTP.

Causa principale: La chiave di autenticazione, l'algoritmo o l'ID della chiave non corrisponde tra ACI e il server NTP, pertanto lo switch rifiuta la risposta NTP come non autenticata.

Soluzione: Allineare la configurazione di autenticazione. Verificare che ID chiave, valore chiave e algoritmo siano configurati in modo identico sia su ACI che sul server NTP. AES128-CMAC è consigliato per APIC versione 6.1(1) e successive.


Nota: Quando la modalità FIPS è attivata, sono supportati solo gli schemi di autenticazione AES128-CMAC e SHA-1. MD5 non funziona in modalità FIPS.

Scenario 5: Offset grande/deriva orologio

Sintomo: Lo switch sembra essere sincronizzato (* presente, reach = 377), ma il valore di `offset` in `show ntp peer-status` o `show ntpq` è molto grande (centinaia o migliaia di millisecondi), o l'orologio è visibilmente errato.

Controllo operativo:

<#root>

```
apic1#
```

```
show ntpq
```

Controllare la colonna `offset`. Un offset integro è in genere inferiore a 100 ms.

Causa principale: L'orologio si è spostato in modo significativo prima che fosse stabilita la sincronizzazione NTP o che l'orologio hardware (RTC) fosse stato reimpostato durante un riavvio (ad esempio, a causa di una batteria CMOS scarica). La tecnologia NTP corregge l'orologio gradualmente tramite il dorso, che può richiedere tempo per grandi offset.

Soluzione: Se l'offset è molto grande e NTP è in fase di sincronizzazione attiva, attendere che l'orologio converga. L'NTP controlla l'orologio gradualmente, mentre per correggere completamente i grandi offset possono essere necessarie ore. Se l'offset non diminuisce, verificare che il server NTP fornisca un'ora precisa. Se il problema si verifica dopo ogni riavvio, verificare l'orologio hardware (batteria RTC/CMOS) sul nodo interessato.

Scenario 6: Errori APIC in standby con NTP in-band

Sintomo: Quando NTP è configurato per la gestione in banda, vengono generati errori su un APIC in standby correlato a NTP o ai criteri di monitoraggio.

Causa principale: Quando si applica una policy NTP per la gestione in banda, l'APIC in standby richiede anche la configurazione in banda. Senza di esso, i difetti vengono sollevati.

Soluzione: Configurare la gestione in banda anche per l'APIC in standby. In questo modo vengono cancellati i difetti.

Scenario 7: Errore IP duplicato

Sintomo: Un errore IP duplicato viene generato dopo l'aggiunta di provider NTP.

Causa principale: È stato aggiunto un FQDN come provider NTP, quindi l'indirizzo IP risolto di tale FQDN è stato aggiunto come secondo provider NTP. ACI rileva il duplicato.

Soluzione: Eliminare il provider duplicato aggiunto più di recente (la voce dell'indirizzo IP se l'FQDN è stato aggiunto per primo o viceversa). Utilizzare una sola voce per server NTP, ovvero FQDN o indirizzo IP, non entrambi.

Scenario 8: Errore di risoluzione DNS per il provider NTP basato su FQDN

Sintomo: Il provider NTP configurato con un nome host non sta eseguendo la risoluzione. `show ntp peers` non visualizza l'indirizzo IP previsto oppure NTP non è in fase di sincronizzazione.

Controllo configurazione:

1. Verificare che i criteri del servizio DNS siano configurati in Fabric > Criteri fabric > Criteri > Globale > Profili DNS.
2. Verificare che il provider DNS (server DNS) sia raggiungibile dal VRF di gestione.
3. Verificare che l'etichetta DNS appropriata sia configurata per l'istanza VRF in banda o fuori banda dell'EPG di gestione.

Causa principale: Il server DNS non è raggiungibile o non è configurato. La risoluzione dei nomi host per il provider NTP non è riuscita.

Soluzione: Configurare i criteri del servizio DNS, verificare la raggiungibilità del DNS e applicare l'etichetta DNS corretta. In alternativa, utilizzare l'indirizzo IP del server NTP al posto del nome host.

Errori ed eventi correlati

Di seguito sono riportate le condizioni relative all'NTP che possono generare errori in ACI:

- Errore IP duplicato — generato quando un FQDN e l'indirizzo IP dello stesso server NTP vengono entrambi aggiunti come provider. Risoluzione: rimuovere la voce duplicata.
- Errori NTP in banda dell'APIC in standby: generati quando si applica una policy di monitoraggio o NTP per il protocollo in banda, ma l'APIC in standby non dispone di una configurazione in banda.
- Stato di sincronizzazione non convergente: nella GUI viene visualizzato "Non sincronizzato" o uno stato diverso da "Sincronizzato con server NTP remoto" per uno o più nodi. Non si tratta di un codice di errore ma di un indicatore di stato operativo. Seguire il flusso di lavoro di risoluzione dei problemi sopra riportato per eseguire la diagnosi.

Criteri di escalation

Prendere in considerazione l'escalation a Cisco TAC se:

- La catena di configurazione è stata verificata correttamente e il server NTP è raggiungibile (il ping funziona, il dump del tcp mostra le risposte NTP), ma lo switch non viene ancora sincronizzato.

- La sincronizzazione NTP viene persa ripetutamente senza modifiche della configurazione o problemi del server NTP.
- L'output `show ntp peer-status` mostra un comportamento imprevisto, ad esempio lo strato persistente 16 su un server di cui è stata confermata la sincronizzazione esterna.
- L'orologio si sposta in modo significativo tra i riavvii, il che può indicare un problema dell'orologio hardware (RTC).

Quando si applica TAC, fornire i seguenti dati:

- Output di `show ntpq` da tutti gli APIC.
- Output di `show ntp peer`, `show ntp peer-status`, `show ntp statistics peer ipaddr <IP>` e `show clock` da tutti gli switch interessati.
- Output di `moquery -c datetimePol`, `moquery -c datetimeNtpProv` e `moquery -c datetimeNtpq` dall'APIC.
- Supporto tecnico dai nodi interessati.

Riferimenti

- Guida alla configurazione di base di Cisco APIC, versione 6.1(x) — Provisioning dei servizi ACI Fabric di base
- Risoluzione dei problemi relativi alla gestione ACI e ai servizi di base — Criteri per i pod
- Guida alla progettazione di Cisco Application Centric Infrastructure (ACI)

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).