Problemen met NTP oplossen in een Cisco ACI Fabric

Inleiding

In dit document wordt beschreven hoe problemen met het Network Time Protocol (NTP) in een Cisco ACI-fabric kunnen worden geverifieerd, opgelost en opgelost. Het omvat het NTP-beleidsmodel, configuratieverificatie, operationele verificatieopdrachten, een triage-workflow voor veelvoorkomende NTP-symptomen en gedetailleerde scenario's voor probleemoplossing.

Achtergrondinformatie

Het materiaal uit dit document is afkomstig uit de handleiding Problemen oplossen met ACI-beheer en kernservices — Pod Policies, de APIC Basic Configuration Guide van Cisco, versie 6.1 (x) — Provisioning Core ACI Fabric Services, en het ACI Design Guide van Cisco.

Overzicht

Tijdsynchronisatie is een cruciale mogelijkheid in een ACI-fabric waarvan bewakings-, operationele en probleemoplossende taken afhankelijk zijn. Kloksynchronisatie zorgt voor een goede analyse van verkeersstromen, correlatie van foutopsporing en fouttijdstempels over meerdere fabric-knooppunten en volledig gebruik van de atomaire tellermogelijkheden waarvan de gezondheidsscores van toepassingen afhankelijk zijn. Niet-bestaande of onjuiste NTP-configuratie leidt niet noodzakelijkerwijs tot een fout of een lage gezondheidsscore, dus het is belangrijk om tijdsynchronisatie vroeg in de fabrikantimplementatie te configureren.

NTP-beleidsmodel in ACI

NTP in ACI wordt beheerd via een keten van vier beleidsobjecten:

1. Datum- en tijdbeleid (`datetimePol`) — definieert de NTP-configuratie, inclusief de beheerdersstatus, de verificatiestatus, de serverstatus en de hoofdmodus. U bevindt zich onder Verbinding > Verbindingsbeleid > Beleid > Pod > Datum en tijd.
2. NTP Provider (`datetimeNtpProv`) — definieert afzonderlijke NTP-serververmeldingen (providers) binnen een datum- en tijdbeleid, inclusief de IP/FQDN-server, EPG-

beheerselectie (out-of-band of in-band), voorkeursvlag en polling-intervallen.
3. Pod Policy Group (`fabricPodPGrp`) — verwijst naar het datum- en tijdbeleid en andere beleidsregels op pod-niveau (BGP RR, SNMP, enz.). U vindt deze onder Verbinding > Verbindingsbeleid > Pods > Beleidsgroepen.
4. Pod Profile (`fabricPodP`) — koppelt een Pod Policy Group aan een pod-selector. Deze bevindt zich onder Verbinding > Verbindingsbeleid > Pods > Profielen.

Alle vier de schakels in deze keten moeten worden geconfigureerd zodat NTP op de fabric-nodes kan worden toegepast. Als een koppeling verbroken is, wordt de NTP-providerconfiguratie niet naar de switches geduwd.

Voorwaarden

- Fabric Discovery moet worden voltooid.
- Adressen voor knooppuntbeheer (OOB of in-band) moeten worden toegewezen aan alle APIC's en switches onder de beheer-tenant.
- Voor out-of-band NTP moet de OOB-beheer-EPG UDP-poort 123 toestaan.
- Voor in-band NTP moet een in-band beheer-EPG met de juiste contracten en bereikbaarheid voor de NTP-server worden geconfigureerd. In-band IP-adressen zijn niet bereikbaar van buiten de verbinding zonder extra beleid.

NTP-verificatie

ACI ondersteunt drie NTP-verificatieschema's: MD5, SHA-1 en AES128-CMAC. AES128-CMAC werd geïntroduceerd in APIC versie 6.1(1) en is het aanbevolen schema, aangezien MD5 als zwak en onveilig wordt beschouwd. Als de FIPS-modus is ingeschakeld, worden alleen AES128-CMAC en SHA-1 ondersteund.

NTP-serverfunctionaliteit

ACI leaf switches kunnen fungeren als NTP-servers voor downstream clients (bijvoorbeeld servers die zijn aangesloten op de fabric). Deze functie is standaard uitgeschakeld en moet expliciet zijn ingeschakeld via de optie Serverstatus in het beleid Datum en tijd. Wanneer ingeschakeld, kunnen clients het in-band, out-of-band, bridge domain SVI of L3Out IP-adres van leaf switch gebruiken als het NTP-serveradres.

Opmerking: switches van stoffen mogen niet worden gesynchroniseerd met andere switches van dezelfde stof. De fabric-switches moeten altijd worden gesynchroniseerd met externe NTP-servers.

De configuratie verifiëren

Voordat u problemen met de operationele status van NTP oplost, moet u controleren of de configuratieketen is voltooid. Misconfiguratie is de meest voorkomende oorzaak van NTP-problemen in ACI.

Stap 1: Controleer de adressen voor knooppuntbeheer

Navigeer naar Tenants > Management > Node Management Addresses (voor statische toewijzing) of Node Management EPG's (voor connectiviteitsgroepen).

Bevestig dat aan elk APIC- en switch-knooppunt een IP-beheeradres is toegewezen. Nodes zonder beheeradressen kunnen niet communiceren met de NTP-server.

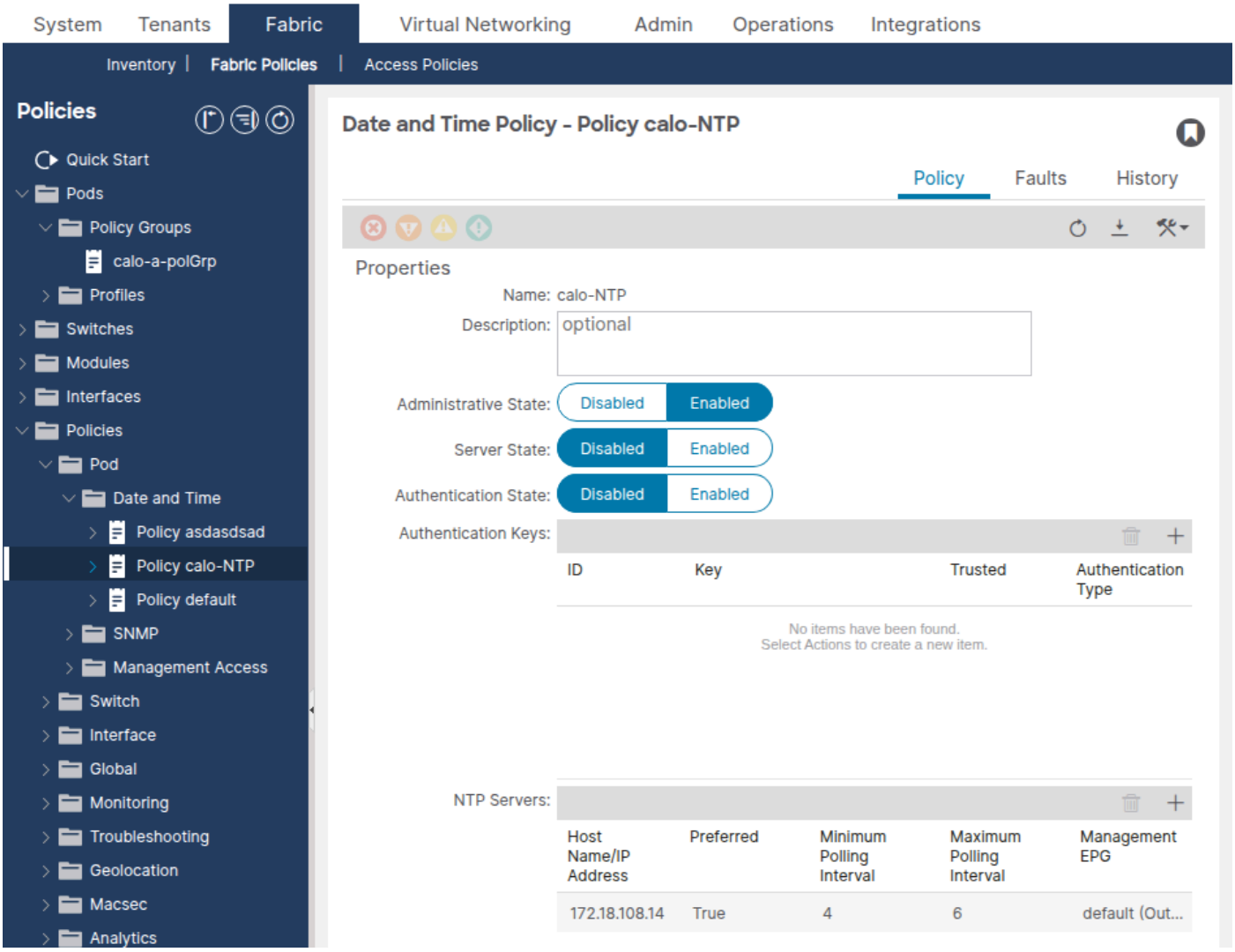
U kunt ook de API opvragen:

<#root>

```
apic1#

moquery -c mgmtRsOoBStNode
```

Stap 2: Controleer of het datum- en tijdbeleid een NTP-provider heeft

Navigeer naar Fabric > Fabric Policies > Policies > Pod > Date and Time > [Uw beleid].



Controleer of ten minste één NTP-provider (server) is geconfigureerd. Als er meerdere providers bestaan, markeert u ten minste één als voorkeursoptie.

Controleer de NTP-provider via de API:

<#root>

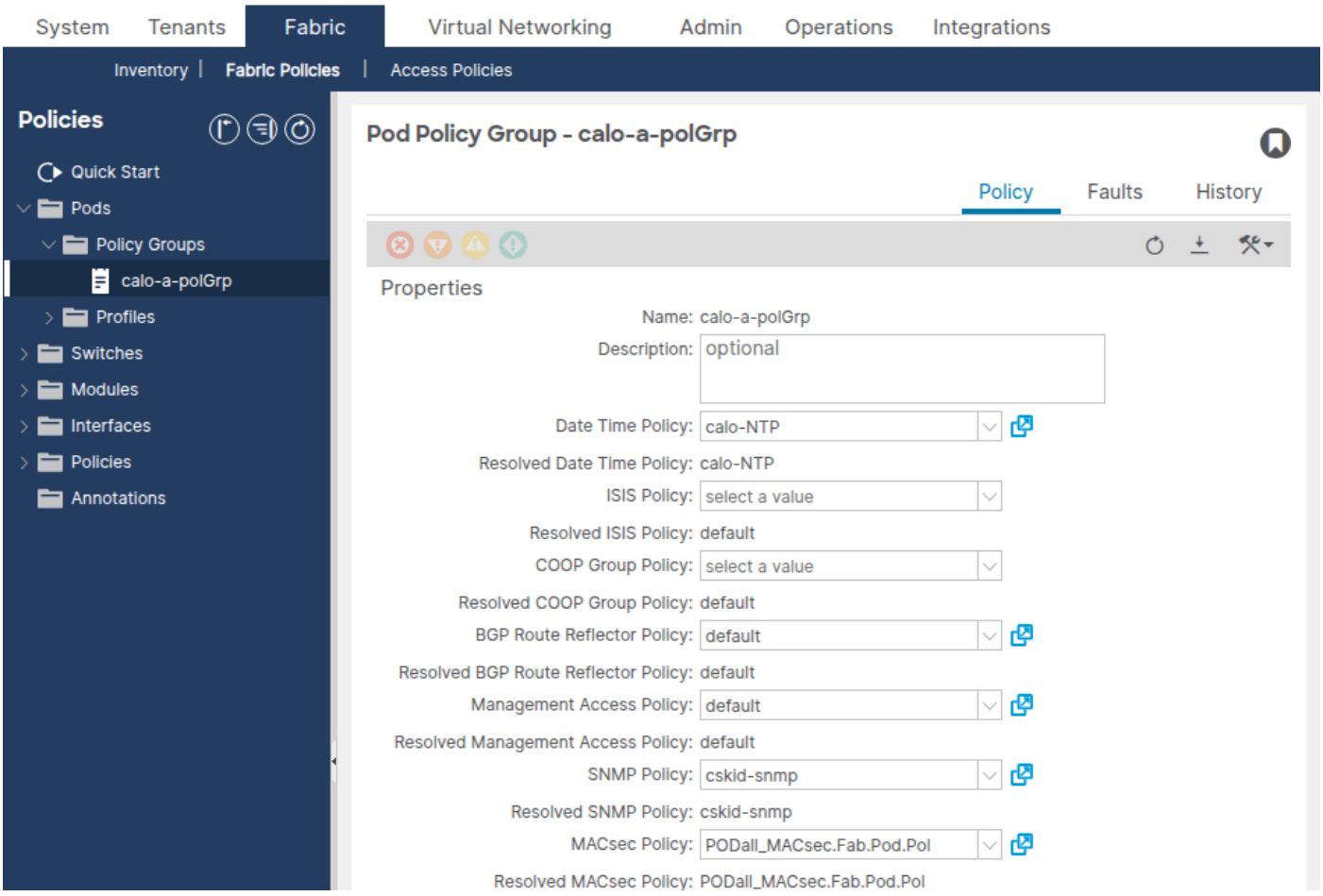
```
apic1#

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
```

Veelvoorkomende misconfiguraties

- Er is geen NTP-provider geconfigureerd — het datum- en tijdbeleid bestaat wel, maar er zijn geen providers. Het beleid wordt toegepast, maar nodes hebben geen NTP-server om tegen te synchroniseren.
- Verkeerd beheer EPG geselecteerd — de NTP-provider verwijst naar de out-of-band EPG, maar de NTP-server is alleen bereikbaar via in-band (of vice versa). Controleer welk EPG-beheer de NTP-server bereikbaar maakt.
- FQDN en IP van dezelfde server toegevoegd als afzonderlijke providers — dit genereert een duplicaat IP-fout. Verwijder de dubbele vermelding.
- FQDN-gebaseerde provider zonder DNS-beleid — als u een hostnaam voor de NTP-provider gebruikt, moet u ervoor zorgen dat een DNS-servicebeleid is geconfigureerd en het juiste DNS-label wordt toegepast op de VRF voor beheer.

Stap 3: Controleer de referenties van de POD-beleidsgroep voor de datum- en tijdbeleid

Navigeer naar Fabric > Fabric Policies > Pods > Policy Groups > [Your Pod Policy Group].



Bevestig dat het veld Datumtijdbeleid verwijst naar het juiste datum- en tijdbeleid.

<#root>

`apic1#`

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

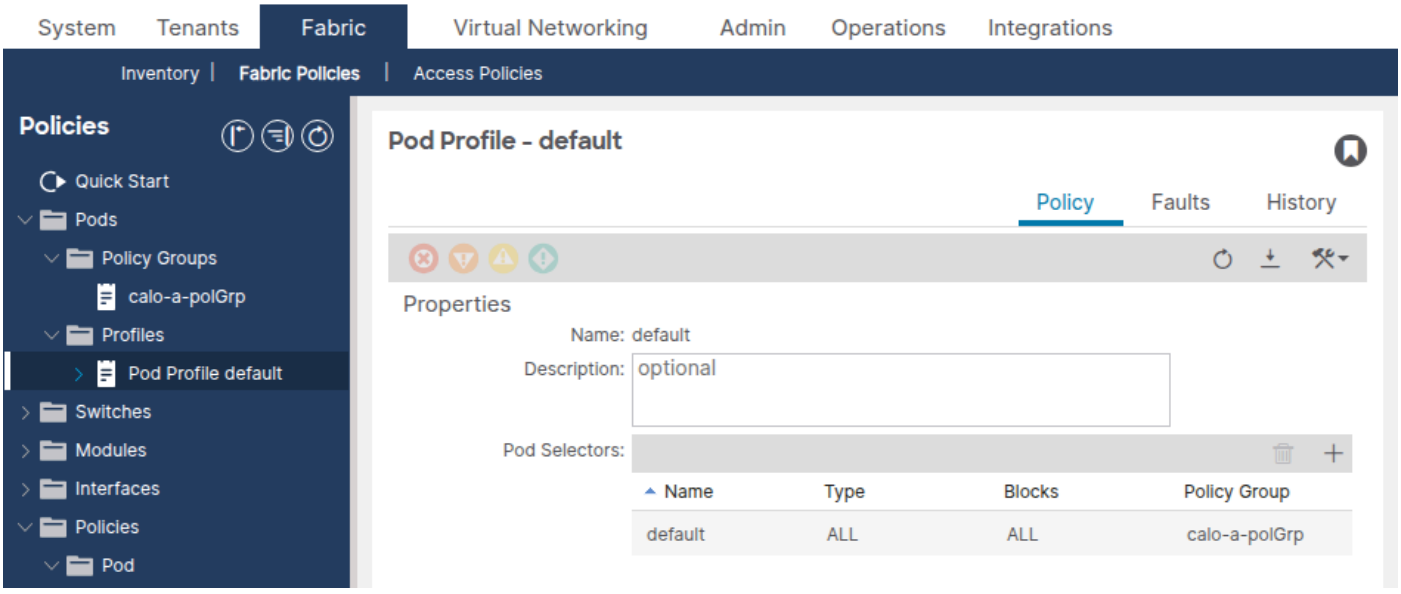
Zoek naar het attribuut `datetimePolName` of de bijbehorende `fabricRsTimePol`-relatie.

Veelvoorkomende misconfiguraties

- Pod Policy Group verwijst naar het verkeerde datum- en tijdbeleid — controleer of de Pod Policy Group verwijst naar het beoogde beleid als er meerdere datum- en tijdbeleidslijnen bestaan (bijv. "standaard" en een aangepast beleid).
- POD-beleidsgroep is helemaal niet gemaakt — de standaard POD-beleidsgroep is mogelijk niet gekoppeld aan het beleid Datum en tijd. Controleer altijd.

Stap 4: Controleer de Pod-profielverwijzingen in de Pod-beleidsgroep

Navigeer naar Fabric > Fabric Policies > Pods > Profiles > [Uw Pod-profiel].



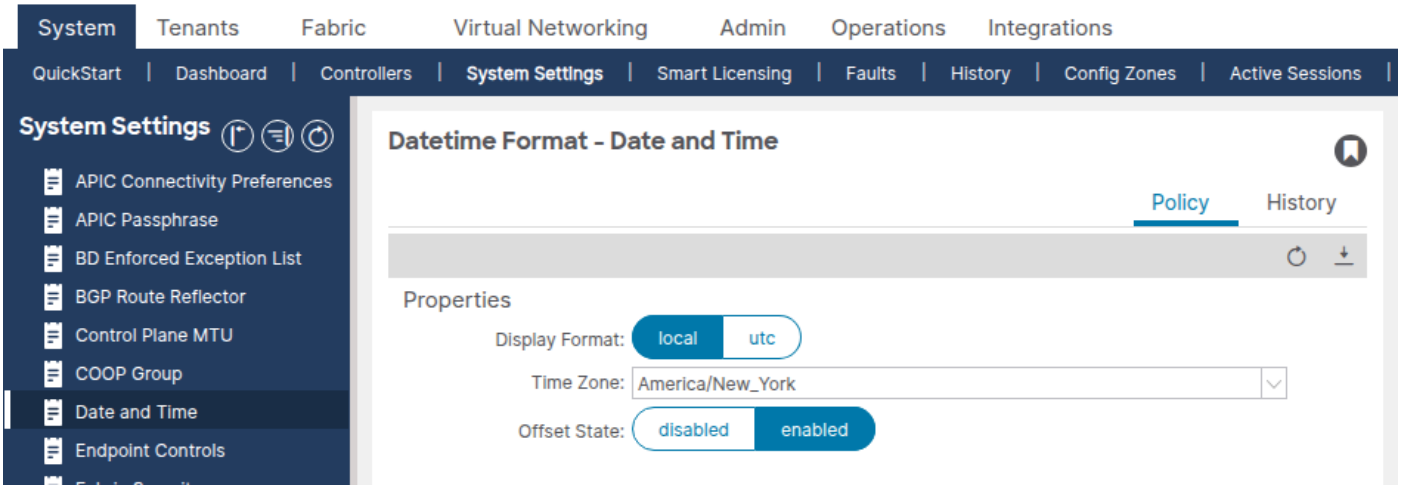
Bevestig de verwijzingen in het veld Verbindingsbeleidsgroep naar de juiste POD-beleidsgroep.

Veelvoorkomende misconfiguraties

- Pod Profile verwijst naar de verkeerde Pod Policy Group — met name in omgevingen met meerdere pods moet elk pod-profiel verwijzen naar de juiste pod-beleidsgroep.

Stap 5: Datum- en tijdnotatie controleren

Navigeer naar Systeem > Systeeminstellingen > Datum en tijd.



Bevestig dat het weergaveformaat (lokaal of UTC) en de tijdzone zijn ingesteld zoals verwacht. Deze instelling is een afzonderlijk standaard beleid voor de datumtijdnotatie dat niet kan worden verwijderd of gedupliceerd.

operationele verificatie

Nadat u hebt bevestigd dat de configuratieketen correct is, gebruikt u de volgende opdrachten om te controleren of NTP tijdens runtime werkt.

APIC-verificatie

NTPQ tonen

Deze opdracht toont de NTP-synchronisatiestatus voor alle APIC's. Het symbool * geeft aan dat de server is geselecteerd voor synchronisatie.

<#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
```

Hoe ziet goed eruit:

- Alle APIC's worden `*` (geselecteerd voor synchronisatie) naast de externe server weergegeven.
- `reach` is `377` (octaal), wat aangeeft dat de laatste 8 enquêtes allemaal succesvol waren.
- `St` (stratum) ligt tussen 1-15. Stratum 16 betekent dat de server niet gesynchroniseerd is.
- `De offset` is laag (meestal minder dan 100 ms voor een gezonde omgeving).

Hoe ziet slecht eruit:

- Nee `*` naast elke server — er is geen server geselecteerd voor synchronisatie.
- `bereik` is `0` — er zijn geen NTP-antwoorden ontvangen.
- `st` is `16` - de NTP-server is niet gesynchroniseerd met de upstream-tijdbron.
- `Offset` is extreem groot (duizenden milliseconden) - de klok is aanzienlijk verschoven.

toonklok

<#root>

```
apic1#

show clock

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

Bevestig dat de tijd nauwkeurig is. Vergelijk met de verwachte tijd om klokdrift te detecteren.

APIC Bash (alternatief)

<#root>

```
apic1#
```

```
bash

admin@apic1:~>

date

Tue Apr 7 11:24:45 EDT 2026
```

Verificatie van de switch (blad/ruggengraat)

NTP-peers weergeven

Controleer of de NTP-provider naar de switch is geduwd.

<#root>

```
leaf1#

show ntp peers

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

Hoe ziet goed eruit: De IP- of hostnaam van de NTP-server wordt weergegeven met `Serv/Peer` = `Server` en de juiste VRF (meestal `beheer` voor OOB).

Hoe slecht ziet eruit: Geen peers vermeld, of de NTP-server IP komt niet overeen met de geconfigureerde provider. Dit geeft meestal aan dat het datum- en tijdbeleid niet is toegepast via de pod-beleidsgroep / pod-profielketen.

NTP-peer-status weergeven

Controleer of de NTP-server is geselecteerd voor synchronisatie.

<#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
```

Het `*` teken is essentieel — het bevestigt dat de NTP-server wordt gebruikt voor synchronisatie.

Hoe ziet slecht eruit:

- Nee `*` naast de server — de switch synchroniseert niet met de server.
- `bereik` is `0` — er zijn geen NTP-antwoorden ontvangen. Dit duidt op een probleem met bereikbaarheid.
- `st` is `16` — de NTP-server is niet gesynchroniseerd en kan geen geldige tijd opgeven.

NTP-statistieken weergeven Peer IPADR

Verifieer de NTP-pakketuitwisseling om de bereikbaarheid te bevestigen. Vervang het IP-adres door het NTP-provideradres voor de betreffende switch.

<#root>

```
leaf1#
```

show ntp statistics peer ipaddr 10.1.1.100

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

Hoe goed ziet eruit: `verzonden pakketten` en `ontvangen pakketten` zijn ongeveer gelijk en nemen toe.

Hoe slecht ziet eruit: `verzonden pakketten` nemen toe, maar `ontvangen pakketten` nemen `0` of nauwelijks toe - NTP-reacties bereiken de switch niet.

toonklok

<#root>

```
leaf1#
```

```
show clock

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

GUI-verificatie

Navigeer naar Fabric > Fabric Policies > Policies > Pod > Date and Time > [Uw beleid] > [NTP-provider].

De kolom Synchronisatiestatus moet Gesynchroniseerd met externe NTP-server voor alle knooppunten weergeven. Het kan enkele minuten duren voordat de synchronisatiestatus is geconvergeerd na de eerste implementatie.

API-verificatie

Vraag de klasse `datetimeNtpq` om NTP-synchronisatie voor alle APIC's te controleren:

```
<#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.
```

Werkstroom voor probleemoplossing

Gebruik deze beslisboom wanneer een NTP-probleem wordt gemeld op een ACI-node.

Stap 1: Zijn NTP-peers geconfigureerd op de switch?

Meld u aan bij de betreffende switch en voer het volgende uit:

<#root>

`leaf1#`

`show ntp peers`

- Geen peers vermeld → het datum- en tijdbeleid is niet toegepast op deze node. Ga naar Scenario 1: NTP-provider niet naar de Switch geduwd.
- Peers vermeld → Ga door naar stap 2.

Stap 2: Is de NTP-server geselecteerd voor synchronisatie?

<#root>

`leaf1#`

`show ntp peer-status`

- `*` present → NTP is syncing. Als de tijd nog steeds verkeerd lijkt, gaat u naar Scenario 5: Grote offset / klokdrift.
- Geen `*` aanwezig → doorgaan naar Stap 3.

Stap 3: Is de bereikwaarde nul?

Controleer de kolom `bereik` in `NTP-peer-status weergeven`.

- **`bereik`** = **`0`** → geen antwoorden van de NTP-server. Ga naar Scenario 2: NTP-server onbereikbaar.
- **`REACH`** > **`0`** maar er komen geen `*` → antwoorden aan, maar de synchronisatie is niet tot stand gebracht. Controleer stratum — ga naar stap 4.

Stap 4: Is de waarde van het stratum 16?

- Stratum = 16 → de NTP-server is niet gesynchroniseerd met zijn eigen upstream-bron. Ga naar Scenario 3: NTP Server Unsynchronized (Stratum 16).
- Stratum 1-15 maar geen synchronisatie → ga naar Scenario 4: NTP-verificatie Mismatch.

Veelvoorkomende scenario's voor probleemoplossing

Scenario 1: NTP-provider niet tot Switch gebracht

Symptoom: `toon ntp-peers` op de switch geeft geen items terug.

Configuratiecontrole:

1. Controleer of in het beleid Datum en tijd ten minste één NTP-provider is geconfigureerd.
2. Controleer of de referenties van de POD-beleidsgroep de juiste datum en tijd bevatten.
3. Controleer de referenties van het Pod-profiel in de juiste Pod-beleidsgroep.
4. Controleer of aan de node een IP-beheeradres is toegewezen onder de beheer-tenant.

Hoofdoorzaak: een van de vier links in de beleidsketen (Datum- en tijdbeleid → NTP Provider → Pod Policy Group → Pod Profile) is verbroken. De meest voorkomende oorzaak is dat de POD-beleidsgroep niet is gekoppeld aan het POD-profiel of dat het beleid Datum en tijd niet is geselecteerd in de POD-beleidsgroep.

Oplossing: Voltooi de ontbrekende schakel in de beleidsketen. Zorg ervoor dat het pod-profiel voor de betreffende pod verwijst naar een pod-beleidsgroep die het juiste datum- en tijdbeleid bevat. Na toepassing wordt de NTP-providerconfiguratie binnen enkele minuten naar de switches geduwd.

Scenario 2: NTP-server onbereikbaar

Symptoom: toon ntp peer-status toont bereik = 0. `toon ntp statistieken peer ipaddr 10.1.1.100` toont `ontvangen pakketten` = `0`.

Configuratiecontrole: Controleer of de NTP-provider is gekoppeld aan het juiste EPG-beheer (OOB of in-band). Als u OOB gebruikt, controleert u of de OOB-contracten UDP-poort 123 toestaan.

Operationele controle:

1. Ping de NTP-server van de getroffen switch met behulp van het beheer VRF:
   <#root>

   ```
   leaf1#
   ```

   ping 10.1.1.100 vrf management

2. Voer een tcpdump uit op de switch om te controleren of NTP-pakketten vertrekken en aankomen:
<#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
```

Hoofdoorzaak: Doorgaans een van de volgende:

- Aan de switch is geen IP-beheeradres toegewezen.
- De standaardgateway voor het beheer van de VRF ontbreekt of is onjuist.
- Een firewall blokkeert UDP-poort 123 tussen de switch en de NTP-server.
- Het OOB-contract staat UDP-poort 123 niet toe.
- De NTP-provider verwijst naar de verkeerde EPG-beheer (bijvoorbeeld OOB geselecteerd, maar alleen in-band heeft bereikbaarheid).

Oplossing: het probleem van bereikbaarheid oplossen. Wijs een beheeradres toe als dit ontbreekt, repareer de standaardgateway, werk firewallregels bij of corrigeer de EPG-beheerselectie op de NTP-provider.

Scenario 3: NTP-server niet-gesynchroniseerd (stratum 16)

Symptoom: `toon ntp peer-status` toont stratum (`st`) = `16`. De switch wordt niet gesynchroniseerd met een stratum 16-server.

Operationele controle: Meld u aan bij de NTP-server of vraag deze op van een externe host om te controleren of deze is gesynchroniseerd met zijn eigen upstream-tijdbron.

Hoofdoorzaak: De NTP-server zelf heeft de synchronisatie met de upstream referentieklok verloren. Een server met stratum 16 adverteert dat deze geen betrouwbare tijdbron heeft.

Oplossing: de NTP-server repareren. Dit bevindt zich buiten de ACI-structuur — controleer de NTP-serverconfiguratie en de upstream-tijdbron. Als de NTP-server niet onmiddellijk kan worden hersteld, configureert u een alternatieve NTP-provider in het beleid Datum en tijd.

Scenario 4: NTP-verificatie komt niet overeen

Symptoom: `NTP-peer-status tonen` toont `bereik` > `0` en stratum is geldig, maar er wordt geen `*` weergegeven. De NTP-server reageert, maar de switch accepteert het antwoord niet.

Configuratiecontrole:

1. Controleer of de NTP-server verificatie vereist.
2. Als verificatie is vereist, controleert u of de verificatiestatus van het beleid Datum en tijd is ingesteld op Ingeschakeld.
3. Controleer of de ID van de verificatiesleutel, de sleutelwaarde en het algoritme (MD5, SHA-1 of AES128-CMAC) overeenkomen tussen de ACI-structuur en de NTP-server.
4. Controleer of de sleutel is gemarkeerd als Vertrouwd in de tabel NTP-clientverificatiesleutels.

Hoofdoorzaak: de verificatiesleutel, het algoritme of de sleutel-ID is niet goed afgestemd tussen ACI en de NTP-server, waardoor de switch de NTP-reactie afwijst als niet-geverifieerd.

Oplossing: de verificatieconfiguratie uitlijnen. Zorg ervoor dat dezelfde sleutel-ID, sleutelwaarde en algoritme zijn geconfigureerd op zowel ACI als de NTP-server. AES128-CMAC wordt aanbevolen voor APIC-release 6.1(1) en hoger.

Opmerking: wanneer de FIPS-modus is ingeschakeld, worden alleen AES128-CMAC- en SHA-1-verificatieschema's ondersteund. MD5 werkt niet in FIPS-modus.

Scenario 5: grote offset / klokdrift

Symptoom: De switch lijkt gesynchroniseerd (`* aanwezig, bereik = 377)`, `maar de offset` waarde in `tonen ntp peer-status` of `tonen ntpq` is erg groot (honderdduizenden milliseconden), of de klok is zichtbaar fout.

Operationele controle:

<#root>

```
apic1#
```

show ntpq

Controleer de kolom `offset`. Een gezonde offset is meestal minder dan 100 ms.

Hoofdoorzaak: de klok is aanzienlijk afgeweken voordat NTP-synchronisatie werd ingesteld of de hardwareklok (RTC) werd gereset tijdens een herstart (bijv. vanwege een lege CMOS-batterij). NTP corrigeert de klok geleidelijk door te draaien, wat tijd kan kosten voor grote offsets.

Oplossing: Als de offset erg groot is en NTP actief synchroniseert, wacht dan tot de klok convergeert. NTP schakelt de klok geleidelijk - grote offsets kunnen uren duren om volledig te corrigeren. Als de offset niet afneemt, controleert u of de NTP-server de juiste tijd levert. Als het probleem zich na elke herstart opnieuw voordoet, onderzoekt u de hardwareklok (RTC / CMOS-batterij) op de getroffen node.

Scenario 6: Standby APIC-fouten met in-band NTP

Symptoom: Fouten worden gegenereerd op een stand-by APIC met betrekking tot NTP of monitoringbeleid wanneer NTP is geconfigureerd voor in-band beheer.

Hoofdoorzaak: wanneer een NTP-beleid wordt toegepast voor in-band beheer, vereist de stand-by APIC ook in-band configuratie. Zonder dat worden de fouten gemaakt.

Oplossing: Configureer ook in-band beheer voor de APIC die stand-by staat. Hiermee worden de fouten opgeruimd.

Scenario 7: IP-fout dupliceren

Symptoom: Een duplicaat IP-fout wordt verhoogd na het toevoegen van NTP-providers.

Root Cause: Een FQDN werd toegevoegd als een NTP-provider, en vervolgens het opgeloste IP-adres van die FQDN werd toegevoegd als een tweede NTP-provider. ACI detecteert het duplicaat.

Oplossing: Verwijder de meest recent toegevoegde duplicaatprovider (het invoeren van het IP-adres als de FQDN eerst is toegevoegd, of vice versa). Gebruik slechts één invoer per NTP-server: FQDN- of IP-adres, niet beide.

Scenario 8: DNS-oplossingsfout voor FQDN-gebaseerde NTP-provider

Symptoom: NTP-provider geconfigureerd met een hostnaam lost niet op. `toon ntp-peers` geeft het verwachte IP-adres niet weer of NTP synchroniseert niet.

Configuratiecontrole:

1. Controleer of een DNS-servicebeleid is geconfigureerd onder Fabric > Fabric Policies > Policies > Global > DNS-profielen.
2. Controleer of de DNS-provider (DNS-server) bereikbaar is via de VRF voor beheer.
3. Controleer of het juiste DNS-label is geconfigureerd voor de in-band of out-of-band VRF-instantie van de EPG-beheerfunctie.

Hoofdoorzaak: de DNS-server kan niet worden bereikt of is niet geconfigureerd, waardoor de hostnaamresolutie voor de NTP-provider mislukt.

Oplossing: Configureer het DNS-servicebeleid, zorg voor DNS-bereikbaarheid en pas het juiste DNS-label toe. U kunt ook het IP-adres van de NTP-server gebruiken in plaats van de hostnaam.

Gerelateerde fouten en gebeurtenissen

De volgende zijn NTP-gerelateerde aandoeningen die fouten in ACI kunnen genereren:

- Dubbele IP-fout — verhoogd wanneer een FQDN en het IP-adres van dezelfde NTP-server beide worden toegevoegd als providers. Resolutie: verwijder de dubbele vermelding.
- Standby APIC in-band NTP-fouten — verhoogd wanneer een bewakings- of NTP-beleid wordt toegepast voor in-band, maar de standby APIC mist in-band configuratie.
- Synchronisatiestatus convergeert niet — de GUI toont "Niet gesynchroniseerd" of een andere status dan "Gesynchroniseerd met externe NTP-server" voor een of meer knooppunten. Dit is geen foutcode, maar een operationele statusindicator. Volg de werkstroom voor probleemoplossing hierboven om een diagnose te stellen.

Escalatiecriteria

Overweeg te escaleren naar Cisco TAC als:

- De configuratieketen is correct geverifieerd en de NTP-server is bereikbaar (ping werkt, tcpdump toont NTP-reacties), maar de switch synchroniseert nog steeds niet.
- NTP-synchronisatie gaat herhaaldelijk verloren zonder configuratiewijzigingen of NTP-serverproblemen.
- De `ntp peer-status` uitvoer toont onverwacht gedrag zoals persistent stratum 16 op een server die extern bevestigd en gesynchroniseerd is.
- De klok verschuift aanzienlijk tussen reboots, wat kan wijzen op een hardwareklok (RTC) probleem.

Verstrek de volgende gegevens wanneer TAC wordt toegepast:

- Uitvoer van `show ntpq` van alle APIC's.
- Uitvoer van `tonen ntp peers`, `tonen ntp peer-status`, `tonen ntp statistieken peer ipaddr <IP>`, en `tonen klok` van alle betrokken switches.
- Uitvoer van `moquery -c datetimePol`, `moquery -c datetimeNtpProv`, en `moquery -c datetimeNtpq` van de APIC.
- Een technische ondersteuning van de getroffen node(s).

Referenties

- Cisco APIC Basic Configuration Guide, versie 6.1(x) — Provisioning Core ACI Fabric Services
- Problemen met ACI-beheer en kernservices oplossen — POD-beleid
- Ontwerphandleiding Cisco Application Centric Infrastructure (ACI)

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.