Fehlerbehebung bei NTP in einer Cisco ACI-Fabric

Einleitung

In diesem Dokument wird beschrieben, wie NTP-Probleme (Network Time Protocol) in einer Cisco ACI-Fabric überprüft, behoben und behoben werden. Es umfasst das NTP-Richtlinienmodell, die Konfigurationsverifizierung, die Befehle zur betrieblichen Verifizierung, einen Triage-Workflow für häufige NTP-Symptome und detaillierte Szenarien zur Fehlerbehebung.

Hintergrundinformationen

Das Material aus diesem Dokument wurde aus dem Leitfaden zur Fehlerbehebung bei ACI-Management- und Core-Services - Pod-Richtlinien, dem Cisco APIC Basic-Konfigurationsleitfaden, dem Kapitel 6.1(x) - Provisioning Core ACI Fabric Services und dem Cisco ACI-Designleitfaden extrahiert.

Überblick

Die Zeitsynchronisierung ist eine wichtige Funktion in einer ACI-Fabric, von der Überwachungs-, Betriebs- und Fehlerbehebungsaufgaben abhängen. Die Synchronisierung der Uhren gewährleistet eine ordnungsgemäße Analyse des Datenverkehrs, die Korrelation von Zeitstempeln für Fehlerbehebung und Fehlerbehebung in mehreren Fabric-Knoten sowie die vollständige Nutzung der Kernzählerfunktion, von der die Bewertung der Anwendungsintegrität abhängt. Eine nicht vorhandene oder falsche NTP-Konfiguration löst nicht unbedingt einen Fehler oder eine niedrige Integritätsbewertung aus. Daher ist es wichtig, die Zeitsynchronisierung in einer frühen Phase der Fabric-Bereitstellung zu konfigurieren.

NTP-Richtlinienmodell in der ACI

Das NTP in der ACI wird über eine Kette von vier Richtlinienobjekten verwaltet:

1. Datums- und Uhrzeitrichtlinie (`datetimePol`): Diese Richtlinie definiert die NTP-Konfiguration einschließlich Verwaltungsstatus, Authentifizierungsstatus, Serverstatus und Master-Modus. Sie finden sie unter Fabric > Fabric Policies > Policies > Pod > Date and Time.

2. NTP-Anbieter (`datetimeNtpProv`): Definiert individuelle NTP-Servereinträge (Provider) innerhalb einer Datums- und Uhrzeitrichtlinie, einschließlich der IP/FQDN des Servers, der EPG-Auswahl für die Verwaltung (Out-of-Band oder In-Band), des bevorzugten Flags und der Abfrageintervalle.
3. Pod Policy Group (`fabricPodPGrp`): Verweist auf die Datum- und Uhrzeitrichtlinie sowie auf andere Richtlinien auf Pod-Ebene (BGP RR, SNMP usw.). Sie finden sie unter Fabric > Fabric Policies > Pods > Policy Groups.
4. Pod-Profil (`fabricPodP`): Weist einer Pod-Richtliniengruppe einen Pod-Selektor zu. Sie finden sie unter Fabric > Fabric Policies > Pods > Profiles.

Alle vier Links in dieser Kette müssen so konfiguriert werden, dass NTP auf die Fabric-Knoten angewendet wird. Wenn eine Verbindung unterbrochen wird, wird die NTP-Provider-Konfiguration nicht per Push an die Switches übertragen.

Voraussetzungen

- Die Fabric-Erkennung muss abgeschlossen sein.
- Node-Management-Adressen (OOB oder In-Band) müssen allen APICs und Switches unter dem mgmt-Tenant zugewiesen werden.
- Für Out-of-Band-NTP muss die OOB-Verwaltungs-EPG den UDP-Port 123 zulassen.
- Für das In-Band-NTP muss eine In-Band-Management-EPG mit den entsprechenden Verträgen und der Erreichbarkeit zum NTP-Server konfiguriert werden. In-Band-IP-Adressen können nicht von außerhalb der Fabric ohne zusätzliche Richtlinien erreicht werden.

NTP-Authentifizierung

Die ACI unterstützt drei NTP-Authentifizierungsschemata: MD5, SHA-1 und AES128-CMAC. AES128-CMAC wurde in APIC Version 6.1(1) eingeführt und ist das empfohlene Schema, da MD5 als schwach und unsicher gilt. Wenn der FIPS-Modus aktiviert ist, werden nur AES128-CMAC und SHA-1 unterstützt.

NTP-Serverfunktion

ACI-Leaf-Switches können als NTP-Server für Downstream-Clients (z. B. mit der Fabric verbundene Server) fungieren. Diese Funktion ist standardmäßig deaktiviert und muss explizit über die Option Serverstatus in der Datums- und Uhrzeitrichtlinie aktiviert werden. Wenn diese Funktion aktiviert ist, können Clients die In-Band-, Out-of-Band-, Bridge-Domain-SVI- oder L3Out-IP-Adresse des Leaf-Switches als NTP-Serveradresse verwenden.

Anmerkung: Fabric-Switches sollten nicht mit anderen Switches derselben Fabric

---

synchronisiert werden. Die Fabric-Switches sollten immer mit externen NTP-Servern synchronisiert werden.

Konfiguration überprüfen

Überprüfen Sie vor der Fehlerbehebung des NTP-Betriebsstatus, ob die Konfigurationskette abgeschlossen ist. Konfigurationsfehler sind die häufigste Ursache für NTP-Probleme in der ACI.

Schritt 1: Knotenverwaltungsadressen überprüfen

Navigieren Sie zu Tenants > mgmt > Node Management Addresses (für statische Zuweisung) oder Node Management EPGs (für Verbindungsgruppen).

Vergewissern Sie sich, dass jedem APIC- und Switch-Knoten eine Management-IP-Adresse zugewiesen ist. Knoten ohne Verwaltungsadressen können nicht mit dem NTP-Server kommunizieren.

Alternativ können Sie die API abfragen:

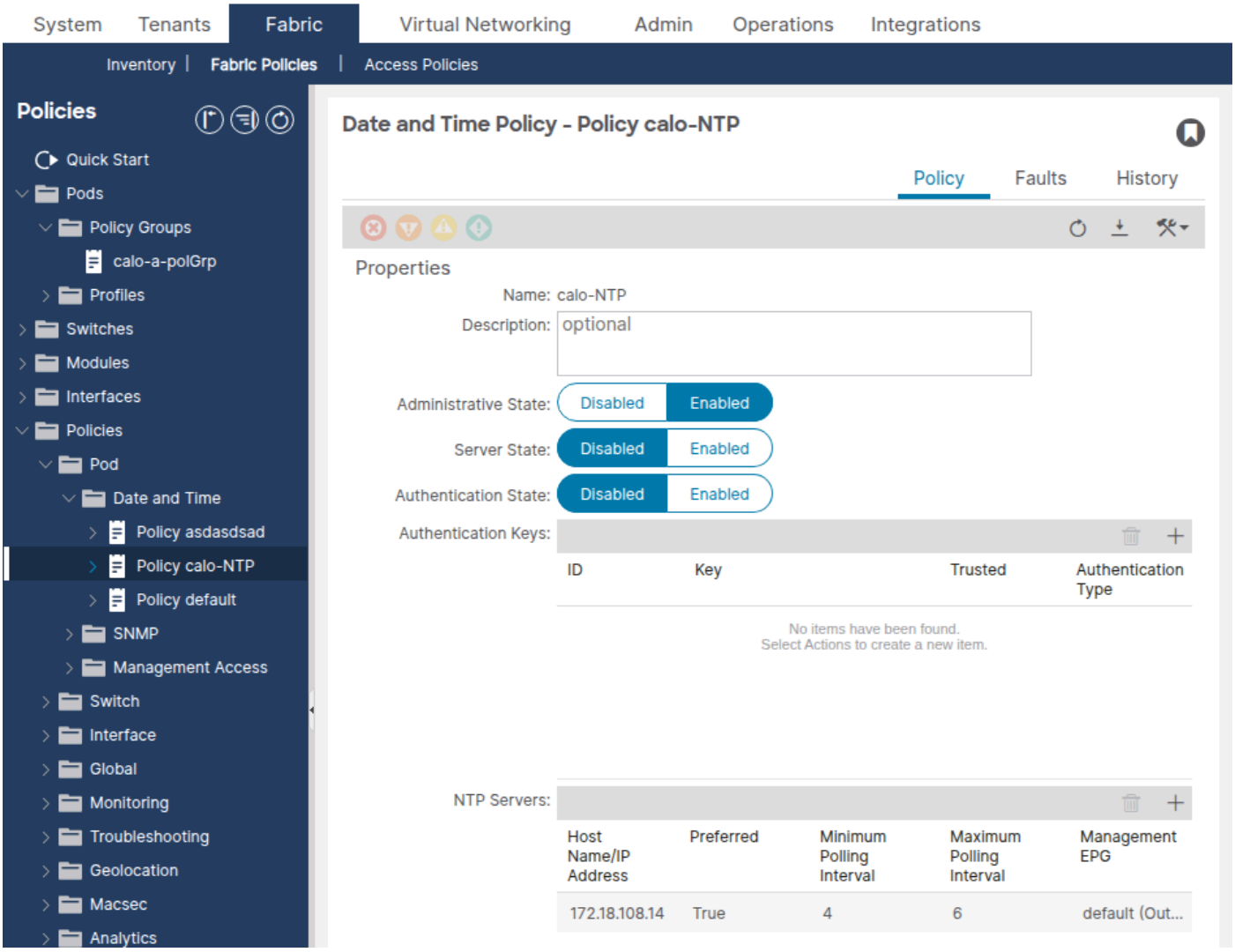
<#root>

```
apic1#
```

moquery -c mgmtRsOoBStNode

Phase 2: Überprüfen Sie, ob die Datums- und Uhrzeitrichtlinie über einen NTP-Anbieter verfügt.

Navigieren Sie zu Fabric > Fabric Policies > Policies > Pod > Date and Time > [Your Policy].



Vergewissern Sie sich, dass mindestens ein NTP-Anbieter (Server) konfiguriert ist. Wenn mehrere Anbieter vorhanden sind, markieren Sie mindestens einen Anbieter als Bevorzugt.

Überprüfen Sie den NTP-Anbieter über die API:

<#root>

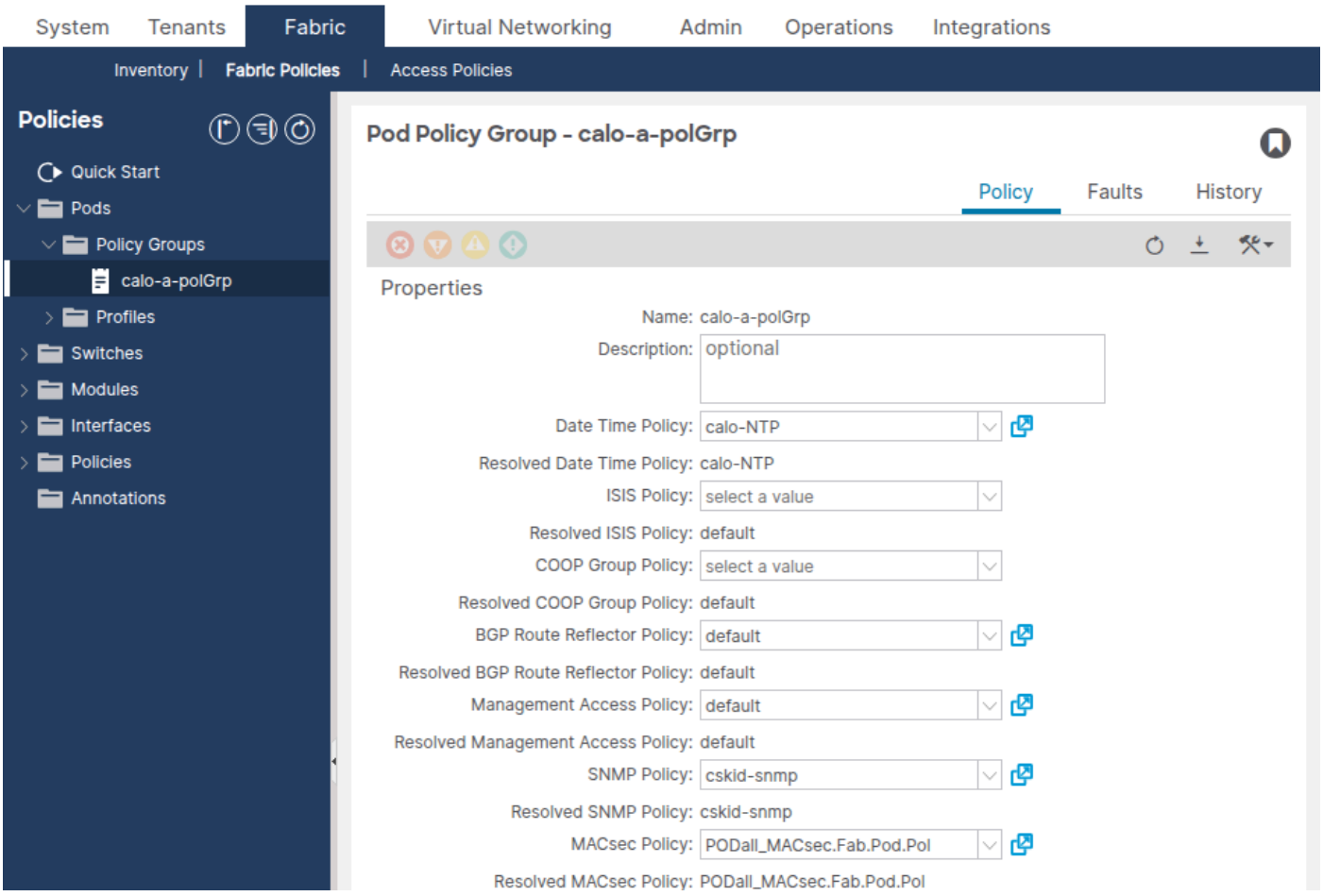
```
apic1#

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
```

Häufige Fehlkonfigurationen

- Kein NTP-Anbieter konfiguriert: Die Richtlinie "Datum und Uhrzeit" ist vorhanden, es sind jedoch keine Anbieter vorhanden. Die Richtlinie wird angewendet, aber die Knoten verfügen nicht über einen NTP-Server, mit dem sie synchronisiert werden können.
- Falsche Management-EPG ausgewählt - Der NTP-Anbieter verweist auf die Out-of-Band-EPG, aber der NTP-Server ist nur über In-Band erreichbar (oder umgekehrt). Überprüfen Sie, welche Management-EPG die Erreichbarkeit des NTP-Servers bereitstellt.
- FQDN und IP desselben Servers werden als separate Provider hinzugefügt — dies erzeugt einen doppelten IP-Fehler. Löschen Sie den doppelten Eintrag.
- FQDN-basierter Anbieter ohne DNS-Richtlinie: Wenn ein Hostname für den NTP-Anbieter verwendet wird, stellen Sie sicher, dass eine DNS-Dienstrichtlinie konfiguriert und das entsprechende DNS-Label auf die Verwaltungs-VRF-Instanz angewendet wird.

Schritt 3: Überprüfen der Pod-Richtliniengruppen-Referenzen in der Datums- und Uhrzeitrichtlinie

Navigieren Sie zu Fabric > Fabric Policies > Pods > Policy Groups > [Your Pod Policy Group].



Bestätigen Sie, dass das Feld "Date Time Policy" auf die richtige Datum- und Uhrzeitrichtlinie verweist.

<#root>

apic1#

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

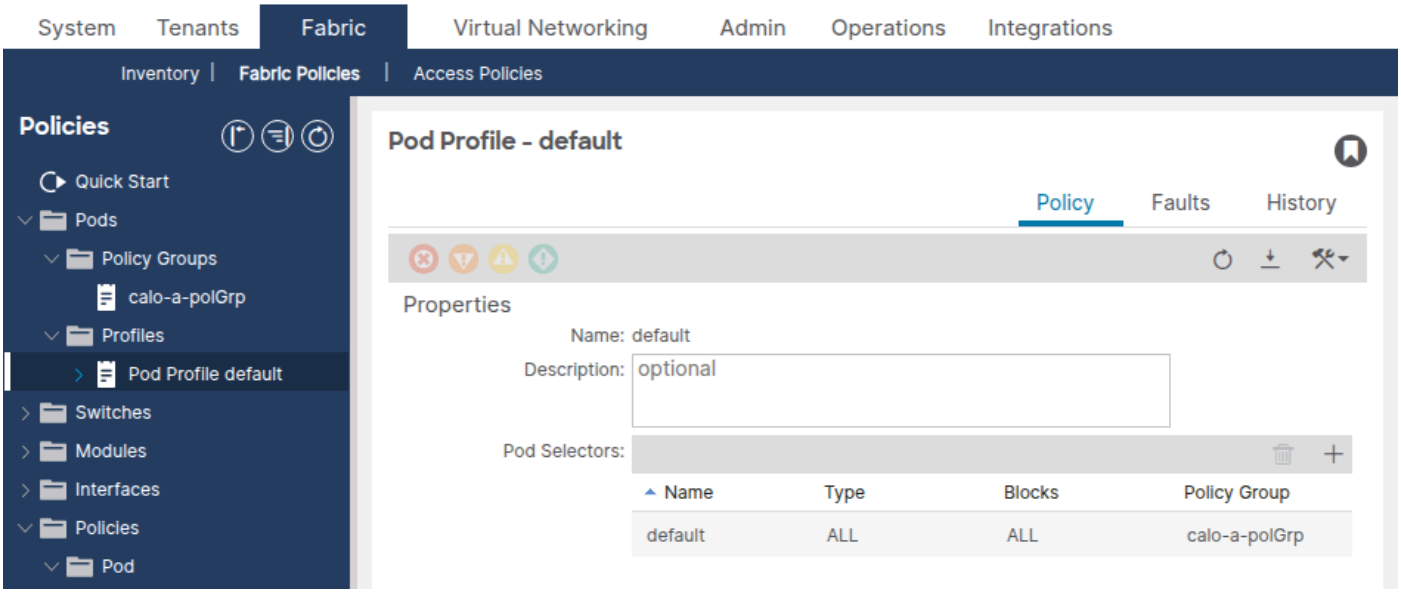
Suchen Sie nach dem `datetimePolName`-Attribut oder der zugeordneten `FabricRsTimePol`-Beziehung.

Häufige Fehlkonfigurationen

- Die Pod Policy Group verweist auf die falsche Datums- und Uhrzeitrichtlinie. Wenn mehrere Datums- und Uhrzeitrichtlinien vorhanden sind (z. B. "default" und eine benutzerdefinierte Richtlinie), überprüfen Sie, ob die Pod Policy Group auf die beabsichtigte Richtlinie verweist.
- Pod-Richtliniengruppe wurde überhaupt nicht erstellt - der Standard-Pod-Richtliniengruppe ist möglicherweise die Datums- und Uhrzeitrichtlinie nicht zugeordnet. Überprüfen Sie dies immer.

Schritt 4: Überprüfen der POD-Profilreferenzen in der POD-Richtliniengruppe

Navigieren Sie zu Fabric > Fabric-Richtlinien > PODs > Profile > [Ihr Pod-Profil].



Vergewissern Sie sich, dass das Feld "Fabric Policy Group" auf die richtige Pod Policy Group

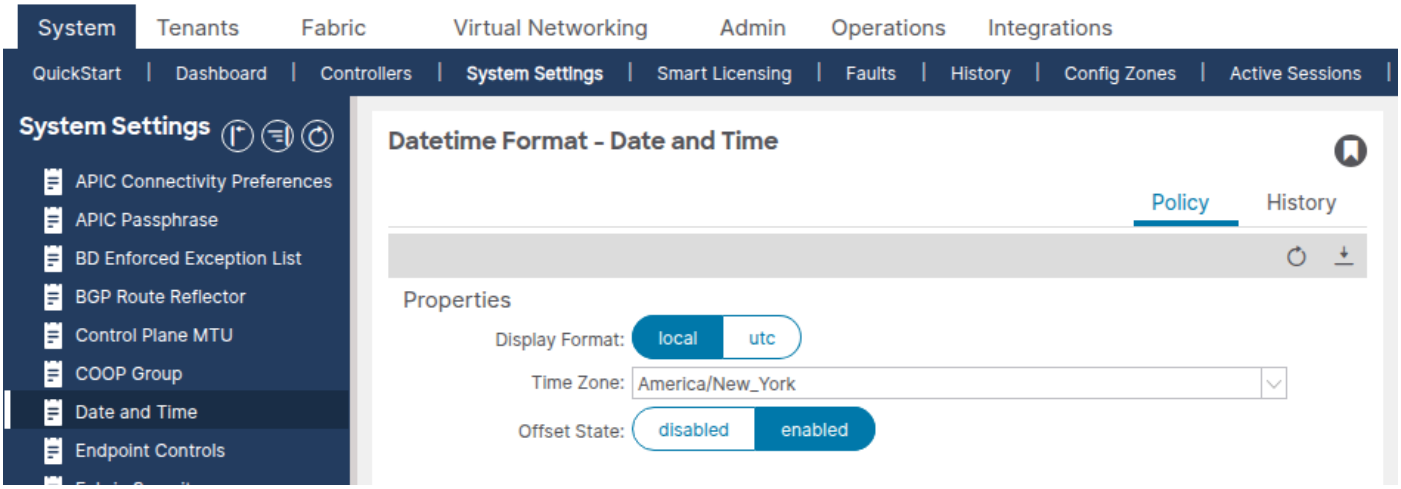
verweist.

Häufige Fehlkonfigurationen

- Das Pod-Profil referenziert die falsche Pod-Richtliniengruppe - insbesondere in Multi-Pod-Umgebungen muss jedes Pod-Profil die richtige Pod-Richtliniengruppe referenzieren.

Schritt 5: Datums- und Uhrzeitformat überprüfen

Navigieren Sie zu System > System Settings > Date and Time (System > Systemeinstellungen > Datum und Uhrzeit).



Überprüfen Sie, ob das Anzeigeformat (lokal oder UTC) und die Zeitzone wie erwartet eingestellt sind. Bei dieser Einstellung handelt es sich um eine separate standardmäßige Datums-/Uhrzeitformatrichtlinie, die nicht gelöscht oder dupliziert werden kann.

Betriebliche Überprüfung

Überprüfen Sie mithilfe der folgenden Befehle, ob das NTP zur Laufzeit funktioniert, nachdem Sie bestätigt haben, dass die Konfigurationskette korrekt ist.

APIC-Verifizierung

ntpq anzeigen

Dieser Befehl zeigt den NTP-Synchronisierungsstatus für alle APICs an. Das * Symbol zeigt an, dass der Server für die Synchronisierung ausgewählt ist.

<#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
```

Wie gut sieht es aus?

- Alle APICs zeigen * (für die Synchronisierung ausgewählt) neben dem Remote-Server an.
- Reichweite ist 377 (oktal), was bedeutet, dass die letzten 8 Umfragen alle erfolgreich waren.
- st (Schicht) liegt zwischen 1-15. Schicht 16 bedeutet, dass der Server nicht synchronisiert ist.
- Offset ist gering (typischerweise unter 100 ms für eine gesunde Umgebung).

Wie schlecht sieht es aus?

- Nein* neben einem Server - kein Server ist für die Synchronisierung ausgewählt.
- reach ist 0 - es wurden keine NTP-Antworten empfangen.
- st ist 16 - der NTP-Server ist nicht mit seiner Upstream-Zeitquelle synchronisiert.
- Offset ist extrem groß (Tausende Millisekunden) - der Takt ist deutlich gedriftet.

show clock

<#root>

apic1#

show clock

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

Bestätigen Sie die Richtigkeit der Uhrzeit. Vergleich mit der erwarteten Zeit zur Erkennung von Uhrzeitdrift

APIC-Bash (alternativ)

<#root>

```
apic1#
```

bash

```
admin@apic1:~>
```

date

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

Switch-Verifizierung (Leaf/Spine)

NTP-Peers anzeigen

Überprüfen Sie, ob der NTP-Anbieter auf den Switch übertragen wurde.

<#root>

```
leaf1#
```

show ntp peers

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

Wie gut sieht es aus? Die IP-Adresse oder der Hostname des NTP-Servers wird mit `Serv/Peer` = `Server` und der korrekten VRF-Instanz (in der Regel `Management` für OOB) angezeigt.

Wie schlecht sieht es aus? Keine Peers aufgeführt, oder die IP-Adresse des NTP-Servers stimmt nicht mit dem konfigurierten Anbieter überein. Dies weist in der Regel darauf hin, dass die Richtlinie für Datum und Uhrzeit nicht über die Pod Policy Group/Pod Profile Chain angewendet wurde.

NTP-Peer-Status anzeigen

Überprüfen Sie, ob der NTP-Server für die Synchronisierung ausgewählt ist.

<#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
```

Das `*`-Zeichen ist erforderlich und bestätigt, dass der NTP-Server für die Synchronisierung verwendet wird.

Wie schlecht sieht es aus?

- Nein`*` neben dem Server - der Switch wird nicht mit dem Server synchronisiert.
- `reach` ist `0` - es wurden keine NTP-Antworten empfangen. Dies weist auf ein Problem mit der Erreichbarkeit hin.
- `st` ist `16` - Der NTP-Server ist nicht synchronisiert und kann keine gültige Zeit angeben.

show ntp statistics peer ipadr

Überprüfen Sie den NTP-Paketaustausch, um die Erreichbarkeit zu bestätigen. Ersetzen Sie die IP-Adresse durch die NTP-Anbieteradresse für den betroffenen Switch.

<#root>

```
leaf1#

show ntp statistics peer ipaddr 10.1.1.100

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

Wie gut sieht es aus? `Gesendete` und `empfangene Pakete` sind in etwa gleich groß und nehmen immer mehr zu.

Wie schlecht sieht es aus? `Gesendete Pakete` werden inkrementiert, aber `empfangene Pakete` sind `0` oder kaum inkrementiert - NTP-Antworten erreichen den Switch nicht.

show clock

<#root>

```
leaf1#

show clock

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

GUI-Überprüfung

Navigieren Sie zu Fabric > Fabric Policies > Policies > Pod > Date and Time > [Your Policy] > [NTP Provider].

In der Spalte Synchronisierungsstatus sollte für alle Knoten "Mit Remote-NTP-Server synchronisiert" angezeigt werden. Nach der Erstbereitstellung kann es einige Minuten dauern, bis der Synchronisierungsstatus konvergiert.

API-Verifizierung

Abfragen der `datetimeNtpq`-Klasse, um die NTP-Synchronisierung in allen APICs zu überprüfen:

<#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.
```

Fehlerbehebung-Workflow

Verwenden Sie diesen Entscheidungsbaum, wenn ein NTP-Problem für einen ACI-Knoten gemeldet wird.

Schritt 1: Sind auf dem Switch NTP-Peers konfiguriert?

Melden Sie sich beim betroffenen Switch an, und führen Sie Folgendes aus:

<#root>

`leaf1#`

`show ntp peers`

- Keine Peers aufgeführt → Die Richtlinie "Datum und Uhrzeit" wurde nicht auf diesen Knoten angewendet. Fahren Sie mit Szenario 1 fort: NTP-Anbieter wurde nicht an den Switch gesendet.
- Die aufgeführten Peers → fahren mit Schritt 2 fort.

Phase 2: Wurde der NTP-Server für die Synchronisierung ausgewählt?

<#root>

`leaf1#`

`show ntp peer-status`

- `*` vorhanden → NTP wird synchronisiert. Wenn die Zeit immer noch falsch erscheint, gehen Sie zu Szenario 5: Großer Offset/Uhrzeitdrift.
- Nein`*` vorhanden → Fahren Sie mit Schritt 3 fort.

Schritt 3: Ist der Erreichbarkeitswert Null?

Überprüfen Sie die Spalte `reach` in `show ntp peer-status`.

- **`reach` = `0`** → keine Antworten vom NTP-Server. Fahren Sie mit Szenario 2 fort: NTP-Server

nicht erreichbar.
- `reach > 0`, aber keine `*`→-Antworten werden empfangen, aber die Synchronisierung wurde nicht hergestellt. Schicht überprüfen - Fahren Sie mit Schritt 4 fort.

Schritt 4: Ist der Schichtwert 16?

- Stratum = 16 → Der NTP-Server ist nicht mit seiner eigenen Upstream-Quelle synchronisiert. Fahren Sie mit Szenario 3 fort: NTP-Server nicht synchronisiert (Schicht 16).
- Schicht 1-15, aber keine Synchronisierung → weiter mit Szenario 4: NTP-Authentifizierungskonflikt.

Häufige Fehlerbehebungsszenarien

Szenario 1: NTP-Anbieter wird nicht an Switch gesendet

Symptom: `show ntp peers` auf dem Switch gibt keine Einträge zurück.

Konfigurationsprüfung:

1. Vergewissern Sie sich, dass für die Richtlinie "Datum und Uhrzeit" mindestens ein NTP-Anbieter konfiguriert ist.
2. Vergewissern Sie sich, dass die POD-Richtliniengruppe auf die richtige Datum- und Uhrzeitrichtlinie verweist.
3. Vergewissern Sie sich, dass das Pod-Profil auf die richtige Pod-Richtliniengruppe verweist.
4. Überprüfen Sie, ob dem Knoten eine Management-IP-Adresse unter dem mgmt-Tenant zugewiesen wurde.

Ursache: Eines der vier Glieder in der Richtlinienkette (Datum- und Uhrzeitrichtlinie → NTP-Anbieter → Pod-Richtliniengruppe → Pod-Profil) ist beschädigt. Die häufigste Ursache ist, dass die Pod-Richtliniengruppe nicht mit dem Pod-Profil verknüpft ist oder dass die Datums- und Uhrzeitrichtlinie nicht in der Pod-Richtliniengruppe ausgewählt ist.

Lösung: Schließen Sie das fehlende Glied in der Richtlinienkette ab. Stellen Sie sicher, dass das Pod-Profil für den betroffenen Pod auf eine Pod-Richtliniengruppe verweist, die die richtige Datums- und Uhrzeitrichtlinie enthält. Nach der Anwendung wird die NTP-Anbieterkonfiguration innerhalb weniger Minuten per Push an die Switches übertragen.

Szenario 2: NTP-Server nicht erreichbar

Symptom: `show ntp peer-status shows reach = 0.show ntp statistics peer ipaddr 10.1.1.100` zeigt `empfangene Pakete` = `0` an.100

Konfigurationsprüfung: Überprüfen Sie, ob der NTP-Anbieter mit der richtigen Management-EPG (OOB oder In-Band) verknüpft ist. Wenn Sie OOB verwenden, überprüfen Sie, ob die OOB-Verträge den UDP-Port 123 zulassen.

Betriebsprüfung:

1. Pingen Sie den NTP-Server vom betroffenen Switch mithilfe des Management-VRF:
   <#root>

   ```
   leaf1#

   ping 10.1.1.100 vrf management
   ```

2. Führen Sie einen tcpdump auf dem Switch aus, um zu überprüfen, ob NTP-Pakete versendet werden und ankommen:
   <#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
   ```

Ursache: In der Regel eine der folgenden:

- Dem Switch wurde keine Management-IP-Adresse zugewiesen.
- Das Standard-Gateway für die Verwaltungs-VRF-Instanz fehlt oder ist falsch.
- Eine Firewall blockiert den UDP-Port 123 zwischen dem Switch und dem NTP-Server.
- Der OOB-Vertrag lässt den UDP-Port 123 nicht zu.
- Der NTP-Anbieter verweist auf die falsche Management-EPG (z. B. OOB ausgewählt, aber nur In-Band-Verbindung erreichbar).

Lösung: Beheben Sie das Erreichbarkeitsproblem. Weisen Sie eine Management-Adresse zu, wenn diese fehlt, beheben Sie das Standard-Gateway, aktualisieren Sie die Firewall-Regeln, oder korrigieren Sie die Auswahl der Management-EPG für den NTP-Anbieter.

Szenario 3: NTP-Server nicht synchronisiert (Schicht 16)

Symptom: `show ntp peer-status` shows stratum (`st`) = `16`. Der Switch wird nicht mit einem stratum 16-Server synchronisiert.

Betriebsprüfung: Melden Sie sich beim NTP-Server an, oder fragen Sie diesen von einem externen Host ab, um zu überprüfen, ob er mit seiner eigenen Upstream-Zeitquelle synchronisiert ist.

Ursache: Der NTP-Server selbst hat die Synchronisierung mit dem Upstream-Referenztakt verloren. Ein Server mit Schicht 16 kündigt an, keine zuverlässige Zeitquelle zu haben.

Lösung: Reparieren Sie den NTP-Server. Diese befindet sich außerhalb der ACI-Fabric. Überprüfen Sie die NTP-Serverkonfiguration und die Upstream-Zeitquelle. Wenn der NTP-Server nicht sofort repariert werden kann, konfigurieren Sie in der Richtlinie "Date and Time" (Datum und Uhrzeit) einen alternativen NTP-Anbieter.

Szenario 4: Nichtübereinstimmung der NTP-Authentifizierung

Symptom: `show ntp peer-status` gibt `reach` **>** `0` und stratum als gültig an, es wird jedoch kein `*` angezeigt. Der NTP-Server antwortet, der Switch akzeptiert die Antwort jedoch nicht.

Konfigurationsprüfung:

1. Überprüfen Sie, ob der NTP-Server eine Authentifizierung erfordert.
2. Wenn eine Authentifizierung erforderlich ist, stellen Sie sicher, dass der Authentifizierungsstatus der Datums- und Uhrzeitrichtlinie auf Aktiviert festgelegt ist.
3. Überprüfen der Übereinstimmung von Authentifizierungsschlüssel-ID, Schlüsselwert und Algorithmus (MD5, SHA-1 oder AES128-CMAC) zwischen der ACI-Fabric und dem NTP-Server
4. Überprüfen Sie, ob der Schlüssel in der Tabelle mit den NTP-Client-Authentifizierungsschlüsseln als vertrauenswürdig markiert ist.

Ursache: Der Authentifizierungsschlüssel, der Algorithmus oder die Schlüssel-ID stimmen nicht mit der ACI und dem NTP-Server überein, sodass der Switch die NTP-Antwort als nicht authentifiziert zurückweist.

Lösung: Richten Sie die Authentifizierungskonfiguration aus. Stellen Sie sicher, dass auf der ACI und dem NTP-Server dieselbe Schlüssel-ID, derselbe Schlüsselwert und derselbe Algorithmus konfiguriert sind. AES128-CMAC wird für APIC-Version 6.1(1) und höher empfohlen.

Anmerkung: Wenn der FIPS-Modus aktiviert ist, werden nur die Authentifizierungsschemata

AES128-CMAC und SHA-1 unterstützt. MD5 funktioniert nicht im FIPS-Modus.

Szenario 5: Großer Offset/Uhrzeitdrift

Symptom: Der Switch scheint synchronisiert zu sein (* vorhanden, erreichen = 377), aber der `Offset`-Wert in `show ntp peer-status` oder `show ntpq` ist sehr groß (Hunderte oder Tausende Millisekunden), oder die Uhr ist offensichtlich falsch.

Betriebsprüfung:

<#root>

apic1#

show ntpq

Überprüfen Sie die `Offset`-Spalte. Ein gesunder Offset liegt typischerweise unter 100 ms.

Ursache: Der Takt driftete deutlich, bevor die NTP-Synchronisation hergestellt wurde, oder der Hardware-Takt (RTC) wurde während eines Neustarts zurückgesetzt (z. B. aufgrund einer ausgestorbenen CMOS-Batterie). NTP korrigiert die Uhr schrittweise durch Drehen, was bei großen Offsets Zeit in Anspruch nehmen kann.

Lösung: Wenn der Offset sehr groß ist und das NTP aktiv synchronisiert wird, warten Sie, bis die Uhr konvergiert. NTP verschiebt die Uhr allmählich - große Offsets können Stunden dauern, bis sie vollständig korrigiert sind. Wenn der Offset nicht kleiner wird, stellen Sie sicher, dass der NTP-Server die korrekte Zeit bereitstellt. Wenn das Problem nach jedem Neustart erneut auftritt, überprüfen Sie die Hardware-Uhr (RTC-/CMOS-Batterie) des betroffenen Knotens.

Szenario 6: Standby-APIC-Fehler mit In-Band-NTP

Symptom: Wenn NTP für das In-Band-Management konfiguriert ist, werden auf einem Standby-APIC Fehler in Bezug auf das NTP oder die Überwachungsrichtlinie generiert.

Ursache: Wenn eine NTP-Richtlinie für das In-Band-Management angewendet wird, erfordert der Standby-APIC auch eine In-Band-Konfiguration. Ohne sie entstehen Fehler.

Lösung: Konfigurieren Sie auch das In-Band-Management für den Standby-APIC. Dadurch

werden die Fehler behoben.

Szenario 7: IP-Fehler duplizieren

Symptom: Nach dem Hinzufügen von NTP-Anbietern wird ein Fehler "Duplicate IP" (Duplizierte IP) ausgelöst.

Ursache: Ein FQDN wurde als NTP-Anbieter hinzugefügt, und dann wurde die aufgelöste IP-Adresse dieses FQDN als zweiter NTP-Anbieter hinzugefügt. ACI erkennt das Duplikat.

Lösung: Löschen Sie den zuletzt hinzugefügten doppelten Anbieter (den IP-Adresseintrag, wenn der FQDN zuerst hinzugefügt wurde, oder umgekehrt). Verwenden Sie nur einen Eintrag pro NTP-Server - entweder FQDN- oder IP-Adresse, nicht beides.

Szenario 8: DNS-Auflösungsfehler für FQDN-basierten NTP-Anbieter

Symptom: Der mit einem Hostnamen konfigurierte NTP-Anbieter wird nicht aufgelöst. `show ntp peers` zeigt nicht die erwartete IP-Adresse an, oder das NTP wird nicht synchronisiert.

Konfigurationsprüfung:

1. Vergewissern Sie sich, dass eine DNS-Dienstrichtlinie unter Fabric > Fabric Policies > Policies > Global > DNS Profiles konfiguriert ist.
2. Überprüfen Sie, ob der DNS-Provider (DNS-Server) über die Management-VRF-Instanz erreichbar ist.
3. Überprüfen Sie, ob das entsprechende DNS-Label für die In-Band- oder Out-of-Band-VRF-Instanz der Verwaltungs-EPG konfiguriert ist.

Ursache: Der DNS-Server kann nicht erreicht werden oder ist nicht konfiguriert, was dazu führt, dass die Auflösung des Hostnamens für den NTP-Anbieter fehlschlägt.

Lösung: Konfigurieren Sie die DNS-Dienstrichtlinie, stellen Sie die DNS-Erreichbarkeit sicher, und wenden Sie die richtige DNS-Bezeichnung an. Alternativ können Sie die IP-Adresse des NTP-Servers anstelle des Hostnamens verwenden.

Zugehörige Fehler und Ereignisse

Im Folgenden sind NTP-bezogene Bedingungen aufgeführt, die zu Fehlern in der ACI führen

können:

- Doppelter IP-Fehler - Wird ausgelöst, wenn ein FQDN und die IP-Adresse desselben NTP-Servers beide als Provider hinzugefügt werden. Auflösung: doppelten Eintrag entfernen.
- In-Band-NTP-Fehler des Standby-APIC — werden ausgelöst, wenn eine Überwachungs- oder NTP-Richtlinie für In-Band angewendet wird, der Standby-APIC jedoch keine In-Band-Konfiguration aufweist.
- Synchronisierungsstatus nicht konvergierend - Die GUI zeigt für einen oder mehrere Knoten "Nicht synchronisiert" oder einen anderen Status als "Mit Remote-NTP-Server synchronisiert" an. Dabei handelt es sich nicht um einen Fehlercode, sondern um eine Betriebsstatusanzeige. Befolgen Sie den oben beschriebenen Workflow zur Fehlerbehebung, um eine Diagnose durchzuführen.

Eskalationskriterien

Ziehen Sie in folgenden Fällen eine Eskalation an das Cisco TAC in Betracht:

- Die Konfigurationskette ist verifiziert und der NTP-Server erreichbar (Ping funktioniert, Tcpdump zeigt NTP-Antworten an), aber der Switch wird immer noch nicht synchronisiert.
- Die NTP-Synchronisierung geht ohne Konfigurationsänderungen oder NTP-Serverprobleme wiederholt verloren.
- Die Ausgabe `von show ntp peer-status` zeigt ein unerwartetes Verhalten, z. B. eine persistente Schicht 16 auf einem Server, der extern synchronisiert wurde.
- Die Uhr bewegt sich erheblich zwischen Neustarts, was auf ein Problem mit der Hardware-Uhr (RTC) hinweisen kann.

Geben Sie bei der Kontaktaufnahme mit dem TAC folgende Daten an:

- Ausgabe von `show ntpq` von allen APICs
- Ausgabe von `show ntp peers`, `show ntp peer-status`, `show ntp statistics peer ipaddr <IP>` und `show clock` von allen betroffenen Switches.
- Ausgabe von `moquery -c datetimePol`, `moquery -c datetimeNtpProv` und `moquery -c datetimeNtpq` vom APIC.
- Ein technischer Support von den betroffenen Knoten.

Referenzen

- Cisco APIC Basic Konfigurationsleitfaden, Version 6.1(x) - Bereitstellung von Core ACI Fabric Services
- Fehlerbehebung bei ACI Management und Core Services - Pod-Richtlinien

- Cisco Application Centric Infrastructure (ACI) - Designleitfaden

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.