對思科ACI交換矩陣中的NTP進行故障排除

簡介

本檔案介紹如何驗證、疑難排解和解決思科ACI交換矩陣中的網路時間協定(NTP)問題。它包括NTP策略模型、配置驗證、操作驗證命令、常見NTP症狀的分類工作流程以及詳細的故障排除場景。

背景資訊

本文檔中的資料摘自ACI管理和核心服務故障排除 — Pod策略指南、思科APIC基本配置指南6.1(x)版 — 調配核心ACI交換矩陣服務一章和思科ACI設計手冊。

概觀

時間同步是ACI交換矩陣中的一項關鍵功能，監控、操作和故障排除任務都依賴於該功能。時鐘同步可確保正確分析通訊流、跨多個交換矩陣節點的調試和故障時間戳的相關性，以及充分利用應用程式運行狀況得分所依賴的原子計數器功能。不存在或不正確的NTP配置不一定觸發故障或低健康評分，因此必須在交換矩陣部署早期配置時間同步。

ACI中的NTP策略模型

ACI中的NTP通過四個策略對象鏈進行管理：

1. 日期和時間策略(`datetimePol`) — 定義NTP配置，包括管理狀態、身份驗證狀態、伺服器狀態和主模式。位於Fabric > Fabric Policies > Policies > Pod > Date and Time下。
2. NTP Provider(`datetimeNtpProv`) — 定義日期和時間策略內的各個NTP伺服器條目（提供程式），包括伺服器IP/FQDN、管理EPG選擇（帶外或帶內）、首選標誌和輪詢間隔。
3. Pod策略組(`fabricPodPGrp`) — 引用日期和時間策略以及其他Pod級別策略（BGP RR、SNMP等）。 位於Fabric > Fabric Policies > Pod > Policy Groups下。
4. Pod配置檔案(`fabricPodP`) — 將Pod策略組與Pod選擇器相關聯。位於Fabric > Fabric Policies > Pod > Profiles下。

必須配置此鏈中的所有四個鏈路，才能將NTP應用於交換矩陣節點。如果任何鏈路斷開，將不會將NTP提供程式配置推送到交換機。

必要條件

- 必須完成交換矩陣發現。
- 節點管理地址（OOB或帶內）必須分配給mgmt租戶下的所有APIC和交換機。
- 對於帶外NTP，OOB管理EPG必須允許UDP埠123。
- 對於帶內NTP，必須配置帶內管理EPG，使之具有適當的合約並可與NTP伺服器連線。如果沒有其他策略，則無法從交換矩陣外部訪問帶內IP地址。

NTP身份驗證

ACI支援三個NTP身份驗證方案：MD5、SHA-1和AES128-CMAC。AES128-CMAC是在APIC版本6.1(1)中引入的，是推薦的方案，因為MD5被認為軟弱和不安全。啟用FIPS模式後，僅支援AES128-CMAC和SHA-1。

NTP伺服器功能

ACI枝葉交換機可以充當下遊客戶端（例如連線到交換矩陣的伺服器）的NTP伺服器。 預設情況下，此功能處於禁用狀態，必須通過「日期和時間」策略中的伺服器狀態選項顯式啟用該功能。啟用時，客戶端可以使用枝葉交換機帶內、帶外、橋接域SVI或L3Out IP地址作為NTP伺服器地址。

附註：交換矩陣交換機不應與同一交換矩陣的其他交換機同步。交換矩陣交換機應始終同步到外部NTP伺服器。

驗證設定

在對NTP運行狀態進行故障排除之前，請驗證配置鏈是否完成。配置錯誤是ACI中NTP問題的最常見根本原因。

步驟 1:驗證節點管理地址

導航到Tenants > mgmt > Node Management Addresses（用於靜態分配）或Node Management EPG（用於連線組）。

確認每個APIC和交換機節點都分配了管理IP地址。沒有管理地址的節點無法與NTP伺服器通訊。

或者，查詢API:

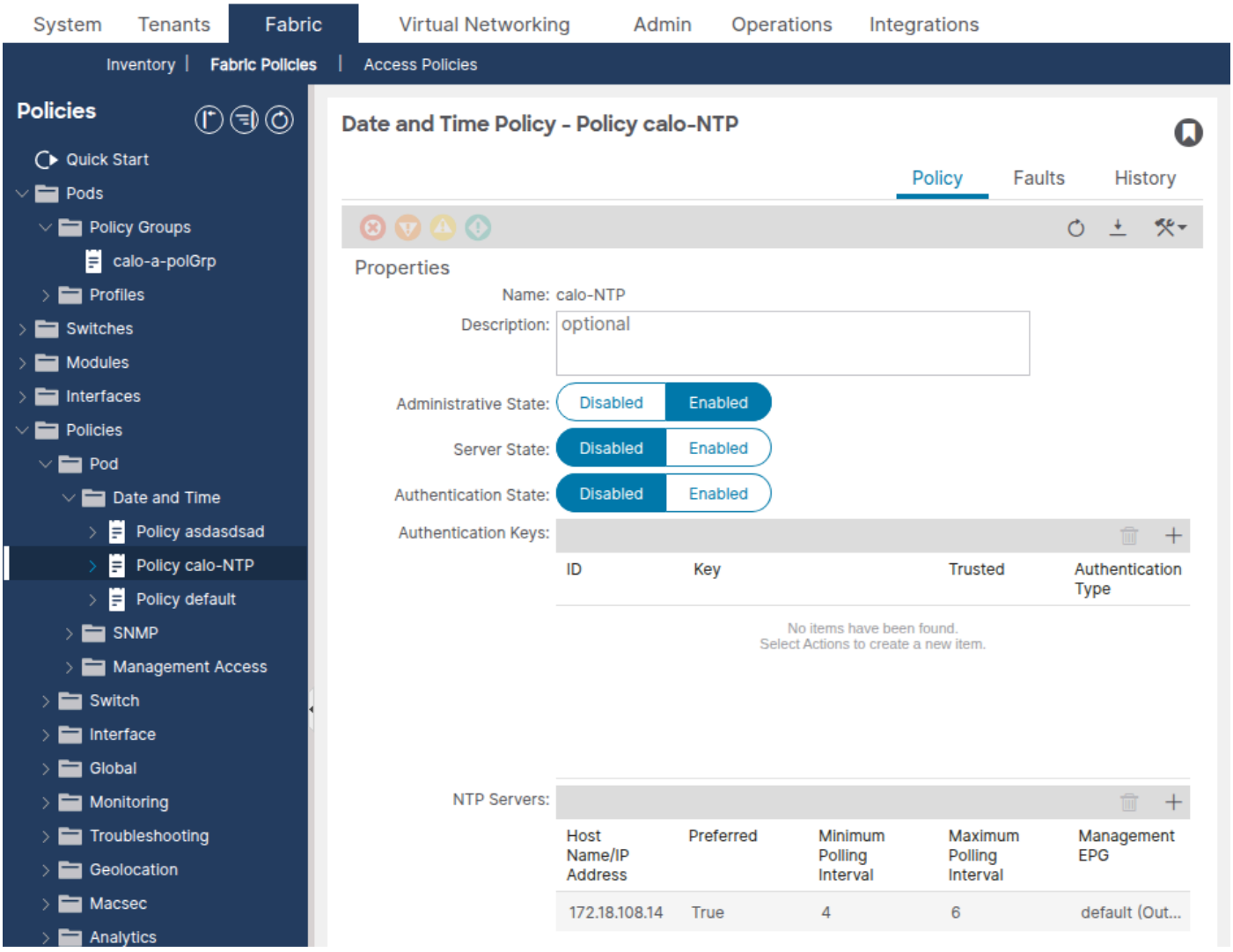
<#root>

apic1#

moquery -c mgmtRsOoBStNode

步驟 2:驗證日期和時間策略是否具有NTP提供程式

導航到Fabric > Fabric Policies > Policies > Pod > Date and Time > [Your Policy]。



確認至少配置了一個NTP提供程式（伺服器）。如果存在多個提供程式，則至少將一個標籤為首選。

通過API驗證NTP提供程式：

<#root>

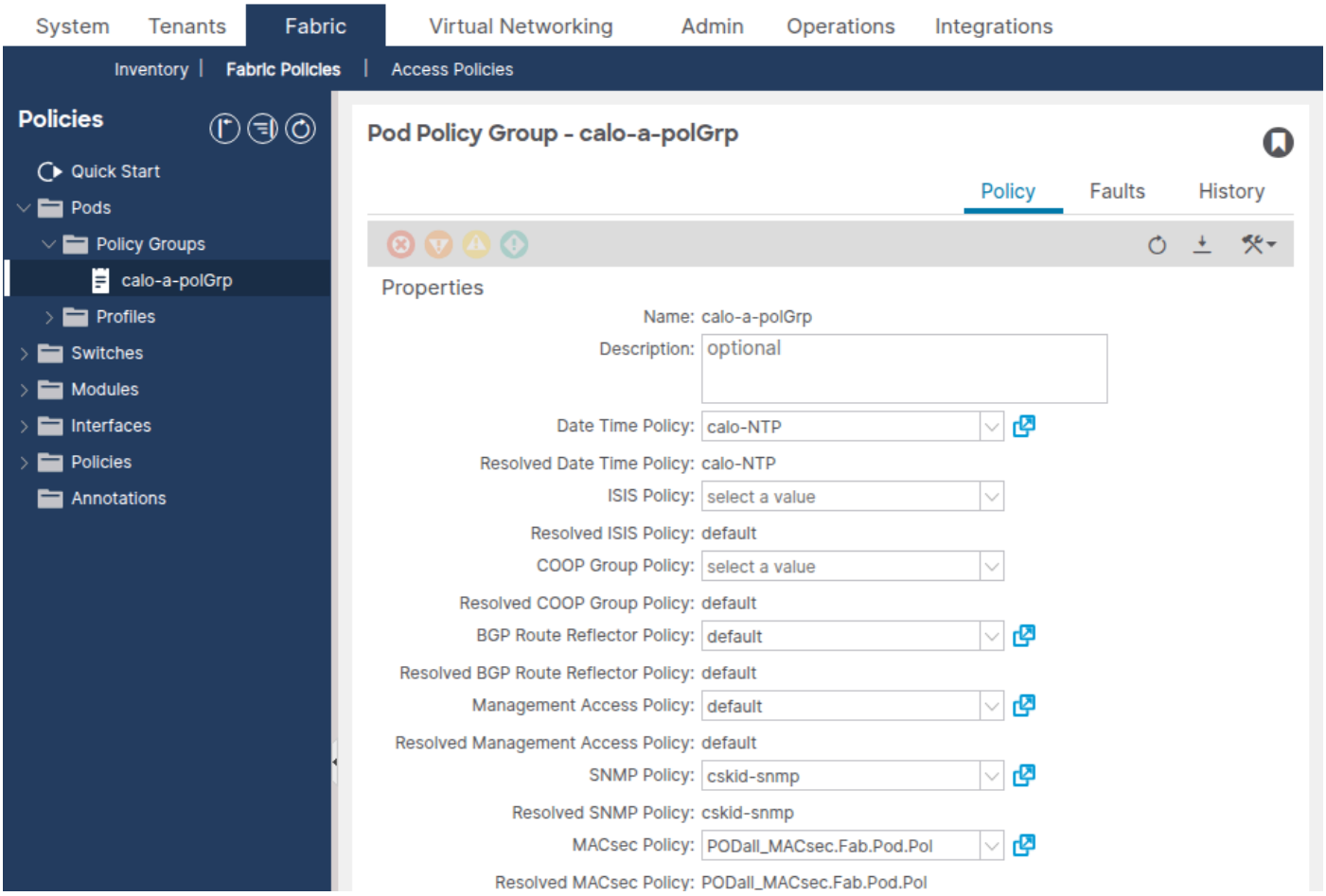
```
apic1#

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
```

常見配置錯誤

- 未配置NTP提供程式 — 「日期和時間」策略存在，但具有零提供程式。將應用該策略，但節點沒有可同步的NTP伺服器。
- 選擇的管理EPG錯誤 — NTP提供程式引用帶外EPG，但NTP伺服器只能通過帶內訪問（反之亦然）。 驗證哪個管理EPG提供了與NTP伺服器的可達性。
- 作為單獨提供程式新增的同一伺服器的FQDN和IP — 這將生成重複IP故障。刪除重複條目。
- 無DNS策略的基於FQDN的提供程式 — 如果為NTP提供程式使用主機名，請確保已配置DNS服務策略並將適當的DNS標籤應用到管理VRF。

步驟 3:驗證Pod策略組引用日期和時間策略

導航到Fabric > Fabric Policies > Pod > Policy Groups > [您的Pod Policy Group]。



確認Date Time Policy欄位引用正確的日期和時間策略。

<#root>

apic1#

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

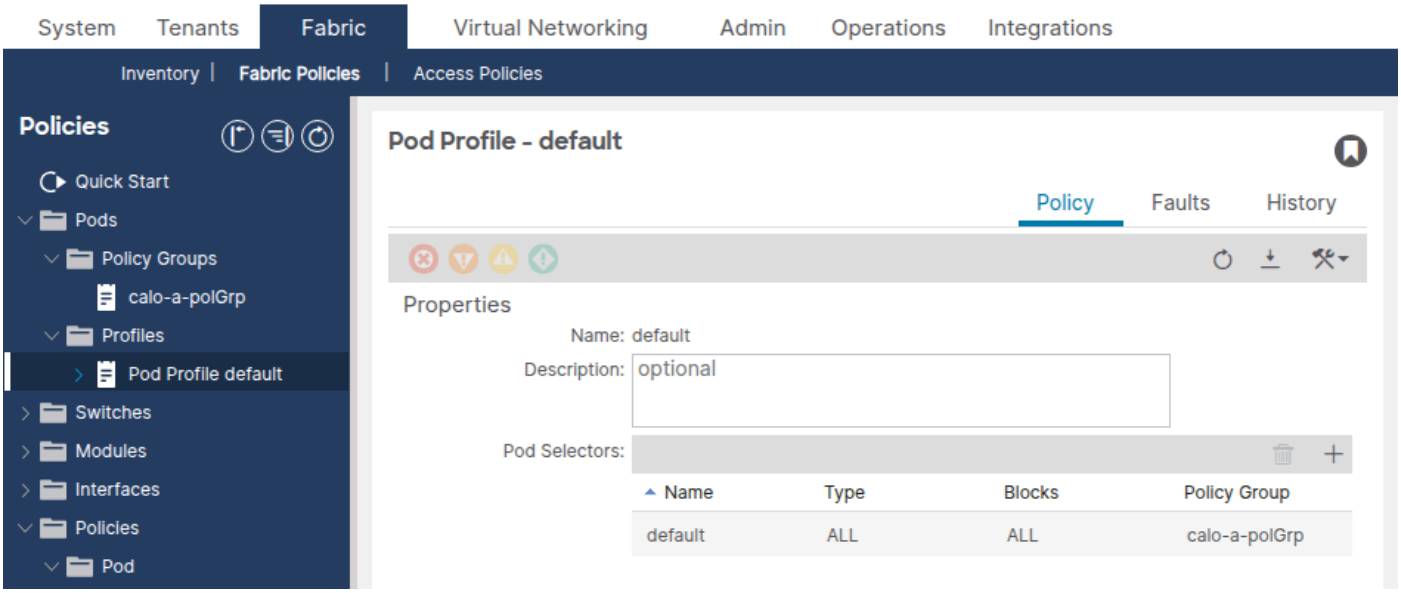
查詢datetimePolName屬性或關聯的fabricRsTimePol關係。

常見配置錯誤

- Pod策略組引用了錯誤的日期和時間策略 — 如果存在多個日期和時間策略(例如，「預設」策略和一個自定義策略)，請驗證Pod策略組是否引用了預期策略。
- Pod策略組完全未建立 — 預設的Pod策略組可能沒有關聯日期和時間策略。請始終驗證。

步驟 4:驗證Pod配置檔案引用Pod策略組

導航到Fabric > Fabric Policies > Pod > Profiles > [Your Pod Profile]。



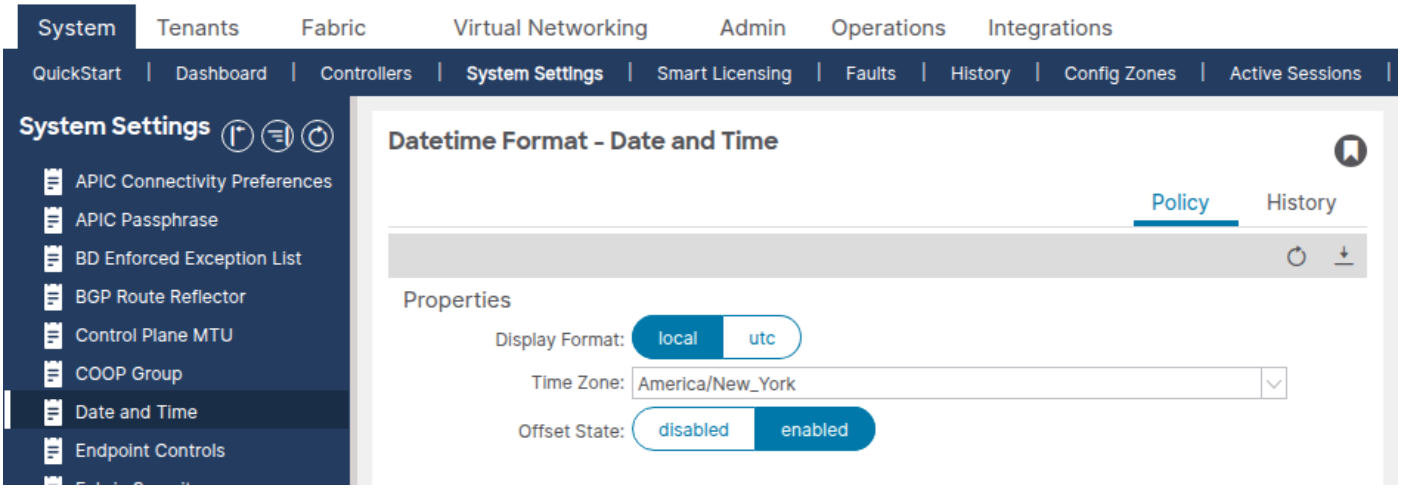
確認Fabric Policy Group欄位引用正確的Pod Policy Group。

常見配置錯誤

- Pod配置檔案引用錯誤的Pod策略組 — 尤其是在多Pod環境中，每個Pod配置檔案必須引用正確的Pod策略組。

步驟 5:驗證日期和時間格式

導航到System > System Settings > Date and Time。



確認顯示格式（本地或UTC）和時區已按預期設定。此設定是單獨的預設日期時間格式策略，不能

刪除或複製。

操作驗證

確認配置鏈正確後，使用以下命令驗證NTP在運行時是否正常工作。

APIC驗證

show ntpq

此命令顯示所有APIC上的NTP同步狀態。*符號表示已選擇伺服器進行同步。

<#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
```

好看的樣子：

- 所有APIC在遠端伺服器旁顯示*（已選定進行同步）。
- reach is 377（八進位），表示最後8次民調均成功。
- st（層）介於1到15之間。第16層表示伺服器不同步。
- 偏移量較低（正常環境通常小於100 ms）。

壞的樣子：

- 任何伺服器旁邊都沒有* — 未選擇要同步的伺服器。
- reach is 0 — 未收到NTP響應。
- st is 16 – NTP伺服器未與其上游時間源同步。
- 偏移非常大（數千毫秒） — 時鐘明顯漂移。

show clock

```
<#root>
apic1#
show clock
Time : 11:24:18.391 UTC-04:00 Tue Apr 07 2026
```

確認時間準確。請比較檢測時鐘漂移的預期時間。

APIC Bash（備選）

```
<#root>
apic1#
bash
admin@apic1:~>
date
Tue Apr 7 11:24:45 EDT 2026
```

交換機驗證（枝葉/主幹）

show ntp peers

驗證是否已將NTP提供程式推送到交換機。

```
<#root>
leaf1#
show ntp peers
-------------------------------------------------------------------------------
  Peer IP Address                 Serv/Peer Prefer KeyId   Vrf
-------------------------------------------------------------------------------
  10.1.1.100                      Server    yes    None    management
```

好看的樣子：NTP伺服器IP或主機名顯示為Serv/Peer = Server，並且有正確的VRF(通常是OOB管理)。

壞的樣子：未列出對等體，或NTP伺服器IP與配置的提供程式不匹配。這通常表示日期和時間策略未通過Pod策略組/Pod配置檔案鏈應用。

show ntp peer-status

驗證是否已選擇NTP伺服器進行同步。

<#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
```

*字元至關重要 — 它確認正在使用NTP伺服器進行同步。

壞的樣子：

- 伺服器旁邊沒有* — 交換機沒有同步到伺服器。
- reach is 0 — 未收到NTP響應。這表示存在可達性問題。
- st is 16 – NTP伺服器未同步，因此無法提供有效時間。

show ntp statistics peer ipaddr

驗證NTP資料包交換以確認可達性。用受影響交換機的NTP提供商地址替換IP地址。

<#root>

```
leaf1#

show ntp statistics peer ipaddr 10.1.1.100

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

...

好看的樣子：傳送的資料包和接收的資料包大致相同，並且呈遞增趨勢。

壞的樣子：傳送的數據包正在遞增，但接收的資料包為0或幾乎沒有遞增 — NTP響應沒有到達交換機。

show clock

<#root>

leaf1#

show clock

11:24:24.121066 EDT Tue Apr 07 2026

GUI驗證

導航到Fabric > Fabric Policies > Policies > Pod > Date and Time > [Your Policy] > [NTP Provider]。

對於所有節點，Sync Status列應顯示Synced to Remote NTP Server。初始部署後可能需要幾分鐘才能使同步狀態收斂。

API驗證

查詢datetimeNtpq類以檢查所有APIC上的NTP同步：

<#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.
```

工作流故障排除

在任何ACI節點上報告NTP問題時，請使用此診斷樹。

步驟 1:交換機上是否配置了NTP對等體？

登入受影響的交換器並執行：

<#root>

leaf1#

show ntp peers

- 「日期和時間→略」中列出的任何對等體均未應用於此節點。前往案例1:NTP提供程式未推送到交換機。
- 列出的對→將繼續執行步驟2。

步驟 2:是否選擇要同步的NTP伺服器？

<#root>

leaf1#

show ntp peer-status

- *存在→ NTP正在同步。如果時間仍顯示錯誤，請轉至案例5:大偏移/時鐘偏移。
- 否*存在→繼續步驟3。

步驟 3:到達值是否為零？

檢查show ntp peer-status中的reach列。

- **reach**

= 0 →沒有來自NTP伺服器的響應。前往案例2:無法訪問NTP伺服器。
- reach > 0，但沒有* →響應到達，但未建立同步。檢查層 — 轉至步驟4。

步驟 4:層值是否為16?

- 層數= 16 → NTP伺服器未與其自己的上游源同步。前往案例3:NTP伺服器不同步（第16層）。
- 第1-15層但無同步→進入場景4:NTP身份驗證不匹配。

常見故障排除場景

案例 1:未將NTP提供程式推送到交換機

症狀：`show ntp peers` on the switch return no entries。

配置檢查：

1. 驗證日期和時間策略是否至少配置了一個NTP提供程式。
2. 驗證Pod策略組引用的日期和時間策略是否正確。
3. 驗證Pod配置檔案引用正確的Pod策略組。
4. 驗證節點是否在mgmt租戶下分配了管理IP地址。

根本原因：→策略鏈中的四個連結之一(NTP Provider和Pod Policy Group和Pod Profile的日期和時間策略→Date and Time Policy → Pod Profile)已損壞。最常見的原因是Pod策略組沒有與Pod配置檔案相關聯，或者在Pod策略組中未選擇「日期和時間」策略。

解決方案：完成策略鏈中缺少的連結。確保受影響的Pod的Pod配置檔案引用包含正確日期和時間策略的Pod策略組。應用後，NTP提供商配置將在幾分鐘內推送到交換機。

案例 2:NTP伺服器無法訪問

症狀：show ntp peer-status顯示`reach = 0`。`show ntp statistics peer ipaddr 10.1.1.100`顯示`packets received = 0`。

配置檢查：驗證NTP提供程式與正確的管理EPG（OOB或帶內）關聯。 如果使用OOB，請驗證OOB合約是否允許UDP埠123。

操作檢查：

1. 使用管理VRF從受影響的交換機ping NTP伺服器：
   <#root>

   ```
   leaf1#

   ping 10.1.1.100 vrf management
   ```

2. 在交換機上運行tcpdump以檢查NTP資料包是否正在離開和到達：
   <#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
   ```

根本原因：通常為以下其中一項：

- 交換機沒有分配管理IP地址。
- 管理VRF的預設網關缺失或不正確。
- 防火牆正在阻止交換機和NTP伺服器之間的UDP埠123。
- OOB合約不允許UDP埠123。
- NTP提供器引用了錯誤的管理EPG（例如，已選擇OOB，但只有帶內才有可達性）。

解決方案：解決可接通性問題。如果缺少管理地址，請分配管理地址，修復預設網關，更新防火牆規則，或更正NTP提供程式上的管理EPG選擇。

案例 3:NTP伺服器不同步（第16層）

症狀：`show ntp peer-status`顯示層(st)= 16。交換機不會同步到層16伺服器。

操作檢查：登入到NTP伺服器或從外部主機查詢它，以驗證它是否與自己的上游時間源同步。

根本原因：NTP伺服器本身已丟失與其上游參考時鐘的同步。第16層的伺服器通告它沒有可靠的時間源。

解決方案：修復NTP伺服器。這是在ACI交換矩陣之外 — 檢查NTP伺服器配置及其上游時間源。如果無法立即修復NTP伺服器，請在「日期和時間」策略中配置備用NTP提供程式。

案例 4:NTP身份驗證不匹配

症狀：`show ntp peer-status`顯示`reach` > `0`和stratum有效，但不會顯示`no`*。NTP伺服器響應，但交換機不接受響應。

配置檢查：

1. 驗證NTP伺服器是否需要身份驗證。
2. 如果需要身份驗證，請驗證Date and Time（日期和時間）策略是否將Authentication State（身份驗證狀態）設定為Enabled(啟用)。
3. 驗證ACI交換矩陣和NTP伺服器之間的身份驗證金鑰ID、金鑰值和演算法（MD5、SHA-1或AES128-CMAC）匹配。
4. 驗證NTP客戶端身份驗證金鑰(NTP Client Authentication Keys)表中將該金鑰標籤為Trusted。

根本原因：身份驗證金鑰、演算法或金鑰ID在ACI和NTP伺服器之間不匹配，導致交換機拒絕NTP響應為未經身份驗證。

解決方案：調整身份驗證配置。確保在ACI和NTP伺服器上配置相同的金鑰ID、金鑰值和演算法。對於APIC 6.1(1)版及更高版本，建議使用AES128-CMAC。

附註：啟用FIPS模式時，僅支援AES128-CMAC和SHA-1身份驗證方案。MD5無法在FIPS模式下工作。

案例 5:大偏移/時鐘偏移

症狀：交換器似乎已同步(* present， reach = 377)，但`show ntp peer-status`或`show ntpq`中的offset值非常大（數百或數千毫秒），或者時鐘明顯錯誤。

操作檢查：

<#root>

apic1#

show ntpq

檢查`偏移`列。正常偏移量通常小於100毫秒。

根本原因：在NTP同步建立之前，時鐘明顯漂移，或者在重新引導期間（例如，由於停用的CMOS電池）重置硬體時鐘(RTC)。NTP通過旋轉來逐步校正時鐘，因為大偏移會花費時間。

解決方案：如果偏移量非常大且NTP正在積極同步，請等待時鐘收斂。NTP會逐漸轉換時鐘 — 較大的偏移可能需要數小時才能完全校正。如果偏移量沒有減少，請驗證NTP伺服器是否提供了準確的時間。如果在每次重新啟動後問題再次出現，請檢查受影響節點的硬體時鐘（RTC/CMOS電池）。

案例 6:帶內NTP的備用APIC故障

症狀：當NTP配置為帶內管理時，與NTP或監控策略相關的備用APIC上生成故障。

根本原因：將NTP策略應用於帶內管理時，備用APIC還需要帶內配置。沒有它，錯誤就會出現。

解決方案：配置備用APIC的帶內管理。這樣可以清除缺陷。

案例 7:重複的IP故障

症狀：新增NTP提供程式後會引發重複IP故障。

根本原因：將FQDN新增為NTP提供程式，然後將該FQDN的解析IP地址新增為第二個NTP提供程式。ACI檢測到重複項。

解決方案：刪除最近新增的重複提供程式（如果先新增FQDN，則為IP地址條目，反之亦然）。 每個NTP伺服器僅使用一個條目 — FQDN或IP地址，而不是同時使用兩者。

案例 8:基於FQDN的NTP提供程式的DNS解析失敗

症狀：未解析使用主機名配置的NTP提供程式。`show ntp peers`未顯示預期的IP地址，或NTP未同步。

配置檢查：

1. 驗證Fabric > Fabric Policies > Policies > Global > DNS Profiles下是否配置了DNS服務策略。
2. 驗證是否可從管理VRF連線至DNS提供者（DNS伺服器）。
3. 驗證為管理EPG的帶內或帶外VRF例項配置了適當的DNS標籤。

根本原因：無法訪問或未配置DNS伺服器，導致NTP提供程式的主機名解析失敗。

解決方案：配置DNS服務策略，確保DNS可達性，並應用正確的DNS標籤。或者，使用NTP伺服器的IP地址而不是主機名。

相關故障和事件

以下是NTP相關條件，這些條件可能在ACI中生成故障：

- 重複的IP故障 — 當同一NTP伺服器的FQDN和IP地址均作為提供程式新增時引發。解析度：刪除重複條目。
- 備用APIC帶內NTP故障 — 當對帶內應用監控或NTP策略但備用APIC缺少帶內配置時引發。
- 未收斂的同步狀態 — GUI顯示一個或多個節點的「未同步」或「已同步到遠端NTP伺服器」以外的狀態。這不是故障代碼，而是運行狀態指示器。按照上面的故障排除工作流程進行診斷。

升級標準

在下列情況下，請考慮升級至Cisco TAC:

- 已驗證配置鏈是否正確並且NTP伺服器可訪問（ping工作正常，tcpdump顯示NTP響應），但交換機仍無法同步。
- 在不更改配置或NTP伺服器問題的情況下，NTP同步會反複丟失。
- `show ntp peer-status`輸出顯示意外行為，例如已在外部確認同步的伺服器上的永續性層16。
- 時鐘在重新引導之間明顯漂移，這可能表明存在硬體時鐘(RTC)問題。

在與TAC接洽時，請提供以下資料：

- 所有APIC的`show ntpq`輸出。
- 所有受影響交換機的`show ntp peers`、`show ntp peer-status`、`show ntp statistics peer ipaddr <IP>`和`show clock`的輸出。
- APIC的`moquery -c datetimePol`、`moquery -c datetimeNtpProv`和`moquery -c datetimeNtpq`的輸出。
- 受影響節點的技術支援。

參考資料

- 思科APIC基本配置指南6.1(x)版 — 調配核心ACI交換矩陣服務
- 排除ACI管理和核心服務故障 — Pod策略
- 思科以應用為中心的基礎設施(ACI)設計手冊

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。