排除Cisco ACI交换矩阵中的NTP故障

简介

本文档介绍如何验证、排除和解决思科ACI交换矩阵中的网络时间协议(NTP)问题。它包括NTP策略模型、配置验证、操作验证命令、常见NTP症状的分类工作流程以及详细的故障排除场景。

背景信息

本文档中的材料摘自ACI管理和核心服务故障排除 — Pod策略指南、思科APIC基本配置指南6.1(x)版 — 调配核心ACI交换矩阵服务一章和思科ACI设计指南。

概述

时间同步是ACI交换矩阵中的一项关键功能，监控、操作和故障排除任务都依赖于该功能。时钟同步可确保正确分析流量流，关联跨多个交换矩阵节点的调试和故障时间戳，以及充分利用应用运行状况得分所依赖的原子计数器功能。不存在或不正确的NTP配置不一定会触发故障或低运行状况得分，因此，在交换矩阵部署早期配置时间同步非常重要。

ACI中的NTP策略模型

ACI中的NTP通过四个策略对象链进行管理：

1. 日期和时间策略(`datetimePol`) — 定义NTP配置，包括管理状态、身份验证状态、服务器状态和主模式。位于Fabric > Fabric Policies > Policies > Pod > Date and Time。
2. NTP Provider(`datetimeNtpProv`) — 定义日期和时间策略中的单个NTP服务器条目（提供程序），包括服务器IP/FQDN、管理EPG选择（带外或带内）、首选标志和轮询间隔。
3. Pod策略组(`fabricPodPGrp`) — 引用日期和时间策略以及其他Pod级别策略（BGP RR、SNMP等）。 位于Fabric > Fabric Policies > Pod > Policy Groups。
4. Pod配置文件(`fabricPodP`) — 将Pod策略组与Pod选择器关联。位于Fabric > Fabric Policies > Pod > Profiles下。

必须配置此链中的所有四个链路，才能将NTP应用于交换矩阵节点。如果任何链路断开，NTP提供程序配置将不会推送到交换机。

先决条件

- 必须完成交换矩阵发现。
- 必须将节点管理地址（OOB或带内）分配给管理租户下的所有APIC和交换机。
- 对于带外NTP，OOB管理EPG必须允许UDP端口123。
- 对于带内NTP，必须配置带内管理EPG，使之具有适当的合同并可到达NTP服务器。如果没有其他策略，则无法从交换矩阵外部访问带内IP地址。

NTP身份验证

ACI支持三个NTP身份验证方案：MD5、SHA-1和AES128-CMAC。AES128-CMAC是在APIC版本6.1(1)中引入的，并且是推荐的方案，因为MD5被视为弱和不安全。启用FIPS模式时，仅支持AES128-CMAC和SHA-1。

NTP服务器功能

ACI枝叶交换机可以充当下游客户端（例如连接到交换矩阵的服务器）的NTP服务器。 默认情况下，此功能处于禁用状态，必须通过Date and Time策略中的Server State选项显式启用此功能。启用时，客户端可以使用枝叶交换机带内、带外、网桥域SVI或L3Out IP地址作为NTP服务器地址。

注意：交换矩阵交换机不应同步到同一交换矩阵的其他交换机。交换矩阵交换机应始终同步到外部NTP服务器。

验证配置

在对NTP运行状态进行故障排除之前，请验证配置链是否完整。配置错误是ACI中NTP问题的最常见根本原因。

步骤 1：验证节点管理地址

导航到租户>管理>节点管理地址（用于静态分配）或节点管理EPG（用于连接组）。

确认每个APIC和交换机节点都分配了管理IP地址。没有管理地址的节点无法与NTP服务器通信。

或者，查询API:

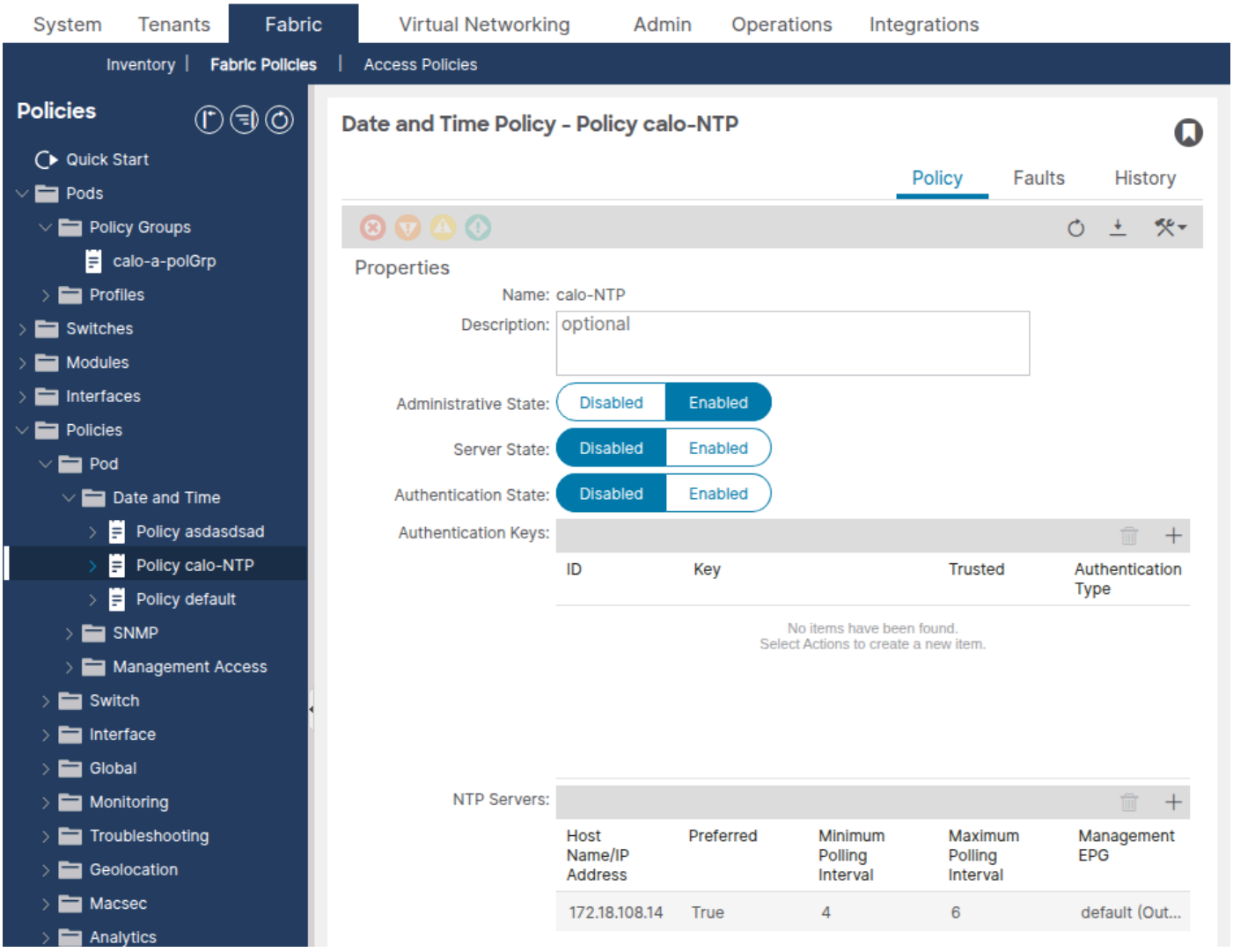
<#root>

```
apic1#

moquery -c mgmtRsOoBStNode
```

步骤 2：验证日期和时间策略是否具有NTP提供程序

导航到交换矩阵>交换矩阵策略>策略> Pod >日期和时间> [您的策略]。



确认至少配置了一个NTP提供程序（服务器）。如果存在多个提供程序，则至少将一个标记为首选。

通过API验证NTP提供程序：

<#root>

```
apic1#
```

```
moquery -c datetimeNtpProv
```

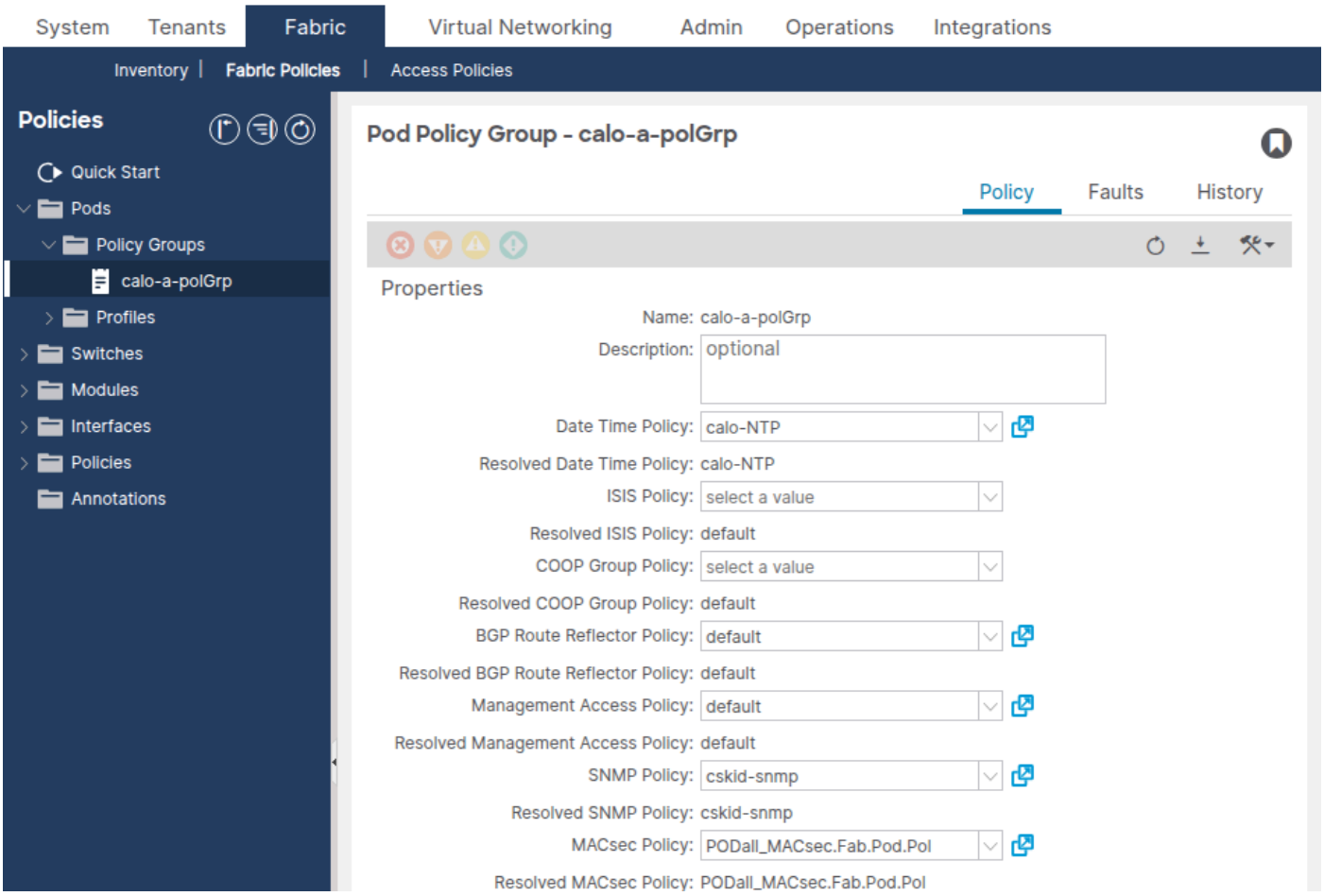
```
# datetimeNtpProv
dn           : uni/fabric/time-NTP-Policy/ntpprov-10.1.1.100
name         : 10.1.1.100
preferred    : yes                    <--- at least one should be "yes"
epgDn        : uni/tn-mgmt/mgmtp-default/oob-default   <--- management EPG
minPoll      : 4
maxPoll      : 6
keyId     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

常见错误配置

- 未配置NTP提供程序 — “日期和时间”策略存在，但无提供程序。将应用策略，但节点没有可同步的NTP服务器。
- 选择的管理EPG错误 — NTP提供程序引用带外EPG，但NTP服务器只能通过带内访问（反之亦然）。 验证哪个管理EPG提供与NTP服务器的可达性。
- 作为单独提供程序添加的同一服务器的FQDN和IP — 这会生成重复的IP故障。删除重复条目。
- 无DNS策略的基于FQDN的提供程序 — 如果使用主机名作为NTP提供程序，请确保已配置DNS服务策略并将适当的DNS标签应用到管理VRF。

步骤 3：验证Pod策略组引用日期和时间策略

导航到交换矩阵>交换矩阵策略> Pod >策略组> [您的Pod策略组]。



确认Date Time Policy字段引用正确的日期和时间策略。

<#root>

apic1#

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

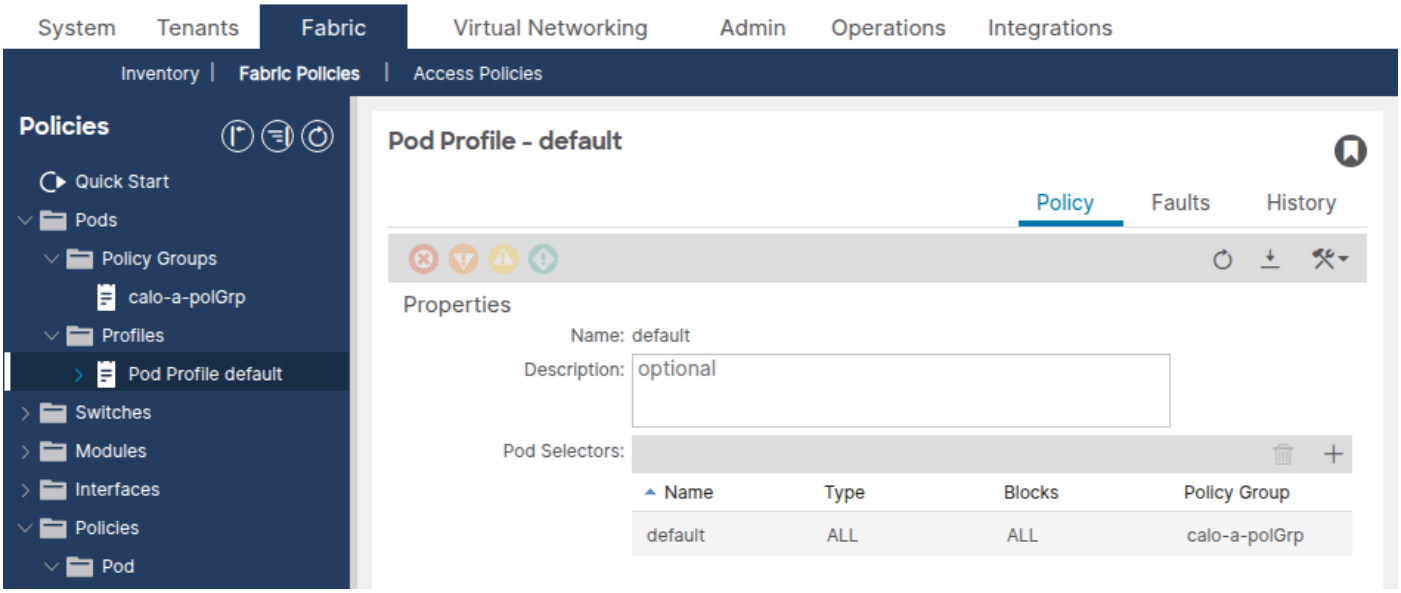
查找`datetimePolName`属性或关联的`fabricRsTimePol`关系。

常见错误配置

- Pod策略组引用了错误的日期和时间策略 — 如果存在多个日期和时间策略(例如“默认”策略和一个自定义策略)，请验证Pod策略组是否引用了预期策略。
- 未创建Pod策略组 — 默认Pod策略组可能没有关联日期和时间策略。始终验证。

步骤 4：验证Pod配置文件引用Pod策略组

导航到交换矩阵>交换矩阵策略> Pod >配置文件> [您的Pod配置文件]。



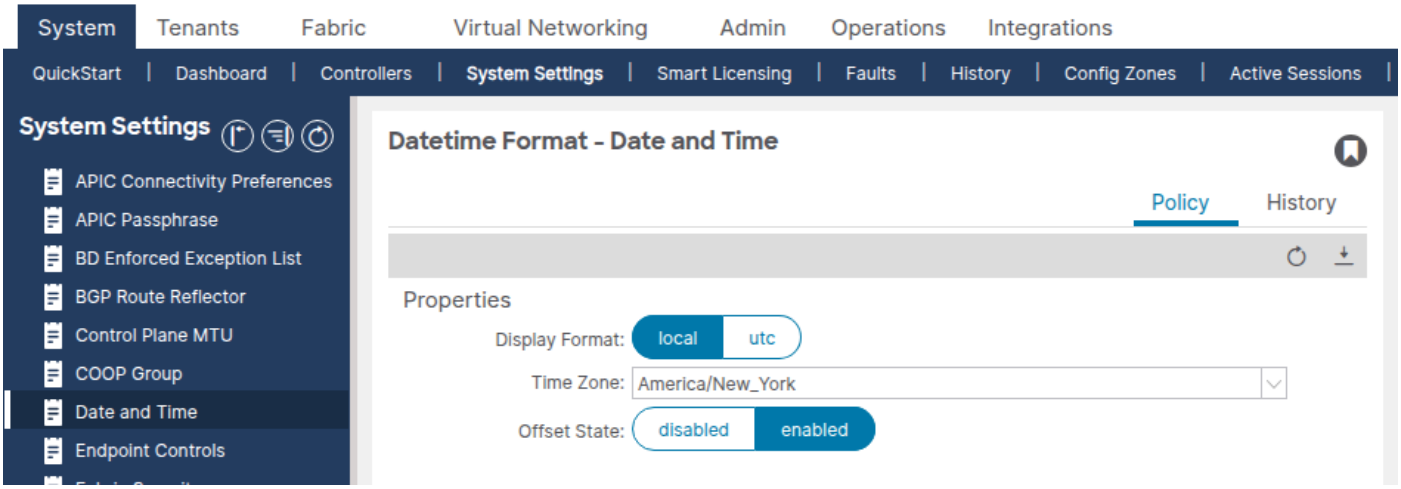
确认Fabric Policy Group字段引用正确的Pod策略组。

常见错误配置

- Pod配置文件引用了错误的Pod策略组 — 尤其是在多Pod环境中，每个Pod配置文件必须引用正确的Pod策略组。

步骤 5：验证日期和时间格式

导航到System > System Settings > Date and Time。



确认显示格式（本地或UTC），并按预期设置时区。此设置是单独的默认日期时间格式策略，不能

删除或复制。

操作验证

确认配置链正确后，使用以下命令验证NTP在运行时是否正常工作。

APIC验证

show ntpq

此命令显示所有APIC上的NTP同步状态。*符号表示已选择服务器进行同步。

<#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
```

看起来不错：

- 所有APIC在远程服务器旁边显示*（已选定进行同步）。
- reach为377（八进制数），表示最后8次投票均成功。
- st(stratum)介于1到15之间。Stratum 16表示服务器不同步。
- 偏移量较低（正常环境通常低于100毫秒）。

不好的看起来是：

- 任何服务器旁边没有* — 未选择要同步的服务器。
- reach为0 – 未收到任何NTP响应。
- st is 16 – NTP服务器未与其上游时间源同步。
- 偏移非常大（千毫秒） — 时钟明显漂移。

show clock

<#root>

apic1#

show clock

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

确认时间准确。请比较检测时钟漂移的预期时间。

APIC Bash（备选）

<#root>

apic1#

bash

admin@apic1:~>

date

Tue Apr 7 11:24:45 EDT 2026

交换机验证（枝叶/主干）

show ntp peers

检验NTP提供程序是否已推送到交换机。

<#root>

leaf1#

show ntp peers

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

看起来不错：显示NTP服务器IP或主机名，其中Serv/Peer = Server和正确的VRF(通常用于OOB的管理)。

不好的看起来是：未列出对等体，或者NTP服务器IP与配置的提供程序不匹配。这通常表示日期和时间策略未通过Pod策略组/Pod配置文件链应用。

show ntp peer-status

验证是否已选择NTP服务器进行同步。

<#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
```

*字符是必需的 — 它确认正在使用NTP服务器进行同步。

不好的看起来是：

- 服务器旁边没有* — 交换机没有同步到服务器。
- reach为0 – 未收到任何NTP响应。这表示存在连通性问题。
- st is 16 – NTP服务器未同步，无法提供有效时间。

show ntp statistics peer ipaddr

验证NTP数据包交换以确认连通性。用受影响交换机的NTP提供商地址替换IP地址。

<#root>

```
leaf1#

show ntp statistics peer ipaddr 10.1.1.100

...
```

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

看起来不错：发送的数据包和接收的数据包大致相等，且呈递增趋势。

不好的看起来是：发送的数据包正在递增，但接收的数据包为0，或者仅略微递增 — NTP响应未到达交换机。

show clock

<#root>

```
leaf1#
```

show clock

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

GUI验证

导航到交换矩阵>交换矩阵策略>策略> Pod >日期和时间> [您的策略] > [NTP提供商]。

对于所有节点，Sync Status列应显示Synced to Remote NTP Server。初始部署后可能需要几分钟才能使同步状态收敛。

API验证

查询datetimeNtpq类以检查所有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.
```

故障排除工作流程

在任何ACI节点上报告NTP问题时，请使用此诊断树。

步骤 1：交换机上是否配置了NTP对等体？

登录受影响的交换机并运行：

<#root>

leaf1#

show ntp peers

- 日期和时→策略中列出的任何对等体未应用于此节点。转至场景1:NTP提供程序未推送到交换机。
- 列出的对→将继续执行步骤2。

步骤 2：是否选择要同步的NTP服务器？

<#root>

leaf1#

show ntp peer-status

- *现→NTP正在同步。如果时间仍然显示错误，请转至场景5:大偏移/时钟漂移。
- 否*存→继续步骤3。

步骤 3：到达值是否为零？

检查show ntp peer-status中的reach列。

- reach = `0` →没有来自NTP服务器的响应。转至场景2:无法访问NTP服务器。
- reach > `0`，但没有* →响应到达，但未建立同步。检查层 — 转至步骤4。

步骤 4：层值是否为16?

- 层数= 16 → NTP服务器未与其自己的上游源同步。转至场景3:NTP服务器不同步（第16层）。
- 第1-15层但无同步→转至场景4:NTP身份验证不匹配。

常见故障排除场景

情形 1：未将NTP提供程序推送到交换机

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

配置检查：

1. 验证日期和时间策略是否至少配置了一个NTP提供程序。
2. 验证Pod策略组引用正确的日期和时间策略。
3. 验证Pod配置文件引用正确的Pod策略组。
4. 验证节点是否在mgmt租户下分配了管理IP地址。

根本原因：策略链中的四个链接之一(日期和时间策略→NTP提供商→Pod策略组→Pod配置文件)已断开。最常见的原因是Pod策略组未与Pod配置文件关联，或者未在Pod策略组中选择日期和时间策略。

解决方案：完成策略链中缺少的链接。确保受影响的Pod的Pod配置文件引用包含正确日期和时间策略的Pod策略组。应用后，NTP提供程序配置将在几分钟内推送到交换机。

方案 2：无法访问NTP服务器

症状：`show ntp peer-status`显示`reach = 0`。`show ntp statistics peer ipaddr 10.1.1.100`显示收到的数据包= 0。

配置检查：验证NTP提供程序是否与正确的管理EPG（OOB或带内）关联。 如果使用OOB，请验证OOB合同是否允许UDP端口123。

运行检查：

1. 使用管理VRF从受影响的交换机ping NTP服务器：
   <#root>

   ```
   leaf1#

   ping 10.1.1.100 vrf management
   ```

2. 在交换机上运行tcpdump以检查NTP数据包是否正在离开和到达：
   <#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：通常为以下其中一项：

- 没有为交换机分配管理IP地址。
- 管理VRF的默认网关缺失或不正确。
- 防火墙阻塞了交换机和NTP服务器之间的UDP端口123。
- OOB合同不允许UDP端口123。
- NTP提供程序引用了错误的管理EPG（例如，已选择OOB，但只有带内可达性）。

解决方案：解决连通性问题。如果缺少管理地址，请分配管理地址、修复默认网关、更新防火墙规则或更正NTP提供程序上的管理EPG选择。

情形 3：NTP服务器不同步（第16层）

症状：`show ntp peer-status`显示stratum(`st`)= `16`。交换机不会同步到stratum 16服务器。

运行检查：登录到NTP服务器，或从外部主机查询该服务器，以验证它是否同步到自己的上游时间源。

根本原因：NTP服务器本身已丢失与其上游参考时钟的同步。第16层的服务器通告它没有可靠的时间源。

解决方案：修复NTP服务器。这位于ACI交换矩阵外部 — 检查NTP服务器配置及其上游时间源。如果无法立即修复NTP服务器，请在日期和时间策略中配置备用NTP提供程序。

场景 4：NTP身份验证不匹配

症状：`show ntp peer-status`显示`reach` > `0`且`stratum`有效，但未显示`*`。NTP服务器响应，但交换机不接受响应。

配置检查：

1. 验证NTP服务器是否需要身份验证。
2. 如果需要身份验证，请验证Date and Time策略是否将Authentication State设置为Enabled。
3. 验证ACI交换矩阵和NTP服务器之间的身份验证密钥ID、密钥值和算法（MD5、SHA-1或AES128-CMAC）匹配。
4. 验证NTP客户端身份验证密钥(NTP Client Authentication Keys)表中密钥是否标记为受信任。

根本原因：ACI和NTP服务器之间的身份验证密钥、算法或密钥ID不匹配，导致交换机拒绝NTP响应为未经身份验证。

解决方案：调整身份验证配置。确保在ACI和NTP服务器上配置相同的密钥ID、密钥值和算法。对于APIC版本6.1(1)及更高版本，建议使用AES128-CMAC。

注意：启用FIPS模式时，仅支持AES128-CMAC和SHA-1身份验证方案。MD5无法在FIPS模式下工作。

场景 5：大偏移/时钟漂移

症状：交换机似乎已同步(* present， reach = 377)，但`show ntp peer-status`或show ntpq中的`offset`值非常大（数百或数千毫秒），或者时钟明显错误。

运行检查：

<#root>

apic1#

show ntpq

选中`offset`列。正常偏移量通常小于100毫秒。

根本原因：在NTP同步建立之前，时钟明显漂移，或者在重新启动期间（例如，由于CMOS电池死

机）硬件时钟(RTC)被重置。NTP通过旋转逐渐校正时钟，这可能需要时间进行较大的偏移。

解决方案：如果偏移量非常大且NTP正在主动同步，请等待时钟收敛。NTP会逐步调整时钟 — 大偏移可能需要几个小时才能完全纠正。如果偏移量没有减少，请验证NTP服务器是否提供了准确的时间。如果在每次重新启动后问题仍然存在，请检查受影响节点的硬件时钟（RTC/CMOS电池）。

场景 6：带内NTP的备用APIC故障

症状：当将NTP配置为带内管理时，在与NTP或监控策略相关的备用APIC上生成故障。

根本原因：将NTP策略应用于带内管理时，备用APIC还需要带内配置。没有它，故障就会产生。

解决方案：配置备用APIC的带内管理。这样可以清除故障。

场景 7：重复的IP故障

症状：添加NTP提供程序后会引发重复IP故障。

根本原因：FQDN添加为NTP提供程序，然后该FQDN的解析IP地址添加为第二个NTP提供程序。ACI检测到重复项。

解决方案：删除最近添加的重复提供程序（如果先添加FQDN，则删除IP地址条目；反之亦然）。每个NTP服务器仅使用一个条目 — FQDN或IP地址，而不是同时使用两者。

场景 8：基于FQDN的NTP提供程序的DNS解析失败

症状：配置了主机名的NTP提供程序未解析。`show ntp peers`未显示预期的IP地址，或者NTP未同步。

配置检查：

1. 验证Fabric > Fabric Policies > Policies > Global > DNS Profiles下是否配置了DNS服务策略。
2. 验证可以从管理VRF访问DNS提供程序（DNS服务器）。
3. 验证为管理EPG的带内或带外VRF实例配置了合适的DNS标签。

根本原因：无法访问DNS服务器或未配置，导致NTP提供程序的主机名解析失败。

解决方案：配置DNS服务策略，确保DNS可达性，并应用正确的DNS标签。或者，使用NTP服务器IP地址而不是主机名。

相关故障和事件

以下是NTP相关条件，这些条件可能会在ACI中生成故障：

- 重复的IP故障 — 当同一NTP服务器的FQDN和IP地址都作为提供程序添加时引发。分辨率：删除重复条目。
- 备用APIC带内NTP故障 — 当监控或NTP策略应用于带内但备用APIC缺少带内配置时引发。
- Sync Status not converging — GUI显示一个或多个节点的“Not Synced”或其状态不是“Synced to Remote NTP Server”。这不是故障代码，而是运行状态指示灯。按照上述故障排除工作流程进行诊断。

升级条件

考虑升级至Cisco TAC，如果：

- 配置链已验证正确并且NTP服务器可访问（ping工作正常，tcpdump显示NTP响应），但交换机仍然无法同步。
- NTP同步会重复丢失，而不会发生配置更改或NTP服务器问题。
- `show ntp peer-status`输出显示意外行为，例如服务器上已确认外部同步的持久层16。
- 在重新启动之间，时钟会明显漂移，这可能表明存在硬件时钟(RTC)问题。

在与TAC接洽时，请提供以下数据：

- 所有APIC的`show ntpq`输出。
- 所有受影响交换机的`show ntp peers`、`show ntp peer-status`、`show ntp statistics peer ipaddr <IP>`和`show clock`的输出。
- 来自APIC的`moquery -c datetimePol`、`moquery -c datetimeNtpProv`和`moquery -c datetimeNtpq`的输出。
- 受影响节点的技术支持。

参考

- 思科APIC基本配置指南，版本6.1(x) — 调配核心ACI交换矩阵服务
- 排除ACI管理和核心服务故障 — Pod策略
- 思科以应用为中心的基础设施(ACI)设计指南

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。