Cisco ACIファブリックのNTPのトラブルシューティング

はじめに

このドキュメントでは、Cisco ACIファブリックのネットワークタイムプロトコル(NTP)の問題を確認、トラブルシューティング、および解決する方法について説明します。NTPポリシーモデル、設定検証、動作検証コマンド、一般的なNTPの症状に対するトリアージワークフロー、および詳細なトラブルシューティングシナリオについて説明します。

バックグラウンド情報

このドキュメントの内容は、『ACIの管理およびコアサービスのトラブルシューティング：ポッドポリシー』、『Cisco APIC基本設定ガイド、リリース6.1(x)：コアACIファブリックサービスのプロビジョニング』の章、および『Cisco ACI設計ガイド』から抽出しました。

概要

時間の同期は、モニタリング、運用、およびトラブルシューティングタスクが依存するACIファブリックの重要な機能です。クロックの同期により、トラフィックフローの適切な分析、複数のファブリックノード間でのデバッグと障害のタイムスタンプの相関、およびアプリケーションのヘルススコアが依存するアトミックカウンタ機能の完全な利用が保証されます。NTPの設定が存在しないか不適切であっても、必ずしも障害が発生したり、ヘルススコアが低下したりするとは限らないため、ファブリックの導入の早い段階で時刻の同期を設定することが重要です。

ACIのNTPポリシーモデル

ACIのNTPは、次の4つのポリシーオブジェクトのチェーンで管理されます。

1. 日時ポリシー(`datetimePol`)：管理状態、認証状態、サーバ状態、およびマスターモードを含むNTP設定を定義します。Fabric > Fabric Policies > Policies > Pod > Date and Timeの下にあります。
2. NTPプロバイダー(`datetimeNtpProv`)：日時ポリシー内の個々のNTPサーバエントリ（プロバイダー）を定義します。サーバIP/FQDN、管理EPG選択（アウトオブバンドまたはインバンド）、優先フラグ、ポーリング間隔などが含まれます。

3. ポッドポリシーグループ(fabricPodPGrp)：日付と時刻のポリシーを、他のポッドレベルのポリシー（BGP RR、SNMPなど）とともに参照します。 Fabric > Fabric Policies > Pods > Policy Groupsの下にあります。
4. ポッドプロファイル(fabricPodP)：ポッドポリシーグループをポッドセレクタに関連付けます。Fabric > Fabric Policies > Pods > Profilesの下にあります。

このチェーンの4つのリンクはすべて、NTPをファブリックノードに適用するように設定する必要があります。リンクが壊れても、NTPプロバイダーの設定はスイッチにプッシュされません。

前提条件

- ファブリック検出を完了する必要があります。
- ノード管理アドレス（OOBまたはインバンド）は、mgmtテナント下のすべてのAPICとスイッチに割り当てる必要があります。
- アウトオブバンドNTPの場合、OOB管理EPGはUDPポート123を許可する必要があります。
- インバンドNTPの場合、適切なコントラクトを持ち、NTPサーバへの到達可能性を持つインバンド管理EPGを設定する必要があります。インバンドIPアドレスは、追加のポリシーがないと、ファブリックの外部から到達できません。

NTP認証

ACIでは、MD5、SHA-1、AES128-CMACの3つのNTP認証スキームがサポートされています。AES128-CMACはAPICリリース6.1(1)で導入されましたが、MD5は脆弱で安全ではないと考えられるため、この方式が推奨されます。FIPSモードを有効にすると、AES128-CMACとSHA-1だけがサポートされます。

NTPサーバの機能

ACIリーフスイッチは、ダウンストリームクライアント（ファブリックに接続されたサーバなど）のNTPサーバとして機能できます。 この機能はデフォルトでは無効になっているため、日時ポリシーのServer Stateオプションで明示的に有効にする必要があります。有効にすると、クライアントはリーフスイッチのインバンド、アウトオブバンド、ブリッジドメインSVI、またはL3Out IPアドレスをNTPサーバアドレスとして使用できます。

注：ファブリックスイッチは、同じファブリック内の他のスイッチと同期できません。ファブリックスイッチは常に外部NTPサーバと同期する必要があります。

設定の確認

NTPの動作状態のトラブルシューティングを行う前に、設定チェーンが完了していることを確認します。設定ミスは、ACIにおけるNTP問題の最も一般的な根本原因です。

手順1：ノード管理アドレスの確認

Tenants > mgmt > Node Management Addresses（静的割り当て用）またはNode Management EPGs（接続グループ用）に移動します。

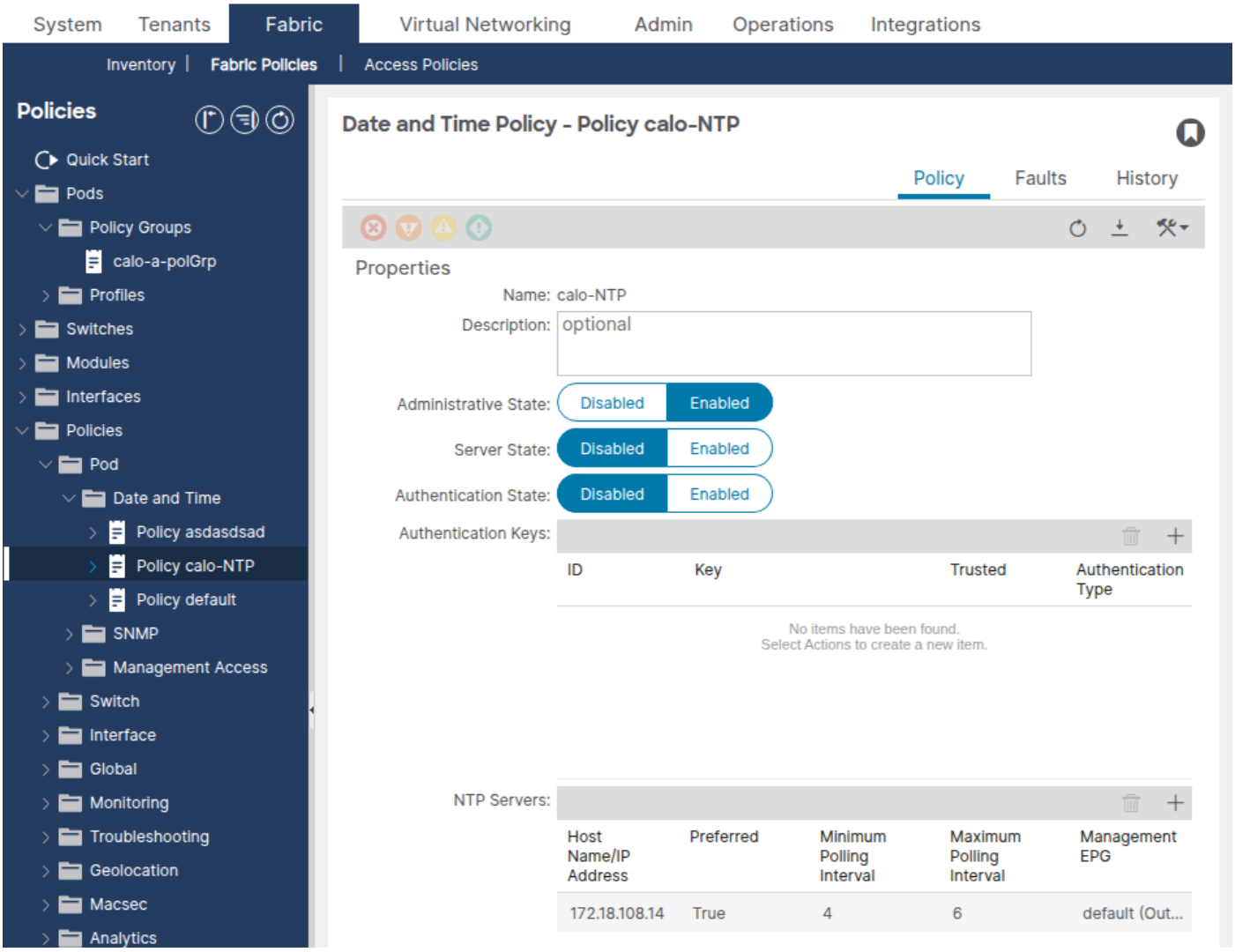
すべてのAPICとスイッチノードに管理IPアドレスが割り当てられていることを確認します。管理アドレスを持たないノードはNTPサーバと通信できません。

または、APIを照会します。

```
<#root>

apic1#

moquery -c mgmtRsOoBStNode
```

ステップ2：日時ポリシーにNTPプロバイダーが含まれていることを確認する

Fabric > Fabric Policies > Policies > Pod > Date and Time > [Your Policy]の順に移動します。



少なくとも1つのNTPプロバイダー（サーバ）が設定されていることを確認します。複数のプロバイダーが存在する場合は、少なくとも1つのプロバイダーに優先フラグを付けます。

APIを使用してNTPプロバイダーを確認します。

<#root>

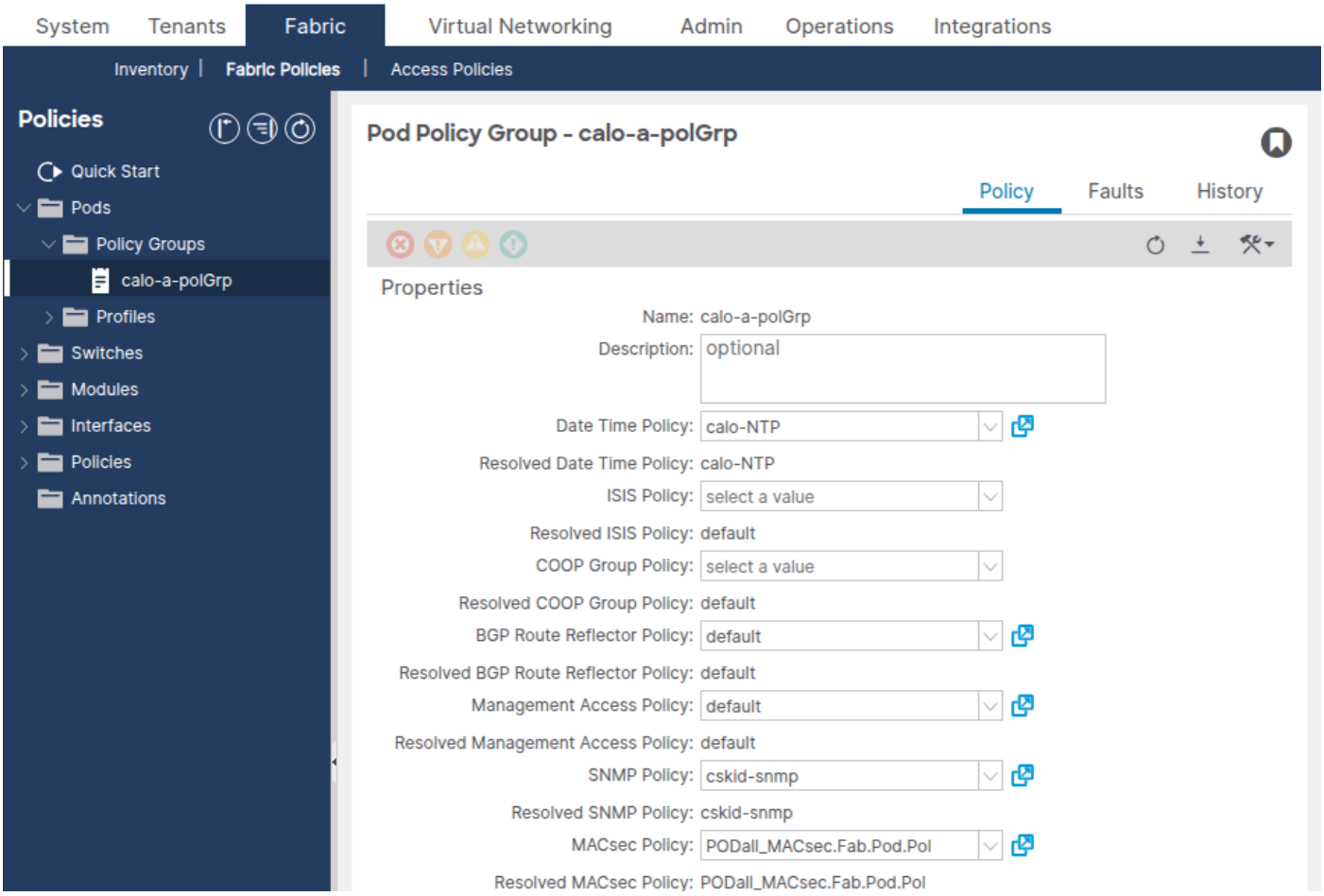
```
apic1#

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
```

よくある設定上の間違い

- No NTP provider configured：日付と時刻のポリシーは存在しますが、プロバイダーはゼロです。ポリシーは適用されますが、ノードには同期対象のNTPサーバがありません。
- Wrong Management EPG selected:NTPプロバイダーはアウトオブバンドEPGを参照しますが、NTPサーバはインバンドでのみ到達可能です（またはその逆）。 NTPサーバへの到達可能性を提供する管理EPGを確認します。
- 同じサーバのFQDNとIPが別個のプロバイダーとして追加される：これにより、重複IPエラーが生成されます。重複するエントリを削除します。
- DNSポリシーのないFQDNベースのプロバイダー:NTPプロバイダーのホスト名を使用する場合、DNSサービスポリシーが設定されており、適切なDNSラベルが管理VRFに適用されていることを確認します。

ステップ3：ポッドポリシーグループが日時ポリシーを参照していることを確認します。

Fabric > Fabric Policies > Pods > Policy Groups > [Your Pod Policy Group]の順に移動します。



Date Time Policyフィールドが正しい日時ポリシーを参照していることを確認します。

<#root>

apic1#

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

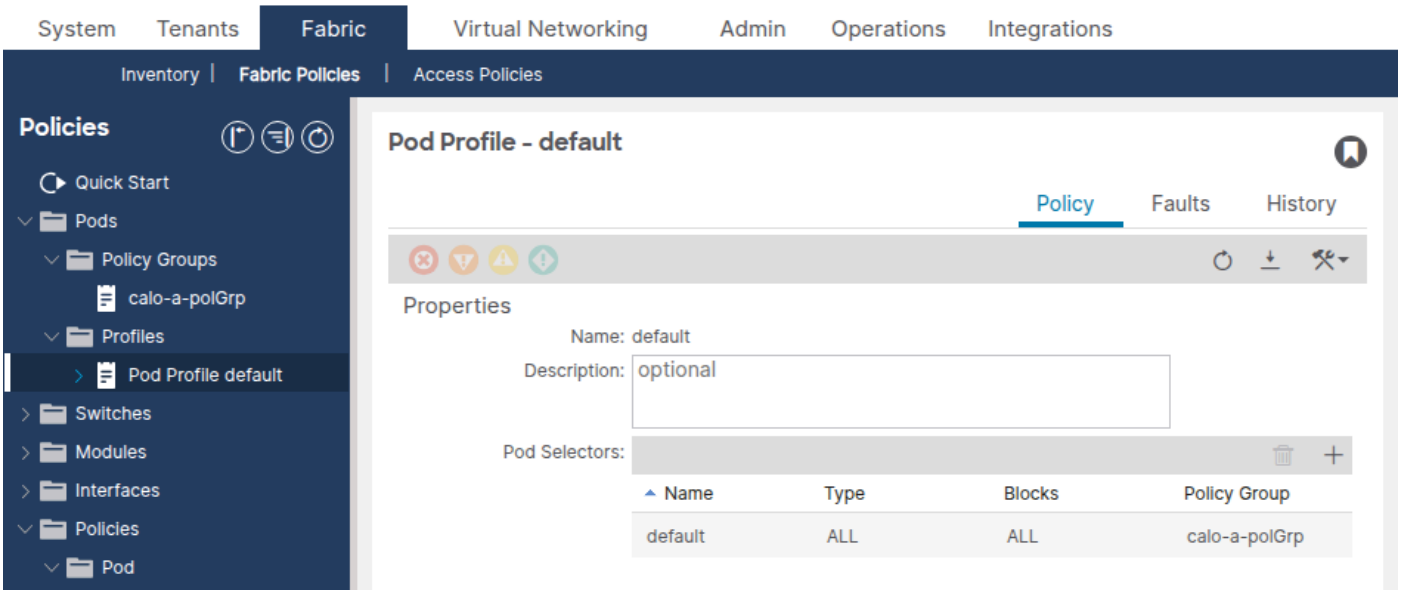
datetimePolName属性または関連するfabricRsTimePol関係を探します。

よくある設定上の間違い

- ポッドポリシーグループが誤った日付と時刻のポリシーを参照している：複数の日付と時刻のポリシー（たとえば「デフォルト」とカスタムポリシー）が存在する場合、ポッドポリシーグループが目的のポリシーを参照していることを確認します。
- ポッドポリシーグループがまったく作成されない：デフォルトのポッドポリシーグループに日時ポリシーが関連付けられていない場合があります。常に確認してください。

ステップ4：ポッドプロファイルがポッドポリシーグループを参照していることを確認します。

Fabric > Fabric Policies > Pods > Profiles > [Your Pod Profile]の順に選択します。



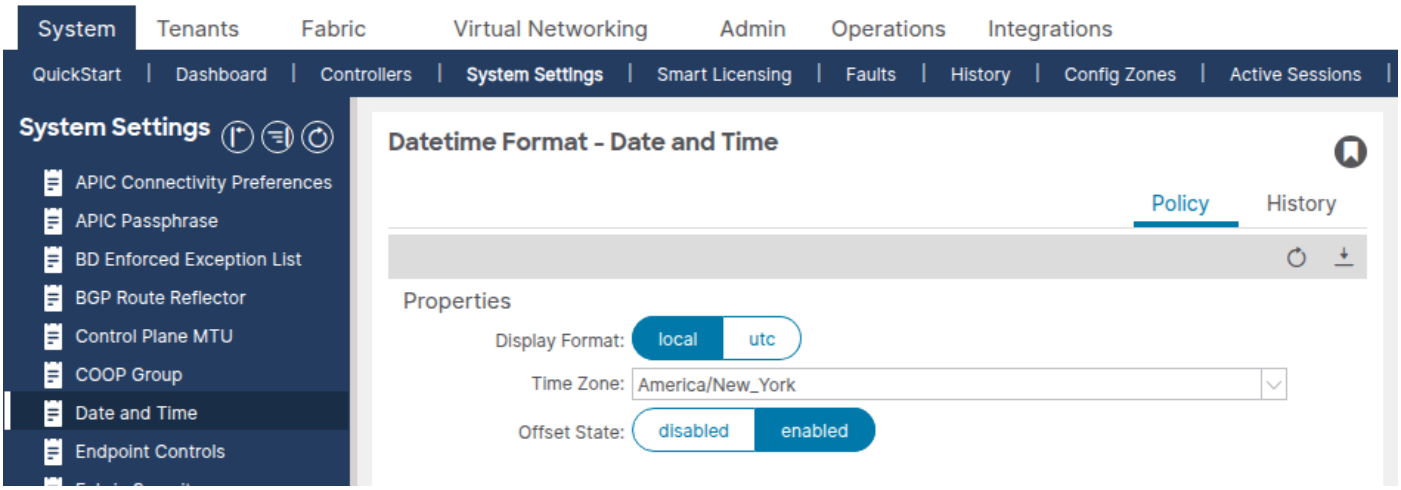
Fabric Policy Groupフィールドが正しいポッドポリシーグループを参照していることを確認します。

よくある設定上の間違い

- ポッドプロファイルが間違ったポッドポリシーグループを参照している：特にマルチポッド環境では、各ポッドプロファイルが正しいポッドポリシーグループを参照する必要があります。

手順5：日付と時刻の形式を確認する

System > System Settings > Date and Timeの順に選択します。



表示形式（ローカルまたはUTC）とタイムゾーンが正しく設定されていることを確認します。この設定は、削除や複製ができない別のデフォルトの日時形式(DATE TIME FORMAT)ポリシーです。

動作検証

設定チェーンが正しいことを確認したら、次のコマンドを使用して、NTPが実行時に機能していることを確認します。

APICの検証

show ntpq（隠しコマンド）

このコマンドは、すべてのAPICのNTP同期ステータスを表示します。*記号は、サーバで同期が選択されていることを示します。

<#root>

```
apic1#
```

show ntpq

```
 nodeid      remote                          refid                           st        t   when      poll
 ------  -   ------------------------------  ------------------------------  --------  --  --------  ----
 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
```

正常な状態は次のとおりです。

- すべてのAPICでは、リモートサーバの横に*（同期用に選択）が表示されます。
- reachは377（8進数）で、最後の8回のポールがすべて成功したことを示します。
- st(stratum)は1 ~ 15の間です。ストラタム16は、サーバが非同期であることを意味します。
- offsetは低い値です（正常な環境では通常100 ms未満）。

次のような問題があります。

- サーバの横に*なし：同期対象のサーバが選択されていません。
- reach is 0:NTP応答は受信されていません。
- stが16の場合：NTPサーバはアップストリームの時刻源に同期されていません。
- offsetは非常に大きい（数千ミリ秒）。クロックが著しくドリフトしている。

show clock

<#root>

apic1#

show clock

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

時刻が正確であることを確認します。クロックドリフトを検出するための予測時間と比較します。

APIC Bash（代替）

<#root>

apic1#

bash

admin@apic1:~>

date

Tue Apr 7 11:24:45 EDT 2026

スイッチの検証（リーフ/スパイン）

NTPピアの表示

NTPプロバイダーがスイッチにプッシュされたことを確認します。

<#root>

leaf1#

show ntp peers

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

次のような出力が得られます。NTPサーバのIPまたはホスト名が、Serv/Peer = Server(通常は管理サーバでOOBを使用)と正しいVRFで表示されます。

問題の内容：ピアがリストされていないか、NTPサーバのIPが設定されたプロバイダーと一致していません。これは通常、日時ポリシーがポッドポリシーグループ/ポッドプロファイルチェーン経由で適用されなかったことを示します。

show ntp peer-status（隠し）

NTPサーバが同期のために選択されていることを確認します。

<#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
```

*文字は必須であり、NTPサーバが同期に使用されていることを確認します。

次のような問題があります。

- サーバの横に*は表示されません。スイッチはサーバと同期していません。
- reach is 0:NTP応答は受信されていません。これは、到達可能性の問題を示しています。
- st is 16:NTPサーバは非同期であり、有効な時間を提供できません。

show ntp statistics peer ipaddr（ntp統計情報ピアのipaddr）

NTPパケット交換を確認して、到達可能性を確認します。このIPアドレスを、該当するスイッチのNTPプロバイダーアドレスに置き換えてください。

<#root>

```
leaf1#

show ntp statistics peer ipaddr 10.1.1.100


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

送信されたパケットと受信されたパケットは、ほぼ等しく増分します。

送信されたパケットは増加しているが、受信されたパケットは0かほとんど増加していない：NTP応答がスイッチに到達していない

show clock

<#root>

```
leaf1#

show clock
```

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

GUI による確認

Fabric > Fabric Policies > Policies > Pod > Date and Time > [Your Policy] > [NTP Provider]の順に移動します。

すべてのノードについて、Sync Status列にSynced to Remote NTP Serverと表示されるはずです。初期導入後に同期ステータスが収束するまでに数分かかることがあります。

APIの検証

datetimeNtpqクラスを照会して、すべてのAPIC間のNTP同期を確認します。

<#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.
```

トラブルシューティングワークフロー

ACIノードでNTPの問題が報告された場合に、このDecision Treeを使用します。

ステップ1：スイッチにNTPピアが設定されていますか。

該当するスイッチにログインし、次のコマンドを実行します。

<#root>

```
leaf1#

show ntp peers
```

- 日時ポリシー→一覧に含まれるピアは、このノードに適用されませんでした。「シナリオ1:NTPプロバイダーがスイッチにプッシュされない」に進みます。
- リストされ→ピアはステップ2に進みます。

ステップ2:NTPサーバは同期対象として選択されていますか。

```
<#root>

leaf1#

show ntp peer-status
```

- * NTP→同期中です。それでも時間が正しく表示されない場合は、「シナリオ5：大きなオフセット/クロックのドリフト」に進みます。
- *は存在しません→ステップ3に進みます。

ステップ3:reach値はゼロですか。

show ntp peer-statusのreachカラムをチェックします。

- **reach = 0**→NTPサーバから応答がありません。シナリオ2:NTPサーバに到達できないに進みます。
- **reach > 0**ですが、*→応答は到着していますが、同期が確立されていません。Stratumのチェック：ステップ4に進みます。

ステップ4：ストラタム値は16ですか。

- Stratum = 16→NTPサーバが自身のアップストリーム送信元に同期されていない場合。シナリオ3:NTPサーバが同期されていない（ストラタム16）に進みます。
- ストラタム1 ~ 15（同期なし）→、「シナリオ4:NTP認証の不一致」に進みます。

一般的なトラブルシューティングのシナリオ

シナリオ1:NTPプロバイダーがスイッチにプッシュされない

症状：スイッチ上の`show ntp peers`がエントリを返しません。

設定チェック：

1. 日時ポリシーに少なくとも1つのNTPプロバイダーが設定されていることを確認します。
2. ポッドポリシーグループが正しい日時ポリシーを参照していることを確認します。
3. ポッドプロファイルが正しいポッドポリシーグループを参照していることを確認します。
4. mgmtテナントの下で、ノードに管理IPアドレスが割り当てられていることを確認します。

根本原因：ポリシーチェーンの4つのリンク(日時ポリシー→NTPプロバイダー→ポッドポリシーグループ→ポッドプロファイル)の1つが壊れています。最も一般的な原因は、ポッドポリシーグループがポッドプロファイルに関連付けられていないか、日時ポリシーがポッドポリシーグループで選択されていないことです。

解決策：ポリシーチェーンで欠落しているリンクを完成させます。影響を受けるポッドのポッドプロファイルが、正しい日時ポリシーを含むポッドポリシーグループを参照していることを確認します。適用後、NTPプロバイダー設定は数分以内にスイッチにプッシュされます。

シナリオ2:NTPサーバが到達不能

症状：show ntp peer-statusはreach = 0を示します。show ntp statistics peer ipaddr 10.1.1.100は受信パケット = 0を示します。

設定確認：NTPプロバイダーが正しい管理EPG（OOBまたはインバンド）に関連付けられていることを確認します。 OOBを使用している場合は、OOBコントラクトでUDPポート123が許可されていることを確認します。

動作確認：

1. 管理VRFを使用して、影響を受けるスイッチからNTPサーバにpingを実行します。
   <#root>

   ```
   leaf1#

   ping 10.1.1.100 vrf management
   ```

2. スイッチでtcpdumpを実行して、NTPパケットが発信および着信しているかどうかを確認します。
   <#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、次のいずれかです。

- スイッチに管理IPアドレスが割り当てられていない。
- 管理VRFのデフォルトゲートウェイがないか、正しくない。
- ファイアウォールが、スイッチとNTPサーバ間のUDPポート123をブロックしている。
- OOBコントラクトはUDPポート123を許可しません。
- NTPプロバイダーが間違った管理EPGを参照している（例：OOBが選択されているが、インバンドのみが到達可能性がある）。

解決策：到達可能性の問題を解決します。管理アドレスが見つからない場合は、割り当て、デフォルトゲートウェイの修正、ファイアウォールルールの更新、またはNTPプロバイダーでの管理EPG選択の修正を行います。

シナリオ3:NTPサーバが同期されていない（ストラタム16）

症状：`show ntp peer-status`でストラタム(st) = 16が表示されます。スイッチがストラタム16サーバに同期されない。

動作確認：NTPサーバにログインするか、外部ホストからクエリを実行して、サーバが自身のアップストリーム時刻源に同期していることを確認します。

根本原因：NTPサーバ自体がアップストリーム基準クロックとの同期を失いました。ストラタム16のサーバは、信頼できる時刻源がないことをアドバタイズしています。

解決策：NTPサーバを修正します。これはACIファブリックの外部です。NTPサーバの設定とアップストリームの時刻源を確認してください。NTPサーバをすぐに修正できない場合は、日時ポリシーで代替NTPプロバイダーを設定します。

シナリオ4:NTP認証の不一致

症状：`show ntp peer-status`で`reach > 0`と表示され、stratumは有効ですが、*は表示されません。NTPサーバは応答しますが、スイッチは応答を受け入れません。

設定チェック：

1. NTPサーバに認証が必要かどうかを確認します。
2. 認証が必要な場合は、日時ポリシーにAuthentication StateがEnabledに設定されていることを確認します。
3. ACIファブリックとNTPサーバ間で、認証キーID、キー値、およびアルゴリズム（MD5、SHA-1、またはAES128-CMAC）が一致していることを確認します。
4. NTP Client Authentication Keysテーブルで、キーがTrustedとマークされていることを確認します。

根本原因：認証キー、アルゴリズム、またはキーIDがACIとNTPサーバ間で不一致であり、スイッチがNTP応答を非認証として拒否する原因になっています。

解決策：認証設定を調整します。ACIとNTPサーバの両方で同じキーID、キー値、およびアルゴリズムが設定されていることを確認します。AES128-CMACは、APICリリース6.1(1)以降に推奨されます。

注:FIPSモードが有効な場合、AES128-CMACおよびSHA-1認証スキームのみがサポートされます。MD5はFIPSモードでは動作しません。

シナリオ5：大きなオフセット/クロックドリフト

症状：スイッチが同期しているように見えますが(* 存在し、reach = 377)、show ntp peer-statusまたはshow ntpqのoffset値が非常に大きいか（数百または数千ミリ秒）、クロックが目に見えて間違っています。

動作確認：

```
<#root>

apic1#

show ntpq
```

offset列をチェックします。通常、正常なオフセットは100ミリ秒未満です。

根本原因：NTP同期が確立される前にクロックが大幅にドリフトしたか、リブート中にハードウェアクロック(RTC)がリセットされました（CMOSバッテリの消耗など）。 NTPでは、旋回によってクロックが徐々に修正されるため、オフセットが大きくなるまでに時間がかかる場合があり

ます。

解決策：オフセットが非常に大きく、NTPがアクティブに同期している場合は、クロックが収束するまで待ちます。NTPはクロックを徐々に回転させます。オフセットが大きくなると、完全に修正されるまで数時間かかることがあります。オフセットが減少しない場合は、NTPサーバが正確な時刻を提供していることを確認します。リブートするたびに問題が再発する場合は、該当ノードのハードウェアクロック（RTC/CMOSバッテリ）を調べてください。

シナリオ6：インバンドNTPによるスタンバイAPICの障害

症状：NTPがインバンド管理用に設定されている場合、NTPに関連するスタンバイAPICまたはモニタリングポリシーで障害が生成されます。

根本原因：NTPポリシーがインバンド管理に適用される場合、スタンバイAPICでもインバンド設定が必要です。それがなければ、障害が発生します。

解決策：スタンバイAPICにもインバンド管理を設定します。これで障害がクリアされます。

シナリオ7：重複したIPの障害

症状：NTPプロバイダーを追加すると、重複IP障害が発生します。

根本原因： FQDNがNTPプロバイダーとして追加された後、そのFQDNの解決済みIPアドレスが2番目のNTPプロバイダーとして追加されました。ACIが重複を検出します。

解決策：最後に追加された重複プロバイダー（FQDNが最初に追加された場合はIPアドレスエントリ、またはその逆）を削除します。 NTPサーバごとに1つのエントリ（FQDNまたはIPアドレスのいずれか、両方ではない）のみを使用します。

シナリオ8:FQDNベースのNTPプロバイダーのDNS解決の失敗

症状：ホスト名が設定されたNTPプロバイダーが解決できない。`show ntp peers`が予期されたIPアドレスを表示しない、またはNTPが同期していない。

設定チェック：

1. Fabric > Fabric Policies > Policies > Global > DNS Profilesの順に選択して、DNSサービスポリシーが設定されていることを確認します。

2. 管理VRFからDNSプロバイダー（DNSサーバ）に到達できることを確認します。
3. 管理EPGのインバンドまたはアウトオブバンドのVRFインスタンスに適切なDNSラベルが設定されていることを確認します。

根本原因： DNSサーバに到達できないか、またはDNSサーバが設定されていないため、NTPプロバイダーのホスト名解決が失敗します。

解決策：DNSサービスポリシーを設定し、DNS到達可能性を確認して、正しいDNSラベルを適用します。または、ホスト名の代わりにNTPサーバのIPアドレスを使用します。

関連する障害およびイベント

ACIで障害を生成する可能性があるNTP関連の条件を次に示します。

- Duplicate IP fault：同じNTPサーバのFQDNとIPアドレスの両方がプロバイダーとして追加されるときに発生します。解決方法：重複するエントリを削除します。
- スタンバイAPICインバンドNTP障害：モニタリングまたはNTPポリシーがインバンドに適用されているが、スタンバイAPICにインバンド設定がない場合に発生します。
- 同期ステータスが収束しない — GUIに「Not Synced」または1つ以上のノードの「Synced to Remote NTP Server」以外のステータスが表示されます。これは障害コードではなく、動作ステータスインジケータです。診断するには、上記のトラブルシューティングワークフローに従ってください。

エスカレーション基準

次の場合は、Cisco TACへのエスカレーションを検討してください。

- 設定チェーンが正しいこと、およびNTPサーバが到達可能であることが確認されますが（pingは成功し、tcpdumpはNTP応答を示します）、スイッチはまだ同期していません。
- NTPの同期が繰り返し失われ、設定が変更されたり、NTPサーバに問題が発生したりすることはありません。
- `show ntp peer-status`の出力には、外部との同期が確認されたサーバ上にストラタム16が存続するなどの、予期しない動作が示されます。
- クロックはリブートの間に著しくドリフトしますが、これはハードウェアクロック(RTC)の問題を示している可能性があります。

TACに問い合わせる際には、次のデータを提供してください。

- すべてのAPICからの`show ntpq`出力。

- 該当するすべてのスイッチからのshow ntp peers、show ntp peer-status、show ntp statistics peer ipaddr <IP>、およびshow clockの出力。
- APICからのmoquery -c datetimePol、moquery -c datetimeNtpProv、およびmoquery -c datetimeNtpqの出力。
- 該当ノードからのテクニカルサポート。

参照資料

- Cisco APIC基本設定ガイド、リリース6.1(x)：コアACIファブリックサービスのプロビジョニング
- ACI管理およびコアサービスのトラブルシューティング：ポッドポリシー
- シスコアプリケーションセントリックインフラストラクチャ(ACI)設計ガイド

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。