Cisco ACI 패브릭에서 NTP 문제 해결

소개

이 문서에서는 Cisco ACI 패브릭에서 NTP(Network Time Protocol) 문제를 확인, 해결 및 해결하는 방법에 대해 설명합니다. NTP 정책 모델, 컨피그레이션 확인, 운영 확인 명령, 일반적인 NTP 증상에 대한 분류 워크플로, 자세한 문제 해결 시나리오를 다룹니다.

배경 정보

이 문서의 자료는 Troubleshoot ACI Management and Core Services — Pod Policies(ACI 관리 및 코어 서비스 트러블슈팅) 가이드, Cisco APIC Basic Configuration Guide(Cisco APIC 기본 컨피그레이션 가이드), Release 6.1(x) — Provisioning Core ACI Fabric Services(코어 ACI 패브릭 서비스 프로비저닝) 장, Cisco ACI Design Guide(Cisco ACI 설계 가이드)에서 발췌한 것입니다.

개요

시간 동기화는 ACI 패브릭에서 모니터링, 운영 및 문제 해결 작업이 의존하는 중요한 기능입니다. 클럭 동기화를 통해 트래픽 플로우의 적절한 분석, 여러 패브릭 노드의 디버그 및 결함 타임스탬프의 상관관계 분석, 애플리케이션 상태 점수가 의존하는 미세 카운터 기능의 전체 활용이 보장됩니다. 존재하지 않거나 부적합한 NTP 컨피그레이션이 반드시 결함이나 낮은 상태 점수를 트리거하는 것은 아니므로, 패브릭 구축 초기에 시간 동기화를 구성하는 것이 중요합니다.

ACI의 NTP 정책 모델

ACI의 NTP는 네 가지 정책 객체의 체인을 통해 관리됩니다.

1. Date and Time Policy(`datetimePol`) - 관리 상태, 인증 상태, 서버 상태 및 마스터 모드를 포함한 NTP 컨피그레이션을 정의합니다. Fabric(패브릭) > Fabric Policies(패브릭 정책) > Policies(정책) > Pod(포드) > Date and Time(날짜 및 시간)에 있습니다.
2. NTP Provider(datetimeNtpProv) — 서버 IP/FQDN, 관리 EPG 선택(대역 외 또는 대역 내), 기본 설정 플래그, 폴링 간격 등 날짜 및 시간 정책 내의 개별 NTP 서버 항목(제공자)을 정의합니다.
3. Pod Policy Group(`fabricPodPGrp`) — 다른 포드 레벨 정책(BGP RR, SNMP 등)과 함께 날짜 및 시간 정책을 참조합니다. Fabric(패브릭) > Fabric Policies(패브릭 정책) > Pods(포드) > Policy Groups(정책 그룹) 아래에 있습니다.

4. Pod 프로파일(`fabricPodP`) — Pod 정책 그룹을 Pod 선택기와 연결합니다. Fabric(패브릭) > Fabric Policies(패브릭 정책) > Pods(포드) > Profiles(프로파일)에 있습니다.

이 체인의 네 링크 모두 패브릭 노드에 NTP를 적용하도록 구성해야 합니다. 링크가 끊어지면 NTP 제공자 컨피그레이션이 스위치에 푸시되지 않습니다.

사전 요구 사항

- 패브릭 검색을 완료해야 합니다.
- 노드 관리 주소(OOB 또는 대역 내)를 관리 테넌트의 모든 APIC 및 스위치에 할당해야 합니다 .
- OOB NTP의 경우 OOB 관리 EPG에서 UDP 포트 123을 허용해야 합니다.
- 인밴드 NTP의 경우, 적절한 계약 및 NTP 서버와의 연결성이 있는 인밴드 관리 EPG를 구성해야 합니다. 추가 정책 없이는 패브릭 외부에서 인밴드 IP 주소에 연결할 수 없습니다.

NTP 인증

ACI는 세 가지 NTP 인증 체계를 지원합니다. MD5, SHA-1 및 AES128-CMAC. AES128-CMAC는 APIC 릴리스 6.1(1)에 도입되었으며 MD5가 취약하고 안전하지 않은 것으로 간주되므로 권장되는 방법입니다. FIPS 모드가 활성화된 경우 AES128-CMAC 및 SHA-1만 지원됩니다.

NTP 서버 기능

ACI 리프 스위치는 다운스트림 클라이언트(예: 패브릭에 연결된 서버)의 NTP 서버 역할을 할 수 있습니다. 이 기능은 기본적으로 비활성화되어 있으며, 날짜 및 시간 정책의 서버 상태 옵션을 통해 명시적으로 활성화해야 합니다. 활성화된 경우 클라이언트는 리프 스위치 대역 내, 대역 외, 브리지 도메인 SVI 또는 L3Out IP 주소를 NTP 서버 주소로 사용할 수 있습니다.

✎ 참고: 패브릭 스위치는 동일한 패브릭의 다른 스위치와 동기화해서는 안 됩니다. 패브릭 스위치는 항상 외부 NTP 서버와 동기화해야 합니다.

컨피그레이션 확인

NTP 운영 상태를 트러블슈팅하기 전에 컨피그레이션 체인이 완료되었는지 확인합니다. 컨피그레이션 오류는 ACI에서 NTP 문제의 가장 일반적인 근본 원인입니다.

1단계: 노드 관리 주소 확인

Tenants(테넌트) > mgmt(관리) > Node Management Addresses(노드 관리 주소)(고정 할당의 경우) 또는 Node Management EPG(노드 관리 EPG)(연결 그룹의 경우)로 이동합니다.

모든 APIC 및 스위치 노드에 관리 IP 주소가 할당되었는지 확인합니다. 관리 주소가 없는 노드는 NTP 서버와 통신할 수 없습니다.

또는 API를 쿼리합니다.

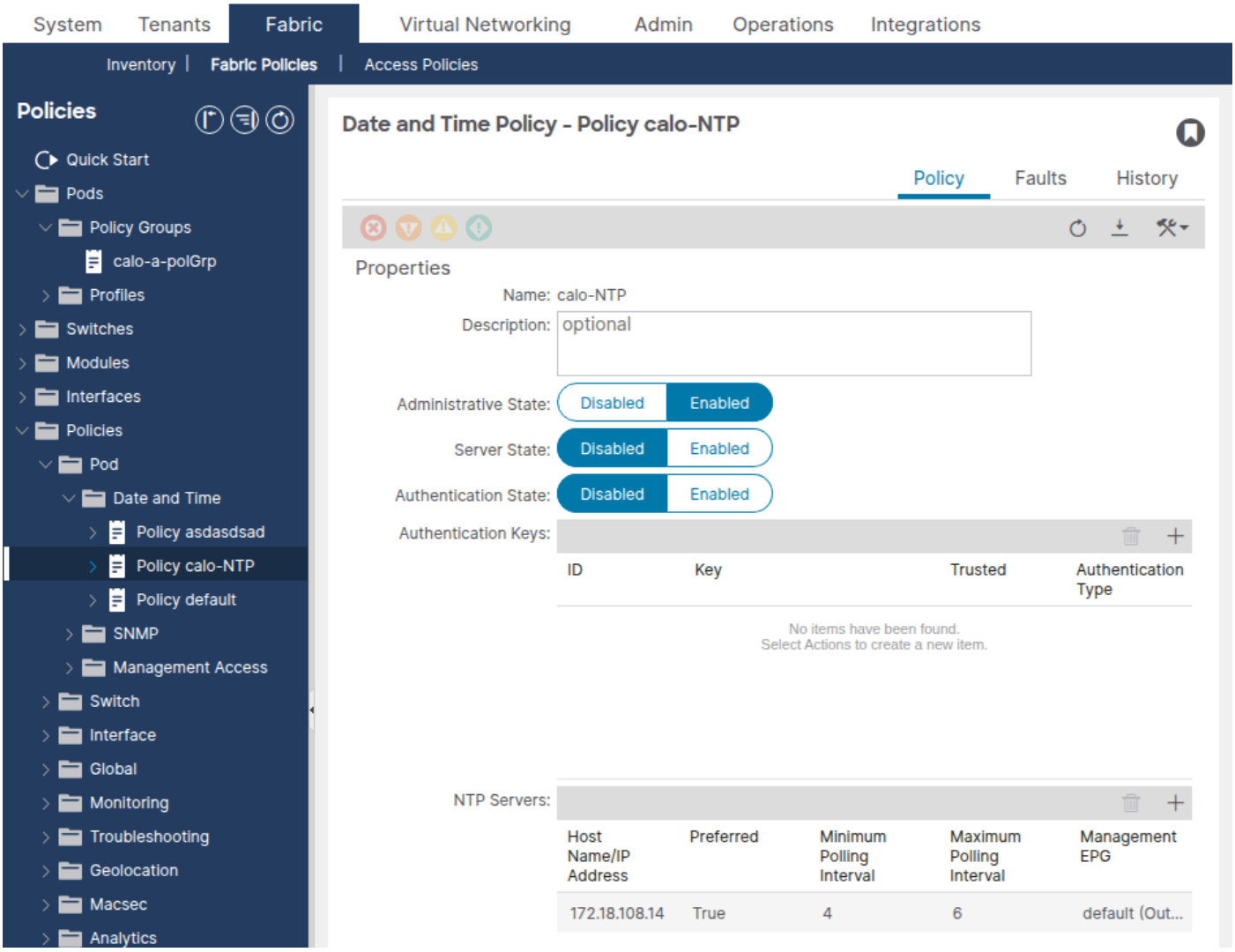
<#root>

apic1#

moquery -c mgmtRsOoBStNode

2단계: 날짜 및 시간 정책에 NTP 공급자가 있는지 확인합니다.

Fabric(패브릭) > Fabric Policies(패브릭 정책) > Policies(정책) > Pod > Date and Time(날짜 및 시간) > [Your Policy](사용자 정책)로 이동합니다.



하나 이상의 NTP 제공자(서버)가 구성되었는지 확인합니다. 공급자가 여러 개인 경우 하나 이상을 Preferred로 플래그 지정합니다.

API를 통해 NTP 제공자를 확인합니다.

<#root>

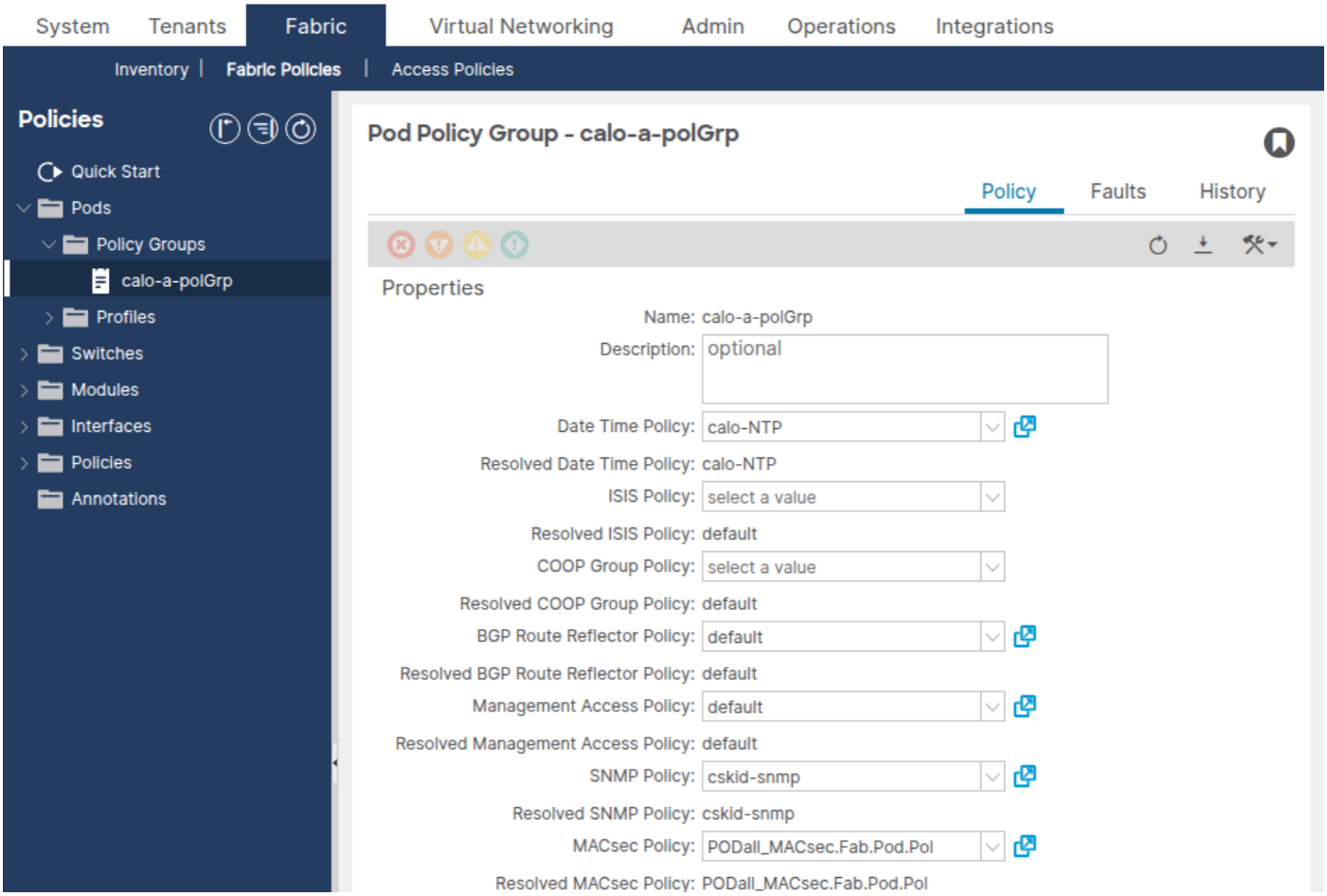
```
apic1#

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
```

일반적인 컨피그레이션 오류

- 구성된 NTP 제공자 없음 - Date and Time 정책이 있지만 제공자가 없습니다. 정책이 적용되지만 노드에 동기화할 NTP 서버가 없습니다.
- 잘못된 관리 EPG 선택 — NTP 제공자가 대역 외 EPG를 참조하지만 NTP 서버는 대역 내를 통해서만(또는 그 반대의 경우) 연결할 수 있습니다. 어떤 관리 EPG가 NTP 서버에 연결성을 제공하는지 확인합니다.
- 동일한 서버의 FQDN 및 IP가 별도의 공급자로 추가됨 - 중복 IP 결함이 생성됩니다. 중복 항목을 삭제합니다.
- DNS 정책이 없는 FQDN 기반 제공자 — NTP 제공자에 호스트 이름을 사용하는 경우 DNS 서비스 정책이 구성되어 있고 관리 VRF에 적절한 DNS 레이블이 적용되었는지 확인합니다.

3단계: Pod 정책 그룹이 날짜 및 시간 정책을 참조하는지 확인

Fabric(패브릭) > Fabric Policies(패브릭 정책) > Pod > Policy Groups(정책 그룹) > [Your Pod Policy Group](포드 정책 그룹)으로 이동합니다.



Date Time Policy 필드가 올바른 날짜 및 시간 정책을 참조하는지 확인합니다.

<#root>

apic1#

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

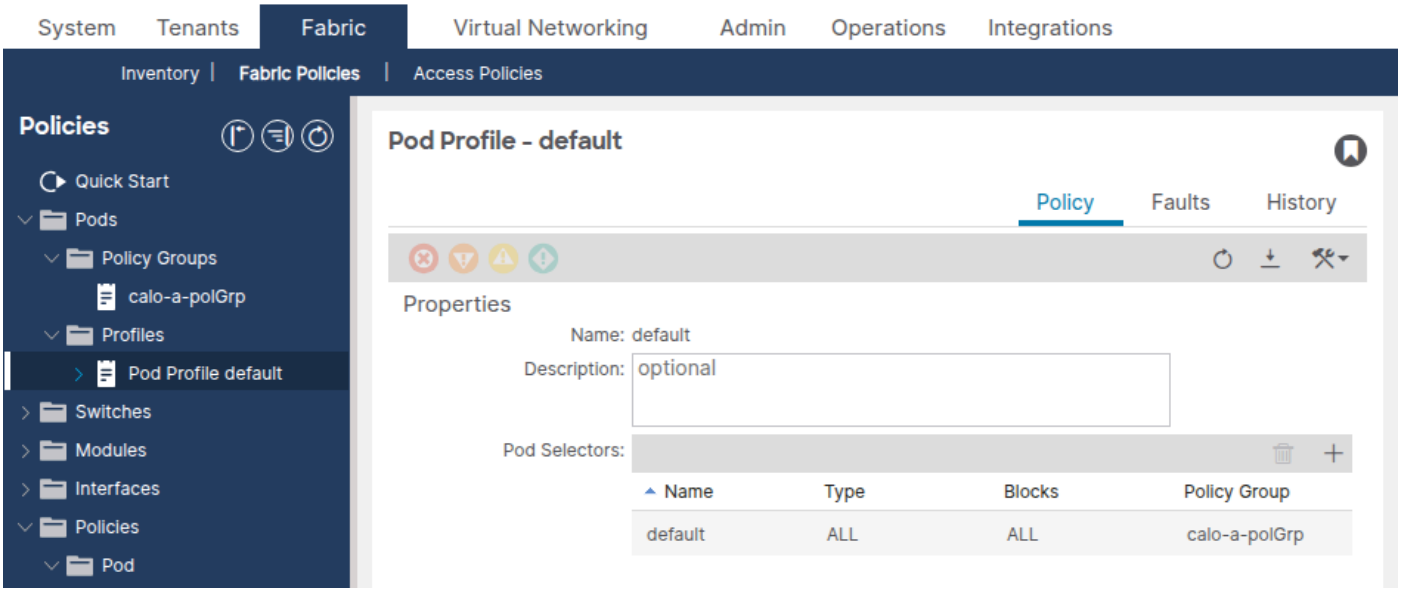
datetimePolName 특성 또는 연결된 fabricRsTimePol 관계를 찾습니다.

일반적인 컨피그레이션 오류

- 포드 정책 그룹이 잘못된 날짜 및 시간 정책을 참조합니다. 여러 날짜 및 시간 정책(예: "기본값" 및 사용자 지정 정책)이 있는 경우 포드 정책 그룹이 원하는 정책을 참조하는지 확인하십시오.
- Pod 정책 그룹이 전혀 생성되지 않음 — 기본 Pod 정책 그룹에 연결된 날짜 및 시간 정책이 없을 수 있습니다. 항상 확인합니다.

4단계: Pod 프로필이 Pod 정책 그룹을 참조하는지 확인

Fabric(패브릭) > Fabric Policies(패브릭 정책) > Pods(포드) > Profiles(프로파일) > [Your Pod Profile](포드 프로파일)로 이동합니다.



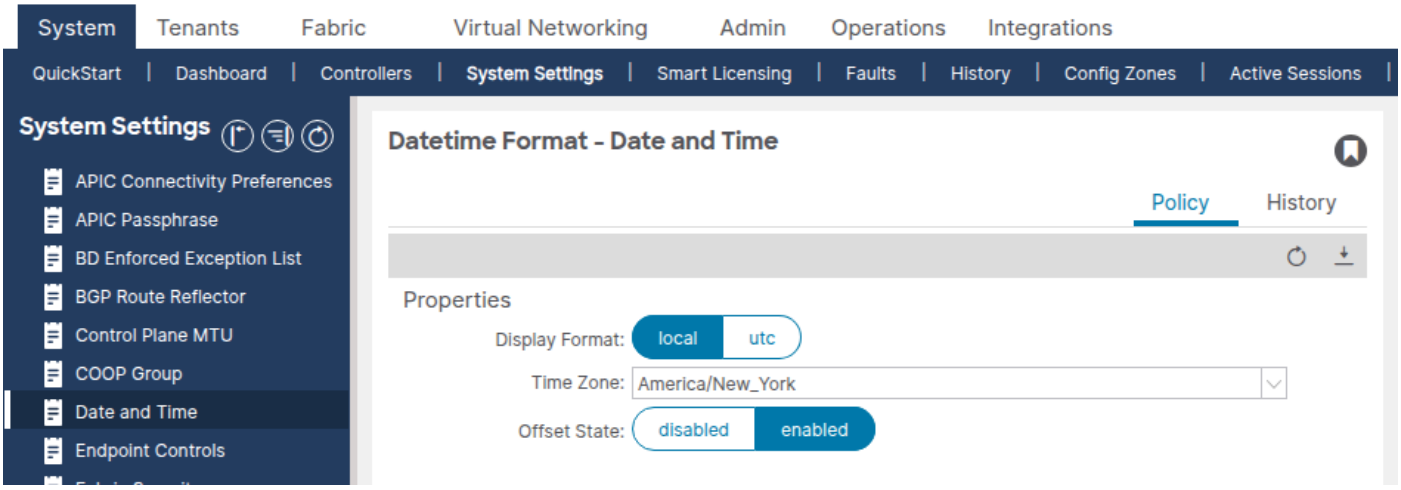
패브릭 정책 그룹 필드가 올바른 포드 정책 그룹을 참조하는지 확인합니다.

일반적인 컨피그레이션 오류

- Pod Profile references wrong Pod Policy Group(잘못된 Pod 정책 그룹 참조) - 특히 다중 Pod 환경에서는 각 Pod 프로필이 올바른 Pod 정책 그룹을 참조해야 합니다.

5단계: 날짜 및 시간 형식 확인

System(시스템) > System Settings(시스템 설정) > Date and Time(날짜 및 시간)으로 이동합니다.



표시 형식(로컬 또는 UTC) 및 표준 시간대가 예상대로 설정되었는지 확인합니다. 이 설정은 삭제하거나 복제할 수 없는 별도의 기본 Date Time Format 정책입니다.

운영 확인

컨피그레이션 체인이 올바른지 확인한 후 다음 명령을 사용하여 런타임에 NTP가 작동하는지 확인합니다.

APIC 확인

ntpq 표시

이 명령은 모든 APIC에서 NTP 동기화 상태를 표시합니다. *기호는 동기화를 위해 서버가 선택되었음을 나타냅니다.

<#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
```

좋은 모습:

- 모든 APIC는 원격 서버 옆에 *(동기화용으로 선택됨)가 표시됩니다.
- 도달 거리는 377(8진수)로, 이는 최근 8개 조사가 모두 성공했음을 나타냅니다.
- st(stratum)은 1~15입니다. stratum 16은 서버가 동기화되지 않았음을 의미합니다.
- offset은 낮음(일반적으로 건강한 환경의 경우 100ms 미만).

어떤 나쁜 모습인가:

- No * 모든 서버 옆에 있음 — 동기화할 서버를 선택하지 않았습니다.
- reach is 0 — 수신된 NTP 응답이 없습니다.
- st는 16입니다. NTP 서버는 업스트림 시간 소스에 동기화되지 않습니다.
- offset은 매우 큽니다(수천 밀리초). 클럭이 상당히 표류합니다.

시계 표시

```
<#root>

apic1#

show clock

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

시간이 정확한지 확인합니다. 클럭 드리프트를 탐지할 예상 시간과 비교합니다.

APIC Bash(대체)

```
<#root>

apic1#

bash

admin@apic1:~>
```

date

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

스위치 확인(리프/스파인)

ntp 피어 표시

NTP 제공자가 스위치에 푸시되었는지 확인합니다.

<#root>

```
leaf1#
```

show ntp peers

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

좋은 모습: NTP 서버 IP 또는 호스트 이름이 `Serv/Peer` = `Server` 및 올바른 VRF(일반적으로 OOB의 `관리`)와 함께 표시됩니다.

어떤 나쁜 모습인가: 나열된 피어가 없거나 NTP 서버 IP가 구성된 공급자와 일치하지 않습니다. 이는 일반적으로 날짜 및 시간 정책이 Pod Policy Group/Pod Profile 체인을 통해 적용되지 않았음을 나타냅니다.

show ntp peer-status

동기화를 위해 NTP 서버가 선택되었는지 확인합니다.

<#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
```

*문자는 반드시 필요합니다. 즉, NTP 서버가 동기화에 사용되고 있는지 확인합니다.

어떤 나쁜 모습인가:

- 아니요 * 서버 옆에 있습니다. 스위치가 서버와 동기화되지 않습니다.
- reach is 0 — 수신된 NTP 응답이 없습니다. 이는 연결 가능성 문제를 나타냅니다.
- st는 16입니다. NTP 서버가 동기화되지 않았으므로 유효한 시간을 제공할 수 없습니다.

show ntp statistics peer ipaddr

NTP 패킷 교환을 확인하여 연결 가능성을 확인합니다. IP 주소를 영향받는 스위치의 NTP 제공자 주소로 교체합니다.

<#root>

```
leaf1#

show ntp statistics peer ipaddr 10.1.1.100


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

좋은 모습: 전송된 패킷과 수신된 패킷은 거의 동일하며 증가하고 있습니다.

어떤 나쁜 모습인가: 전송된 패킷은 증가하지만 수신된 패킷은 0이거나 간신히 증가합니다. NTP 응답이 스위치에 도달하지 않습니다.

시계 표시

<#root>

```
leaf1#

show clock

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

GUI 확인

Fabric(패브릭) > Fabric Policies(패브릭 정책) > Policies(정책) > Pod > Date and Time(날짜 및 시간) > [Your Policy](사용자 정책) > [NTP Provider](NTP 제공자)로 이동합니다.

Sync Status(동기화 상태) 열에는 모든 노드에 대해 Synced to Remote NTP Server(원격 NTP 서버에 동기화됨)가 표시되어야 합니다. 초기 구축 후 동기화 상태가 통합되는 데 몇 분 정도 걸릴 수 있습니다.

API 확인

모든 APIC에서 NTP 동기화를 확인하려면 datetimeNtpq 클래스를 쿼리합니다.

<#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.
```

문제 해결 워크플로

ACI 노드에서 NTP 문제가 보고될 때 이 진단트리를 사용합니다.

1단계: 스위치에 NTP 피어가 구성되어 있습니까?

영향을 받는 스위치에 로그인하고 다음을 실행합니다.

<#root>

```
leaf1#
```

```
show ntp peers
```

- 이 노드→ Date and Time 정책이 적용되지 않아 나열된 피어가 없습니다. 시나리오 1로 이동합니다. NTP 제공자가 스위치에 푸시되지 않았습니다.
- 나열된 피어→ 2단계로 진행합니다.

2단계: 동기화를 위해 NTP 서버가 선택되었습니까?

<#root>

```
leaf1#

show ntp peer-status
```

- ***NTP**가 동기화 중인 → 존재합니다. 그래도 시간이 틀리면 시나리오 5로 이동합니다. 큰 오프셋/클럭 드리프트.
- 아니요 * → 3단계로 넘어갑니다.

3단계: 도달 거리 값이 0입니까?

show ntp peer-status에서 reach 열을 확인합니다.

- **reach = 0** → NTP 서버의 응답이 없습니다. 시나리오 2로 이동합니다. NTP 서버에 연결할 수 없습니다.
- **연결이 0**을 초과하지만 * → 응답이 도착하지만 동기화가 설정되지 않습니다. 계층 확인 — 4단계로 이동합니다.

4단계: 계층 값은 16입니까?

- 계층 = 16 → NTP 서버가 자체 업스트림 소스에 동기화되지 않습니다. 시나리오 3으로 이동합니다. NTP 서버가 동기화되지 않았습니다(계층 16).
- 계층 1-15에서 동기화가 수행되지 → 시나리오 4: NTP 인증이 일치하지 않습니다.

일반적인 문제 해결 시나리오

시나리오 1: 스위치에 푸시되지 않은 NTP 제공자

증상: `show ntp peers` on the switch returns no entries.

컨피그레이션 확인:

1. Date and Time(날짜 및 시간) 정책에 하나 이상의 NTP 공급자가 구성되어 있는지 확인합니다
   .
2. 포드 정책 그룹이 올바른 날짜 및 시간 정책을 참조하는지 확인합니다.
3. 포드 프로필이 올바른 포드 정책 그룹을 참조하는지 확인합니다.
4. 노드에 관리 테넌트 아래에 할당된 관리 IP 주소가 있는지 확인합니다.

근본 원인: 정책 체인에 있는 네 개의 링크(Date and Time Policy → NTP Provider → Pod Policy Group → Pod Profile) 중 하나가 끊어졌습니다. 가장 일반적인 원인은 포드 정책 그룹이 포드 프로필과 연결되지 않았거나 Pod 정책 그룹에서 날짜 및 시간 정책이 선택되지 않았기 때문입니다.

해결책: 정책 체인의 누락된 링크를 완료합니다. 영향을 받는 포드의 포드 프로필이 올바른 날짜 및 시간 정책을 포함하는 포드 정책 그룹을 참조하는지 확인합니다. NTP 사업자 컨피그레이션이 적용되면 몇 분 내에 스위치에 푸시됩니다.

시나리오 2: NTP 서버에 연결할 수 없음

증상: `show ntp peer-status`는 `reach = 0`을 보여 줍니다. `show ntp statistics peer ipaddr 10.1.1.100`은 수신된 패킷 = 0을 보여 줍니다.

컨피그레이션 확인: NTP 제공자가 올바른 관리 EPG(OOB 또는 대역 내)와 연결되어 있는지 확인합니다. OOB를 사용하는 경우 OOB 계약에서 UDP 포트 123을 허용하는지 확인합니다.

운영 확인:

1. 관리 VRF를 사용하여 영향을 받는 스위치에서 NTP 서버를 ping합니다.
   <#root>

   ```
   leaf1#

   ping 10.1.1.100 vrf management
   ```

2. 스위치에서 tcpdump를 실행하여 NTP 패킷이 떠나고 도착하는지 확인합니다.
   <#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
```

근본 원인: 일반적으로 다음 중 하나입니다.

- 스위치에 관리 IP 주소가 할당되어 있지 않습니다.
- 관리 VRF의 기본 게이트웨이가 없거나 잘못되었습니다.
- 방화벽이 스위치와 NTP 서버 간의 UDP 포트 123을 차단하고 있습니다.
- OOB 계약은 UDP 포트 123을 허용하지 않습니다.
- NTP 제공자가 잘못된 관리 EPG를 참조합니다(예: OOB를 선택했지만 인밴드(in-band)에만 연결 가능).

해결책: 연결 문제 해결 누락된 경우 관리 주소를 할당하거나, 기본 게이트웨이를 수정하거나, 방화벽 규칙을 업데이트하거나, NTP 공급자에서 관리 EPG 선택을 수정합니다.

시나리오 3: NTP 서버 비동기화(계층 16)

증상: `show ntp peer-status`는 stratum (`st`) = `16`을 표시합니다. 스위치는 stratum 16 서버로 동기화되지 않습니다.

운영 확인: NTP 서버에 로그인하거나 외부 호스트에서 쿼리하여 자체 업스트림 시간 소스에 동기화되었는지 확인합니다.

근본 원인: NTP 서버 자체가 업스트림 참조 클럭과의 동기화를 상실했습니다. 계층 16이 있는 서버는 신뢰할 수 있는 시간원이 없다고 광고하고 있다.

해결책: NTP 서버를 수정합니다. ACI 패브릭 외부에 있음 — NTP 서버 컨피그레이션 및 업스트림 시간 소스를 확인합니다. NTP 서버를 즉시 수정할 수 없는 경우 날짜 및 시간 정책에서 대체 NTP 공급자를 구성합니다.

시나리오 4: NTP 인증 불일치

증상: `show ntp peer-status`는 reach > `0`을 보여 주며 stratum이 유효하지만 `*`는 표시되지 않습니다. NTP 서버가 응답하지만 스위치에서 응답을 허용하지 않습니다.

컨피그레이션 확인:

1. NTP 서버에 인증이 필요한지 확인합니다.
2. 인증이 필요한 경우 날짜 및 시간 정책의 Authentication State(인증 상태)가 Enabled(활성화

됨)로 설정되어 있는지 확인합니다.
3. ACI 패브릭과 NTP 서버 간의 인증 키 ID, 키 값 및 알고리즘(MD5, SHA-1 또는 AES128-CMAC)이 일치하는지 확인합니다.
4. NTP Client Authentication Keys(NTP 클라이언트 인증 키) 테이블에서 키가 Trusted(신뢰할 수 있음)로 표시되는지 확인합니다.

근본 원인: ACI와 NTP 서버 간에 인증 키, 알고리즘 또는 키 ID가 일치하지 않아 스위치가 NTP 응답을 인증되지 않은 것으로 거부합니다.

해결책: 인증 컨피그레이션을 맞춥니다. ACI와 NTP 서버 모두에서 동일한 키 ID, 키 값 및 알고리즘이 구성되었는지 확인합니다. APIC 릴리스 6.1(1) 이상에서는 AES128-CMAC가 권장됩니다.

 참고: FIPS 모드가 활성화된 경우 AES128-CMAC 및 SHA-1 인증 체계만 지원됩니다. MD5는 FIPS 모드에서 작동하지 않습니다.

시나리오 5: 큰 오프셋/클럭 드리프트

증상: 스위치가 동기화된 것 같습니다(* present, reach = 377). 그러나 `show ntp peer-status` 또는 show ntpq의 `offset` 값이 매우 크거나(수백 또는 수천 밀리초) 시계가 잘못되어 있습니다.

운영 확인:

```
<#root>

apic1#

show ntpq
```

`offset` 열을 선택합니다. 정상 오프셋은 일반적으로 100ms 미만입니다.

근본 원인: NTP 동기화가 설정되거나 재부팅 중에(예: 데드 CMOS 배터리 때문에) 하드웨어 클럭(RTC)이 재설정되기 전에 클럭이 크게 감소했습니다. NTP는 큰 오프셋에 시간이 걸릴 수 있는 눈썰기를 통해 시계를 점진적으로 수정합니다.

해결책: 오프셋이 매우 크고 NTP가 능동적으로 동기화되는 경우 시계가 수렴할 때까지 기다립니다. NTP는 시계를 서서히 기울입니다. 큰 오프셋은 완전히 바로잡는 데 몇 시간이 걸릴 수 있습니다. 오프셋이 감소하지 않으면 NTP 서버가 정확한 시간을 제공하는지 확인합니다. 재부팅할 때마다 문제가 반복되면 영향을 받는 노드의 하드웨어 클럭(RTC/CMOS 배터리)을 조사합니다.

시나리오 6: 대역 내 NTP를 사용하는 대기 APIC 결함

증상: NTP가 대역 내 관리용으로 구성된 경우 NTP 또는 모니터링 정책과 관련된 대기 APIC에서 장애가 생성됩니다.

근본 원인: 대역 내 관리를 위해 NTP 정책을 적용할 경우 대기 APIC에도 대역 내 컨피그레이션이 필요합니다. 그것이 없으면, 결함은 제기된다.

해결책: 대기 APIC에 대한 대역 내 관리도 구성합니다. 이렇게 하면 결함이 제거됩니다.

시나리오 7: 중복 IP 결함

증상: NTP 공급자를 추가하면 중복 IP 결함이 발생합니다.

근본 원인: FQDN을 NTP 제공자로 추가한 다음 해당 FQDN의 확인된 IP 주소를 두 번째 NTP 제공자로 추가했습니다. ACI에서 중복을 탐지합니다.

해결책: 가장 최근에 추가한 중복 공급자(FQDN을 먼저 추가한 경우 IP 주소 항목 또는 그 반대의 경우)를 삭제합니다. NTP 서버당 하나의 항목(FQDN 또는 IP 주소 중 하나만 사용, 둘 다 사용 안 함)만 사용합니다.

시나리오 8: FQDN 기반 NTP 공급자에 대한 DNS 확인 실패

증상: 호스트 이름으로 구성된 NTP 제공자가 확인되지 않습니다. `show ntp peers` does not show the expected IP address or NTP is syncing.(show ntp 피어가 예상 IP 주소를 표시하지 않거나 NTP가 동기화되지 않습니다).

컨피그레이션 확인:

1. DNS 서비스 정책이 Fabric(패브릭) > Fabric Policies(패브릭 정책) > Policies(정책) > Global(전역) > DNS Profiles(DNS 프로필)에서 구성되었는지 확인합니다.
2. 관리 VRF에서 DNS 제공자(DNS 서버)에 연결할 수 있는지 확인합니다.
3. 관리 EPG의 대역 내 또는 대역 외 VRF 인스턴스에 대해 적절한 DNS 레이블이 구성되어 있는지 확인합니다.

근본 원인: DNS 서버에 연결할 수 없거나 DNS 서버가 구성되지 않아 NTP 공급자의 호스트 이름 확인이 실패했습니다.

해결책: DNS 서비스 정책을 구성하고, DNS 연결성을 확인하고, 올바른 DNS 레이블을 적용합니다. 또는 호스트 이름 대신 NTP 서버 IP 주소를 사용합니다.

관련 결함 및 이벤트

다음은 ACI에서 오류를 생성할 수 있는 NTP 관련 조건입니다.

- Duplicate IP fault(중복 IP 결함) - FQDN과 동일한 NTP 서버의 IP 주소가 모두 제공자로 추가된 경우 발생합니다. 해결 방법: 중복 항목을 제거합니다.
- 스탠바이 APIC 인밴드 NTP 결함 - 모니터링 또는 NTP 정책이 인밴드에 적용되었지만 스탠바이 APIC에 인밴드 컨피그레이션이 없을 때 발생합니다.
- Sync Status not converging — GUI에서 하나 이상의 노드에 대해 "Not Synced" 또는 "Synced to Remote NTP Server" 이외의 상태를 표시합니다. 이는 결함 코드가 아니라 작동 상태 표시기입니다. 위의 문제 해결 워크플로에 따라 진단합니다.

에스컬레이션 기준

다음과 같은 경우 Cisco TAC로 이관하는 것이 좋습니다.

- 컨피그레이션 체인이 올바르게 확인되고 NTP 서버에 연결할 수 있지만(ping이 작동하고, tcpdump에 NTP 응답이 표시됨) 스위치가 여전히 동기화되지 않습니다.
- 컨피그레이션 변경 또는 NTP 서버 문제 없이 NTP 동기화가 반복적으로 손실됩니다.
- show `ntp peer-status` 출력은 외부에서 동기화된 것으로 확인된 서버의 persistent stratum 16과 같은 예기치 않은 동작을 표시합니다.
- 재부팅할 때마다 클럭이 크게 이동하며, 이는 하드웨어 클럭(RTC) 문제를 나타낼 수 있습니다.

TAC 계약 시 다음 데이터를 제공하십시오.

- 모든 APIC의 `show` ntpq의 출력입니다.
- `show ntp peers`, `show ntp peer-status`, `show ntp statistics peer ipaddr <IP>` 및 `show clock`의 영향받는 모든 스위치의 출력
- APIC의 `moquery -c datetimePol`, `moquery -c datetimeNtpProv` 및 `moquery -c datetimeNtpq`의 출력입니다.
- 영향을 받는 노드의 기술 지원.

참조

- Cisco APIC 기본 컨피그레이션 가이드, 릴리스 6.1(x) — 코어 ACI 패브릭 서비스 프로비저닝
- ACI 관리 및 코어 서비스 문제 해결 — 포드 정책
- Cisco ACI(Application Centric Infrastructure) 설계 가이드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.