Identificar e solucionar problemas de NTP em uma estrutura da Cisco ACI

Introdução

Este documento descreve como verificar, solucionar problemas e resolver problemas de Network Time Protocol (NTP) em uma estrutura da Cisco ACI. Ele aborda o modelo de política de NTP, a verificação de configuração, os comandos de verificação operacional, um fluxo de trabalho de triagem para sintomas de NTP comuns e cenários detalhados de solução de problemas.

Informações de Apoio

O material deste documento foi extraído do capítulo Troubleshoot ACI Management and Core Services — Pod Policies, do Cisco APIC Basic Configuration Guide, Release 6.1(x) — Provisioning Core ACI Fabric Services e do Cisco ACI Design Guide.

Overview

A sincronização de tempo é um recurso crucial em uma malha da ACI, da qual dependem as tarefas de monitoramento, operacionais e de solução de problemas. A sincronização de relógio garante a análise adequada dos fluxos de tráfego, a correlação dos timestamps de depuração e de falha em vários nós de estrutura e a utilização completa do recurso do contador atômico do qual dependem as pontuações de integridade do aplicativo. A configuração de NTP inexistente ou inadequada não aciona necessariamente uma falha ou uma pontuação de integridade baixa, portanto, é importante configurar a sincronização de tempo no início da implantação da malha.

Modelo de política NTP na ACI

O NTP na ACI é gerenciado por uma cadeia de quatro objetos de política:

1. Política de data e hora (`datetimePol`) — define a configuração do NTP incluindo estado administrativo, estado de autenticação, estado do servidor e modo mestre. Localizada em Fabric > Fabric Policies > Policies > Pod > Date and Time.
2. Provedor NTP (`datetimeNtpProv`) — define entradas individuais do servidor NTP (provedores) em uma política de Data e Hora, incluindo o IP/FQDN do servidor, seleção de EPG de

gerenciamento (fora da banda ou dentro da banda), flag preferencial e intervalos de polling.
3. Pod Policy Group (`fabricPodPGrp`) — faz referência à política de data e hora junto com outras políticas de nível de pod (BGP RR, SNMP, etc.). Localizada em Fabric > Fabric Policies > Pods > Policy Groups.
4. Pod Profile (`fabricPodP`) — associa um grupo de políticas de pods a um seletor de pods. Localizada em Fabric > Fabric Policies > Pods > Profiles.

Todos os quatro links nessa cadeia devem ser configurados para que o NTP seja aplicado aos nós de estrutura. Se algum link for quebrado, a configuração do provedor NTP não será enviada aos switches.

Pré-requisitos

- A descoberta de malha deve ser concluída.
- Os endereços de gerenciamento de nó (OOB ou in-band) devem ser atribuídos a todos os APICs e switches sob o locatário mgmt.
- Para NTP fora da banda, o EPG de gerenciamento OOB deve permitir a porta UDP 123.
- Para o NTP em banda, um EPG de gerenciamento em banda com contratos apropriados e acessibilidade ao servidor NTP deve ser configurado. Os endereços IP em banda não podem ser acessados de fora da malha sem uma política adicional.

Autenticação NTP

A ACI suporta três esquemas de autenticação NTP: MD5, SHA-1 e AES128-CMAC. O AES128-CMAC foi introduzido no APIC versão 6.1(1) e é o esquema recomendado, pois o MD5 é considerado fraco e inseguro. Quando o modo FIPS está habilitado, somente AES128-CMAC e SHA-1 são suportados.

Funcionalidade do servidor NTP

Os switches leaf da ACI podem atuar como servidores NTP para clientes downstream (por exemplo, servidores conectados à malha). Este recurso está desabilitado por padrão e deve ser explicitamente habilitado por meio da opção Estado do Servidor na política de Data e Hora. Quando habilitados, os clientes podem usar o switch leaf na banda, fora da banda, SVI de domínio de bridge ou endereço IP L3Out como o endereço do servidor NTP.

 Note: Os switches de malha não devem ser sincronizados com outros switches da mesma malha. Os switches de estrutura devem sempre sincronizar com servidores NTP externos.

Verifique a configuração

Antes de solucionar problemas do estado operacional do NTP, verifique se a cadeia de configuração está completa. A configuração incorreta é a causa raiz mais comum de problemas de NTP na ACI.

Passo 1: Verificar endereços de gerenciamento de nó

Navegue para Locatários > gerenciamento > Endereços de gerenciamento de nó (para atribuição estática) ou EPGs de gerenciamento de nó (para grupos de conectividade).

Confirme se cada APIC e nó de switch tem um endereço IP de gerenciamento atribuído. Nós sem endereços de gerenciamento não podem se comunicar com o servidor NTP.

Como alternativa, consulte a API:

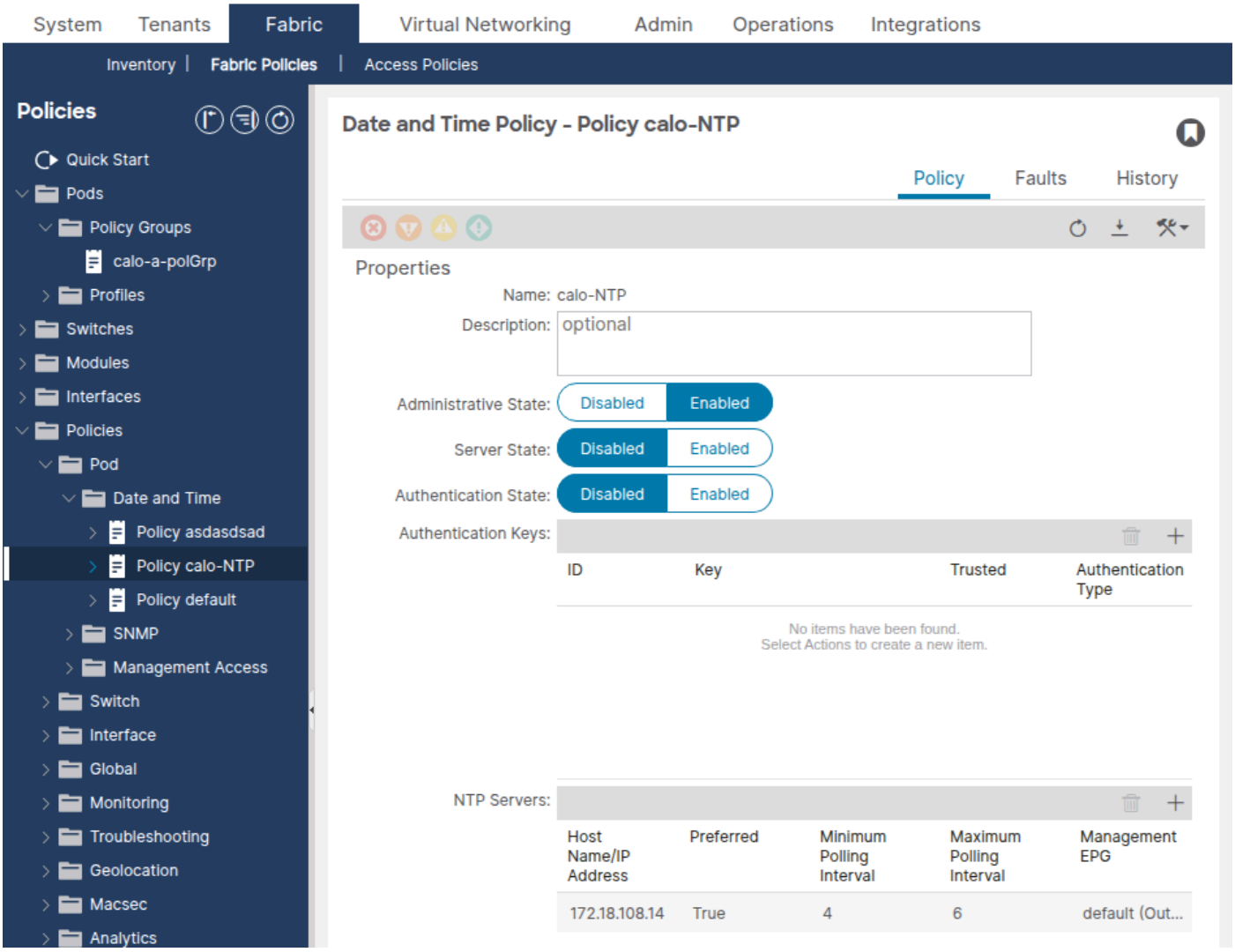
<#root>

apic1#

moquery -c mgmtRsOoBStNode

Passo 2: Verifique se a política de data e hora tem um provedor de NTP

Navegue até Fabric > Fabric Policies > Policies > Pod > Date and Time > [Your Policy].



Confirme se pelo menos um provedor de NTP (servidor) está configurado. Se houver vários provedores, sinalize pelo menos um como Preferencial.

Verifique o provedor de NTP via API:

<#root>

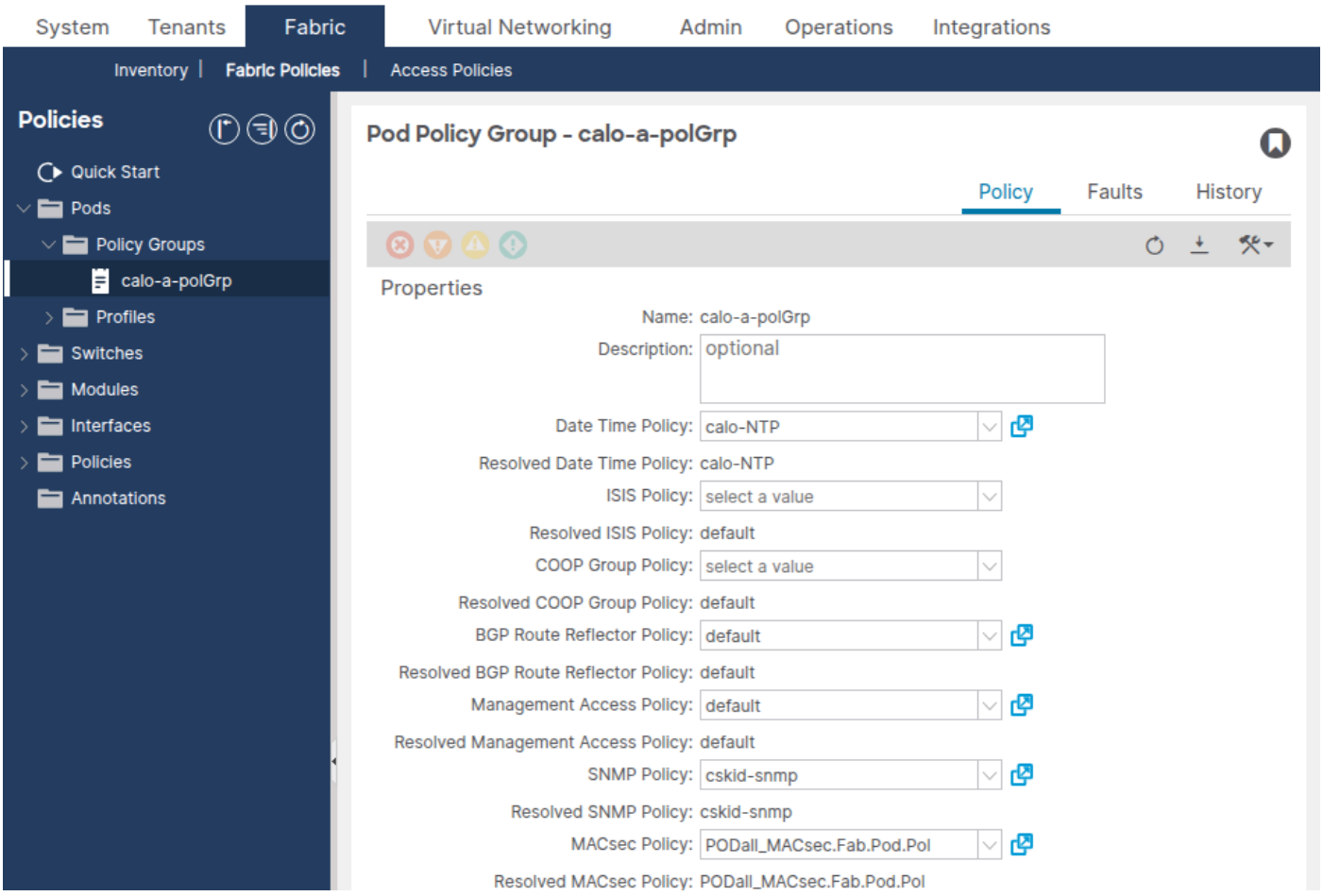
```
apic1#

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
```

Erros comuns de configuração

- Nenhum provedor NTP configurado — a política de Data e Hora existe, mas não tem nenhum provedor. A política será aplicada, mas os nós não terão nenhum servidor NTP para sincronização.
- EPG de gerenciamento incorreto selecionado — o provedor NTP faz referência ao EPG fora da banda, mas o servidor NTP só pode ser acessado via in-band (ou vice-versa). Verifique qual EPG de gerenciamento fornece acessibilidade ao servidor NTP.
- FQDN e IP do mesmo servidor adicionados como provedores separados — isso gera uma falha de IP duplicado. Exclua a entrada duplicada.
- Provedor baseado em FQDN sem política DNS — se estiver usando um nome de host para o provedor NTP, verifique se uma política de serviço DNS está configurada e se o rótulo DNS apropriado está aplicado ao VRF de gerenciamento.

Passo 3: Verifique se o grupo de políticas do Pod faz referência à política de data e hora

Navegue até Fabric > Fabric Policies > Pods > Policy Groups > [Your Pod Policy Group].



O campo Confirm the Date Time Policy faz referência à política correta de Data e Hora.

<#root>

apic1#

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

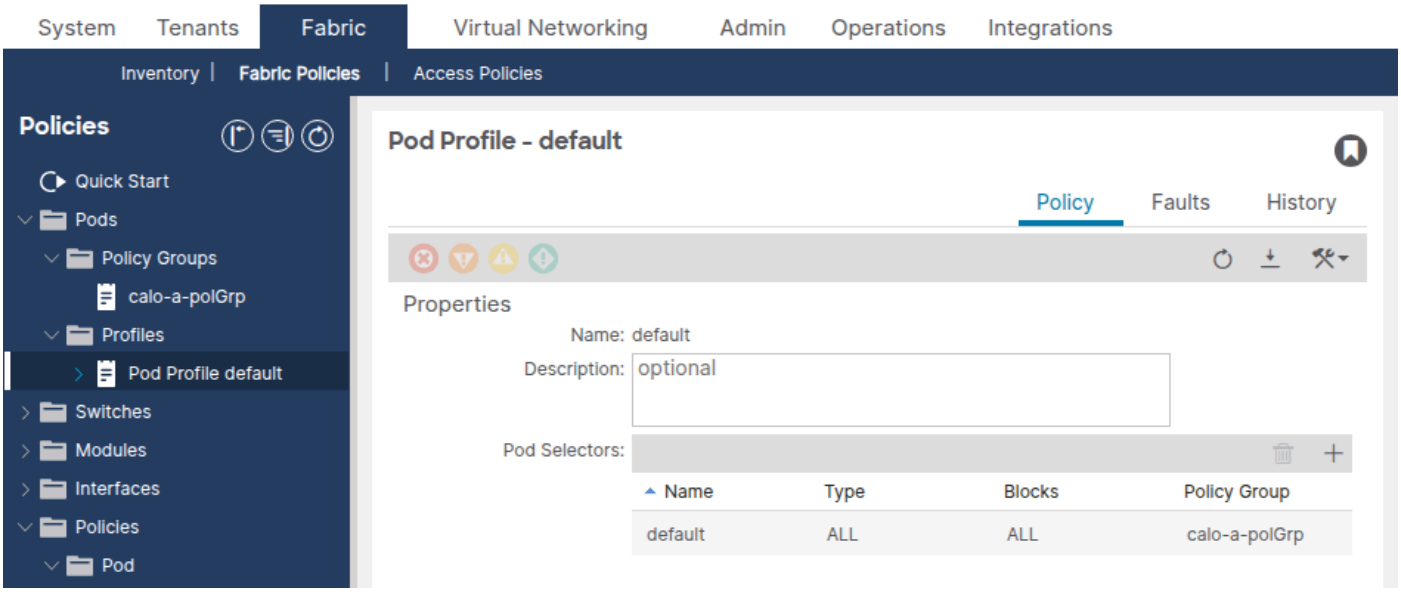
Procure o atributo `datetimePolName` ou a relação `fabricRsTimePol` associada.

Erros comuns de configuração

- O Pod Policy Group faz referência à política incorreta de Data e Hora — se existirem várias políticas de Data e Hora (por exemplo, "padrão" e uma personalizada), verifique se o Pod Policy Group faz referência à política pretendida.
- Grupo de Políticas de Pod não criado de forma alguma — o Grupo de Políticas de Pod padrão pode não ter a política de Data e Hora associada. Sempre verificar.

Passo 4: Verifique se o perfil do Pod faz referência ao grupo de políticas do Pod

Navegue até Fabric > Fabric Policies > Pods > Profiles > [Your Pod Profile].



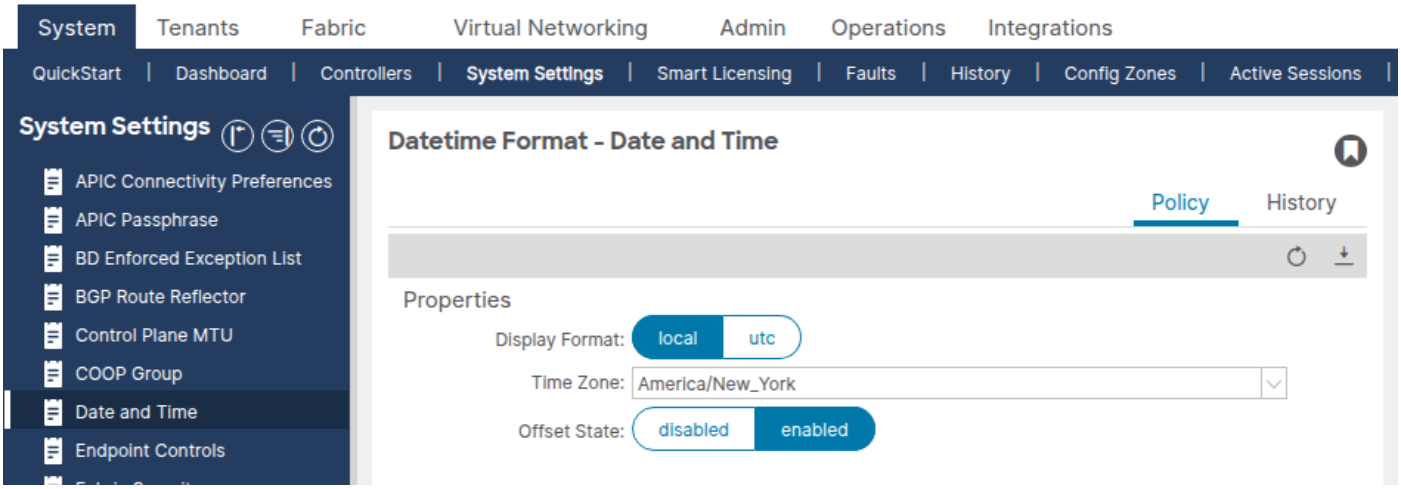
Confirme se o campo Grupo de política de estrutura faz referência ao Grupo de política de pod correto.

Erros comuns de configuração

- O Perfil do Pod faz referência ao Grupo de políticas do Pod errado — especialmente em ambientes de vários pods, cada perfil de pod deve fazer referência ao grupo de políticas do pod correto.

Passo 5: Verificar Formato de Data e Hora

Navegue até System > System Settings > Date and Time.



Confirme se o formato de exibição (local ou UTC) e o fuso horário estão definidos como esperado. Essa configuração é uma política de formato de data e hora padrão separada que não pode ser excluída ou duplicada.

Verificação operacional

Depois de confirmar se a cadeia de configuração está correta, use os seguintes comandos para verificar se o NTP está funcionando em tempo de execução.

Verificação APIC

show ntpq

Esse comando mostra o status de sincronização de NTP em todos os APICs. O símbolo * indica que o servidor está selecionado para sincronização.

<#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
```

O que parece bom:

- Todos os APICs mostram `*` (selecionados para sincronização) ao lado do servidor remoto.
- `reach` é `377` (octal), indicando que as últimas 8 votações foram todas bem-sucedidas.
- `st` (stratum) está entre 1 e 15. Stratum 16 significa que o servidor não está sincronizado.
- `o deslocamento` é baixo (geralmente abaixo de 100 ms para um ambiente saudável).

Qual é a aparência ruim:

- No `*` ao lado de qualquer servidor — nenhum servidor está selecionado para sincronização.
- `reach` é `0` — nenhuma resposta de NTP foi recebida.
- `st` is `16` — o servidor NTP não está sincronizado com sua origem de tempo de upstream.
- `offset` é extremamente grande (milhares de milissegundos) — o relógio é significativamente desviado.

show clock

<#root>

```
apic1#

show clock

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

Confirme se a hora está correta. Compare com o tempo esperado para detectar desvio de relógio.

Bash APIC (alternativo)

<#root>

```
apic1#

bash

admin@apic1:~>

date

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

Verificação do switch (folha/lombada)

show ntp peers

Verifique se o provedor de NTP foi enviado para o switch.

<#root>

```
leaf1#

show ntp peers

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

O que parece bom: O IP ou o nome de host do servidor NTP é exibido com `Serv/Peer` = `Server` e o VRF correto (normalmente `management` para OOB).

Qual é a aparência ruim: Nenhum par listado ou o IP do servidor NTP não corresponde ao provedor configurado. Isso geralmente indica que a política de Data e Hora não foi aplicada por meio da cadeia Grupo de Políticas do Pod/Perfil do Pod.

show ntp peer-status

Verifique se o servidor NTP está selecionado para sincronização.

<#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
```

O caractere `*` é essencial — ele confirma que o servidor NTP está sendo usado para sincronização.

Qual é a aparência ruim:

- Não `*` ao lado do servidor — o switch não está sincronizando com o servidor.
- `reach` é `0` — nenhuma resposta de NTP foi recebida. Isso indica um problema de acessibilidade.
- `st` is `16` — o servidor NTP não está sincronizado e não pode fornecer uma hora válida.

show ntp statistics peer ipaddr

Verifique a troca de pacotes NTP para confirmar a acessibilidade. Substitua o endereço IP pelo endereço do provedor NTP do switch afetado.

<#root>

```
leaf1#

show ntp statistics peer ipaddr 10.1.1.100

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

O que parece bom: `os pacotes enviados` e os `pacotes recebidos` são aproximadamente iguais e estão aumentando.

Qual é a aparência ruim: `os pacotes enviados` estão aumentando, mas os `pacotes recebidos` são `0` ou estão quase aumentando - as respostas de NTP não estão chegando ao switch.

show clock

<#root>

leaf1#

show clock

11:24:24.121066 EDT Tue Apr 07 2026

Verificação de GUI

Navegue até Fabric > Fabric Policies > Policies > Pod > Date and Time > [Your Policy] > [NTP Provider].

A coluna Sync Status deve mostrar Synced to Remote NTP Server para todos os nós. Pode levar vários minutos para que o status de sincronização convirja após a implantação inicial.

Verificação de API

Consulte a classe `datetimeNtpq` para verificar a sincronização de NTP em todos os APICs:

<#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.
```

Troubleshooting de Fluxo de Trabalho

Use esta árvore decisória quando um problema de NTP for relatado em qualquer nó da ACI.

Passo 1: Os pares NTP estão configurados no switch?

Faça login no switch afetado e execute:

<#root>

leaf1#

show ntp peers

- Nenhum par listado → a política de Data e Hora não foi aplicada a este nó. Vá para o cenário 1: Provedor de NTP não enviado para o Switch.
- Os correspondentes listados → continuar na Etapa 2.

Passo 2: O servidor NTP está selecionado para sincronização?

<#root>

leaf1#

show ntp peer-status

- `*` presente → NTP está sincronizando. Se o tempo ainda parecer incorreto, vá para o Cenário 5: Deslocamento Grande / Desvio De Relógio.
- No `*` present → continuar na Etapa 3.

Passo 3: O valor de alcance é zero?

Verifique a coluna `reach` em `show ntp peer-status`.

- **`reach` = `0`** → nenhuma resposta do servidor NTP. Vá para o cenário 2: Servidor NTP inacessível.
- **`reach` > `0`** mas nenhuma resposta **`* → está chegando, mas a sincronização não está estabelecida.`** Verifique o stratum — vá para a Etapa 4.

Passo 4: O valor do stratum é 16?

- Stratum = 16 → o servidor NTP não está sincronizado com sua própria origem de upstream. Vá para o cenário 3: Servidor NTP não sincronizado (Stratum 16).
- Estrato 1-15, mas sem sincronização → ir para Cenário 4: Incompatibilidade de autenticação de NTP.

Cenários comuns de solução de problemas

Cenário 1: Provedor de NTP não enviado para switch

Sintoma: `show ntp peers` no switch não retorna nenhuma entrada.

Verificação de configuração:

1. Verifique se a política de Data e Hora tem pelo menos um provedor de NTP configurado.
2. Verifique se o Grupo de Políticas do Pod faz referência à política correta de Data e Hora.
3. Verifique se o Perfil do Pod faz referência ao Grupo de Políticas do Pod correto.
4. Verifique se o nó tem um endereço IP de gerenciamento atribuído sob o locatário mgmt.

Causa raiz: Um dos quatro links na cadeia de políticas (política de data e hora → provedor de NTP → grupo de políticas de Pod → perfil de Pod) está quebrado. A causa mais comum é o Grupo de Políticas do Pod não estar associado ao Perfil do Pod, ou a política de Data e Hora não estar sendo selecionada no Grupo de Políticas do Pod.

Solução: Conclua o link ausente na cadeia de políticas. Verifique se o Perfil do Pod do pod afetado faz referência a um Grupo de Políticas do Pod que contenha a política de Data e Hora correta. Uma vez aplicada, a configuração do provedor de NTP será enviada aos switches dentro de alguns minutos.

Cenário 2: Servidor NTP inalcançável

Sintoma: `show ntp peer-status` mostra `reach = 0`. `show ntp statistics peer ipaddr 10.1.1.100` mostra `pacotes recebidos = 0`.

Verificação de configuração: Verifique se o provedor de NTP está associado ao EPG de gerenciamento correto (OOB ou in-band). Se estiver usando OOB, verifique se os contratos OOB permitem a porta UDP 123.

Verificação operacional:

1. Faça ping no servidor NTP do switch afetado usando o VRF de gerenciamento:
   <#root>

   ```
   leaf1#

   ping 10.1.1.100 vrf management
   ```

2. Execute um tcpdump no switch para verificar se os pacotes NTP estão saindo e chegando:
   <#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
   ```

Causa raiz: Normalmente, uma das seguintes opções:

- O switch não tem um endereço IP de gerenciamento atribuído.
- O gateway padrão para o VRF de gerenciamento está ausente ou incorreto.
- Um firewall está bloqueando a porta UDP 123 entre o switch e o servidor NTP.
- O contrato OOB não permite a porta UDP 123.
- O provedor de NTP faz referência ao EPG de gerenciamento incorreto (por exemplo, OOB selecionado, mas apenas in-band tem acessibilidade).

Solução: Resolva o problema de acessibilidade. Atribua um endereço de gerenciamento, se estiver faltando, corrija o gateway padrão, atualize as regras de firewall ou corrija a seleção de EPG de gerenciamento no provedor de NTP.

Cenário 3: Servidor NTP não sincronizado (Stratum 16)

Sintoma: `show ntp peer-status` mostra stratum (`st`) = `16`. O switch não será sincronizado com um servidor stratum 16.

Verificação operacional: Efetue login no servidor NTP ou consulte-o a partir de um host externo para verificar se ele está sincronizado com sua própria origem de tempo upstream.

Causa raiz: O próprio servidor NTP perdeu a sincronização com seu relógio de referência de upstream. Um servidor com estrato 16 está anunciando que não tem uma fonte de tempo confiável.

Solução: Corrija o servidor NTP. Isso está fora da estrutura da ACI — verifique a configuração do servidor NTP e sua origem de tempo de upstream. Se o servidor NTP não puder ser corrigido imediatamente, configure um provedor NTP alternativo na política de Data e Hora.

Cenário 4 : Incompatibilidade de autenticação de NTP

Sintoma: `show ntp peer-status` mostra `reach` > `0` e stratum é válido, mas nenhum `*` é exibido. O servidor NTP responde, mas o switch não aceita a resposta.

Verificação de configuração:

1. Verifique se o servidor NTP requer autenticação.
2. Se a autenticação for necessária, verifique se a política de Data e Hora tem Estado de Autenticação definido como Habilitado.
3. Verifique se o ID da chave de autenticação, o valor da chave e o algoritmo (MD5, SHA-1 ou AES128-CMAC) correspondem entre a estrutura da ACI e o servidor NTP.
4. Verifique se a chave está marcada como Confiável na tabela Chaves de autenticação do cliente NTP.

Causa raiz: A chave de autenticação, o algoritmo ou a ID da chave não correspondem entre a ACI e o servidor NTP, fazendo com que o switch rejeite a resposta de NTP como não autenticada.

Solução: Alinhe a configuração de autenticação. Certifique-se de que o mesmo ID de chave, valor de chave e algoritmo estejam configurados na ACI e no servidor NTP. AES128-CMAC é recomendado para o APIC versão 6.1(1) e posterior.

Note: Quando o modo FIPS está habilitado, somente esquemas de autenticação AES128-CMAC e SHA-1 são suportados. MD5 não funcionará no modo FIPS.

Cenário 5 : Deslocamento Grande / Desvio Do Relógio

Sintoma: O switch parece estar sincronizado (* presente, alcance = 377), mas o valor do deslocamento em show ntp peer-status ou show ntpq é muito grande (centenas ou milhares de milissegundos), ou o relógio está visivelmente errado.

Verificação operacional:

<#root>

```
apic1#
```

```
show ntpq
```

Verifique a coluna `offset`. Um deslocamento íntegro geralmente está abaixo de 100 ms.

Causa raiz: O relógio variou significativamente antes do estabelecimento da sincronização NTP ou do reinício do relógio de hardware (RTC) durante uma reinicialização (por exemplo, devido a uma bateria inoperante do CMOS). O NTP corrige o relógio gradualmente através da rotação, o que pode levar tempo para grandes deslocamentos.

Solução: Se o deslocamento for muito grande e o NTP estiver sincronizando ativamente, aguarde o relógio convergir. O NTP gira o relógio gradualmente — grandes deslocamentos podem levar horas para serem totalmente corrigidos. Se o deslocamento não diminuir, verifique se o servidor NTP está fornecendo o tempo exato. Se o problema ocorrer novamente após cada reinicialização, investigue o relógio de hardware (bateria RTC/CMOS) no nó afetado.

Cenário 6 : Falhas de APIC em standby com NTP em banda

Sintoma: As falhas são geradas em um APIC em espera relacionado ao NTP ou à política de monitoramento quando o NTP é configurado para gerenciamento em banda.

Causa raiz: Quando uma política de NTP é aplicada ao gerenciamento em banda, o APIC em standby também exige a configuração em banda. Sem ele, as falhas são levantadas.

Solução: Configure também o gerenciamento em banda para o APIC em standby. Isso apaga as falhas.

Cenário 7 : Falha de IP duplicado

Sintoma: Uma falha de IP duplicado é gerada após a adição de provedores NTP.

Causa raiz: Um FQDN foi adicionado como um provedor NTP e, em seguida, o endereço IP resolvido desse FQDN foi adicionado como um segundo provedor NTP. A ACI detecta a duplicação.

Solução: Exclua o provedor duplicado adicionado mais recentemente (a entrada de endereço IP se o FQDN tiver sido adicionado primeiro ou vice-versa). Use apenas uma entrada por servidor NTP — FQDN ou endereço IP, não ambos.

Cenário 8 : Falha de Resolução DNS para Provedor NTP Baseado em FQDN

Sintoma: O provedor NTP configurado com um nome de host não está resolvendo. `show ntp peers` não mostra o endereço IP esperado ou o NTP não está sincronizando.

Verificação de configuração:

1. Verifique se uma política de serviço DNS está configurada em Fabric > Fabric Policies > Policies > Global > DNS Profiles.
2. Verifique se o provedor DNS (servidor DNS) pode ser acessado do VRF de gerenciamento.
3. Verifique se o rótulo DNS apropriado está configurado para a instância VRF dentro ou fora da banda do EPG de gerenciamento.

Causa raiz: O servidor DNS não pode ser acessado ou não está configurado, fazendo com que a resolução do nome de host falhe para o provedor NTP.

Solução: Configure a política de serviço DNS, assegure a acessibilidade do DNS e aplique o rótulo DNS correto. Como alternativa, use o endereço IP do servidor NTP em vez do nome do host.

Falhas e eventos relacionados

A seguir estão condições relacionadas ao NTP que podem gerar falhas na ACI:

- Falha de IP duplicado — gerado quando um FQDN e o endereço IP do mesmo servidor NTP são adicionados como provedores. Resolução: remova a entrada duplicada.
- Falhas de NTP em banda do APIC em standby — acionadas quando uma política de monitoramento ou NTP é aplicada para o APIC em banda, mas o APIC em standby não possui configuração em banda.
- Sync Status not converging — a GUI mostra "Not Synced" (Não sincronizado) ou um status diferente de "Synced to Remote NTP Server" (Sincronizado com servidor NTP remoto) para um ou mais nós. Este não é um código de falha, mas um indicador de status operacional. Siga o fluxo de trabalho de solução de problemas acima para diagnosticar.

Critérios de escalonamento

Considere escalar para o Cisco TAC se:

- A cadeia de configuração é verificada corretamente e o servidor NTP está acessível (ping funciona, tcpdump mostra respostas NTP), mas o switch ainda não sincroniza.
- A sincronização NTP é perdida repetidamente sem alterações de configuração ou problemas de servidor NTP.
- A saída de `show ntp peer-status` mostra um comportamento inesperado, como o stratum persistente 16 em um servidor que está confirmado como sincronizado externamente.
- O relógio oscila significativamente entre as reinicializações, o que pode indicar um problema de relógio de hardware (RTC).

Ao contratar o TAC, forneça os seguintes dados:

- Saída de `show ntpq` de todos os APICs.
- Saída de `show ntp peers`, `show ntp peer-status`, `show ntp statistics peer ipaddr <IP>` e `show clock` de todos os switches afetados.
- Saída de `moquery -c datetimePol`, `moquery -c datetimeNtpProv` e `moquery -c datetimeNtpq` do APIC.
- Um suporte técnico dos nós afetados.

Referências

- Guia de configuração básica do Cisco APIC, versão 6.1(x) — Provisionamento do Core ACI Fabric Services
- Solução de problemas de gerenciamento da ACI e Core Services — Políticas de Pod
- Guia de design da Cisco Application Centric Infrastructure (ACI)

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.