Resolución de problemas de NTP en un fabric de Cisco ACI

Introducción

Este documento describe cómo verificar, resolver y resolver problemas de protocolo de tiempo de red (NTP) en un fabric de Cisco ACI. Abarca el modelo de políticas de NTP, la verificación de la configuración, los comandos de verificación operativa, un flujo de trabajo de clasificación para los síntomas comunes de NTP y los escenarios detallados de solución de problemas.

Antecedentes

El material de este documento se extrajo de la guía Troubleshooting ACI Management and Core Services — Pod Policies, la Guía de Configuración Básica de Cisco APIC, Release 6.1(x) — Provisioning Core ACI Fabric Services y la Guía de Diseño de Cisco ACI.

Overview

La sincronización horaria es una capacidad crucial en un fabric de ACI de la que dependen las tareas de supervisión, operativas y de resolución de problemas. La sincronización del reloj garantiza un análisis adecuado de los flujos de tráfico, la correlación de las marcas de tiempo de los errores y los errores en varios nodos de fabric y el uso completo de la capacidad del contador atómico, de la que dependen las puntuaciones del estado de las aplicaciones. Una configuración de NTP inexistente o inadecuada no provoca necesariamente un fallo o una puntuación de estado baja, por lo que es importante configurar la sincronización de tiempo en una fase temprana de la implementación del fabric.

Modelo de política NTP en ACI

NTP en ACI se gestiona a través de una cadena de cuatro objetos de políticas:

1. Política de fecha y hora (`datetimePol`): define la configuración de NTP, incluidos el estado administrativo, el estado de autenticación, el estado del servidor y el modo maestro. Se encuentra en Fabric > Fabric Policies > Policies > Pod > Date and Time.
2. Proveedor NTP (`datetimeNtpProv`): define entradas de servidor NTP individuales

(proveedores) dentro de una política de fecha y hora, incluida la IP/FQDN del servidor, selección de EPG de administración (fuera de banda o en banda), indicador preferido e intervalos de sondeo.
3. Grupo de políticas de POD (`fabricPodPGrp`): hace referencia a la política de fecha y hora junto con otras políticas de nivel de POD (BGP RR, SNMP, etc.). Se encuentra en Fabric > Fabric Policies > Pods > Policy Groups.
4. Perfil de grupo de dispositivos (`fabricPodP`): asocia un grupo de políticas de grupo de dispositivos con un selector de grupo de dispositivos. Se encuentra en Fabric > Fabric Policies > Pods > Profiles.

Los cuatro eslabones de esta cadena deben configurarse para que NTP se aplique a los nodos de fabric. Si se rompe cualquier link, la configuración del proveedor NTP no se enviará a los switches.

Prerequisites

- Debe completarse la detección de fabric.
- Las direcciones de administración de nodos (OOB o en banda) deben asignarse a todos los APIC y switches bajo el arrendatario mgmt.
- Para NTP fuera de banda, el EPG de administración OOB debe permitir el puerto UDP 123.
- Para el NTP en banda, se debe configurar un EPG de administración en banda con los contratos adecuados y disponibilidad al servidor NTP. Las direcciones IP en banda no son accesibles desde fuera del fabric sin políticas adicionales.

Autenticación NTP

ACI admite tres esquemas de autenticación NTP: MD5, SHA-1 y AES128-CMAC. AES128-CMAC se introdujo en la versión 6.1(1) de APIC y es el esquema recomendado, ya que MD5 se considera débil e inseguro. Cuando el modo FIPS está activado, solo se admiten AES128-CMAC y SHA-1.

Funcionalidad del servidor NTP

Los switches de hoja de ACI pueden actuar como servidores NTP para los clientes de flujo descendente (por ejemplo, servidores conectados al fabric). Esta característica está deshabilitada de forma predeterminada y debe habilitarse explícitamente mediante la opción Estado del servidor en la directiva Fecha y hora. Cuando está habilitada, los clientes pueden utilizar el switch de hoja en banda, fuera de banda, el dominio de puente SVI o la dirección IP L3Out como la dirección del servidor NTP.

Nota: Los switches de fabric no deben sincronizarse con otros switches del mismo fabric. Los switches de fabric siempre deben sincronizarse con los servidores NTP externos.

Verifique la configuración

Antes de solucionar problemas del estado operativo de NTP, verifique que la cadena de configuración esté completa. La configuración incorrecta es la causa principal más común de los problemas de NTP en ACI.

Paso 1: Verificar direcciones de administración de nodos

Navegue hasta Arrendatarios > Administración > Direcciones de administración de nodos (para asignación estática) o EPG de administración de nodos (para grupos de conectividad).

Confirme que cada APIC y nodo de switch tenga asignada una dirección IP de administración. Los nodos sin direcciones de administración no pueden comunicarse con el servidor NTP.

Como alternativa, consulte la API:

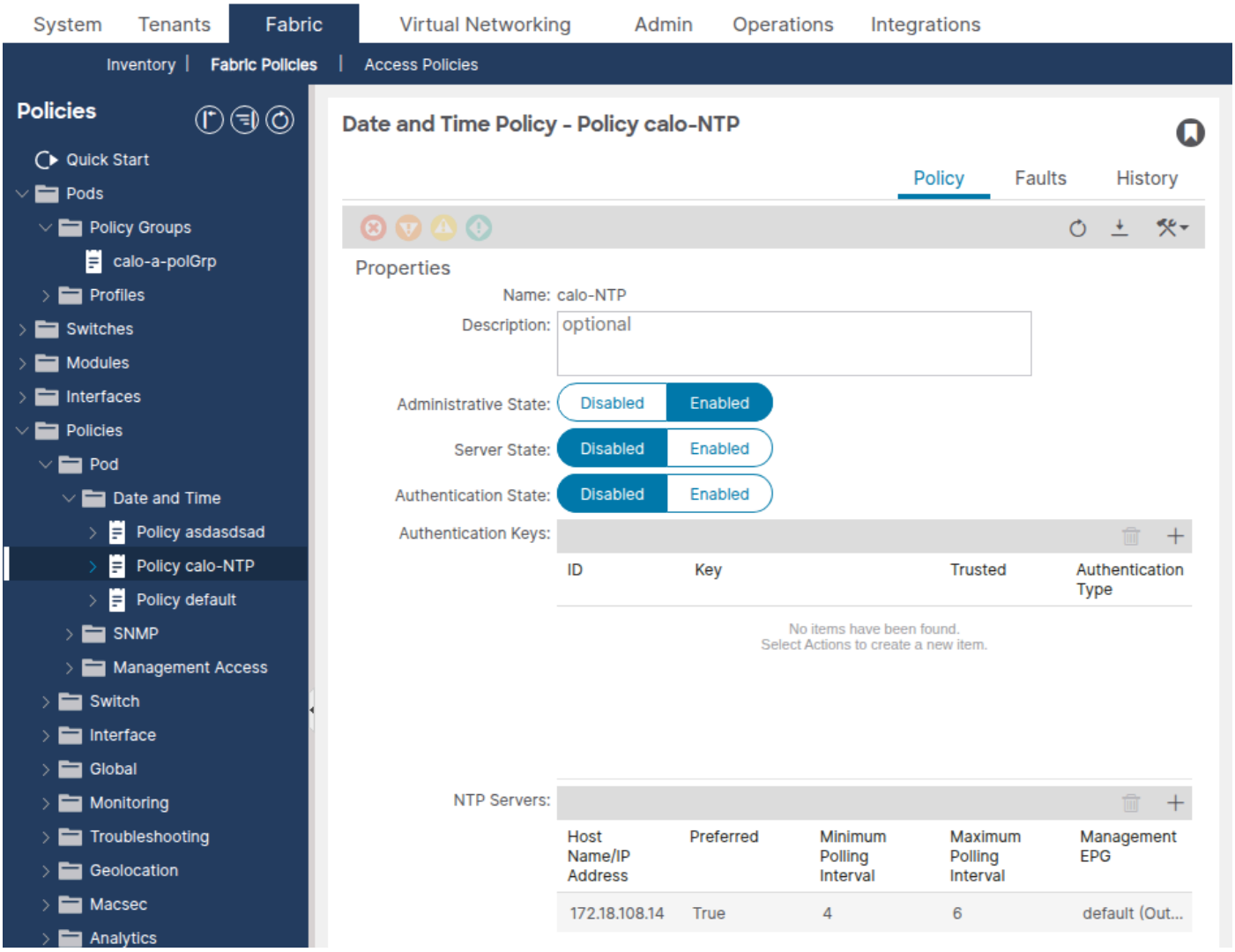
<#root>

apic1#

moquery -c mgmtRsOoBStNode

Paso 2: Verifique que la política de fecha y hora tenga un proveedor NTP

Vaya a Fabric > Fabric Policies > Policies > Pod > Date and Time > [Your Policy].



Confirme que al menos un proveedor NTP (servidor) esté configurado. Si existen varios proveedores, marque al menos uno como Preferido.

Verifique el proveedor NTP a través de la API:

<#root>

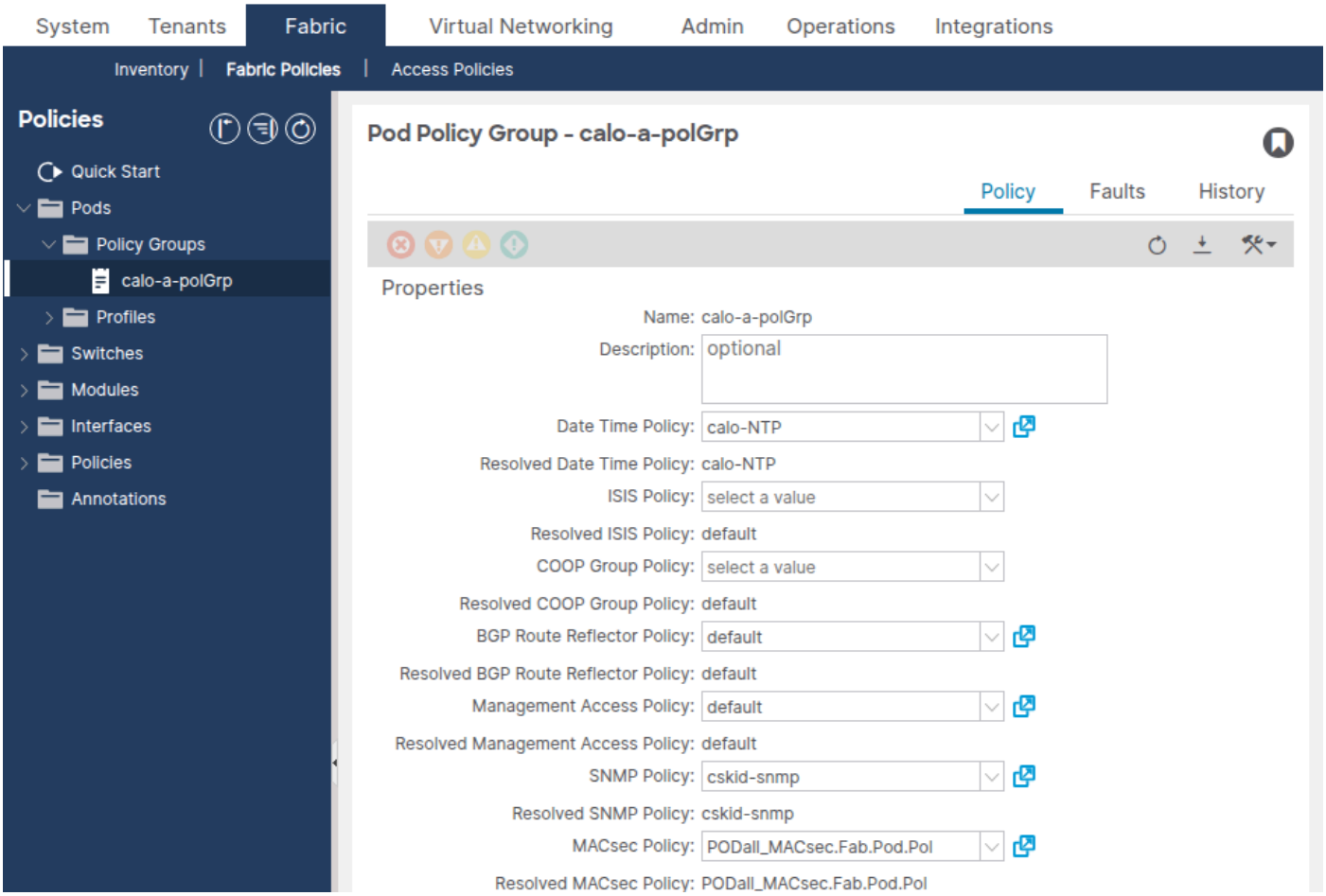
```
apic1#

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
```

Problemas comunes de configuración incorrecta

- No se ha configurado ningún proveedor NTP: la directiva de fecha y hora existe, pero no tiene ningún proveedor. Se aplicará la política, pero los nodos no tendrán ningún servidor NTP con el que sincronizar.
- Se ha seleccionado un EPG de administración incorrecto: el proveedor NTP hace referencia al EPG fuera de banda, pero el servidor NTP sólo es accesible a través de dentro de banda (o viceversa). Verifique qué EPG de administración proporciona accesibilidad al servidor NTP.
- FQDN e IP del mismo servidor agregado como proveedores separados: esto genera un error IP duplicado. Elimine la entrada duplicada.
- Proveedor basado en FQDN sin política DNS: si utiliza un nombre de host para el proveedor NTP, asegúrese de que se haya configurado una política de servicio DNS y de que se haya aplicado la etiqueta DNS adecuada al VRF de administración.

Paso 3: Verifique que el grupo de políticas de grupo de dispositivos haga referencia a la política de fecha y hora

Vaya a Fabric > Fabric Policies > Pods > Policy Groups > [Your Pod Policy Group].



Confirme que el campo Política de fecha y hora haga referencia a la política de fecha y hora correcta.

<#root>

`apic1#`

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

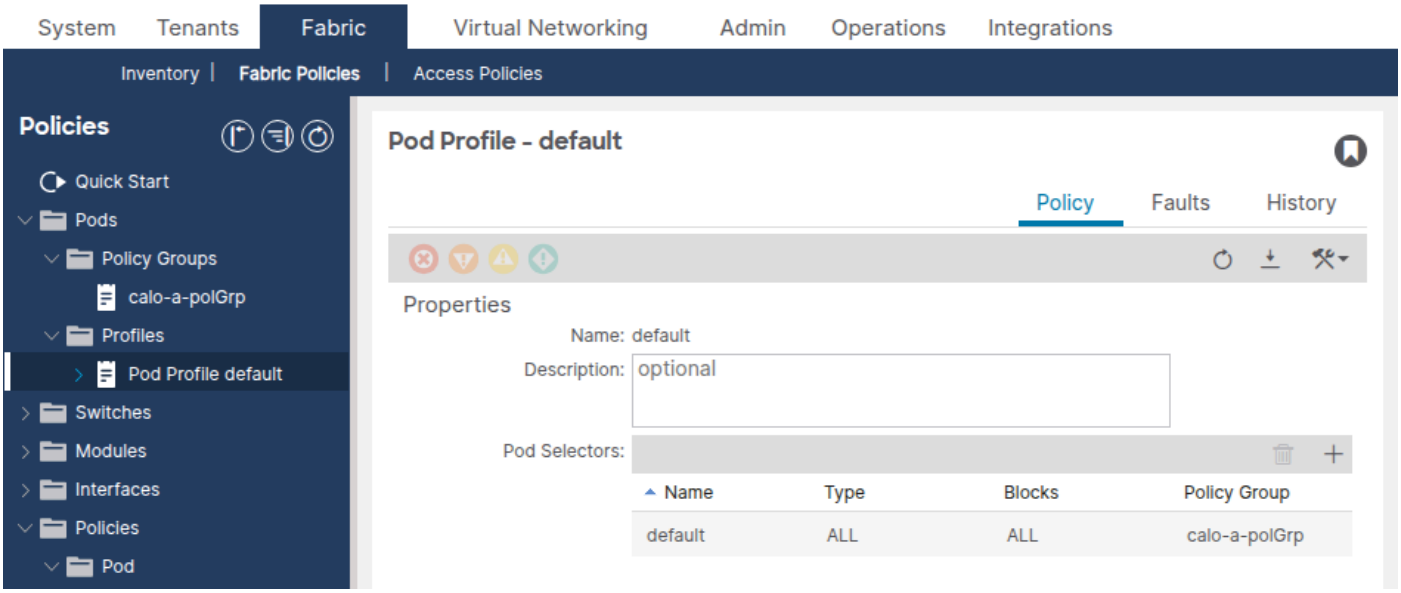
Busque el atributo `datetimePolName` o la relación `fabricRsTimePol` asociada.

Problemas comunes de configuración incorrecta

- El grupo de políticas de grupo de políticas de grupo hace referencia a una política de fecha y hora incorrecta: si existen varias políticas de fecha y hora (por ejemplo, "predeterminadas" y una personalizada), verifique que el grupo de políticas de grupo de políticas de grupo hace referencia a la política deseada.
- El grupo de políticas de grupo de dispositivos no se ha creado en absoluto: es posible que el grupo de políticas de grupo de dispositivos predeterminado no tenga asociada la política de fecha y hora. Verifique siempre.

Paso 4: Verificar que el Perfil Pod Hace Referencia al Grupo de Políticas Pod

Vaya a Fabric > Fabric Policies > Pods > Profiles > [Your Pod Profile].



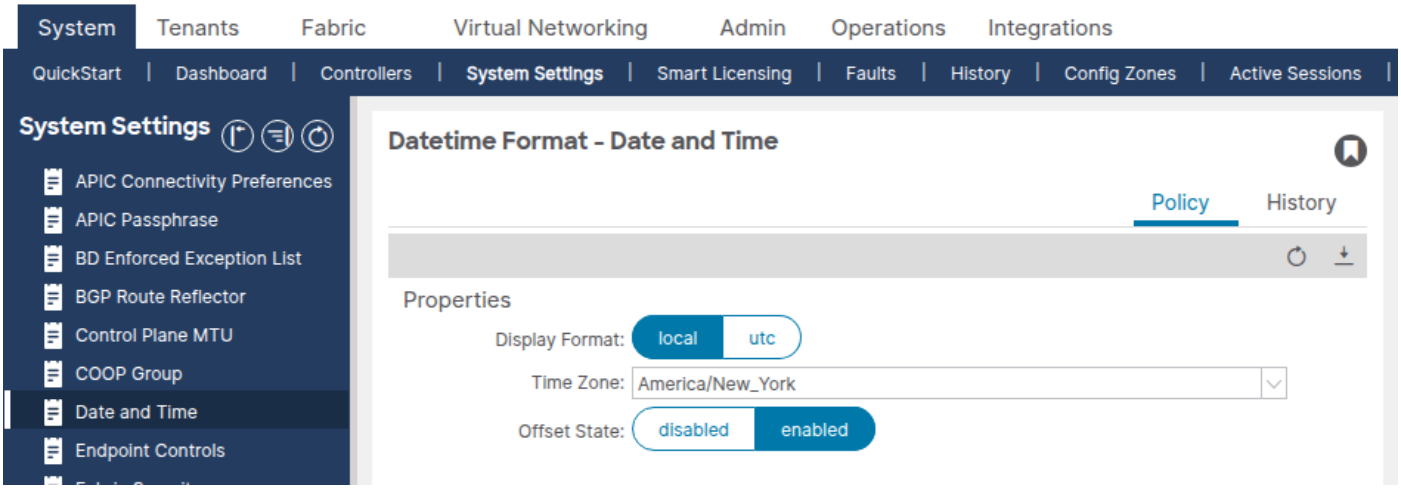
Confirme que el campo Fabric Policy Group haga referencia al grupo de políticas de grupo de dispositivos correcto.

Problemas comunes de configuración incorrecta

- El perfil de grupo de dispositivos hace referencia al grupo de políticas de grupo incorrecto; especialmente en entornos de varios grupos de dispositivos, cada perfil de grupo de dispositivos debe hacer referencia al grupo de políticas de grupo de dispositivos correcto.

Paso 5: Verificar formato de fecha y hora

Vaya a Sistema > Configuración del sistema > Fecha y hora.



Confirme que el formato de visualización (local o UTC) y la zona horaria están establecidos como se esperaba. Esta configuración es una directiva de formato de fecha y hora predeterminada independiente que no se puede eliminar ni duplicar.

Verificación operativa

Después de confirmar que la cadena de configuración es correcta, utilice los siguientes comandos para verificar que NTP funciona en tiempo de ejecución.

Verificación de APIC

show ntpq

Este comando muestra el estado de sincronización de NTP en todos los APIC. El símbolo `*` indica que el servidor está seleccionado para la sincronización.

<#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
```

Qué buena apariencia tiene:

- Todos los APIC muestran `*` (seleccionado para la sincronización) junto al servidor remoto.
- `alcance` es `377` (octal), lo que indica que las últimas 8 encuestas se realizaron correctamente.
- `st` (estrato) está entre 1 y 15. El estrato 16 significa que el servidor no está sincronizado.
- `el desplazamiento` es bajo (normalmente menos de 100 ms para un entorno saludable).

Qué mal se ve:

- No `*` junto a ningún servidor: no se ha seleccionado ningún servidor para la sincronización.
- `reach` es `0`: no se han recibido respuestas de NTP.
- `st` es `16`: el servidor NTP no está sincronizado con su fuente de tiempo ascendente.
- `El desplazamiento` es extremadamente grande (miles de milisegundos): el reloj está significativamente a la deriva.

show clock

<#root>

```
apic1#

show clock

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

Confirme que la hora es correcta. Compare con el tiempo esperado para detectar la desviación del reloj.

APIC Bash (alternativa)

<#root>

```
apic1#
```

bash

```
admin@apic1:~>
```

date

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

Verificación de switch (hoja/columna)

show ntp peers

Verifique que el proveedor NTP se haya enviado al switch.

<#root>

```
leaf1#
```

show ntp peers

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

Qué buena apariencia tiene: El IP o nombre de host del servidor NTP aparece con `Serv/Peer` = `Server` y el VRF correcto (normalmente `administración` para OOB).

Qué mal se ve: No se muestran pares o la IP del servidor NTP no coincide con el proveedor configurado. Esto suele indicar que la política de fecha y hora no se aplicó a través de la cadena Grupo de políticas de grupo de dispositivos/Perfil de grupo de dispositivos.

show ntp peer-status

Compruebe que el servidor NTP está seleccionado para la sincronización.

<#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
```

El carácter `*` es esencial: confirma que el servidor NTP se está utilizando para la sincronización.

Qué mal se ve:

- No `*` junto al servidor: el switch no se está sincronizando con el servidor.
- `reach` es `0`: no se han recibido respuestas de NTP. Esto indica un problema de disponibilidad.
- `st` es `16`: el servidor NTP no está sincronizado y no puede proporcionar una hora válida.

show ntp statistics peer ipaddr

Verifique el intercambio de paquetes NTP para confirmar la disponibilidad. Reemplace la dirección IP por la dirección del proveedor NTP para el switch afectado.

<#root>

```
leaf1#

show ntp statistics peer ipaddr 10.1.1.100

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

Qué buena apariencia tiene: `los paquetes enviados` y los `paquetes recibidos` son aproximadamente iguales e incrementales.

Qué mal se ve: `los paquetes enviados` aumentan, pero los `paquetes recibidos` son `0` o apenas aumentan: las respuestas NTP no llegan al switch.

show clock

<#root>

```
leaf1#

show clock

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

Verificación de GUI

Vaya a Fabric > Fabric Policies > Policies > Pod > Date and Time > [Your Policy] > [NTP Provider].

La columna Estado de sincronización debe mostrar Sincronizado con servidor NTP remoto para todos los nodos. El estado de sincronización puede tardar varios minutos en converger tras la implementación inicial.

Verificación de API

Consulte la clase `datetimeNtpq` para verificar la sincronización NTP en todos los APIC:

<#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 Flujo

Utilice este árbol de decisiones cuando se informe de un problema NTP en cualquier nodo ACI.

Paso 1: ¿Están configurados los peers NTP en el switch?

Inicie sesión en el switch afectado y ejecute:

<#root>

leaf1#

show ntp peers

- No hay ningún par en la lista → la directiva de fecha y hora no se aplicó a este nodo. Vaya a la situación 1: Proveedor NTP no enviado al switch.
- Los pares enumerados → continúan con el paso 2.

Paso 2: ¿Está seleccionado el servidor NTP para la sincronización?

<#root>

leaf1#

show ntp peer-status

- `*` presente → NTP se está sincronizando. Si la hora sigue apareciendo mal, vaya a la situación 5: Desplazamiento grande / Desviación del reloj.
- No `*` present → continúe con el paso 3.

Paso 3: ¿Es cero el valor de alcance?

Verifique la columna `reach` en `show ntp peer-status`.

- reach = `0` → no hay respuestas del servidor NTP. Vaya a la situación 2: Servidor NTP inalcanzable.
- alcance **>** `0` pero no `*`→ llegan respuestas pero no se ha establecido la sincronización.

Compruebe el estrato: vaya al paso 4.

Paso 4: ¿El valor del estrato es 16?

- Estrato = 16 → el servidor NTP no está sincronizado con su propia fuente ascendente. Vaya a la situación 3: Servidor NTP no sincronizado (estrato 16).
- Estrato 1-15 pero sin sincronización → vaya a la situación 4: Discordancia de autenticación NTP.

Escenarios comunes de solución de problemas

Escenario 1: Proveedor NTP no enviado al switch

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

Comprobación de configuración:

1. Verifique que la política de fecha y hora tenga al menos un proveedor NTP configurado.
2. Compruebe que el grupo de políticas de grupo de dispositivos hace referencia a la política de fecha y hora correcta.
3. Verifique que el perfil de grupo de dispositivos haga referencia al grupo de políticas de grupo de dispositivos correcto.
4. Verifique que el nodo tenga una dirección IP de administración asignada bajo el arrendatario mgmt.

Causa raíz: Uno de los cuatro eslabones de la cadena de políticas (Política de fecha y hora → Proveedor NTP → Grupo de políticas Pod → Perfil Pod) está roto. La causa más común es que el grupo de políticas de grupo de dispositivos no está asociado con el perfil de grupo de dispositivos o que la política de fecha y hora no está seleccionada en el grupo de políticas de grupo de dispositivos.

Solución: Complete el eslabón que falta en la cadena de políticas. Asegúrese de que el perfil de grupo de dispositivos para el grupo de dispositivos afectado haga referencia a un grupo de políticas de grupo de dispositivos que contenga la política de fecha y hora correcta. Una vez aplicada, la configuración del proveedor NTP se enviará a los switches en unos minutos.

Escenario 2: Servidor NTP inalcanzable

Síntoma: `show ntp peer-status muestra reach = 0`. `show ntp statistics peer ipaddr 10.1.1.100 muestra paquetes recibidos = 0`.

Comprobación de configuración: Verifique que el proveedor NTP esté asociado con el EPG de administración correcto (OOB o en banda). Si utiliza OOB, verifique que los contratos de OOB permiten el puerto UDP 123.

Comprobación operativa:

1. Haga ping al servidor NTP desde el switch afectado usando el VRF de administración:
   <#root>

   ```
   leaf1#

   ping 10.1.1.100 vrf management
   ```

2. Ejecute un tcpdump en el switch para verificar si los paquetes NTP están saliendo y llegando:
   <#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 raíz: Por lo general, una de las siguientes opciones:

- El switch no tiene asignada una dirección IP de administración.
- Falta el gateway predeterminado para el VRF de administración o es incorrecto.
- Un firewall está bloqueando el puerto UDP 123 entre el switch y el servidor NTP.
- El contrato OOB no permite el puerto UDP 123.
- El proveedor NTP hace referencia al EPG de administración incorrecto (por ejemplo, OOB seleccionado pero solo en banda tiene disponibilidad).

Solución: Resuelva el problema de disponibilidad. Asigne una dirección de administración si falta, corrija el gateway predeterminado, actualice las reglas de firewall o corrija la selección de EPG de administración en el proveedor NTP.

Escenario 3: Servidor NTP no sincronizado (estrato 16)

Síntoma: `show ntp peer-status` muestra stratum (`st`) = `16`. El switch no se sincronizará con un servidor del estrato 16.

Comprobación operativa: Inicie sesión en el servidor NTP o realice una consulta desde un host externo para comprobar que está sincronizado con su propio origen de tiempo de flujo ascendente.

Causa raíz: El propio servidor NTP ha perdido la sincronización con su reloj de referencia ascendente. Un servidor con estrato 16 anuncia que no tiene una fuente de tiempo confiable.

Solución: Corrija el servidor NTP. Esto está fuera del fabric de ACI: verifique la configuración del servidor NTP y su fuente de tiempo de flujo ascendente. Si el servidor NTP no se puede corregir inmediatamente, configure un proveedor NTP alternativo en la directiva Fecha y hora.

Escenario 4: Discordancia de autenticación NTP

Síntoma: `show ntp peer-status` muestra `reach` **>** `0` y stratum is valid, pero no `*` se muestra. El servidor NTP responde pero el switch no acepta la respuesta.

Comprobación de configuración:

1. Verifique si el servidor NTP requiere autenticación.
2. Si se requiere autenticación, verifique que la política de Fecha y hora tenga el Estado de autenticación establecido en Habilitado.
3. Verifique que el ID de clave de autenticación, el valor de clave y el algoritmo (MD5, SHA-1 o AES128-CMAC) coincidan entre el fabric de ACI y el servidor NTP.
4. Verifique que la clave esté marcada como de confianza en la tabla Claves de autenticación de cliente NTP.

Causa raíz: La clave de autenticación, el algoritmo o el ID de clave no coinciden entre ACI y el servidor NTP, lo que hace que el switch rechace la respuesta NTP como no autenticada.

Solución: Alinee la configuración de autenticación. Asegúrese de que se configuran el mismo ID de clave, valor de clave y algoritmo en ACI y en el servidor NTP. Se recomienda AES128-CMAC para la versión APIC 6.1(1) y posteriores.

Nota: Cuando el modo FIPS está activado, solo se admiten los esquemas de autenticación AES128-CMAC y SHA-1. MD5 no funcionará en el modo FIPS.

Escenario 5: Desplazamiento grande / Desviación del reloj

Síntoma: El switch parece estar sincronizado (* presente, alcance = 377), pero el `valor de desplazamiento` en `show ntp peer-status` o show ntpq es muy grande (cientos o miles de milisegundos), o el reloj es visiblemente incorrecto.

Comprobación operativa:

<#root>

apic1#

show ntpq

Compruebe la columna `de desvío`. Un desplazamiento correcto suele ser inferior a 100 ms.

Causa raíz: El reloj varió significativamente antes de que se estableciera la sincronización NTP o el reloj de hardware (RTC) se restableció durante un reinicio (por ejemplo, debido a una batería CMOS inactiva). NTP corrige el reloj gradualmente a través de la rotación, que puede tomar tiempo para grandes desplazamientos.

Solución: Si el desplazamiento es muy grande y NTP se está sincronizando activamente, espere a que el reloj converja. El NTP hace girar el reloj gradualmente — los grandes desplazamientos pueden tardar horas en corregirse completamente. Si el desplazamiento no disminuye, verifique que el servidor NTP está proporcionando una hora precisa. Si el problema se repite después de cada reinicio, investigue el reloj de hardware (batería RTC/CMOS) en el nodo afectado.

Escenario 6: Errores de APIC en espera con NTP en banda

Síntoma: Los fallos se generan en un APIC en espera relacionado con NTP o con la política de supervisión cuando NTP se configura para la gestión en banda.

Causa raíz: Cuando se aplica una política NTP para la administración en banda, el APIC en espera también requiere configuración en banda. Sin él, se plantean las faltas.

Solución: Configure también la administración en banda para el APIC en espera. Esto aclara los fallos.

Escenario 7: Fallo de IP duplicado

Síntoma: Se genera un error de IP duplicado después de agregar proveedores NTP.

Causa raíz: Se agregó un FQDN como proveedor NTP y, a continuación, la dirección IP resuelta de ese FQDN se agregó como segundo proveedor NTP. ACI detecta el duplicado.

Solución: Elimine el proveedor de duplicados agregado más recientemente (la entrada de dirección IP si el FQDN se agregó primero, o viceversa). Utilice sólo una entrada por servidor NTP: FQDN o dirección IP, no ambos.

Escenario 8: Error de resolución de DNS para el proveedor NTP basado en FQDN

Síntoma: El proveedor NTP configurado con un nombre de host no se está resolviendo. `show ntp peers` no muestra la dirección IP esperada o NTP no se está sincronizando.

Comprobación de configuración:

1. Verifique que una política de servicio DNS esté configurada en Fabric > Fabric Policies > Policies > Global > DNS Profiles.
2. Verifique que el proveedor DNS (servidor DNS) sea accesible desde el VRF de administración.
3. Verifique que la etiqueta DNS apropiada esté configurada para la instancia VRF dentro o fuera de banda del EPG de administración.

Causa raíz: No se puede alcanzar el servidor DNS o no está configurado, lo que provoca un error en la resolución del nombre de host para el proveedor NTP.

Solución: Configure la directiva de servicio DNS, garantice la disponibilidad de DNS y aplique la etiqueta DNS correcta. También puede utilizar la dirección IP del servidor NTP en lugar del nombre de host.

Eventos y fallos relacionados

A continuación se indican las condiciones relacionadas con NTP que pueden generar errores en ACI:

- Error IP duplicado: se produce cuando se agregan como proveedores un FQDN y la

dirección IP del mismo servidor NTP. Resolución: elimine la entrada duplicada.
- Errores NTP en banda de APIC en espera: se producen cuando se aplica una política de supervisión o NTP para APIC en banda pero el APIC en espera carece de configuración en banda.
- El estado de sincronización no converge: la GUI muestra "Not Synced" (No sincronizado) o un estado distinto de "Synced to Remote NTP Server" (Sincronizado con servidor NTP remoto) para uno o más nodos. No se trata de un código de fallo, sino de un indicador de estado operativo. Siga el flujo de trabajo de solución de problemas anterior para realizar el diagnóstico.

Criterios de escalado

Considere la posibilidad de derivar al TAC de Cisco si:

- La cadena de configuración se verifica correctamente y el servidor NTP es accesible (ping funciona, tcpdump muestra respuestas NTP), pero el switch aún no se sincroniza.
- La sincronización NTP se pierde repetidamente sin cambios de configuración o problemas del servidor NTP.
- El resultado de `show ntp peer-status` muestra un comportamiento inesperado como el estrato persistente 16 en un servidor que se confirma sincronizado externamente.
- El reloj varía significativamente entre los reinicios, lo que puede indicar un problema de reloj de hardware (RTC).

Al contratar al TAC, proporcione los siguientes datos:

- Salida de `show ntpq` de todos los APIC.
- Salida de `show ntp peers`, `show ntp peer-status`, `show ntp statistics peer ipaddr <IP>` y `show clock` de todos los switches afectados.
- Salida de `moquery -c datetimePol`, `moquery -c datetimeNtpProv` y `moquery -c datetimeNtpq` desde el APIC.
- Soporte técnico de los nodos afectados.

Referencias

- Guía de configuración básica de Cisco APIC, versión 6.1(x): aprovisionamiento de servicios de fabric de Core ACI
- Solución de problemas de administración de ACI y servicios principales: políticas de POD
- Guía de diseño de Cisco Application Centric Infrastructure (ACI)

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).