Dépannage du protocole NTP dans un fabric Cisco ACI

Introduction

Ce document décrit comment vérifier, dépanner et résoudre les problèmes NTP (Network Time Protocol) dans un fabric Cisco ACI. Il couvre le modèle de stratégie NTP, la vérification de la configuration, les commandes de vérification opérationnelle, un workflow de triage pour les symptômes NTP courants et des scénarios de dépannage détaillés.

Informations générales

Le contenu de ce document a été extrait du guide Troubleshoot ACI Management and Core Services — Pod Policies, du guide Cisco APIC Basic Configuration Guide, du chapitre Release 6.1(x) — Provisioning Core ACI Fabric Services et du guide de conception Cisco ACI.

Aperçu

La synchronisation temporelle est une fonctionnalité essentielle d'un fabric ACI dont dépendent les tâches de surveillance, d'exploitation et de dépannage. La synchronisation d'horloge garantit une analyse correcte des flux de trafic, la corrélation des horodatages de débogage et de panne sur plusieurs noeuds de fabric et l'utilisation complète de la fonctionnalité de compteur atomique dont dépendent les scores d'intégrité des applications. Une configuration NTP inexistante ou incorrecte ne déclenche pas nécessairement une panne ou un faible score d'intégrité. Il est donc important de configurer la synchronisation de l'heure au début du déploiement du fabric.

Modèle de politique NTP dans l'ACI

Le protocole NTP de l'ACI est géré via une chaîne de quatre objets de stratégie :

1. Date and Time Policy (`datetimePol`) : définit la configuration NTP, notamment l'état administratif, l'état d'authentification, l'état du serveur et le mode maître. Situé sous Fabric > Fabric Policies > Policies > Pod > Date and Time.
2. NTP Provider (`datetimeNtpProv`) : définit les entrées de serveur NTP individuelles (fournisseurs) dans une politique de date et d'heure, y compris l'IP/FQDN du serveur, la

sélection d'EPG de gestion (hors bande ou en bande), l'indicateur préféré et les intervalles d'interrogation.
3. Pod Policy Group (`fabricPodPGrp`) — référence la politique Date et heure avec d'autres politiques au niveau pod (BGP RR, SNMP, etc.). Situé sous Fabric > Fabric Policies > Pods > Policy Groups.
4. Pod Profile (`fabricPodP`) : associe un groupe de politiques de pod à un sélecteur de pod. Situé sous Fabric > Fabric Policies > Pods > Profiles.

Les quatre liaisons de cette chaîne doivent être configurées pour que le protocole NTP soit appliqué aux noeuds du fabric. Si une liaison est rompue, la configuration du fournisseur NTP ne sera pas envoyée aux commutateurs.

Conditions préalables

- La découverte du fabric doit être terminée.
- Les adresses de gestion de noeud (OOB ou intrabande) doivent être attribuées à tous les APIC et commutateurs sous le locataire de gestion.
- Pour le NTP hors bande, l'EPG de gestion OOB doit autoriser le port UDP 123.
- Pour le protocole NTP intrabande, un EPG de gestion intrabande avec les contrats appropriés et l'accessibilité au serveur NTP doit être configuré. Les adresses IP intrabande ne sont pas accessibles depuis l'extérieur du fabric sans stratégie supplémentaire.

Authentification NTP

L'ACI prend en charge trois schémas d'authentification NTP : MD5, SHA-1 et AES128-CMAC. AES128-CMAC a été introduit dans APIC version 6.1(1) et est le schéma recommandé, car MD5 est considéré comme faible et non sécurisé. Lorsque le mode FIPS est activé, seuls AES128-CMAC et SHA-1 sont pris en charge.

Fonctionnalité du serveur NTP

Les commutateurs Leaf ACI peuvent servir de serveurs NTP pour les clients en aval (par exemple, les serveurs connectés au fabric). Cette fonctionnalité est désactivée par défaut et doit être explicitement activée via l'option État du serveur dans la stratégie Date et heure. Lorsque cette option est activée, les clients peuvent utiliser l'adresse IP intrabande, hors bande, de domaine de pont SVI ou L3Out du commutateur Leaf comme adresse de serveur NTP.

Remarque : Les commutateurs du fabric ne doivent pas être synchronisés avec d'autres commutateurs du même fabric. Les commutateurs de fabric doivent toujours être synchronisés avec les serveurs NTP externes.

Vérifier la configuration

Avant de dépanner l'état opérationnel NTP, vérifiez que la chaîne de configuration est terminée. La mauvaise configuration est la cause principale des problèmes NTP dans l'ACI.

Étape 1: Vérifier les adresses de gestion des noeuds

Accédez à Tenants > mgmt > Node Management Addresses (pour l'affectation statique) ou Node Management EPGs (pour les groupes de connectivité).

Vérifiez qu'une adresse IP de gestion est attribuée à chaque APIC et noeud de commutateur. Les noeuds sans adresse de gestion ne peuvent pas communiquer avec le serveur NTP.

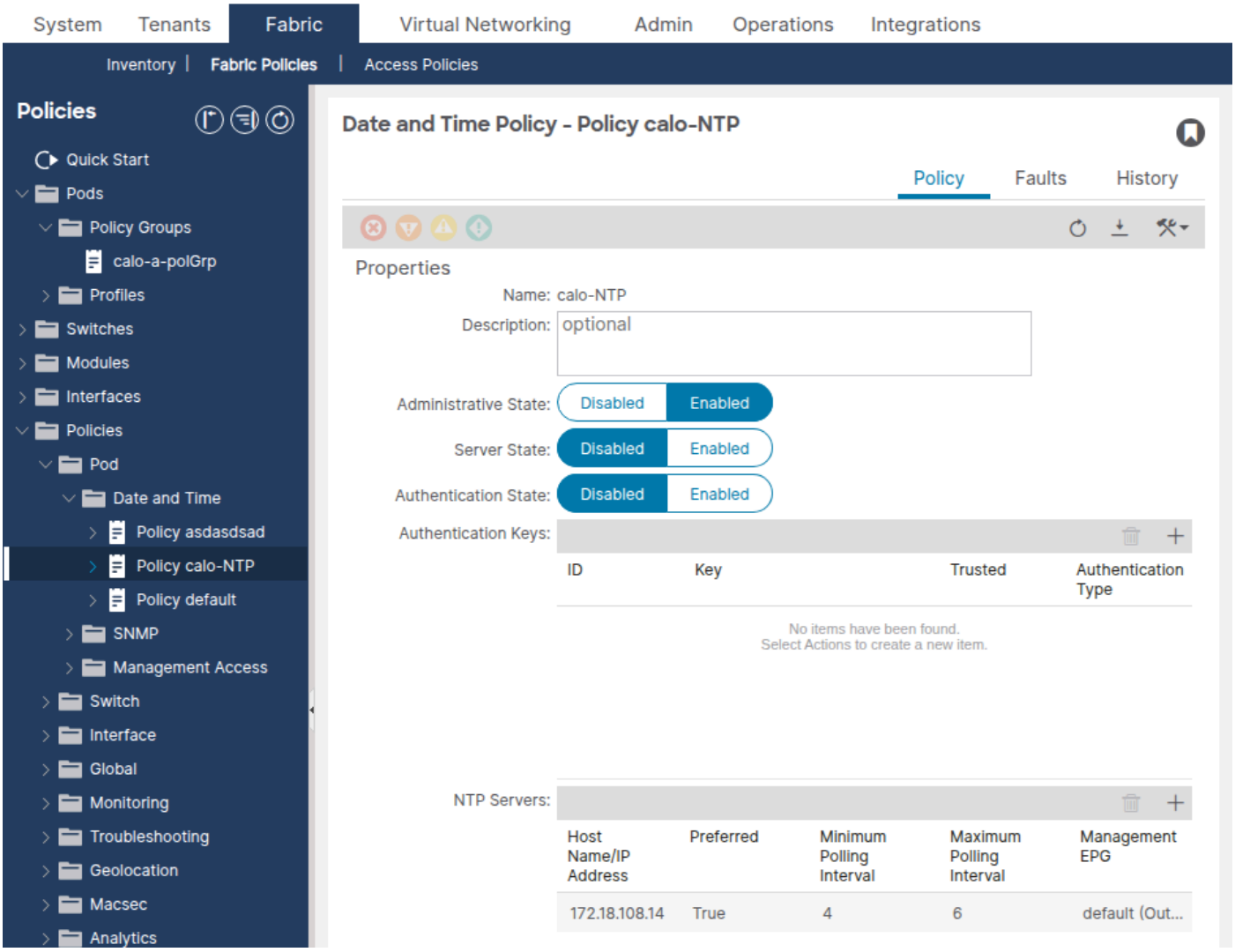
Vous pouvez également interroger l'API :

<#root>

```
apic1#

moquery -c mgmtRsOoBStNode
```

Étape 2: Vérifiez que la politique de date et d'heure dispose d'un fournisseur NTP

Accédez à Fabric > Fabric Policies > Policies > Pod > Date and Time > [Your Policy].



Vérifiez qu'au moins un fournisseur NTP (serveur) est configuré. S'il existe plusieurs fournisseurs, marquez au moins l'un d'entre eux comme Preferred.

Vérifiez le fournisseur NTP via l'API :

<#root>

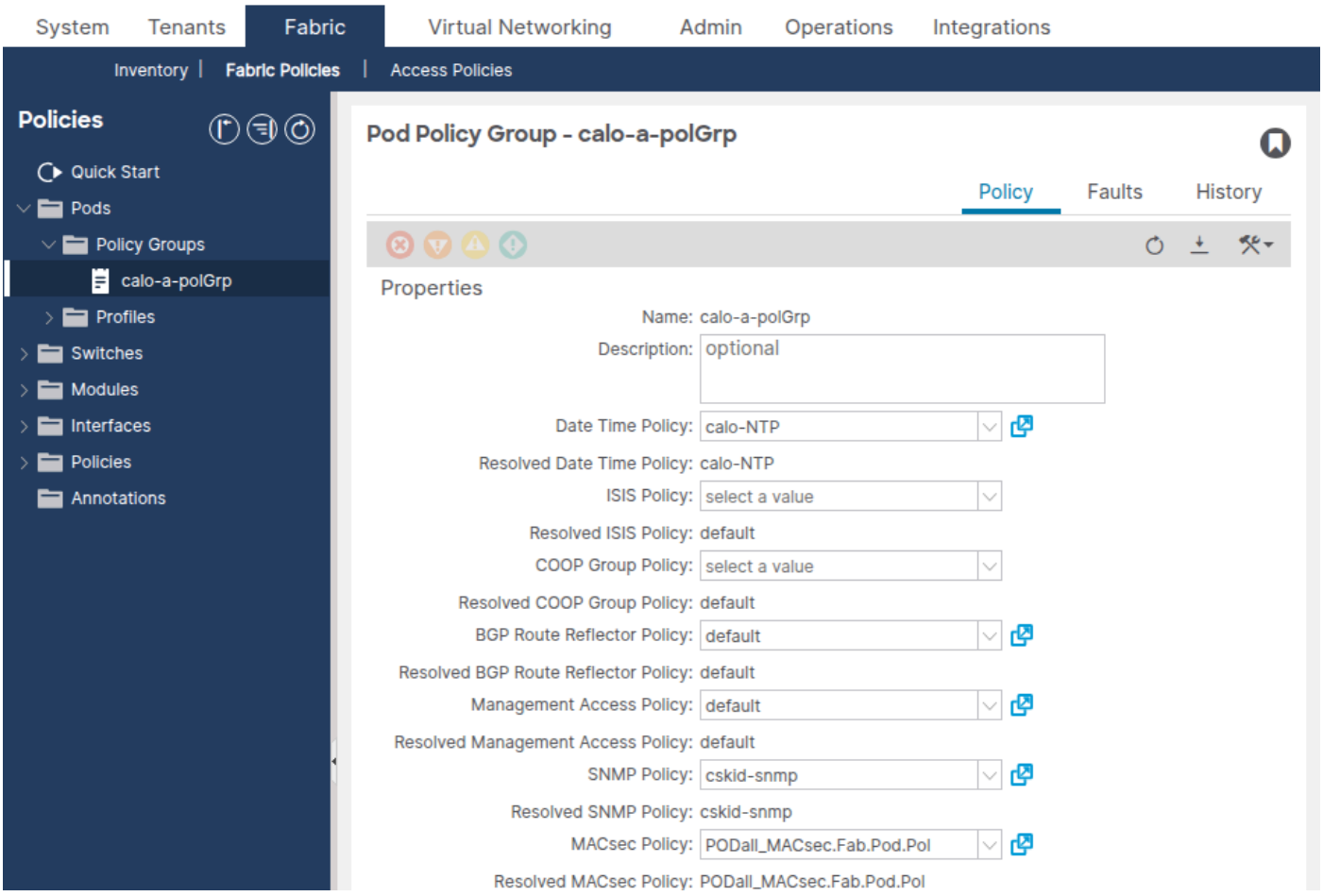
```
apic1#

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
```

Mauvaises configurations courantes

- Aucun fournisseur NTP configuré — la stratégie Date et heure existe mais n'a aucun fournisseur. La stratégie sera appliquée, mais les noeuds n'auront pas de serveur NTP sur lequel se synchroniser.
- EPG de gestion incorrect sélectionné — le fournisseur NTP fait référence à l'EPG hors bande, mais le serveur NTP n'est accessible que par l'intermédiaire de l'EPG intrabande (ou vice versa). Vérifiez quel EPG de gestion fournit l'accessibilité au serveur NTP.
- FQDN et IP du même serveur ajoutés en tant que fournisseurs distincts — ceci génère une erreur IP dupliquée. Supprimez l'entrée dupliquée.
- Fournisseur basé sur le nom de domaine complet sans stratégie DNS — si vous utilisez un nom d'hôte pour le fournisseur NTP, assurez-vous qu'une stratégie de service DNS est configurée et que l'étiquette DNS appropriée est appliquée au VRF de gestion.

Étape 3: Vérifier que le groupe de politiques de pod fait référence à la politique de date et d'heure

Accédez à Fabric > Fabric Policies > Pods > Policy Groups > [Your Pod Policy Group].



Confirmez que le champ Politique de date et d'heure fait référence à la politique de date et d'heure correcte.

<#root>

apic1#

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

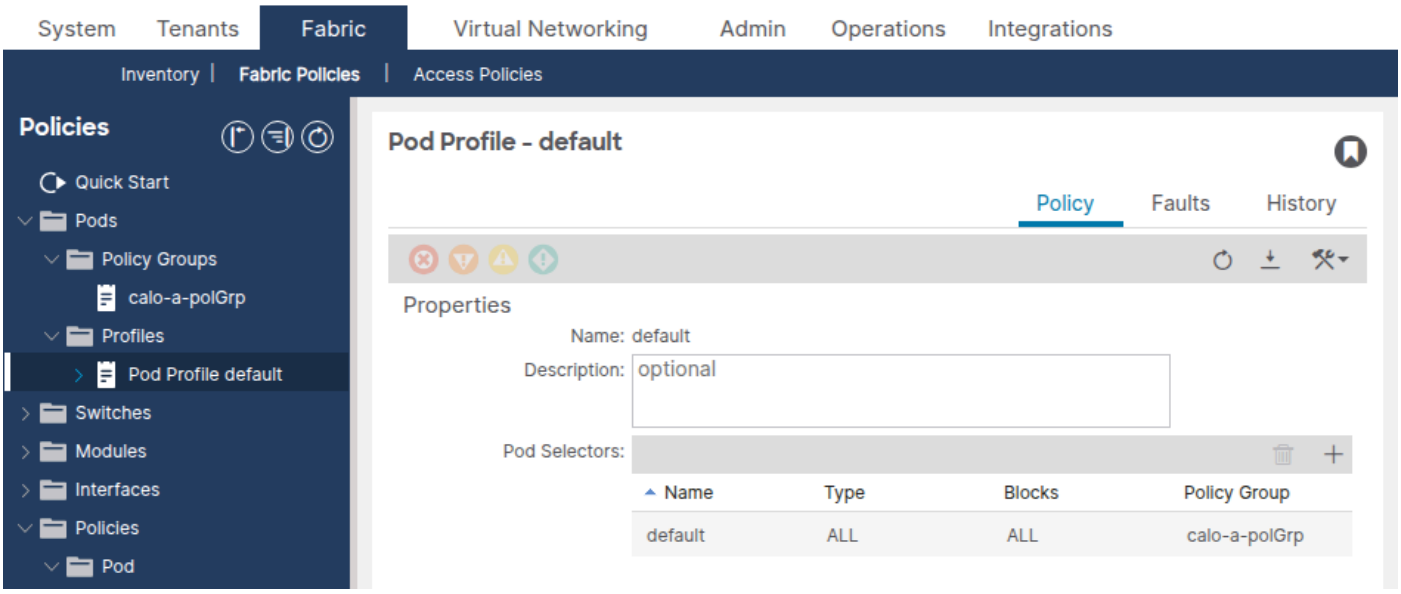
Recherchez l'attribut `datetimePolName` ou la relation `fabricRsTimePol` associée.

Mauvaises configurations courantes

- Le groupe de stratégies de pod fait référence à une stratégie de date et d'heure incorrecte — s'il existe plusieurs stratégies de date et d'heure (par exemple, « par défaut » et personnalisées), vérifiez que le groupe de stratégies de pod fait référence à la stratégie voulue.
- Le groupe de stratégies de pod n'a pas été créé du tout — la stratégie Date et heure n'est peut-être pas associée au groupe de stratégies de pod par défaut. Vérifiez toujours.

Étape 4: Vérification des références du profil de pod dans le groupe de stratégies de pod

Accédez à Fabric > Fabric Policies > Pods > Profiles > [Your Pod Profile].



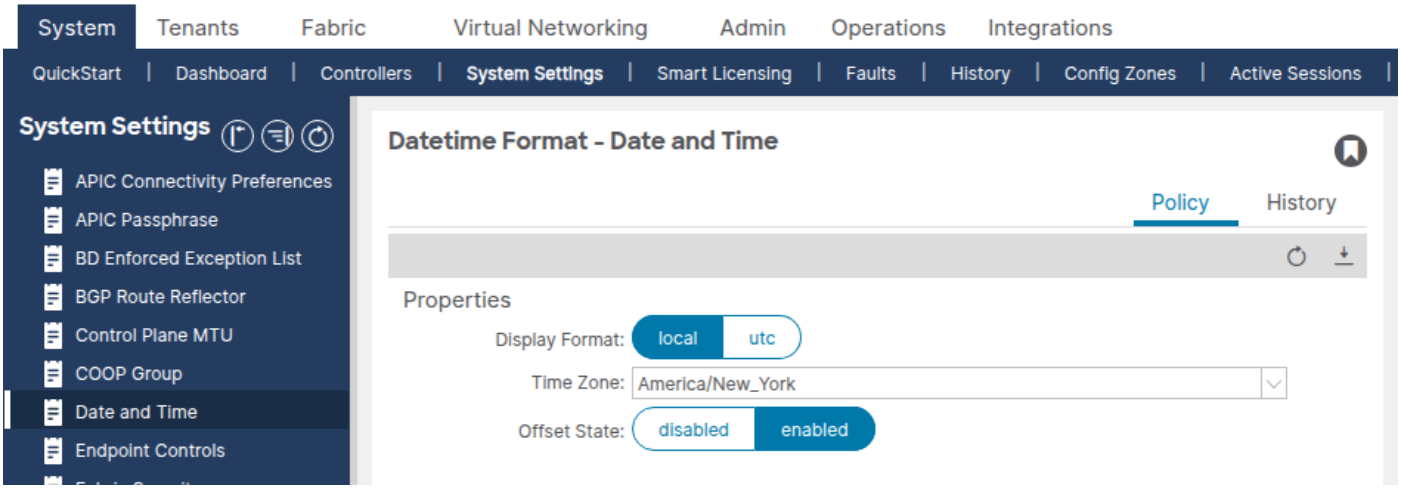
Vérifiez que le champ Groupe de stratégies de fabric fait référence au groupe de stratégies de pod approprié.

Mauvaises configurations courantes

- Le profil de pod fait référence au groupe de politiques de pod incorrect — en particulier dans les environnements à pod multiples, chaque profil de pod doit faire référence au groupe de politiques de pod correct.

Étape 5: Vérifier le format de date et d'heure

Accédez à System > System Settings > Date and Time.



Vérifiez que le format d'affichage (local ou UTC) et le fuseau horaire sont définis comme prévu. Ce paramètre est une stratégie de format de date et d'heure par défaut distincte qui ne peut pas être supprimée ou dupliquée.

Vérification opérationnelle

Après avoir vérifié que la chaîne de configuration est correcte, utilisez les commandes suivantes pour vérifier que le protocole NTP fonctionne au moment de l'exécution.

Vérification APIC

show ntpq

Cette commande affiche l'état de synchronisation NTP sur tous les APIC. Le symbole `*` indique que le serveur est sélectionné pour la synchronisation.

<#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
```

A quoi ressemble le bien :

- Tous les APIC affichent `*` (sélectionné pour la synchronisation) à côté du serveur distant.
- `reach` est de `377` (octal), ce qui indique que les 8 derniers sondages ont tous réussi.
- `st` (strate) est compris entre 1 et 15. La strate 16 signifie que le serveur n'est pas synchronisé.
- `le décalage` est faible (généralement inférieur à 100 ms pour un environnement sain).

A quoi ressemble le mauvais :

- Non `*` en regard d'un serveur : aucun serveur n'est sélectionné pour la synchronisation.
- `reach` is `0` — aucune réponse NTP n'a été reçue.
- `st` is `16` — le serveur NTP n'est pas synchronisé avec sa source de temps en amont.
- `offset` est extrêmement grand (des milliers de millisecondes) — l'horloge est considérablement déviée.

show clock

<#root>

```
apic1#

show clock

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

Vérifiez que l'heure est correcte. Comparer avec le temps prévu pour détecter la dérive d'horloge.

APIC Bash (alternatif)

<#root>

```
apic1#
```

bash

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

date

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

Vérification du commutateur (Leaf/Spine)

show ntp peers

Vérifiez que le fournisseur NTP a été envoyé au commutateur.

<#root>

```
leaf1#
```

show ntp peers

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

A quoi ressemble le bien : L'adresse IP ou le nom d'hôte du serveur NTP apparaît avec `Serv/Peer` = `Server` et le VRF correct (généralement la `gestion` pour OOB).

A quoi ressemble le mauvais : Aucun homologue répertorié ou l'adresse IP du serveur NTP ne correspond pas au fournisseur configuré. Cela indique généralement que la politique de date et d'heure n'a pas été appliquée via la chaîne Groupe de politiques de pod / Profil de pod.

show ntp peer-status

Vérifiez que le serveur NTP est sélectionné pour la synchronisation.

<#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
```

Le caractère `*` est essentiel : il confirme que le serveur NTP est utilisé pour la synchronisation.

A quoi ressemble le mauvais :

- Non `*` à côté du serveur — le commutateur n'est pas synchronisé avec le serveur.
- `reach` is `0` — aucune réponse NTP n'a été reçue. Cela indique un problème d'accessibilité.
- `st` is `16` — le serveur NTP n'est pas synchronisé et ne peut pas fournir d'heure valide.

show ntp statistics peer ipaddr

Vérifiez l'échange de paquets NTP pour confirmer l'accessibilité. Remplacez l'adresse IP par l'adresse du fournisseur NTP du commutateur concerné.

<#root>

```
leaf1#
```

show ntp statistics peer ipaddr 10.1.1.100

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

A quoi ressemble le bien : `les paquets envoyés` et les `paquets reçus` sont à peu près égaux et augmentent.

A quoi ressemble le mauvais : `Les paquets envoyés` sont incrémentés, mais les `paquets reçus` sont

de `0` ou à peine incrémentés : les réponses NTP n'atteignent pas le commutateur.

show clock

<#root>

```
leaf1#

show clock

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

Vérification GUI

Accédez à Fabric > Fabric Policies > Policies > Pod > Date and Time > [Your Policy] > [NTP Provider].

La colonne Sync Status doit afficher Synchronced to Remote NTP Server pour tous les noeuds. La convergence de l'état de synchronisation après le déploiement initial peut prendre plusieurs minutes.

Vérification API

Interrogez la classe `datetimeNtpq` pour vérifier la synchronisation NTP sur tous les 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.
```

Workflow de dépannage

Utilisez cet arbre de décision lorsqu'un problème NTP est signalé sur un noeud ACI.

Étape 1: Des homologues NTP sont-ils configurés sur le commutateur ?

Connectez-vous au commutateur concerné et exécutez :

<#root>

leaf1#

show ntp peers

- Aucun homologue répertorié → la stratégie Date et heure n'a pas été appliquée à ce noeud. Accédez au scénario 1 : Fournisseur NTP non envoyé au commutateur.
- Les homologues répertoriés → passent à l'étape 2.

Étape 2: Le serveur NTP est-il sélectionné pour la synchronisation ?

<#root>

leaf1#

show ntp peer-status

- `*` présent → NTP est en cours de synchronisation. Si l'heure semble toujours incorrecte, passez au Scénario 5 : Décalage important / dérive d'horloge.
- Non `*` présent → passez à l'étape 3.

Étape 3: La valeur de portée est-elle zéro ?

Vérifiez la colonne `reach` dans `show ntp peer-status`.

- **`reach` = `0`** → aucune réponse du serveur NTP. Accédez au scénario 2 : Serveur NTP inaccessible.
- **`atteignez` > `0`** mais aucune réponse `*` → n'est arrivée, mais la synchronisation n'est pas

établie. Vérifier la strate : passez à l'étape 4.

Étape 4: La valeur de strate est-elle 16 ?

- Stratum = 16 → le serveur NTP n'est pas synchronisé avec sa propre source en amont. Passez au scénario 3 : Serveur NTP non synchronisé (strate 16).
- Strate 1-15 mais pas de synchronisation → passez au scénario 4 : Non-concordance d'authentification NTP.

Scénarios de dépannage courants

Scénario 1 : Fournisseur NTP non envoyé au commutateur

Symptôme : `show ntp peers` on the switch ne renvoie aucune entrée.

Vérification de la configuration :

1. Vérifiez qu'au moins un fournisseur NTP est configuré pour la stratégie de date et d'heure.
2. Vérifiez que le groupe de politiques de pod fait référence à la politique de date et d'heure correcte.
3. Vérifiez que le profil de pod fait référence au groupe de stratégies de pod approprié.
4. Vérifiez que le noeud dispose d'une adresse IP de gestion attribuée sous le locataire mgmt.

Cause première : L'un des quatre liens de la chaîne de stratégie (Stratégie de date et d'heure → Fournisseur NTP → Groupe de stratégies Pod → Profil Pod) est rompu. La cause la plus fréquente est le fait que le groupe de politiques de pod n'est pas associé au profil de pod ou que la politique de date et d'heure n'est pas sélectionnée dans le groupe de politiques de pod.

Solution : Complétez le maillon manquant dans la chaîne des stratégies. Assurez-vous que le profil de pod du pod concerné fait référence à un groupe de stratégies de pod qui contient la stratégie de date et d'heure correcte. Une fois appliquée, la configuration du fournisseur NTP sera envoyée aux commutateurs dans quelques minutes.

Scénario 2 : Serveur NTP inaccessible

Symptôme : `show ntp peer-status` indique `reach = 0`. `show ntp statistics peer ipaddr 10.1.1.100` indique les `paquets reçus` = `0`.

Vérification de la configuration : Vérifiez que le fournisseur NTP est associé au bon EPG de gestion (OOB ou intrabande). Si vous utilisez OOB, vérifiez que les contrats OOB autorisent le port UDP 123.

Contrôle opérationnel :

1. Envoyez une requête ping au serveur NTP à partir du commutateur concerné en utilisant le VRF de gestion :
   <#root>

   `leaf1#`

   `ping 10.1.1.100 vrf management`

2. Exécutez une commande tcpdump sur le commutateur pour vérifier si les paquets NTP partent et arrivent :
   <#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
   ```

Cause première : En général, l'un des éléments suivants :

- Aucune adresse IP de gestion n’est attribuée au commutateur.
- La passerelle par défaut du VRF de gestion est manquante ou incorrecte.
- Un pare-feu bloque le port UDP 123 entre le commutateur et le serveur NTP.
- Le contrat OOB n'autorise pas le port UDP 123.
- Le fournisseur NTP fait référence au mauvais EPG de gestion (par exemple, OOB sélectionné, mais seul le trafic intrabande est accessible).

Solution : Résolvez le problème d'accessibilité. Attribuez une adresse de gestion si elle est manquante, corrigez la passerelle par défaut, mettez à jour les règles de pare-feu ou corrigez la sélection de l'EPG de gestion sur le fournisseur NTP.

Scénario 3 : Serveur NTP non synchronisé (strate 16)

Symptôme : `show ntp peer-status` montre strate (`st`) = `16`. Le commutateur ne se synchronisera pas avec un serveur strate 16.

Contrôle opérationnel : Connectez-vous au serveur NTP ou interrogez-le à partir d'un hôte externe pour vérifier qu'il est synchronisé avec sa propre source temporelle en amont.

Cause première : Le serveur NTP lui-même a perdu la synchronisation avec son horloge de référence en amont. Un serveur avec la strate 16 annonce qu'il n'a pas de source temporelle fiable.

Solution : Réparez le serveur NTP. Ceci se trouve en dehors du fabric ACI : vérifiez la configuration du serveur NTP et sa source temporelle en amont. Si le serveur NTP ne peut pas être réparé immédiatement, configurez un autre fournisseur NTP dans la stratégie Date et heure.

Scénario 4 : Non-concordance d'authentification NTP

Symptôme : `show ntp peer-status` affiche `reach` **>** `0` et stratum est valide, mais no `*` s'affiche. Le serveur NTP répond, mais le commutateur n'accepte pas la réponse.

Vérification de la configuration :

1. Vérifiez si le serveur NTP nécessite une authentification.
2. Si l'authentification est requise, vérifiez que l'état d'authentification de la stratégie Date et heure est Activé.
3. Vérifiez que l'ID de clé d'authentification, la valeur de clé et l'algorithme (MD5, SHA-1 ou AES128-CMAC) correspondent entre le fabric ACI et le serveur NTP.
4. Vérifiez que la clé est marquée comme Trusted dans le tableau NTP Client Authentication Keys.

Cause première : La clé d'authentification, l'algorithme ou l'ID de clé ne correspond pas entre l'ACI et le serveur NTP, ce qui entraîne le rejet de la réponse NTP comme non authentifiée par le commutateur.

Solution : Alignez la configuration de l’authentification. Assurez-vous que l'ID de clé, la valeur de clé et l'algorithme sont configurés de la même manière sur l'ACI et le serveur NTP. AES128-CMAC est recommandé pour les versions APIC 6.1(1) et ultérieures.

Remarque : Lorsque le mode FIPS est activé, seuls les schémas d'authentification AES128-CMAC et SHA-1 sont pris en charge. MD5 ne fonctionne pas en mode FIPS.

Scénario 5 : Décalage important / dérive d'horloge

Symptôme : Le commutateur semble synchronisé (* présent, portée = 377), mais la valeur de `décalage` dans `show ntp peer-status` ou dans show ntpq est très grande (des centaines ou des milliers de millisecondes), ou l'horloge est visiblement incorrecte.

Contrôle opérationnel :

<#root>

apic1#

show ntpq

Vérifiez la colonne `offset`. Un décalage sain est généralement inférieur à 100 ms.

Cause première : L'horloge a dévié de manière significative avant l'établissement de la synchronisation NTP, ou l'horloge matérielle (RTC) a été réinitialisée lors d'un redémarrage (par exemple, en raison d'une batterie CMOS morte). Le NTP corrige l'horloge progressivement par pivotement, ce qui peut prendre du temps pour les grands décalages.

Solution : Si le décalage est très grand et que le protocole NTP est en cours de synchronisation, attendez que l'horloge converge. Le protocole NTP fait pivoter l'horloge progressivement : les décalages importants peuvent prendre des heures pour être entièrement corrigés. Si le décalage ne diminue pas, vérifiez que le serveur NTP fournit l'heure exacte. Si le problème se reproduit après chaque redémarrage, examinez l'horloge matérielle (pile RTC/CMOS) sur le noeud affecté.

Scénario 6 : Défaillances APIC de secours avec NTP intra-bande

Symptôme : Des erreurs sont générées sur un APIC de secours lié à NTP ou à la politique de surveillance lorsque NTP est configuré pour la gestion intrabande.

Cause première : Lorsqu’une stratégie NTP est appliquée pour la gestion intrabande, le contrôleur APIC de secours requiert également une configuration intrabande. Sans elle, les défauts sont augmentés.

Solution : Configurez également la gestion intrabande pour le contrôleur APIC de secours. Cela efface les défauts.

Scénario 7 : Erreur IP dupliquée

Symptôme : Une erreur IP dupliquée est déclenchée après l'ajout de fournisseurs NTP.

Cause première : Un nom de domaine complet a été ajouté en tant que fournisseur NTP, puis l'adresse IP résolue de ce nom de domaine complet a été ajoutée en tant que deuxième fournisseur NTP. L'ACI détecte le doublon.

Solution : Supprimez le dernier fournisseur dupliqué ajouté (l'entrée d'adresse IP si le nom de domaine complet a été ajouté en premier, ou vice versa). Utilisez une seule entrée par serveur NTP : soit le nom de domaine complet (FQDN), soit l'adresse IP, et non les deux.

Scénario 8 : Échec de la résolution DNS pour le fournisseur NTP basé sur FQDN

Symptôme : Le fournisseur NTP configuré avec un nom d'hôte n'est pas résolu. `show ntp peers` n'affiche pas l'adresse IP attendue ou NTP ne se synchronise pas.

Vérification de la configuration :

1. Vérifiez qu'une stratégie de service DNS est configurée sous Fabric > Fabric Policies > Policies > Global > DNS Profiles.
2. Vérifiez que le fournisseur DNS (serveur DNS) est accessible à partir du VRF de gestion.
3. Vérifiez que l'étiquette DNS appropriée est configurée pour l'instance VRF intrabande ou hors bande de l'EPG de gestion.

Cause première : Le serveur DNS n'est pas accessible ou n'est pas configuré, ce qui entraîne l'échec de la résolution du nom d'hôte pour le fournisseur NTP.

Solution : Configurez la stratégie de service DNS, assurez l'accessibilité DNS et appliquez l'étiquette DNS correcte. Vous pouvez également utiliser l'adresse IP du serveur NTP au lieu du nom d'hôte.

Erreurs et événements associés

Les conditions suivantes sont liées au protocole NTP et peuvent générer des défaillances dans l'ACI :

- Duplicate IP fault - Déclenché lorsqu'un nom de domaine complet et l'adresse IP du même serveur NTP sont tous deux ajoutés en tant que fournisseurs. Résolution : supprimez l'entrée dupliquée.
- Défauts NTP intrabande du contrôleur APIC de secours — déclenchés lorsqu'une

surveillance ou une politique NTP est appliquée pour l'intrabande, mais que le contrôleur APIC de secours n'a pas de configuration intrabande.
- État de synchronisation non convergent — l'interface graphique utilisateur affiche « Non synchronisé » ou un état autre que « Synchronisé avec le serveur NTP distant » pour un ou plusieurs noeuds. Il ne s'agit pas d'un code d'erreur mais d'un indicateur d'état opérationnel. Suivez le workflow de dépannage ci-dessus pour effectuer le diagnostic.

Critères de remontée

Envisagez de transférer le problème au TAC Cisco si :

- La chaîne de configuration est vérifiée correctement et le serveur NTP est accessible (ping fonctionne, tcpdump affiche les réponses NTP), mais le commutateur ne se synchronise toujours pas.
- La synchronisation NTP est perdue à plusieurs reprises sans modification de la configuration ou sans problème de serveur NTP.
- La sortie `show ntp peer-status` montre un comportement inattendu tel que la strate persistante 16 sur un serveur qui est confirmé synchronisé en externe.
- L'horloge dérive considérablement entre les redémarrages, ce qui peut indiquer un problème d'horloge matérielle (RTC).

Lorsque vous faites appel au TAC, fournissez les données suivantes :

- Résultat de la commande `show ntpq` de tous les APIC.
- Résultats de `show ntp peer`, `show ntp peer-status`, `show ntp statistics peer ipaddr <IP>` et `show clock` de tous les commutateurs affectés.
- Sortie de `moquery -c datetimePol`, `moquery -c datetimeNtpProv`, et `moquery -c datetimeNtpq` de l'APIC.
- Une assistance technique du ou des noeuds affectés.

Références

- Cisco APIC Basic Configuration Guide, version 6.1(x) — Provisioning Core ACI Fabric Services
- Dépannage de la gestion ACI et des services principaux — Politiques de pod
- Guide de conception de l'infrastructure axée sur les applications (ACI)

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.