Configuration et dépannage des paramètres NTP sur Firepower et Secure Firewall

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Configurer
  - NTP sur FPR4100/9300
    - Points clés
  - NTP sur CSF200/1200/3100/4200/6100
  - Configuration du protocole NTP sur FPR2100/4100/9300
- Vérifier
  - Vérification de la synchronisation NTP sur les appareils FPR4100/9300
    - Référence d'état du serveur
  - Vérification de la synchronisation NTP entre MIO et le périphérique logique (lame) sur les appareils FPR4100/9300
- Dépannage des problèmes courants
  - 1. FXOS ne peut pas résoudre le nom d'hôte du serveur NTP
    - Action recommandée
    - Causes possibles
  - 2. Problèmes de connectivité entre FXOS et le serveur NTP sur le port UDP 123
    - Action recommandée
    - Causes possibles
  - 3. Problèmes de connectivité intermittente entre FXOS et le serveur NTP
    - Actions recommandées
    - Cause possible
- Défauts associés
- Informations connexes

Introduction

Ce document décrit comment configurer, vérifier et dépanner le protocole NTP (Network Time Protocol) sur les périphériques Cisco Firepower et Cisco Secure Firewall.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

- FPR4140 exécutant FXOS 2.3(1.130) et 2.8(1.105).
- FPR2110 en mode plate-forme ASA.
- FPR1140 exécutant le mode appliance ASA.
- CSF220 exécutant FTD 10.x.

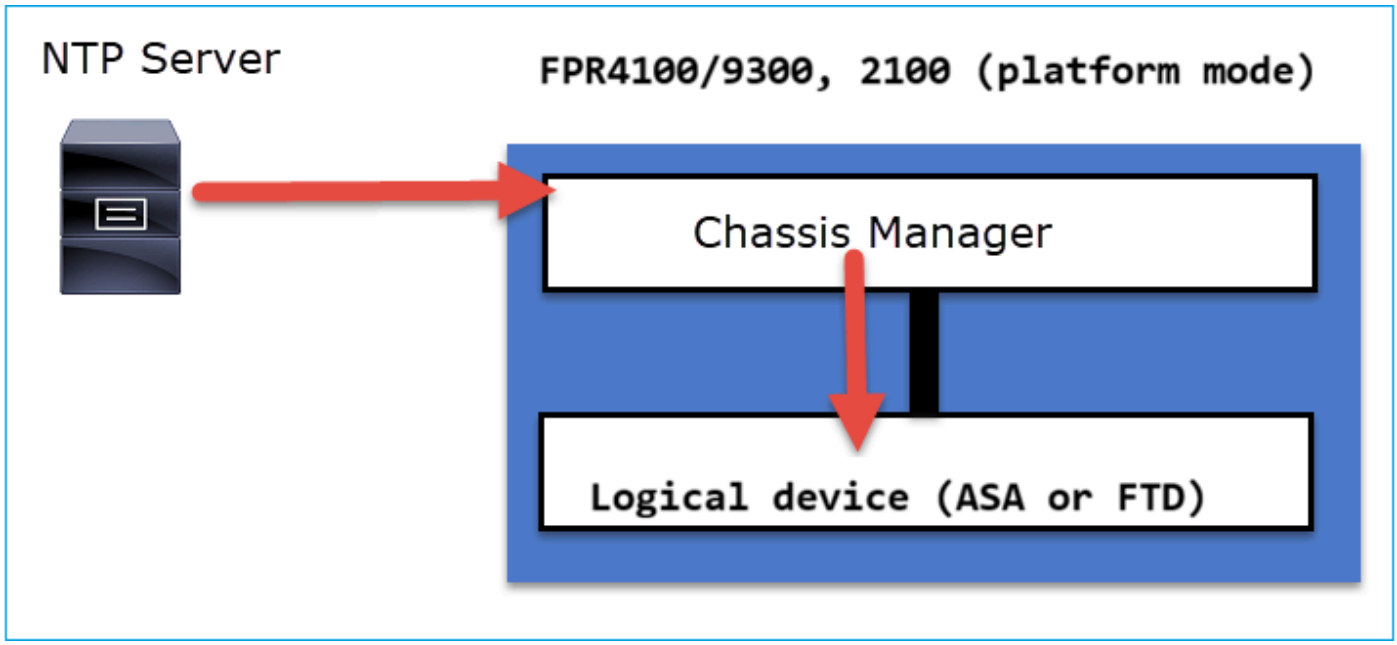
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Le fonctionnement du protocole NTP dépend de la plate-forme.

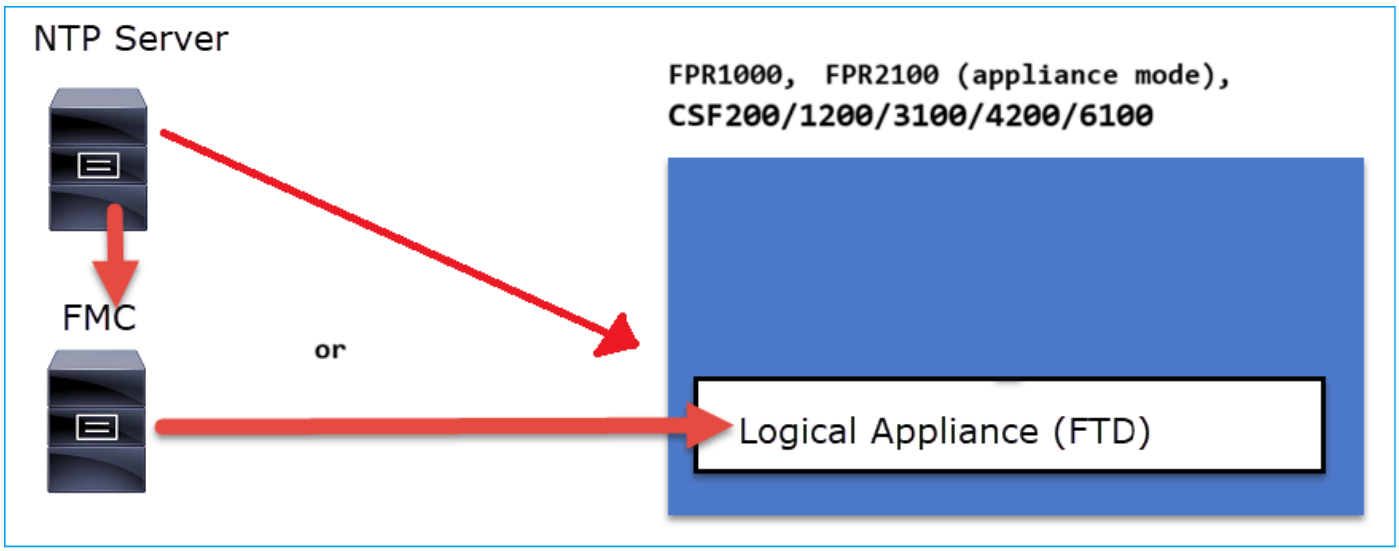
FPR4100/FPR9300, FPR2100 (mode plate-forme)

L'heure ASA ou FTD provient de l'entrée/sortie de gestion (MIO) du gestionnaire de châssis Firepower (FCM) du châssis. MIO est le superviseur du châssis Firepower.



FPR1000, FPR2100 (mode appliance), CSF200/3100/4200/6100

Sur FTD, le temps est pris à partir du FMC ou d'un serveur NTP :



Pour ce déploiement, consultez les documents suivants :

- Configuration de la synchronisation NTP pour la défense contre les menaces
- Résolution des problèmes liés au protocole NTP (Network Time Protocol) sur les systèmes Firepower

Informations complémentaires :
NTP est utilisé pour la synchronisation temporelle. NTP utilise comme transport le numéro de port UDP 123.

Remarque : NTP version 4 n'est pas officiellement pris en charge. NTP version 4 est rétrocompatible avec NTP version 3.

Configurer

NTP sur FPR4100/9300

Points clés

- Pour configurer le protocole NTP sur un appareil FPR4100/9300, connectez-vous à FCM et accédez à l'onglet Platform Settings.
- Le NTP sur les périphériques logiques (ASA ou FTD) est synchronisé avec le MIO.
- Il n'y a aucune possibilité de synchroniser NTP sur FTD avec Firewall Management Center (FMC), même si vous choisissez cette option, NTP sur FTD est synchronisé avec MIO. Par conséquent, il est fortement recommandé que FMC et FCM utilisent le même serveur NTP.
- Le FMC n’est pas un serveur NTP complet. Il peut simplement fournir des paramètres de temps à ses périphériques gérés via le sftunnel. Il ne peut donc pas être utilisé comme serveur NTP pour le châssis FPR4100/9300.
- Une configuration NTP appropriée est requise pour une installation de licence Smart réussie.

NTP sur CSF200/1200/3100/4200/6100

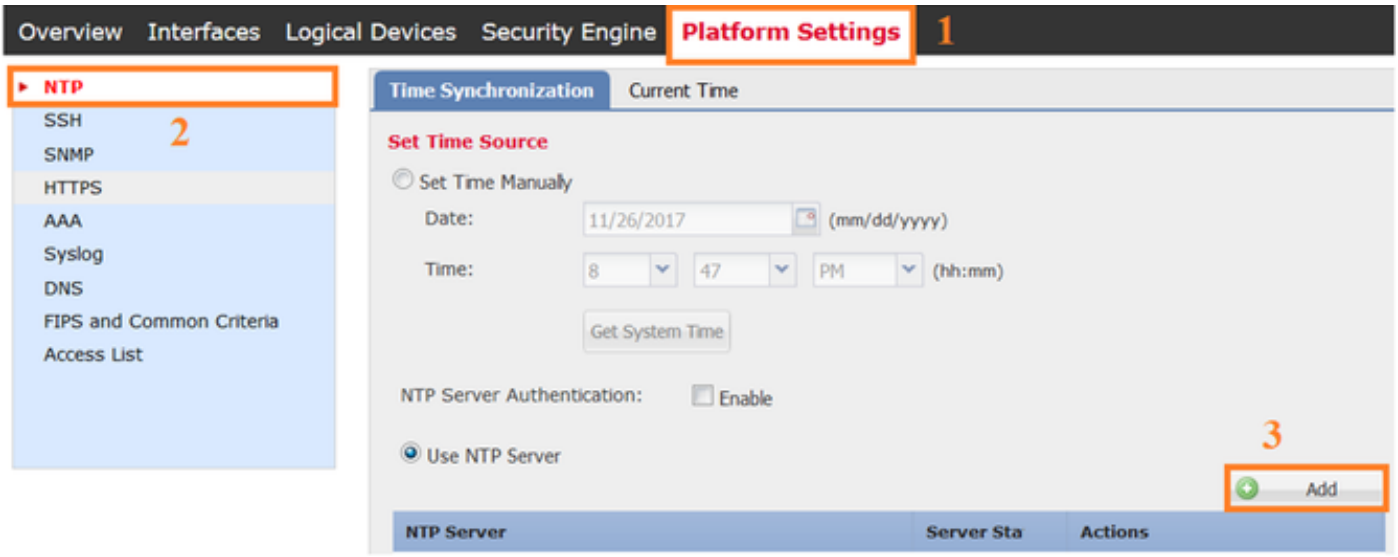
- Configurez les paramètres NTP sur l'application logique elle-même. L'ASA en mode appliance ou en cas de gestion FTD « on-box » à partir du Gestionnaire de périphériques de pare-feu (FDM).
- Si le FTD est géré par le FMC (gestion off-box), configurez le NTP sur le FMC.

Configuration du protocole NTP sur FPR2100/4100/9300

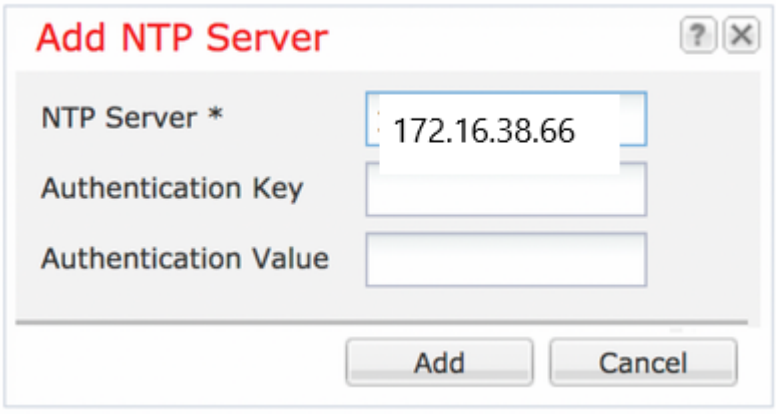
- Pour configurer le protocole NTP sur un appareil FPR2100 en mode plate-forme, accédez à l'onglet Platform Settings à partir du gestionnaire de châssis.

Remarque : Dans les versions postérieures à la version 9.13(1) FPR2100, vous pouvez exécuter le mode appliance (par défaut) et le mode plate-forme. Le mode Appliance vous permet de configurer tous les paramètres, y compris NTP, sur l'ASA. Seules les commandes de dépannage avancées sont disponibles à partir de l'ILC FXOS. D'autre part, en mode plate-forme, vous devez configurer les paramètres de base (y compris NTP) et les paramètres d'interface matérielle dans le gestionnaire de châssis (FCM).

Étape 1. Connectez-vous à l'interface graphique utilisateur du gestionnaire de châssis avec les informations d'identification de l'utilisateur local et accédez à Platform Settings > NTP. Cliquez sur le bouton Ajouter :



Étape 2 : spécifiez l'adresse IP ou le nom d'hôte du serveur NTP (si vous utilisez un nom d'hôte pour le serveur NTP, vous devez configurer un serveur DNS).



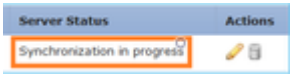
Remarque : Vous pouvez configurer jusqu'à 4 serveurs NTP

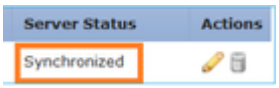
- Dans le cas d'un ASA en mode plate-forme, le NTP sur le périphérique logique est synchronisé avec le MIO.
- Pour FTD sur FPR2100 qui utilise le mode appliance, vous devez configurer le NTP sur FMC.
- Pour ASA sur FPR2100 qui utilise le mode appliance, vous configurez le NTP sur l'ASA.

Vérifier

Vérification de la synchronisation NTP sur les appareils FPR4100/9300

Surveillez l'état du serveur.





Référence d'état du serveur

- Non disponible: État par défaut affiché immédiatement après la configuration du serveur NTP.
- Inaccessible/non valide : Présenté dans les scénarios suivants :
  - Lorsque l'adresse IP ou le nom d'hôte du serveur NTP est inaccessible par le protocole NTP.
  - Lorsque l'adresse IP ou le nom d'hôte du serveur NTP est accessible, mais que l'hôte distant n'est pas un serveur NTP.
  - D'autres échecs internes, tels que l'échec de l'exécution de la requête, la levée d'une exception, la détection d'un état de synchronisation de durée non définie, etc.
- Synchronisation en cours : Le serveur est accessible et prend en charge le protocole NTP, la convergence initiale est toujours en cours et n'est pas encore terminée.
- Synchronisé : L'hôte est déclaré comme homologue de synchronisation du système et l'horloge est synchronisée avec lui.
- Candidat : L'hôte est l'homologue candidat (en veille). Un serveur NTP candidat signifie qu'il est valide et qu'il a correctement communiqué avec l'appliance Firepower, mais que le

module a été synchronisé avec un autre serveur NTP et qu'il est donc en veille. Il peut être sélectionné comme homologue synchronisé suivant si l'homologue actuel est supprimé.
- Absolu : Un serveur NTP qui est rejeté en raison d'une différence significative (décalage temporel et délai aller-retour) par rapport au reste des serveurs NTP.

Vérifiez l'état de l'homologue NTP :

<#root>

```
FPR4100#

connect fxos


FPR4100(fxos)#

show ntp peer-status


Total peers : 4
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode
    remote               local                st   poll   reach delay
-------------------------------------------------------------------------------
=172.16.38.66           10.62.148.196           1 1024      17   0.20996
*172.31.201.67          10.62.148.196           1 1024     377   0.03035
=172.16.38.65           10.62.148.196           1 1024     377   0.19914
=172.31.20.115          10.62.148.196           1 1024     377   0.02905
```

Vérifiez la configuration et la synchronisation du serveur NTP :

<#root>

```
FPR4100#

scope system


FPR4100 /system #

scope services


FPR4100 /system/services #

show ntp-server detail
```

```
NTP server hostname:
    Name: 172.16.38.65Time Sync Status: Candidate
    NTP SHA-1 key id: 0
    Error Msg:

    Name: 172.16.38.66
    Time Sync Status: Time Sync In Progress
    NTP SHA-1 key id: 0
    Error Msg:

    Name: 172.31.20.115
    Time Sync Status: Candidate
    NTP SHA-1 key id: 0
    Error Msg:

    Name: 172.31.201.67
    Time Sync Status: Time Synchronized
    NTP SHA-1 key id: 0
    Error Msg:
```

Vérifiez l'association NTP :

<#root>

```
FPR4100#

connect module 1 console


Firepower-module1>show ntp association

     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*203.0.113.126   172.31.201.67   2 u   39   64  370    0.070    0.445   0.210

ind assid status  conf reach auth condition  last_event cnt
===========================================================
  1 16696  961a   yes   yes  none  sys.peer    sys_peer  1

associd=16696 status=961a conf, reach, sel_sys.peer, 1 event, sys_peer,
srcadr=203.0.113.126, srcport=123, dstadr=203.0.113.1, dstport=123,
leap=00, stratum=2, precision=-21, rootdelay=29.053, rootdisp=70.496,
refid=172.31.201.67,
reftime=e24d4bd9.3b680f6d  Fri, Apr 24 2020 11:28:25.232,
rec=e24d4d34.170bd724  Fri, Apr 24 2020 11:34:12.090, reach=370,
unreach=0, hmode=3, pmode=4, hpoll=6, ppoll=6, headway=0,
flash=20 pkt_stratum, keyid=0, offset=0.445, delay=0.070,
dispersion=2.152, jitter=0.210, xleave=0.017,

filtdelay=     0.08    0.11    0.08    0.10    0.07    0.08    0.09    0.07,
filtoffset=    0.17    0.18    0.29    0.29    0.45    0.45    0.69    0.69,
filtdisp=      0.00    0.03    0.99    1.02    2.03    2.06    3.03    3.06

associd=16696 status=961a conf, reach, sel_sys.peer, 1 event, sys_peer,
remote host:           203.0.113.126:123
local address:         203.0.113.1:123
```

```
time last received:    39
time until next send:  26
reachability change:   170025
packets sent:          5048
packets received:      5048
bad authentication:    0
bogus origin:          0
duplicate:             0
bad dispersion:        27
bad reference time:    0
```

Vérifiez les informations système NTP :

<#root>

```
FPR4100#
```

connect module 1 console

```
Firepower-module1>
```

show ntp sysinfo

```
associd=0 status=0615 leap_none, sync_ntp, 1 event, clock_sync,
version="ntpd 4.2.8p11@1.3728-o Sat Dec  8 06:11:47 UTC 2018 (2)",
processor="x86_64", system="Linux/3.10.62-ltsi-WR10.0.0.29_standard",
leap=00, stratum=3, precision=-24, rootdelay=29.129, rootdisp=24.276,
refid=203.0.113.126,
reftime=e24dd3bf.170a6210  Fri, Apr 24 2020 21:08:15.090,
clock=e24dd437.59b86104  Fri, Apr 24 2020 21:10:15.350, peer=16696, tc=6,
mintc=3, offset=0.009911, frequency=7.499, sys_jitter=0.023550,
clk_jitter=0.004, clk_wander=0.001

associd=0 status=0615 leap_none, sync_ntp, 1 event, clock_sync,
system peer:        203.0.113.126:123
system peer mode:   client
leap indicator:     00
stratum:            3
log2 precision:     -24
root delay:         29.129
root dispersion:    24.276
reference ID:       203.0.113.126
reference time:     e24dd3bf.170a6210  Fri, Apr 24 2020 21:08:15.090
system jitter:      0.023550
clock jitter:       0.004
clock wander:       0.001
broadcast delay:    -50.000
symm. auth. delay:  0.000

uptime:                 204908
sysstats reset:         204908
packets received:       19928
current version:        6069
older version:          0
```

```
bad length or format:   0
authentication failed:  0
declined:               0
restricted:             0
rate limited:           0
KoD responses:          0
processed for time:     6040

associd=0 status=0615 leap_none, sync_ntp, 1 event, clock_sync,
pll offset:             0.006196
pll frequency:          7.49899
maximum error:          0.097039
estimated error:        3e-06
kernel status:          pll nano
pll time constant:      6
precision:              1e-06
frequency tolerance:    500
pps frequency:          0
pps stability:          0
pps jitter:             0
calibration interval    0
calibration cycles:     0
jitter exceeded:        0
stability exceeded:     0
calibration errors:     0

time since reset:       204908
receive buffers:        10
free receive buffers:   9
used receive buffers:   0
low water refills:      1
dropped packets:        0
ignored packets:        0
received packets:       19930
packets sent:           26811
packet send failures:   0
input wakeups:          224931
useful input wakeups:   20034
```

Vérification supplémentaire :

<#root>

```
FTD220 /eth-uplink #
```

scope eth-uplink ; scope fabric a

```
FTD220 /eth-uplink/fabric #
```

show ntp-overall-status

```
NTP Overall Time-Sync Status: Time Synchronized
```

Vérification de la synchronisation NTP entre MIO et le périphérique logique (lame) sur les appareils FPR4100/9300

Sur le FPR4100/9300, les paramètres NTP sont transmis au FTD via le MIO (châssis). La configuration NTP à partir de l'interface de ligne de commande FTD ou de l'interface utilisateur FMC n'est pas possible.

Chaque lame FTD utilise un ID de référence interne : 203.0.113.126 pour communiquer avec le MIO pour la synchronisation temporelle et sur cette base, il indique s'il est synchronisé ou non. L'interface de ligne de commande FTD reflète cela. Dans cet exemple, l'IP NTP est l'ID de référence interne et non l'IP réelle du serveur NTP. Une modification de l'adresse IP du serveur NTP dans le FCM n'affecte pas ce résultat puisque l'id de référence est toujours le même :

<#root>

```
 >

show ntp

NTP Server                : 203.0.113.126
Status                    : Being Used
Offset                    : -0.078 (milliseconds)
Last Update               : 43 (seconds)
```

Vérifiez la configuration NTP en mode plate-forme FRP2100 et CSF200/1200/3100/4200/6100 :

<#root>

```
FTD220#

scope system

FTD220 /system #

scope services

FTD220 /system/services #

show ntp-server detail


NTP server hostname:
    Name: 172.31.201.67
```

```
    Time Sync Status: Time Synchronized
    Error Msg:
```

Sur FTD, vous pouvez également vérifier les paramètres NTP à partir du mode CLISH :

```
<#root>

>

show ntp



NTP Server : 172.31.201.67



Status : Being Used


Offset : +0.819 (milliseconds)
Last Update : 3 (seconds)

NTP Server : 127.127.1.1
Status : Available
Offset : +0.000 (milliseconds)
Last Update : 418 (seconds)
```

Si le FTD obtient son heure du FMC, vous voyez l'adresse IP 127.0.0.2 :

```
<#root>

FTD220 /system/services #

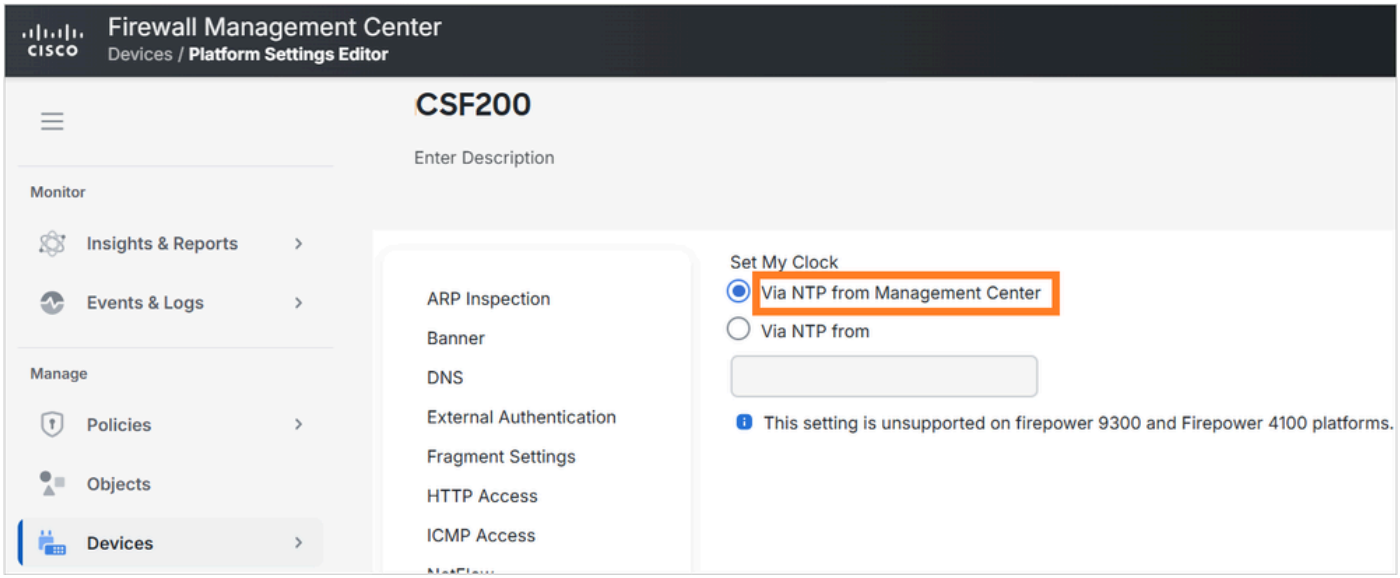
show ntp-server detail expand



NTP server hostname:

Name: 127.0.0.2


Time Sync Status: Time Synchronized
Error Msg:
```



Dans ce cas, l'adresse IP 127.0.0.2 s'affiche également à partir de CLISH :

<#root>

>

show ntp

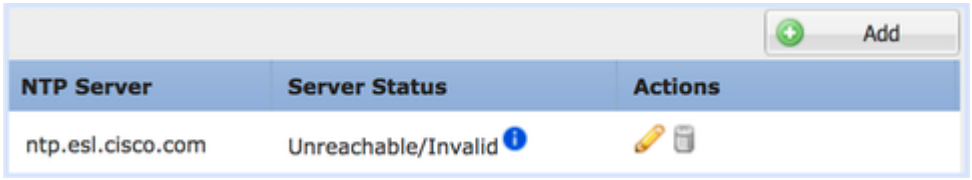
```
NTP Server : 127.0.0.2
Status : Being Used
Offset : +0.008 (milliseconds)
Last Update : 6 (seconds)

NTP Server : 127.127.1.1
Status : Available
Offset : +0.000 (milliseconds)
Last Update : - (seconds)
```

Dépannage des problèmes courants

1. FXOS ne peut pas résoudre le nom d'hôte du serveur NTP

L'interface utilisateur FCM affiche :



Action recommandée

Utilisez la commande ping pour vérifier la résolution du nom d'hôte du serveur NTP

<#root>

```
FPR4100(local-mgmt)#

ping ntp.esl.cisco.com

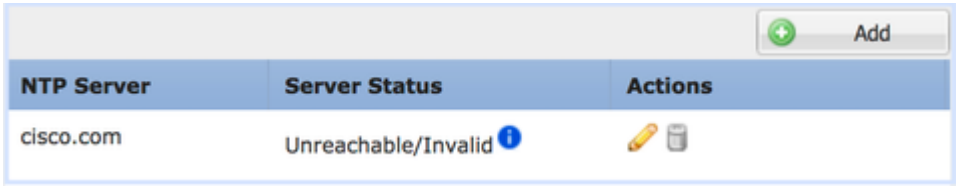
Invalid Host Name.
```

Causes possibles

- Le serveur DNS n'est pas configuré.
- Le serveur DNS ne peut pas résoudre le nom d'hôte.

2. Problèmes de connectivité entre FXOS et le serveur NTP sur le port UDP 123

L'interface utilisateur FCM affiche :



Action recommandée

⚠ Mise en garde : La capture d'analyseur Ethernet sur l'interface de gestion du châssis est uniquement disponible sur les appliances FPR4100/9300.

Effectuez des captures sur l'interface de gestion du châssis et vérifiez la communication

bidirectionnelle sur le port UDP 123 :

<#root>

```
FPR4100(fxos)#

ethanalyzer local interface mgmt capture-filter "udp port 123"

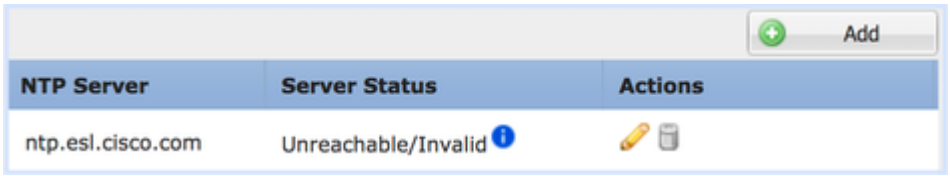
Capturing on 'eth0'
1 2020-04-30 20:09:54.150237760 10.62.148.196 → 172.16.4.161 NTP 90 NTP Version 3, client
2 2020-04-30 20:14:14.150172804 10.62.148.196 → 172.16.4.161 NTP 90 NTP Version 3, client
3 2020-04-30 20:23:13.150171682 10.62.148.196 → 172.16.4.161 NTP 90 NTP Version 3, client
```

Causes possibles

- Le serveur configuré n'est pas un serveur NTP.
- Un périphérique dans le chemin (par exemple, un pare-feu) bloque ou modifie le trafic.

3. Problèmes de connectivité intermittente entre FXOS et le serveur NTP

L'interface utilisateur FCM affiche :



Actions recommandées

⚠ Mise en garde : Uniquement pour les appareils FPR4100/9300.

Lancez le processus de synchronisation NTP à partir de l'interface CLI FXOS

<#root>

```
FPR4100#
```

```
connect fxos

FPR4100(fxos)#

ntp sync-retry
```

Effectuez des captures sur l'interface de gestion du châssis avec l'outil de commande CLI ethanalyzer.

Cause possible

- Problèmes de connectivité intermittents entre FXOS et le serveur NTP

Défauts associés

Recherchez les défauts connus/corrigés dans les notes de version.

Informations connexes

- Guides de configuration FXOS
- Résolution des problèmes liés au protocole NTP (Network Time Protocol) sur les systèmes Firepower

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.