

Configuration et dépannage des paramètres NTP sur les appliances Firepower

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[NTP sur FPR 41xx/9300](#)

[NTP sur FPR 1xxx/2100](#)

[Configuration du protocole NTP sur les appliances FPR 1xxx/2100/41xx/9300](#)

[Vérifier](#)

[Vérification de la synchronisation NTP sur les appareils FPR41xx/9300](#)

[Vérification de la configuration NTP sur les appareils FPR41xx/9300](#)

[Vérification de la synchronisation NTP entre MIO et le périphérique logique \(lame\) sur les appareils FPR41xx/9300](#)

[Vérification de la configuration NTP sur les appareils FPR1xxx/2100](#)

[Dépannage des problèmes courants](#)

[1. FXOS ne peut pas résoudre le nom d'hôte du serveur NTP](#)

[2. Problèmes de connectivité entre FXOS et le serveur NTP sur le port UDP 123](#)

[3. Problèmes de connectivité intermittente entre FXOS et le serveur NTP](#)

[Défauts associés](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer, vérifier et dépanner le protocole NTP (Network Time Protocol) sur les appliances Firepower FXOS.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

- FPR4140 qui exécute FXOS 2.3(1.130) et 2.8(1.105)
- FPR2110 qui exécute le mode plate-forme ASA
- FPR1140 qui exécute le mode appliance ASA

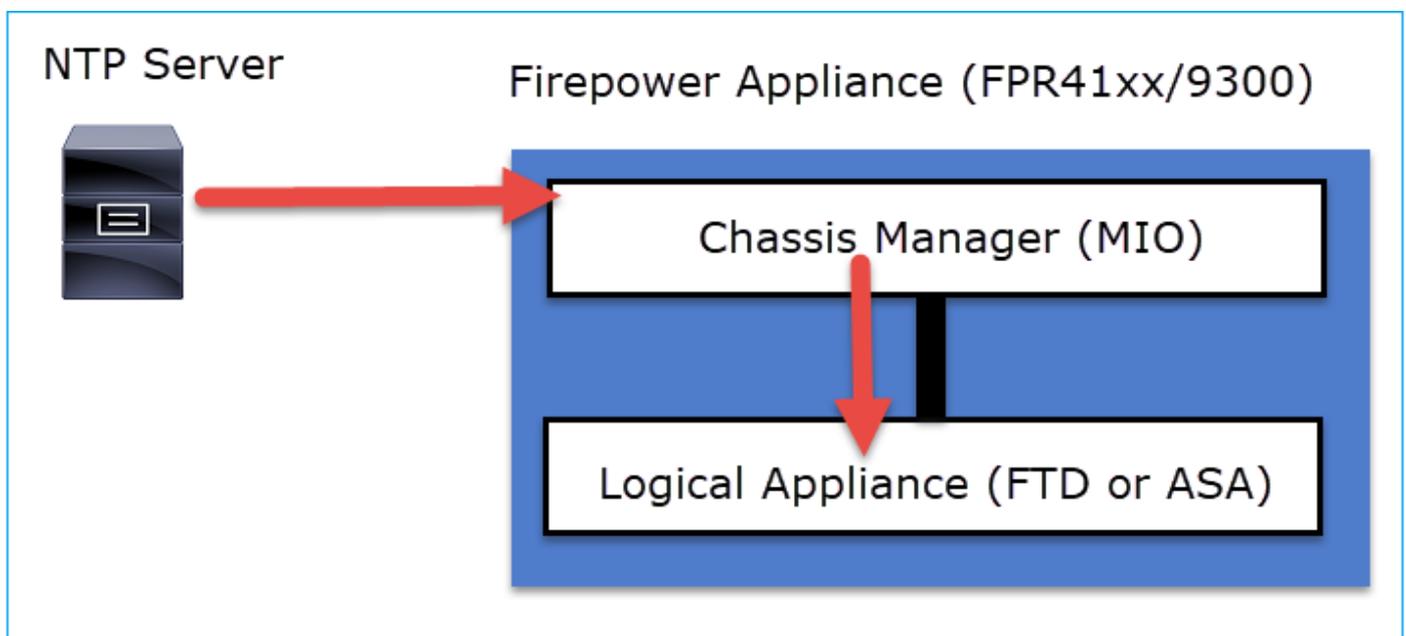
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Sur Firepower, le fonctionnement du protocole NTP dépend de la plate-forme.

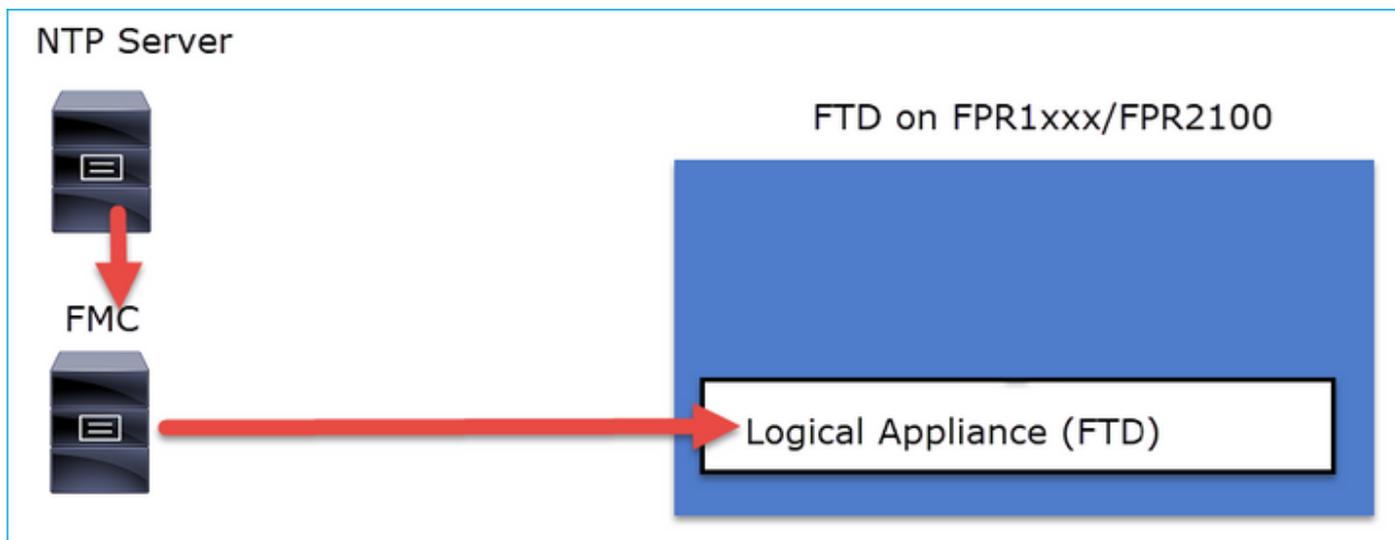
FPR41xx/FPR9300

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.



FPR1xxx/FPR2100

Sur FTD, le temps est pris à partir du FMC :



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](#)

Additional Information

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

Versions NTP prises en charge sur FXOS :

- FXOS 10.2.2.7 et versions ultérieures utilisent NTP version 3
- FXOS plus ancien que 10.2.2.7 utilise NTP version 2

Version prise en charge modifiée en raison du bogue Cisco ID [CSCve58269](#) - NTP : remplacer v2 par v3

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

Configurer

NTP sur FPR 41xx/9300

Points clés

- Pour configurer le protocole NTP sur un appareil Firepower 41xx/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.
- Actuellement, il n'y a aucune possibilité de synchroniser NTP sur FTD avec Firepower 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 Firepower 41xx/9300.
- Une configuration NTP appropriée est requise pour une installation de licence Smart réussie.

NTP sur FPR 1xxx/2100

- Pour configurer NTP sur un appareil Firepower 1xxx/2100, accédez à l'onglet **Platform Settings** à partir de Firepower Chassis Manager (FCM), Firepower for ASA en mode Platform.
- Dans le cas d'un ASA en mode Plate-forme, le NTP sur le périphérique logique est synchronisé avec le MIO.
- Configurez les paramètres NTP sur l'application logique elle-même. L'ASA en mode Appliance ou en cas de gestion FTD sur le boîtier à partir du Gestionnaire de périphériques Firepower (FDM).
- Si le FTD est géré par le FMC (gestion off-box), configurez le NTP sur le FMC.

Remarque : sur les versions postérieures à la version 9.13(1), vous pouvez exécuter Firepower 1xxx/2100 pour ASA dans les modes suivants : Appliance mode (mode par défaut) et Platform mode. 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).

Configuration du protocole NTP sur les appliances FPR 1xxx/2100/41xx/9300

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

The screenshot shows the 'Platform Settings' page for NTP configuration. The navigation menu on the left includes 'NTP' (highlighted with a red box and a '2'), 'SSH', 'SNMP', 'HTTPS', 'AAA', 'Syslog', 'DNS', 'FIPS and Common Criteria', and 'Access List'. The main content area is titled 'Time Synchronization' and 'Current Time'. It features a 'Set Time Source' section with two radio buttons: 'Set Time Manually' (selected) and 'Use NTP Server'. The 'Set Time Manually' section includes fields for 'Date' (11/26/2017), 'Time' (8:47 PM), and a 'Get System Time' button. The 'Use NTP Server' section has an 'NTP Server Authentication' checkbox (disabled) and an 'Add' button (highlighted with a red box and a '3'). The bottom of the page shows a table with columns for 'NTP Server', 'Server Sta', and 'Actions'.

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).

Add NTP Server

NTP Server *

Authentication Key

Authentication Value

Remarque : vous pouvez configurer jusqu'à 4 serveurs NTP

Vérifier

Vérification de la synchronisation NTP sur les appareils FPR41xx/9300

Surveillez l'état du serveur.



Référence État du serveur

- Non disponible : état par défaut affiché immédiatement après la configuration du serveur NTP.
- Inaccessible/non valide : affiché 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 temporelle non défini, etc.
- Synchronisation en cours : le serveur est accessible et prend en charge le protocole NTP, la convergence de l'heure initiale est toujours en cours et n'est pas encore terminée.
- Synchronized : 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'apppliance 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.
- Outlier : un serveur NTP qui est rejeté en raison d'une grande différence (décalage temporel et délai aller-retour) par rapport au reste des serveurs NTP.

Vérification de la configuration NTP sur les appareils FPR41xx/9300

Vérifiez l'état de l'homologue NTP :

```
FPR4100-8-A# connect fxos
FPR4100-8-A(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 :

```
FPR4100-8-A# scope system
FPR4100-8-A /system # scope services
FPR4100-8-A /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 :

```
FPR4100-8-A# 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 :

```
FPR4100-8-A# 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 de la synchronisation NTP entre MIO et le périphérique logique (lame) sur les appareils FPR41xx/9300

Sur le FPR41xx/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, en fonction de cela, elle indique si elle est synchronisée 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 :

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

Vérification de la configuration NTP sur les appareils FPR1xxx/2100

Attention : ceci s'applique uniquement aux appliances FPR1xxx/2100 pour ASA en mode Plate-forme.

```
firepower-2140# scope system
firepower-2140 /system # scope services
firepower-2140 /system/services # show ntp-server detail
```

```
NTP server hostname:
Name: 172.31.201.67
Time Sync Status: Time Synchronized
Error Msg:
```

```
Name: ntp.esl.cisco.com
Time Sync Status: Candidate
Error Msg:
```

Dépannage des problèmes courants

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

L'interface utilisateur FCM affiche :

+ Add		
NTP Server	Server Status	Actions
ntp.esl.cisco.com	Unreachable/Invalid 	 

Action recommandée

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

```
KSEC-FPR4100-8-A(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 :

+ Add		
NTP Server	Server Status	Actions
cisco.com	Unreachable/Invalid 	 

Action recommandée

Attention : la capture d'analyseur Ethernet sur l'interface de gestion du châssis est uniquement disponible sur les appliances FPR41xx/9300.

Effectuez des captures sur l'interface de gestion du châssis et vérifiez la communication bidirectionnelle sur le port UDP 123 :

```
KSEC- FPR4100-8-A(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 :

NTP Server	Server Status	Actions
ntp.esl.cisco.com	Unreachable/Invalid 	 

Actions recommandées

Attention : uniquement pour les appareils FPR41xx/9300.

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

```
FPR4100-8-A# connect fxos
FPR4100-8-A(fxos)# ntp sync-retry
```

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

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.