配置Firepower裝置上的NTP設定並對其進行故障排除

目錄

簡介

本文檔介紹如何配置、驗證和排除Firepower FXOS裝置上的網路時間協定(NTP)故障。

必要條件

需求

本文件沒有特定需求。

採用元件

- 執行FXOS 2.3(1.130)和2.8(1.105)的FPR4140
- 運行ASA平台模式的FPR2110
- 運行ASA裝置模式的FPR1140

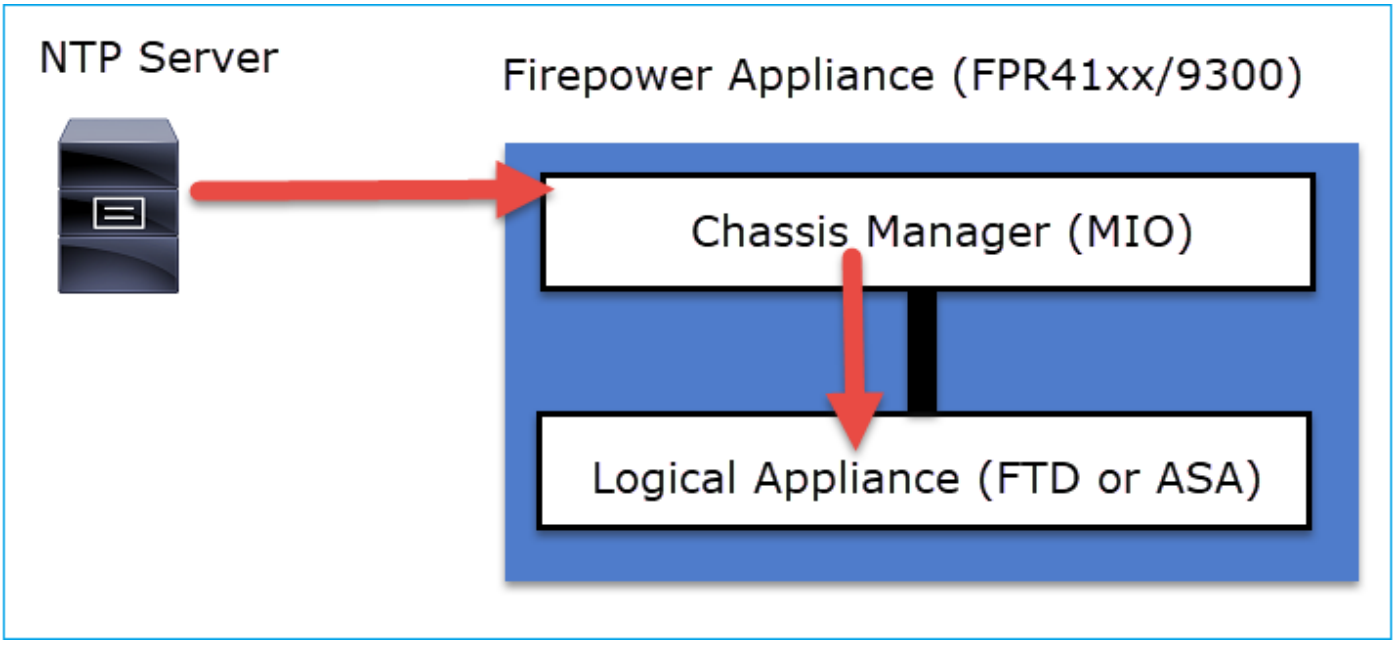
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

在Firepower上，NTP操作取決於平台。

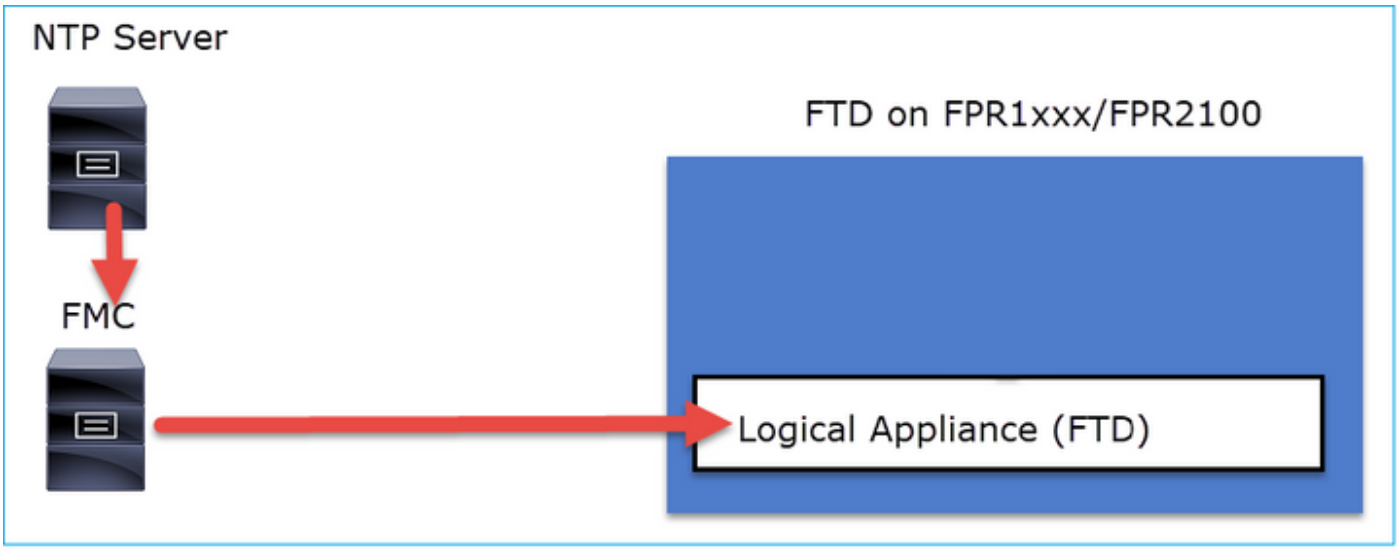
FPR41xx/FPR9300

ASA或FTD時間取自機箱Firepower機箱管理器(FCM)管理輸入/輸出(MIO)。MIO是Firepower機箱的管理引擎。



FPR1xxx/FPR2100

在FTD上，時間取自FMC：



對於此部署，請檢查以下文檔：

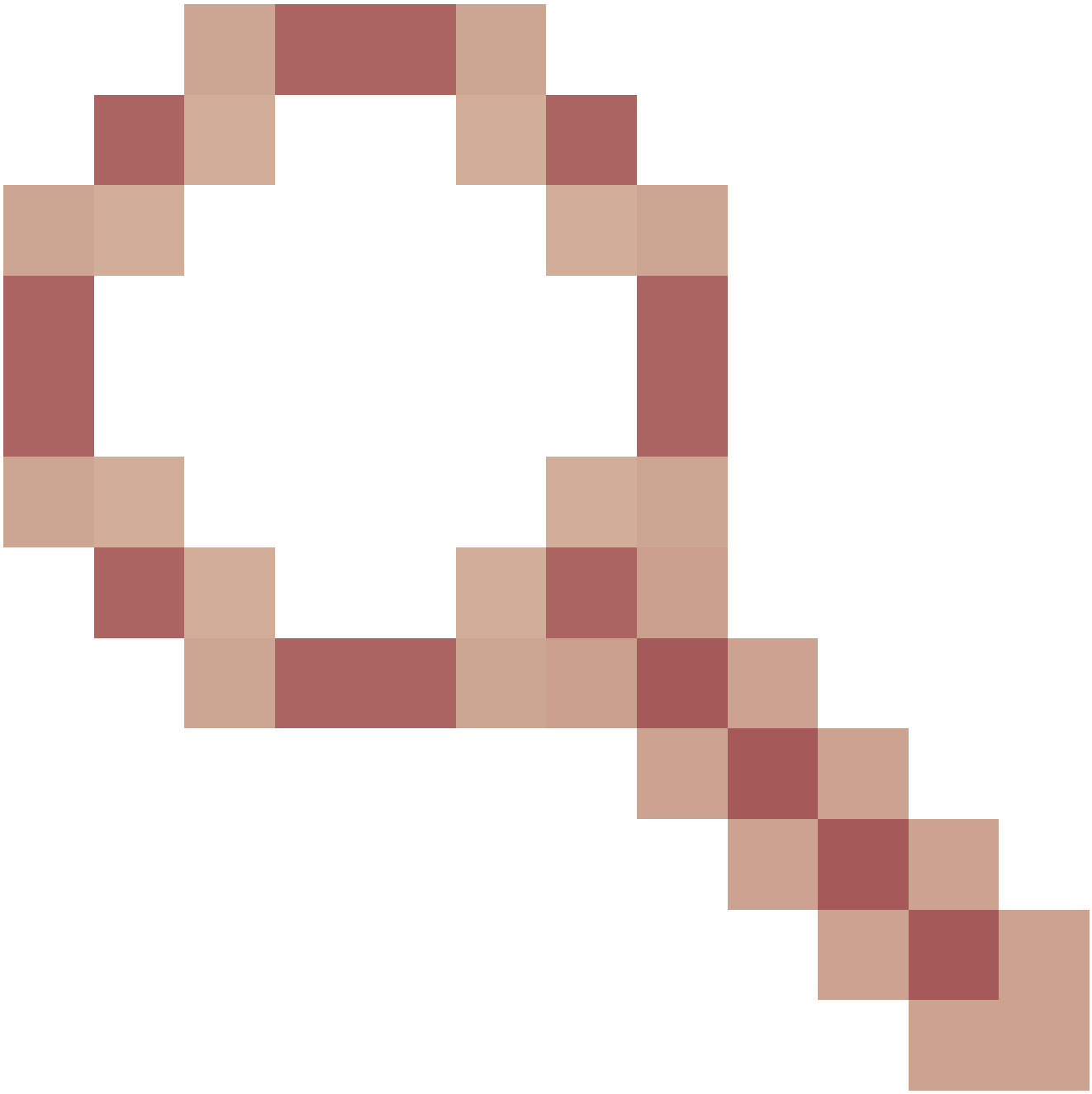
- 為威脅防禦配置NTP時間同步
- 排除Firepower系統上的網路時間協定(NTP)故障

其他資訊

NTP用於時間同步。NTP使用UDP埠號123作為傳輸。

FXOS上支援的NTP版本：

- FXOS 10.2.2.7及更高版本使用NTP版本3
- 早於10.2.2.7的FXOS使用NTP版本2



支援的版本因思科漏洞ID CSCve58269而更改- NTP：將v2更改為v3

注意：NTP第4版不受官方支援。NTP版本4與NTP版本3向後相容。

設定

FPR 41xx/9300上的NTP

要點

- 要在Firepower 41xx/9300裝置上配置NTP，請登入FCM並導航到Platform Settings頁籤。

- 邏輯裝置（ASA或FTD）上的NTP與MIO同步。
- 目前，無法將FTD上的NTP與Firepower管理中心(FMC)同步，即使您選擇該選項，FTD上的NTP也會與MIO同步。因此，強烈建議FMC和FCM使用同一個NTP伺服器。
- FMC不是全面的NTP伺服器。它只能透過sftunnel為其受管裝置提供時間設定。因此，它不能用作Firepower 41xx/9300機箱的NTP伺服器。
- 需要正確的NTP配置才能成功安裝智慧許可證。

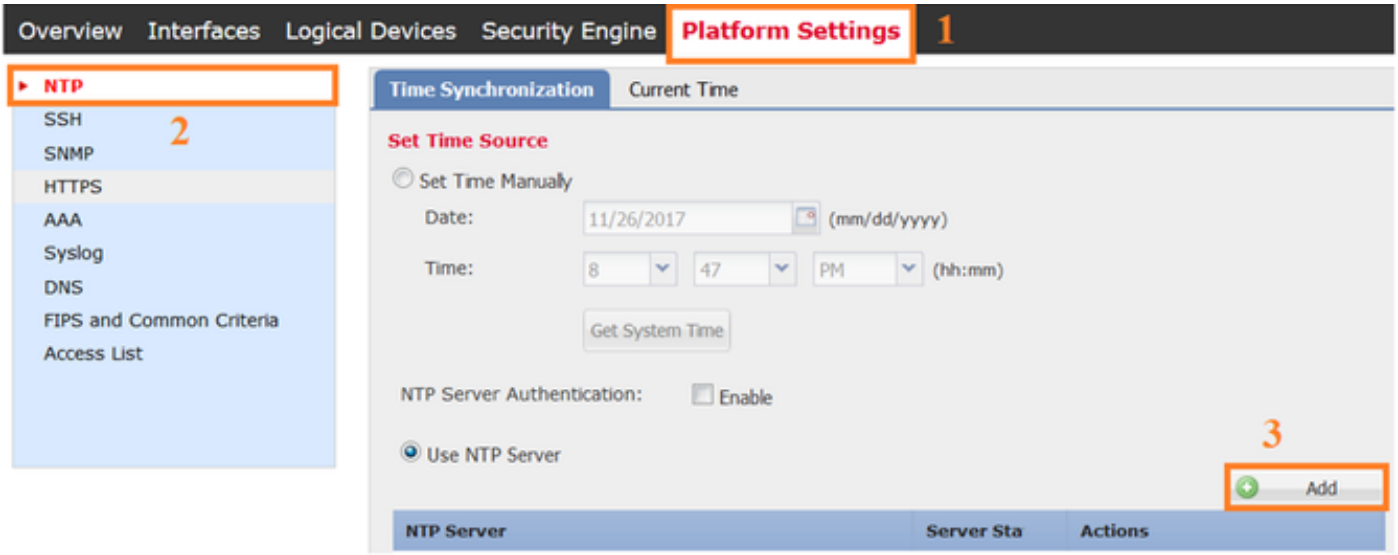
FPR 1xxx/2100上的NTP

- 要在Firepower 1xxx/2100裝置上配置NTP，請從Firepower機箱管理器(FCM)和平台模式下的Firepower for ASA導航到Platform Settings頁籤。
- 在ASA處於平台模式的情況下，邏輯裝置上的NTP與MIO同步。
- 在邏輯應用程式自身上配置NTP設定。ASA處於裝置模式，或者從Firepower裝置管理器(FDM)進行FTD內建管理。
- 如果FTD是由FMC （機上管理）管理，請在FMC上設定NTP。

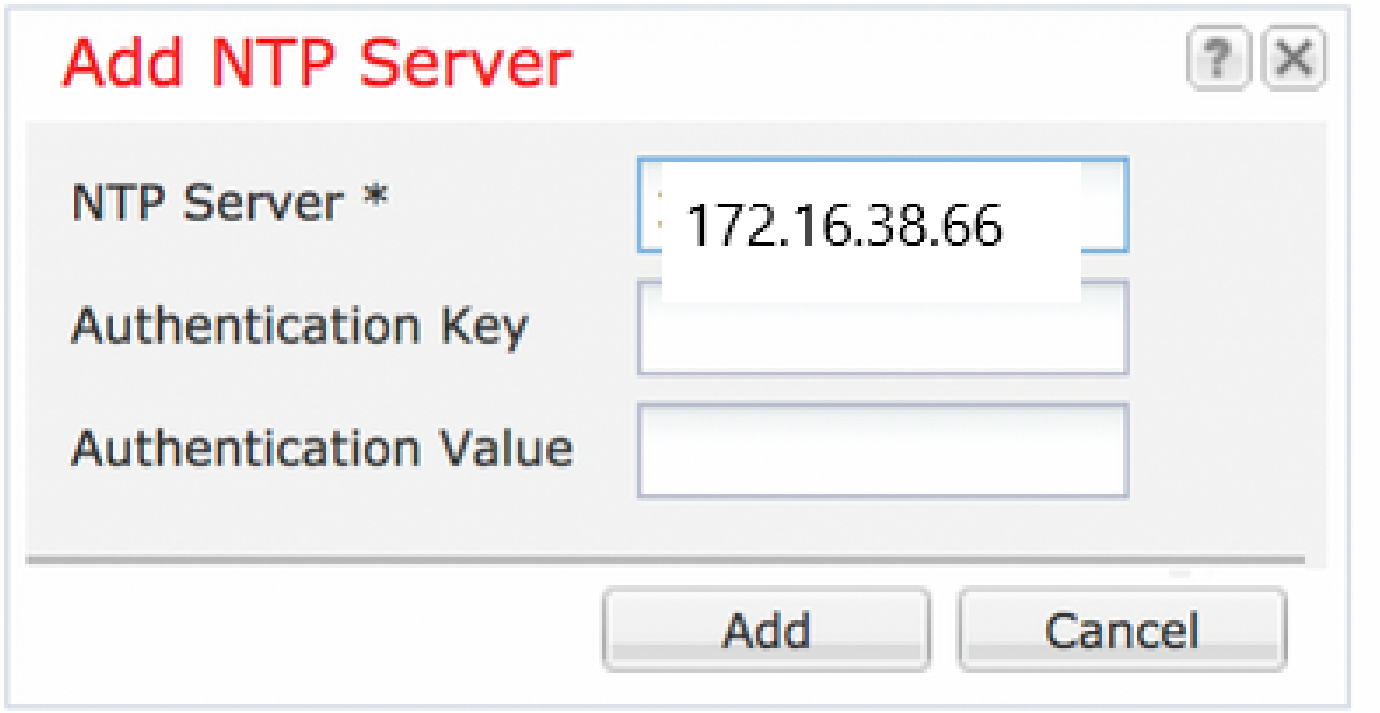
注意：在9.13(1)以後版本中，可以在以下模式下運行Firepower 1xxx/2100 for ASA：裝置模式（預設）和平台模式。裝置模式允許您在ASA上配置所有設定，包括NTP。FXOS CLI僅提供高級故障排除命令。另一方面，在平台模式下，您必須在機箱管理器(FCM)中配置基本設定（包括NTP）和硬體介面設定。

在FPR 1xxx/2100/41xx/9300裝置上配置NTP

步驟 1.使用本地使用者憑證登入到Firepower機箱管理器GUI，然後導航到平台設定 > NTP。選擇Add按鈕：



步驟 2.指定NTP伺服器IP地址或主機名（如果您使用NTP伺服器的主機名，則必須配置DNS伺服器）。



注意：您最多可以配置4個NTP伺服器

驗證

驗證FPR41xx/9300裝置上的NTP同步

監控伺服器狀態。

伺服器狀態參照

- 不可用：在NTP伺服器配置後立即顯示的預設狀態。
- 無法連線/無效：在下列案例中顯示：
  - NTP協定無法訪問NTP伺服器IP地址或主機名時。
  - 可訪問NTP伺服器IP地址或主機名，但遠端主機不是NTP伺服器時。
  - 其他內部失敗，例如查詢無法執行、擲回例外狀況、發生未定義的時間同步狀態等等。
- 同步處理進行中：伺服器可連線並支援NTP通訊協定，初始時間收斂仍在進行中，尚未完成。
- 已同步：主機被宣告為系統同步對等體，並且時間時鐘與其同步。
- 候選：主機是候選（備用）對等體。候選NTP伺服器表示它是有效伺服器並且已與Firepower裝置成功通訊，但該模組已與另一台NTP伺服器同步，因此它是備用伺服器。如果當前同步對等體被刪除，則可以將其選為下一個同步對等體。
- 異常值：由於與其他NTP伺服器相比存在較大差異（時間偏移和往返延遲）而被丟棄的NTP伺服器。

驗證FPR41xx/9300裝置上的NTP配置

驗證NTP對等體狀態：

```
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
```

驗證NTP伺服器配置和同步：

```
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:
```

驗證NTP關聯：

```
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
```

驗證NTP sysinfo：

```
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
```

驗證FPR41xx/9300裝置上MIO和邏輯裝置（刀片）之間的NTP同步

在FPR41xx/9300上，NTP設定透過MIO（機箱）推送到FTD。無法從FTD CLI或FMC UI進行NTP設定。

每個FTD刀鋒使用內部參考ID 203.0.113.126與MIO進行時間同步通訊，並根據此資訊顯示是否同步。FTD CLI會反映此情況。本示例中的NTP IP是內部ref-id，而不是實際的NTP伺服器IP。在FCM中更改NTP伺服器IP不會影響此輸出，因為reference-id始終相同：

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

驗證FPR1xxx/2100裝置上的NTP配置

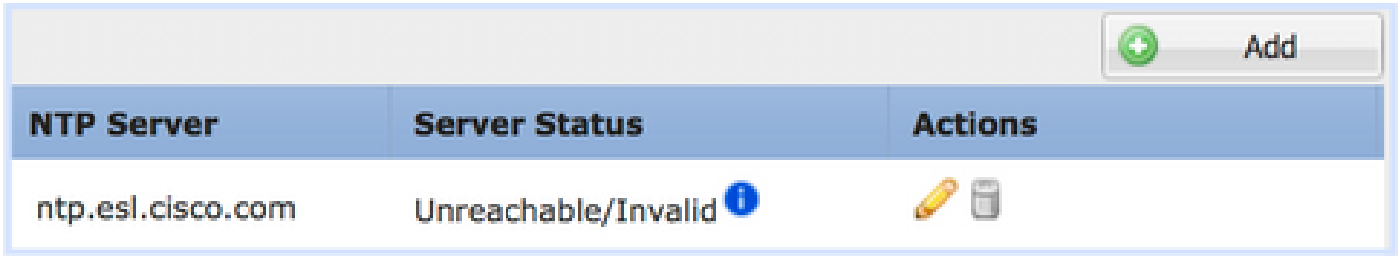
⚠ 注意：這只適用於在平台模式下用於ASA的FPR1xxx/2100裝置。

```
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:
```

排除常見問題

1. FXOS無法解析NTP伺服器主機名

FCM UI顯示：



建議的動作

使用ping命令檢驗NTP伺服器主機名解析

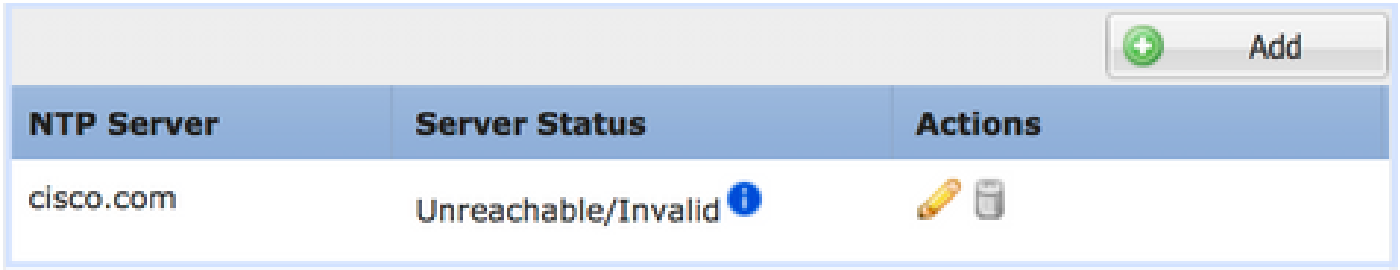
```
KSEC-FPR4100-8-A(local-mgmt)# ping ntp.esl.cisco.com
Invalid Host Name.
```

可能原因

- 未配置DNS伺服器。
- DNS伺服器無法解析主機名。

2. FXOS - UDP埠123上的NTP伺服器之間的連線問題

FCM UI顯示：



建議的動作

⚠ 注意：機箱管理介面上的Ethanalyzer捕獲僅在FPR41xx/9300裝置上可用。

獲取機箱管理介面的捕獲資訊，並驗證UDP埠123上的雙向通訊：

<#root>

```
KSEC- FPR4100-8-A(fxos)# ethanalyzer local interface mgmt capture-filter "udp port 123"
Capturing on 'eth0'
```

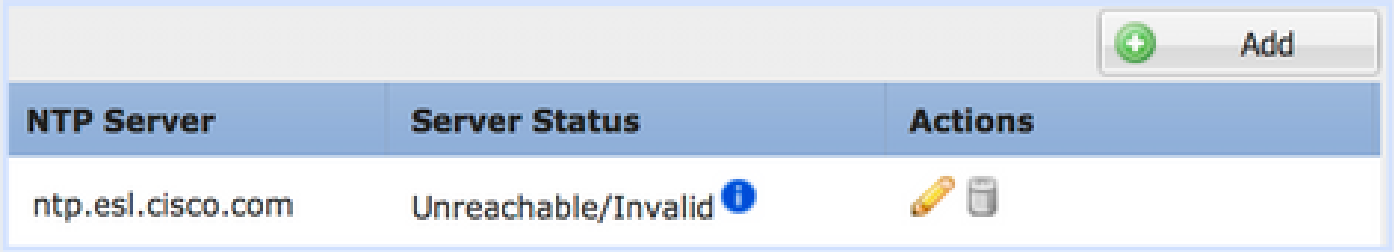
```
1 2020-04-30 20:09:54.150237760 10.62.148.196 → 172.16.4.161 NTP 90 NTP Version 3, client
2 2020-04-30 20:14:14.150172804 10.62.148.196 → 172.16.4.161 NTP 90 NTP Version 3, client
3 2020-04-30 20:23:13.150171682 10.62.148.196 → 172.16.4.161 NTP 90 NTP Version 3, client
```

可能原因

- 配置的伺服器不是NTP伺服器。
- 路徑中的裝置（例如防火牆）會封鎖或修改流量。

3. FXOS和NTP伺服器之間的間歇性連線問題

FCM UI顯示：



建議的動作

⚠ 注意：僅適用於FPR41xx/9300裝置。

從FXOS CLI啟動NTP同步過程

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

使用ethanalyzer CLI命令工具捕獲機箱管理介面。

可能起因

- FXOS - NTP伺服器之間出現間歇性連線問題

相關瑕疵

檢查「版本說明」以瞭解已知/已修復的缺陷。

相關資訊

- FXOS 組態設定指南
- 排除Firepower系統上的網路時間協定(NTP)故障

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。