Firepower FXOS 어플라이언스에서 NTP(Network Time Protocol) 설정 구성, 확인 및 문제 해결

목차

소개

이 문서에서는 Firepower Appliance(FPR1xxx, FPR2100, FPR41xx, FPR9300)에서 NTP의 구성, 확인 및 문제 해결에 대해 설명합니다.

기고자: Anita Pietrzyk, Mikis Zafeiroudis, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

- FXOS 2.3(1.130) 및 2.8(1.105)을 실행하는 FPR4140
- ASA 플랫폼 모드를 실행하는 FPR2110
- ASA 어플라이언스 모드를 실행하는 FPR1140

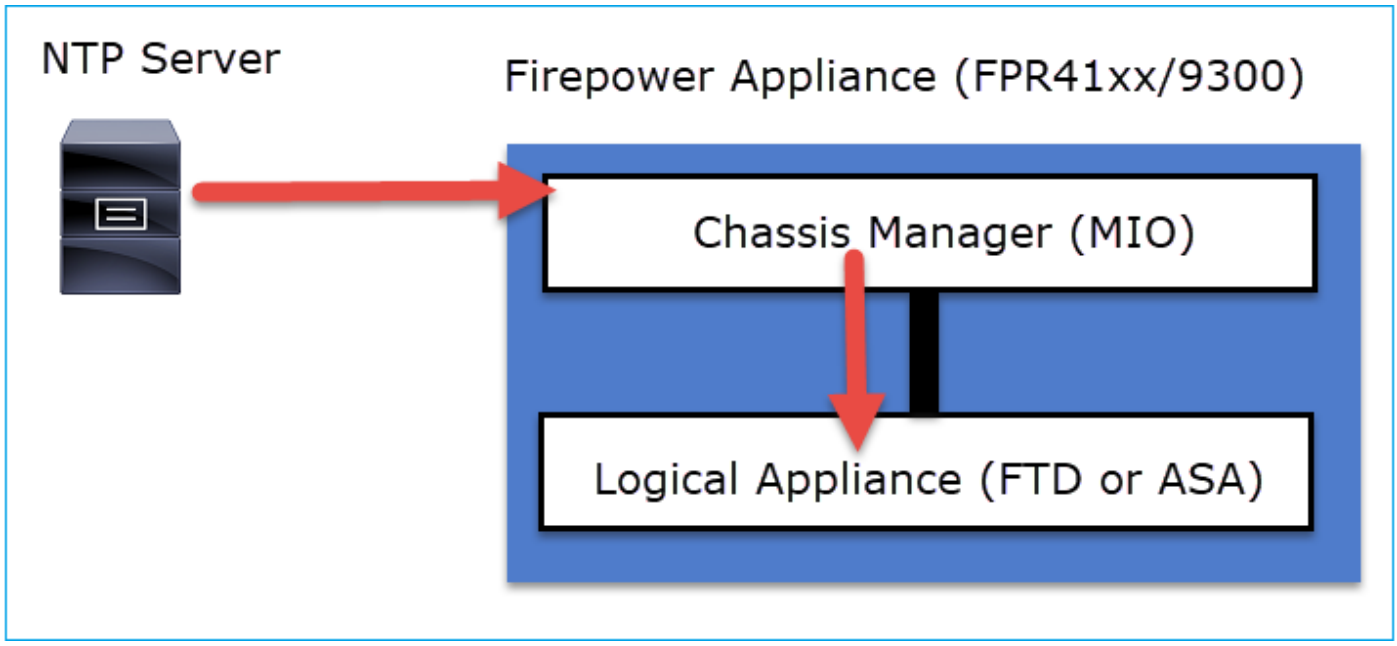
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

Firepower에서 NTP 작업은 플랫폼에 따라 달라집니다.

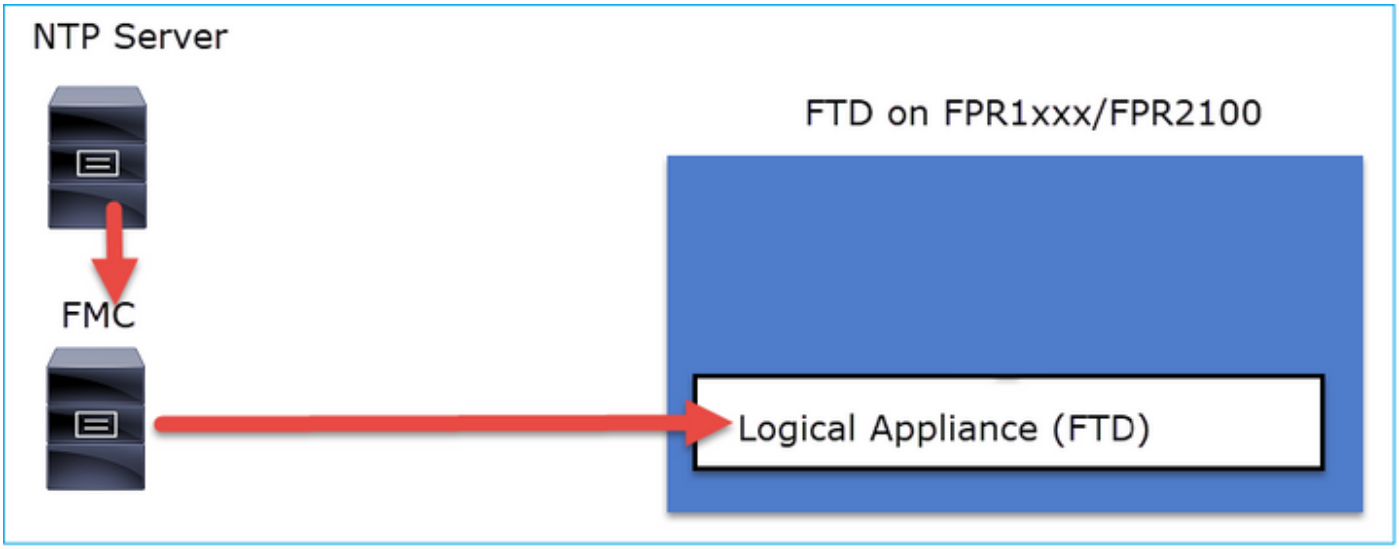
FPR41xx/FPR9300

ASA 또는 FTD 시간은 섀시 FCM(Firepower Chassis Manager) MIO(Management Input/Output)에서 가져옵니다.MIO는 Firepower 섀시의 수퍼바이저입니다.



FPR1xxx/FPR2100

FTD에 FMC에서 시간을 가져옵니다.



이 구축의 경우 다음 문서를 확인하십시오.

- 위협 방어를 위한 NTP 시간 동기화 구성
- Firepower Systems의 NTP(Network Time Protocol) 문제 해결

추가 정보

NTP는 시간 동기화에 사용됩니다.NTP는 UDP 포트 번호 123을 전송으로 사용합니다.

FXOS에서 지원되는 NTP 버전:

- **FXOS 2.2.2.7 이상에서는 NTP 버전 3 사용**
- **이전 FXOS가 2.2.2.7보다 오래된 NTP 버전 2 사용**

CSCve58269로 인해 지원되는 버전이 변경되었습니다. - NTP:v2를 v3로 변경

> **참고:NTP 버전 4는 공식적으로 지원되지 않습니다.NTP 버전 4는 NTP 버전 3과 역호환됩니다.**

구성

FPR 41xx/9300의 NTP

주요 내용

- Firepower 41xx/9300 어플라이언스에서 NTP를 구성하려면 FCM에 로그인하고 **Platform Settings** 탭으로 이동합니다.
- 논리적 디바이스(ASA 또는 FTD)의 NTP는 MIO와 동기화됩니다.
- 현재 FTD의 NTP를 FMC(Firepower Management Center)와 동기화할 가능성이 없습니다. 이 옵션을 선택해도 FTD의 NTP는 MIO와 동기화됩니다.따라서 FMC와 FCM은 동일한 NTP 서버를 사용하는 것이 좋습니다.
- FMC는 완전한 NTP 서버가 아닙니다.sftunnel을 통해 관리되는 디바이스에 시간 설정을 제공

할 수 있습니다.따라서 Firepower 41xx/9300 섀시의 NTP 서버로 사용할 수 없습니다.
- Smart License를 성공적으로 설치하려면 적절한 NTP 컨피그레이션이 필요합니다.

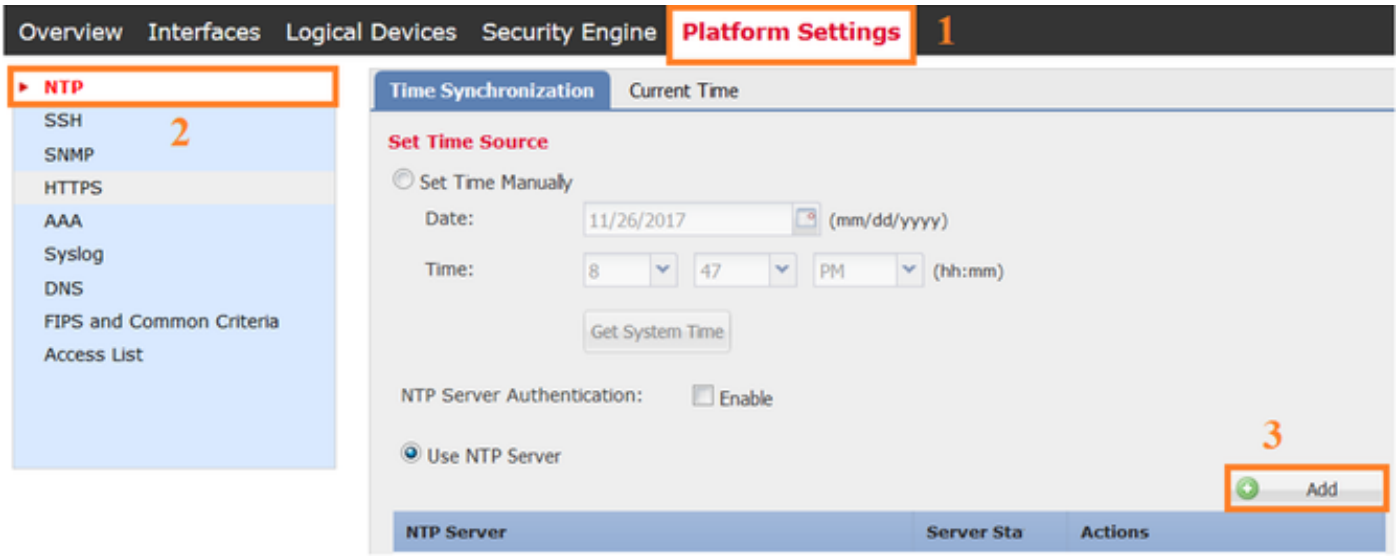
FPR의 NTP 1xxx/2100

- Firepower 1xxx/2100 어플라이언스에서 NTP를 구성하려면 FCM(Firepower Chassis Manager)의 **Platform Settings(플랫폼 설정)** 탭(플랫폼 모드의 ASA용 Firepower)으로 이동합니다.
- 플랫폼 모드의 ASA의 경우 논리적 디바이스의 NTP가 MIO와 동기화됩니다.
- 논리적 애플리케이션 자체에서 NTP 설정을 구성합니다.어플라이언스 모드의 ASA 또는 FDM(Firepower Device Manager)에서 FTD 온박스 관리를 수행하는 경우
- FTD가 FMC에 의해 관리되는 경우(오프박스 관리) FMC에서 NTP를 구성합니다.

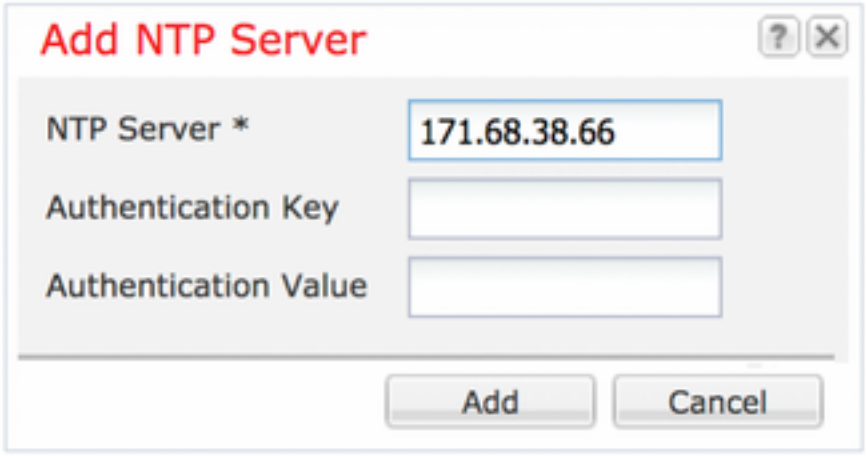
참고:9.13(1) 이후 버전에서는 다음 모드에서 ASA용 Firepower 1xxx/2100을 실행할 수 있습니다.어플라이언스 모드(기본값) 및 플랫폼 모드.어플라이언스 모드에서는 ASA에서 NTP를 비롯한 모든 설정을 구성할 수 있습니다.FXOS CLI에서는 고급 문제 해결 명령만 사용할 수 있습니다.반면 플랫폼 모드에서는 FCM(섀시 관리자)에서 기본 설정(NTP 포함) 및 하드웨어 인터페이스 설정을 구성해야 합니다.

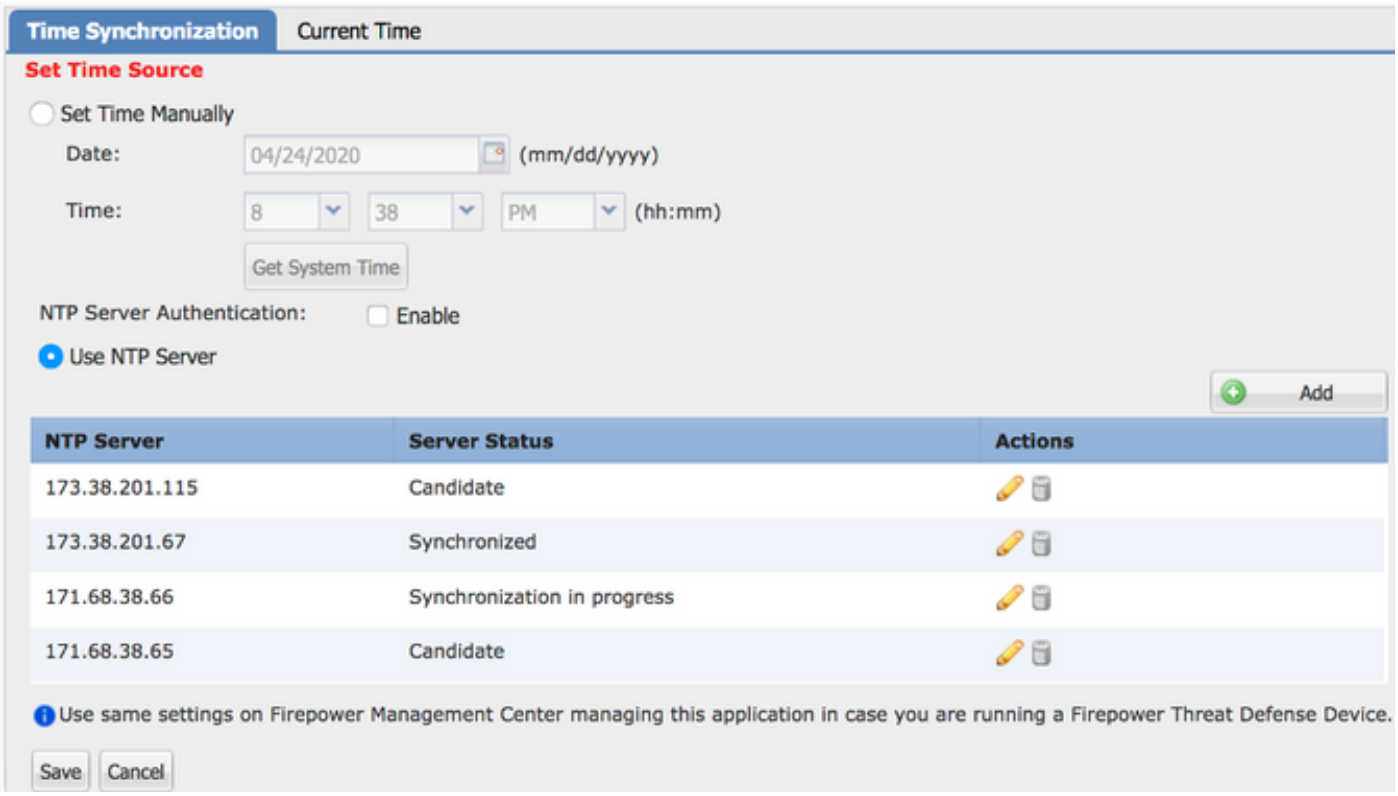
FPR 1xxx/2100/41xx/9300 어플라이언스에서 NTP 구성

1단계. 로컬 사용자 자격 증명으로 Firepower Chassis Manager GUI에 로그인하고 Platform Settings(플랫폼 설정) > NTP로 이동합니다.추가 버튼을 선택합니다.



2단계. NTP 서버 IP 주소 또는 호스트 이름을 지정합니다(NTP 서버에 호스트 이름을 사용하는 경우 DNS 서버를 구성해야 함).



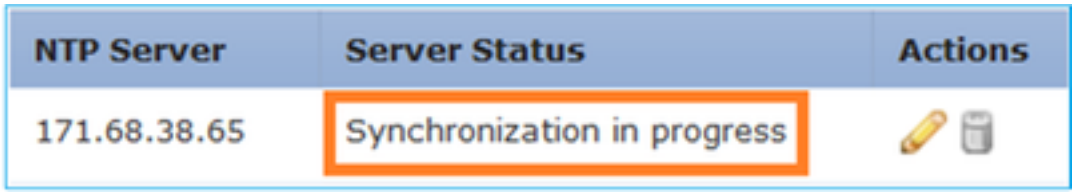


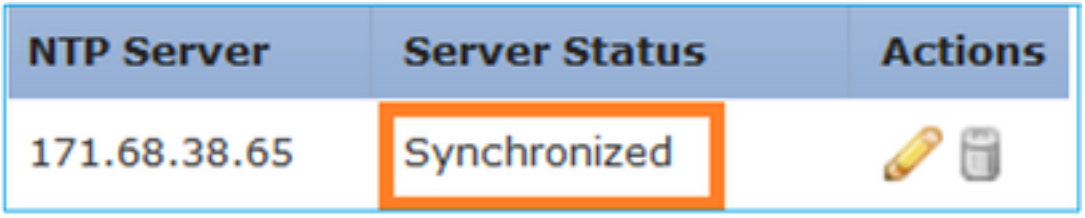
참고:최대 4개의 NTP 서버를 구성할 수 있습니다.

다음을 확인합니다.

FPR41xx/9300 어플라이언스에서 NTP 동기화 확인

서버 **상태 모니터링**





서버 상태 참조

- **사용할 수 없음:NTP 서버 컨피그레이션 바로 다음에 표시되는 기본 상태.**
- **연결할 수 없음/유효하지 않음: 다음 시나리오에서 볼 수 있습니다.** NTP 프로토콜에서 NTP 서버 IP 주소 또는 호스트 이름에 연결할 수 없는 경우.NTP 서버 IP 주소 또는 호스트 이름에 연결할 수 있지만 원격 호스트가 NTP 서버가 아닌 경우쿼리 실행 실패, 예외 발생, 정의되지 않은 시간 동기화 상태 발생 등 기타 내부 오류
- **동기화 진행 중:서버에 연결할 수 있으며 NTP 프로토콜을 지원합니다. 초기 시간 통합이 계속 진행 중이며 아직 완료되지 않았습니다.**
- **동기화됨:호스트가 시스템 동기화 피어로 선언되고 시간 클럭이 동기화됩니다.**
- **후보자:호스트는 후보(대기) 피어입니다.후보 NTP 서버는 유효한 서버이며 Firepower 어플라이언스와 성공적으로 통신했지만 모듈이 다른 NTP 서버와 동기화되어 대기 서버임을 의미합니다.현재 피어가 삭제된 경우 다음 동기화 피어로 선택할 수 있습니다.**
- **외부:다른 NTP 서버와 비교하여 큰 차이(시간 오프셋 및 왕복 지연)로 인해 삭제된 NTP 서버.**

FPR41xx/9300 어플라이언스에서 NTP 컨피그레이션 확인

NTP 피어 상태를 확인합니다.

```
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
-------------------------------------------------------------------------------
=171.68.38.66           10.62.148.196           1 1024      17   0.20996
*173.38.201.67 10.62.148.196 1 1024 377 0.03035
=171.68.38.65           10.62.148.196           1 1024     377   0.19914
=173.38.201.115         10.62.148.196           1 1024     377   0.02905
```

NTP 서버 컨피그레이션 및 동기화를 확인합니다.

```
FPR4100-8-A# scope system
FPR4100-8-A /system # scope services
FPR4100-8-A /system/services # show ntp-server detail
NTP server hostname: Name: 171.68.38.65
    Time Sync Status: Candidate
    NTP SHA-1 key id: 0
    Error Msg:

    Name: 171.68.38.66
    Time Sync Status: Time Sync In Progress
    NTP SHA-1 key id: 0
    Error Msg:
```

```
    Name: 173.38.201.115
    Time Sync Status: Candidate
    NTP SHA-1 key id: 0
    Error Msg:

    Name: 173.38.201.67
    Time Sync Status: Time Synchronized
    NTP SHA-1 key id: 0
    Error Msg:
```

NTP 연결을 확인합니다.

```
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   173.38.201.67   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=173.38.201.67,
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
```

NTP sysinfo를 확인합니다.

```
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-WR6.0.0.29_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
```

FPR41xx/9300 어플라이언스에서 MIO와 논리적 디바이스(블레이드) 간의 NTP 동기

화 확인

FPR41xx/9300에서 NTP 설정은 MIO(섀시)를 통해 FTD로 푸시됩니다. FTD CLI 또는 FMC UI의 NTP 컨피그레이션은 사용할 수 없습니다.

각 FTD 블레이드는 **내부 참조 ID**를 사용합니다.**203.0.116.126**을 사용하여 시간 동기화를 위해 MIO와 통신하고 이를 기반으로 동기화되었는지 여부를 표시합니다. FTD CLI는 이를 반영합니다 .이 예에서 NTP IP는 실제 NTP 서버 IP가 아니라 내부 ref-id입니다.FCM에서 NTP 서버 IP를 변경해도 reference-id는 항상 동일하므로 이 출력에 영향을 주지 않습니다.

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

FPR1xxx/2100 어플라이언스에서 NTP 컨피그레이션 확인

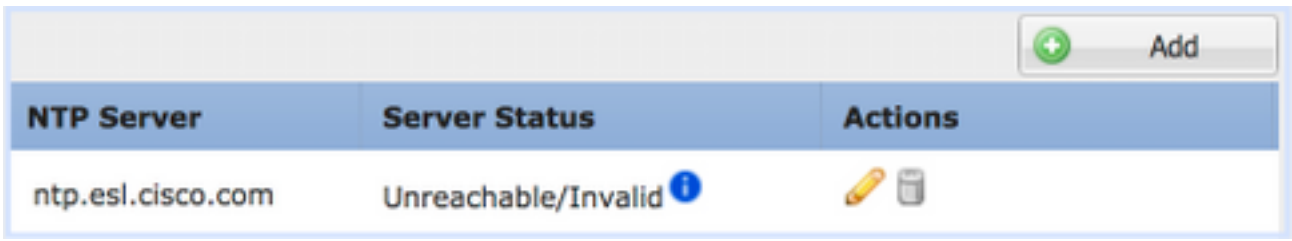
> **주의:이는 플랫폼 모드에서 ASA용 FPR1xxx/2100 어플라이언스에만 적용됩니다.**

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

NTP server hostname:
    Name: 173.38.201.67
    Time Sync Status: Time Synchronized
    Error Msg:

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

일반적인 문제 해결

1. FXOS가 NTP 서버 호스트 이름을 확인할 수 없음

FCM UI에는 다음이 표시됩니다.



권장 작업

ping 명령을 사용하여 NTP 서버 호스트 이름 확인 확인

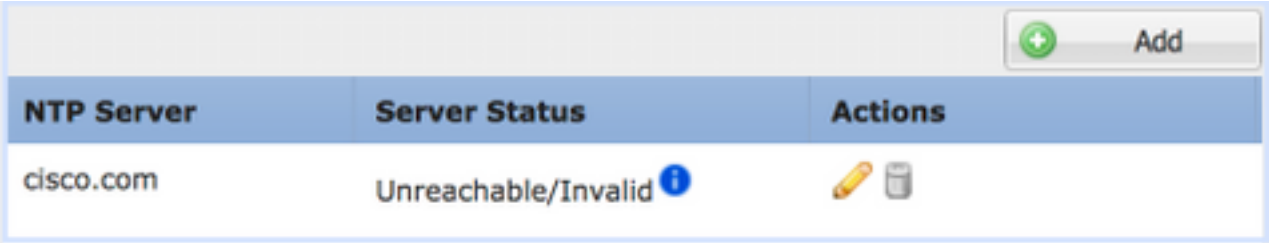
```
KSEC-FPR4100-8-A(local-mgmt)# ping ntp.esl.cisco.com
Invalid Host Name.
```

가능한 원인

- DNS 서버가 구성되지 않았습니다.
- DNS 서버가 호스트 이름을 확인할 수 없습니다.

2. FXOS 간 연결 문제 - UDP 포트 123의 NTP 서버

FCM UI에는 다음이 표시됩니다.



권장 작업

> **주의:섀시 관리 인터페이스의 Ethanalyzer 캡처는 FPR41xx/9300 어플라이언스에서만 사용할 수 있습니다.**

섀시 관리 인터페이스에서 캡처를 가져오고 UDP 포트 123에서 양방향 통신을 확인합니다.

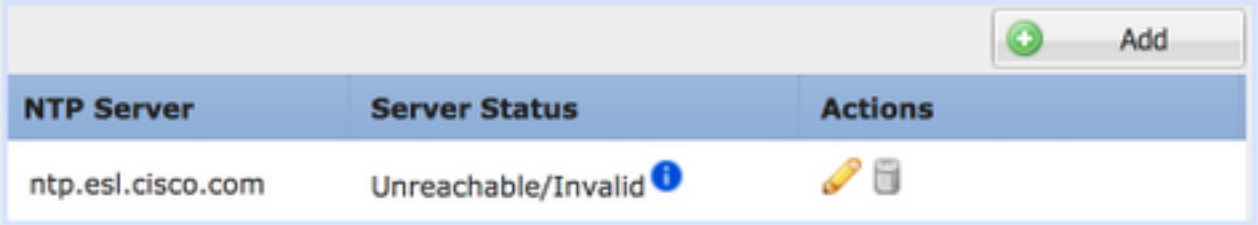
```
KSEC- FPR4100-8-A(fxos)# ethanalyzer local interface mgmt capture-filter "udp port 123"
Capturing on 'eth0'
1 2020-04-30 20:09:54.150237760 10.62.148.196  72.163.4.161 NTP 90 NTP Version 3, client
2 2020-04-30 20:14:14.150172804 10.62.148.196  72.163.4.161 NTP 90 NTP Version 3, client
3 2020-04-30 20:23:13.150171682 10.62.148.196  72.163.4.161 NTP 90 NTP Version 3, client
```

가능한 원인

- 구성된 서버가 NTP 서버가 아닙니다.
- 경로의 디바이스(예: 방화벽)가 트래픽을 차단하거나 수정합니다.

3. FXOS와 NTP 서버 간의 간헐적인 연결 문제

FCM UI에는 다음이 표시됩니다.



권장 작업

주의:FPR41xx/9300 어플라이언스에만 적용됩니다.

FXOS CLI에서 NTP 동기화 프로세스 시작

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

Ethanalyzer CLI 명령 툴을 사용하여 섀시 관리 인터페이스**에서** 캡처를 수행합니다.

가능한 원인

- FXOS - NTP 서버 간 간헐적인 연결 문제

관련 결함

Release Notes에서 알려진/고정 결함이 있는지 확인합니다.

관련 정보

- FXOS 컨피그레이션 가이드
- Firepower Systems의 NTP(Network Time Protocol) 문제 해결