Definir e solucionar problemas de configurações de NTP no Firepower e no Secure Firewall

Contents

- Introdução
- Pré-requisitos
  - Requisitos
  - Componentes Utilizados
- Informações de Apoio
- Configurar
  - NTP em FPR4100/9300
    - Pontos principais
  - NTP em CSF200/1200/3100/4200/6100
  - Configure o NTP em FPR2100/4100/9300
- Verificar
  - Verifique a sincronização de NTP em dispositivos FPR4100/9300
    - Referência de Status do Servidor
  - Verifique a sincronização de NTP entre o MIO e o dispositivo lógico (blade) nos dispositivos FPR4100/9300
- Solucionar problemas comuns
  - 1. FXOS não Pode Resolver o Nome de Host do Servidor NTP
    - Ação recomendada
    - Possíveis causas
  - 2. Problemas de Conectividade entre o FXOS e o Servidor NTP na Porta UDP 123
    - Ação recomendada
    - Possíveis causas
  - 3. Problemas de conectividade intermitente entre o servidor FXOS e NTP
    - Ações recomendadas
    - Possível causa
- Defeitos relacionados
- Informações Relacionadas

Introdução

Este documento descreve como configurar, verificar e solucionar problemas do Network Time Protocol (NTP) nos dispositivos Cisco Firepower e Cisco Secure Firewall.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

- FPR4140 executando FXOS 2.3(1.130) e 2.8(1.105).
- FPR2110 executando o modo de plataforma ASA.
- FPR1140 executando o modo de dispositivo ASA.
- CSF220 executando o FTD 10.x.

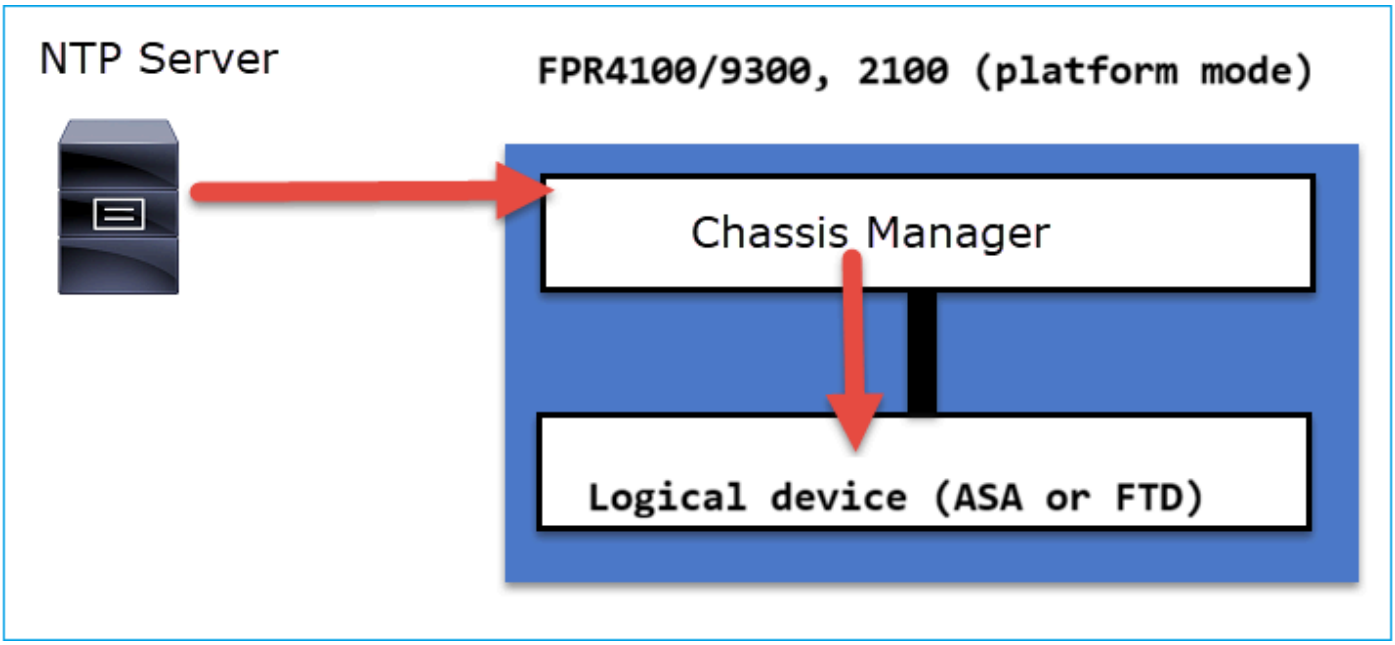
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A operação do NTP depende da plataforma.

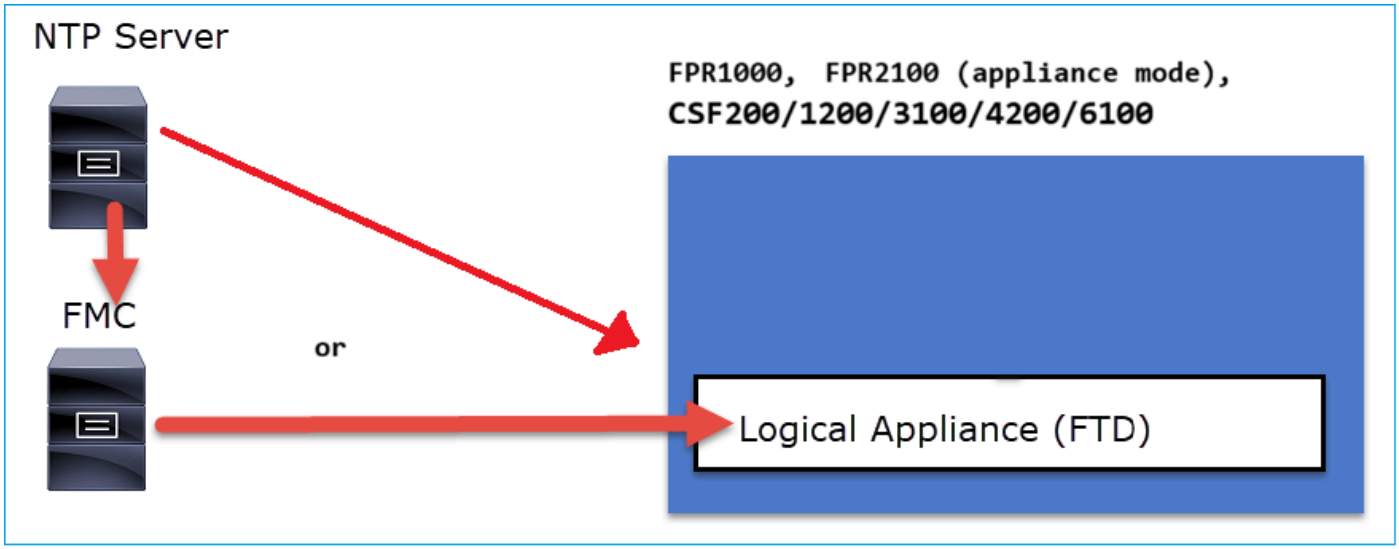
FPR4100/FPR9300, FPR2100 (modo de plataforma)

O tempo do ASA ou do FTD é obtido do MIO (Management Input/Output) do Firepower Chassis Manager (FCM) do chassi. O MIO é o supervisor do chassi Firepower.



FPR1000, FPR2100 (modo de dispositivo), CSF200/3100/4200/6100

No FTD, a hora é obtida no FMC ou em um servidor NTP:



Para esta implantação, verifique estes documentos:

- Configurar a sincronização de tempo do NTP para defesa contra ameaças
- Solucionar problemas com o Network Time Protocol (NTP) em sistemas Firepower

Informações adicionais:
O NTP é usado para sincronização de horário. O NTP usa como transporte o número de porta UDP 123.

Note: O NTP versão 4 não é oficialmente suportado. O NTP versão 4 é compatível com o NTP versão 3.

Configurar

NTP em FPR4100/9300

Pontos principais

- Para configurar o NTP em um dispositivo FPR4100/9300, faça login no FCM e navegue até a guia Configurações de plataforma.
- O NTP nos dispositivos lógicos (ASA ou FTD) é sincronizado com o MIO.
- Não há possibilidade de sincronizar o NTP no FTD com o Firewall Management Center (FMC), mesmo que você escolha essa opção, o NTP no FTD é sincronizado com o MIO. Portanto, é altamente recomendável que o FMC e o FCM usem o mesmo servidor NTP.
- O FMC não é um servidor NTP completo. Ele pode apenas fornecer configurações de tempo para seus dispositivos gerenciados através do túnel sf. Assim, ele não pode ser usado como o servidor NTP para o chassi FPR4100/9300.
- A configuração adequada do NTP é necessária para uma instalação de Smart License bem-sucedida.

NTP em CSF200/1200/3100/4200/6100

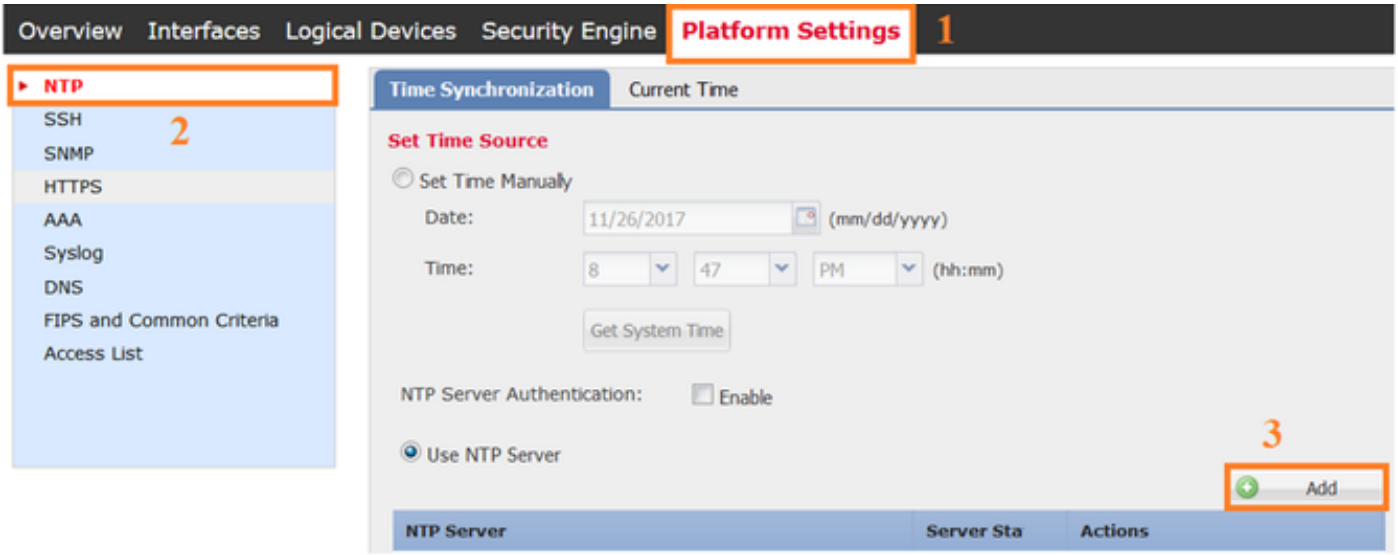
- Defina as configurações de NTP no próprio aplicativo lógico. O ASA no modo de dispositivo ou no caso de gerenciamento de FTD em pacote no Gerenciador de dispositivos de firewall (FDM).
- Se o FTD for gerido pelo FMC (gestão não embalado), configurar o NTP no FMC.

Configure o NTP em FPR2100/4100/9300

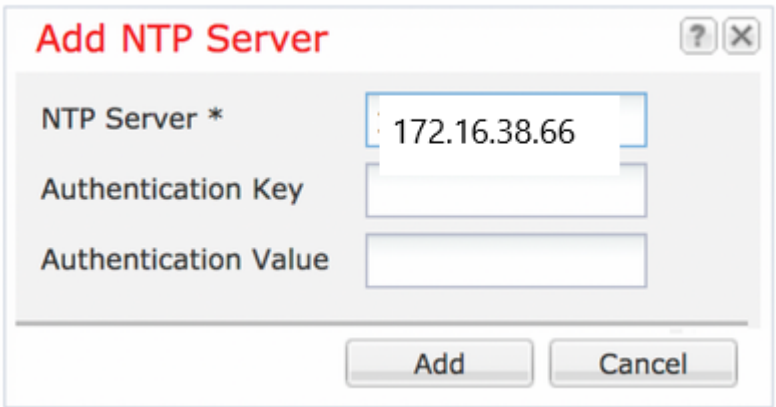
- Para configurar o NTP em um dispositivo FPR2100 no modo de plataforma, navegue até a guia Configurações de plataforma no gerenciador de chassis.

Note: Nas versões pós-9.13(1) FPR2100, é possível executar o modo de dispositivo (o padrão) e o modo de plataforma. O modo do dispositivo permite que você defina todas as configurações, incluindo NTP, no ASA. Somente comandos avançados de solução de problemas estão disponíveis na CLI do FXOS. Por outro lado, no modo de plataforma, você deve definir configurações básicas (incluindo NTP) e configurações de interface de hardware no gerenciador de chassis (FCM).

Etapa 1. Faça login na GUI do gerenciador de chassis com as credenciais do usuário local e navegue para Platform Settings > NTP. Selecione o botão Add:



Etapa 2. Especifique o endereço IP ou o nome de host do servidor NTP (se você usar um nome de host para o servidor NTP, deverá configurar um servidor DNS).



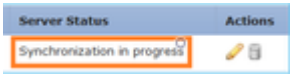
Note: Você pode configurar até 4 servidores NTP

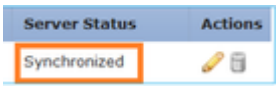
- No caso de um ASA no modo de plataforma, o NTP no dispositivo lógico é sincronizado com o MIO.
- Para o FTD em FPR2100 que esteja usando o modo de dispositivo, configure o NTP no FMC.
- Para o ASA no FPR2100 que está usando o modo de dispositivo, configure o NTP no ASA.

Verificar

Verifique a sincronização de NTP em dispositivos FPR4100/9300

Monitore o status do servidor.





Referência de Status do Servidor

- Não disponível: O status padrão mostrado imediatamente após a configuração do servidor NTP.
- Inalcançável/Inválido: Mostrado nestes cenários:
  - Quando o endereço IP ou o nome do host do servidor NTP não puder ser alcançado pelo protocolo NTP.
  - Quando o endereço IP ou o nome do host do servidor NTP estiver acessível, mas o host remoto não for um servidor NTP.
  - Outras falhas internas, como quando a consulta falha na execução, exceção lançada, status de sincronização de tempo indefinido é encontrado e assim por diante.
- Sincronização em andamento: O servidor está acessível e suporta o protocolo NTP; a convergência de tempo inicial ainda está em andamento e ainda não foi concluída.
- Sincronizado: O host é declarado como o peer de sincronização do sistema e o relógio de ponto está em sincronização com ele.
- Candidato: O host é o peer candidato (standby). Um servidor NTP candidato significa que é um servidor válido e se comunicou com êxito com o dispositivo Firepower, mas o módulo foi

sincronizado com outro servidor NTP, portanto, é o servidor em espera. Ele pode ser escolhido como o próximo peer em sincronia se o atual for excluído.
- Valor atípico: Um servidor NTP que é descartado devido à diferença significativa (deslocamento de tempo e atraso de ida e volta) em comparação com o restante dos servidores NTP.

Verifique o status do peer 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
```

Verifique a configuração e a sincronização do servidor 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:
```

Verifique a associação 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
```

Verifique o sysinfo de 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
```

Verificação adicional:

<#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
```

Verifique a sincronização de NTP entre o MIO e o dispositivo lógico (blade) nos dispositivos FPR4100/9300

No FPR4100/9300, as configurações de NTP são enviadas ao FTD por meio do MIO (chassi). A configuração NTP do FTD CLI ou da interface do FMC não é possível.

Cada blade de FTD usa um ID de referência interno: 203.0.113.126 para se comunicar com o MIO para sincronização de tempo e, com base nisso, ele mostra se está sincronizado ou não. A CLI do FTD reflete isso. O IP do NTP neste exemplo é o ID de referência interno, não o IP do servidor NTP real. Uma alteração do IP do servidor NTP no FCM não afeta essa saída, já que o ID de referência é sempre o mesmo:

<#root>

```
 >

show ntp

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

Verifique a configuração de NTP no modo de plataforma FRP2100 e 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
```

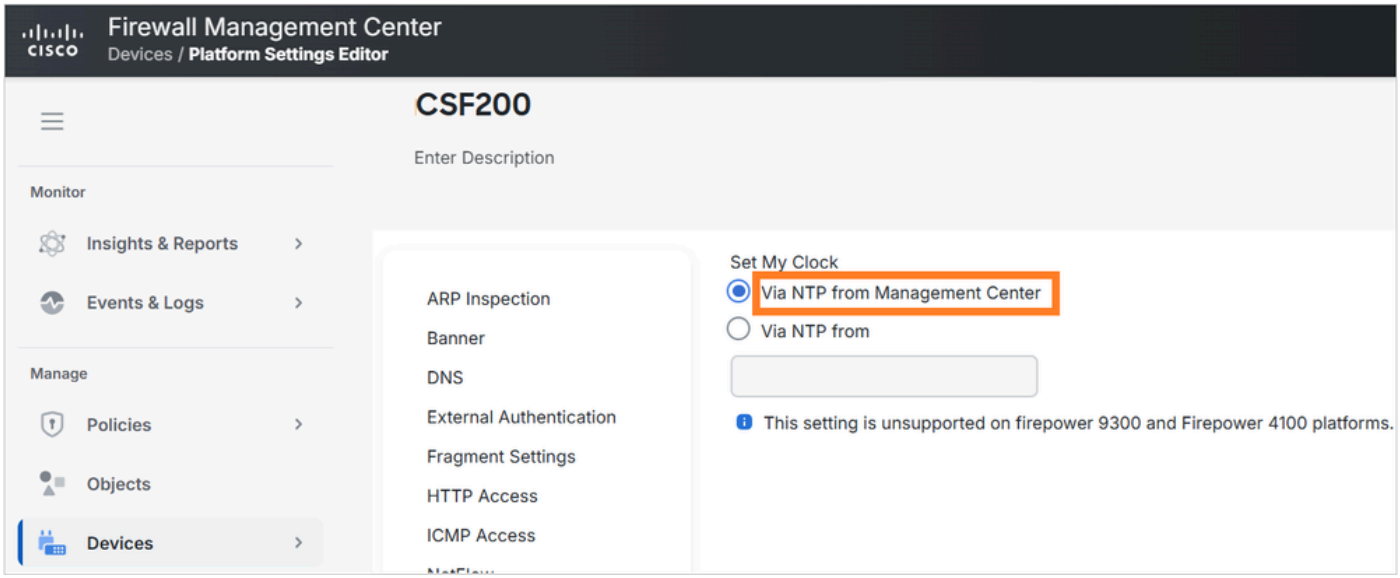
```
    Time Sync Status: Time Synchronized
    Error Msg:
```

No FTD, você também pode verificar as configurações de NTP no modo 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)
```

Se o FTD receber seu tempo do FMC, você verá o endereço 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:
```



Nesse caso, no CLISH, você também verá o endereço IP 127.0.0.2:

<#root>

>

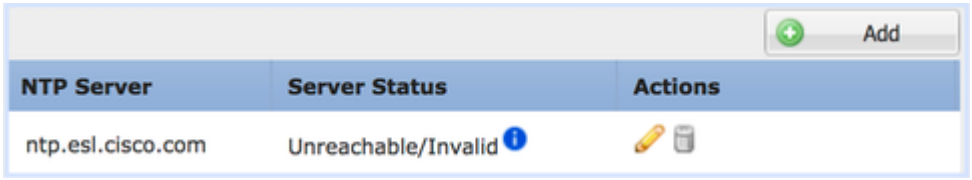
show ntp

```
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)
```

Solucionar problemas comuns

1. FXOS não Pode Resolver o Nome de Host do Servidor NTP

A interface do usuário do FCM mostra:



Ação recomendada

Use o comando ping para verificar a resolução do nome de host do servidor NTP

<#root>

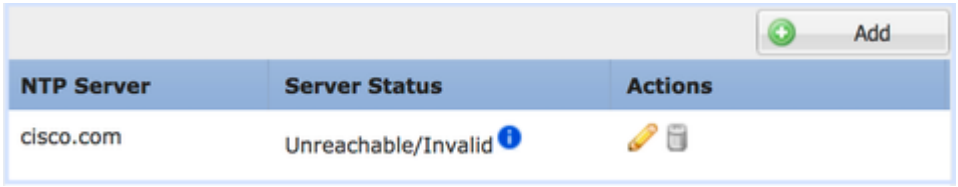
```
FPR4100(local-mgmt)#

ping ntp.esl.cisco.com

Invalid Host Name.
```

Possíveis causas

- O servidor DNS não está configurado.
- O servidor DNS não pode resolver o nome de host.

2. Problemas de Conectividade entre o FXOS e o Servidor NTP na Porta UDP 123

A interface do usuário do FCM mostra:



Ação recomendada

⚠ Caution: A captura do Ethanalyzer na interface de gerenciamento do chassi está disponível apenas em dispositivos FPR4100/9300.

Faça capturas na interface de gerenciamento do chassi e verifique a comunicação bidirecional na

porta UDP 123:

<#root>

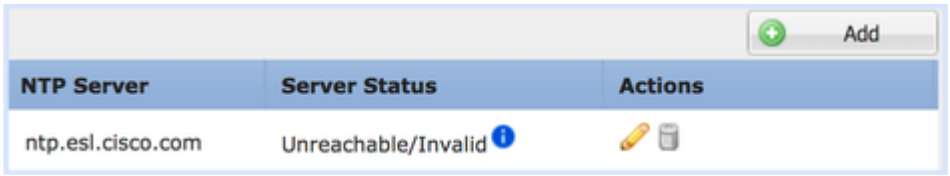
```
FPR4100(fxos)#

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
```

Possíveis causas

- O servidor configurado não é um Servidor NTP.
- Um dispositivo no caminho (por exemplo, firewall) bloqueia ou modifica o tráfego.

3. Problemas de conectividade intermitente entre o servidor FXOS e NTP

A interface do usuário do FCM mostra:



Ações recomendadas

⚠ Caution: Apenas para dispositivos FPR4100/9300.

Inicie o processo de sincronização NTP a partir da CLI FXOS

<#root>

```
FPR4100#
```

```
connect fxos

FPR4100(fxos)#

ntp sync-retry
```

Faça capturas na interface de gerenciamento do chassi com a ferramenta de comando ethanalyzer CLI.

Possível causa

- Problemas de conectividade intermitente entre FXOS e o servidor NTP

Defeitos relacionados

Verifique se há defeitos conhecidos/corrigidos nas Notas de versão.

Informações Relacionadas

- Guias de configuração do FXOS
- Solucionar problemas com o Network Time Protocol (NTP) em sistemas Firepower

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.