在Firepower和安全防火墙上配置并排除NTP设置故障

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- FPR4100/9300上的NTP
  - 要点
- CSF200/1200/3100/4200/6100上的NTP
- 在FPR2100/4100/9300上配置NTP

验证

- 验证FPR4100/9300设备上的NTP同步
  - 服务器状态参考
- 验证FPR4100/9300设备上MIO和逻辑设备（刀片）之间的NTP同步

排除常见问题

- 1. FXOS无法解析NTP服务器主机名
  - 建议操作
  - 可能的原因
- 2. FXOS和UDP端口123上的NTP服务器之间的连接问题
  - 建议操作
  - 可能的原因
- 3. FXOS和NTP服务器之间的间歇性连接问题
  - 推荐的操作
  - 可能的原因

相关问题

相关信息

简介

本文档介绍如何在Cisco Firepower和Cisco安全防火墙设备上配置、验证网络时间协议(NTP)并对其进行故障排除。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

- 运行FXOS 2.3(1.130)和2.8(1.105)的FPR4140。
- 运行ASA平台模式的FPR2110。
- 运行ASA设备模式的FPR1140。
- 运行FTD 10.x的CSF220

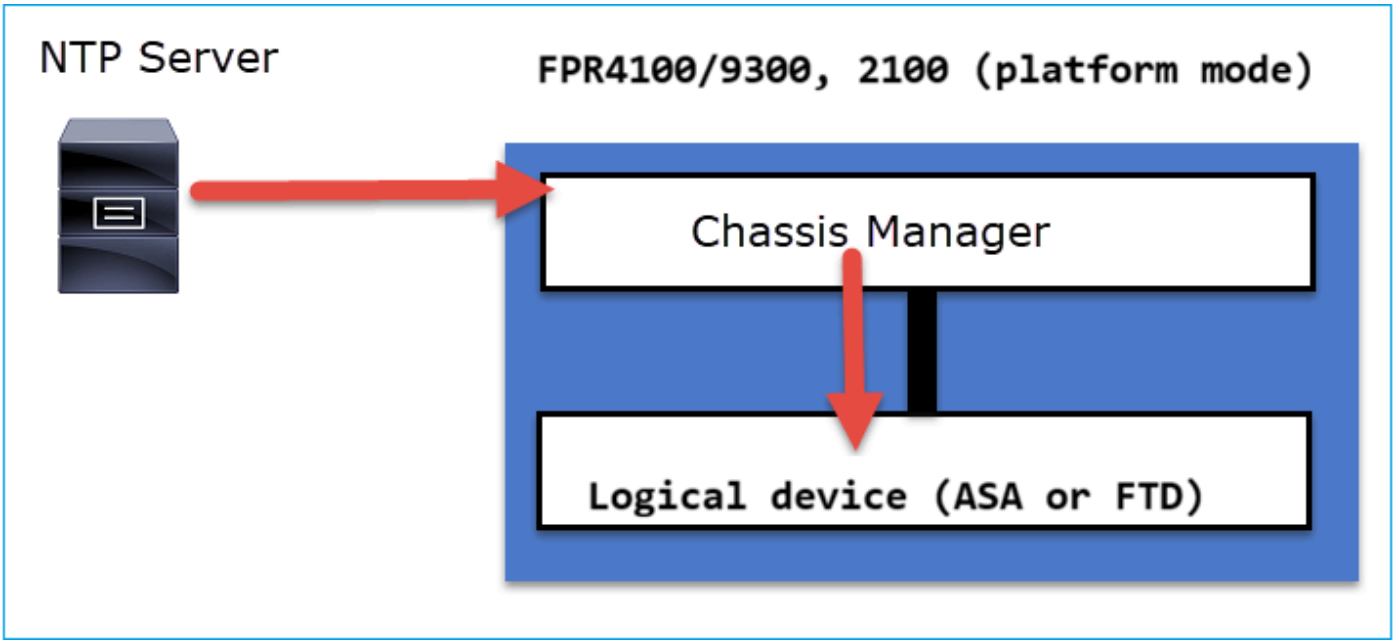
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

NTP操作取决于平台。

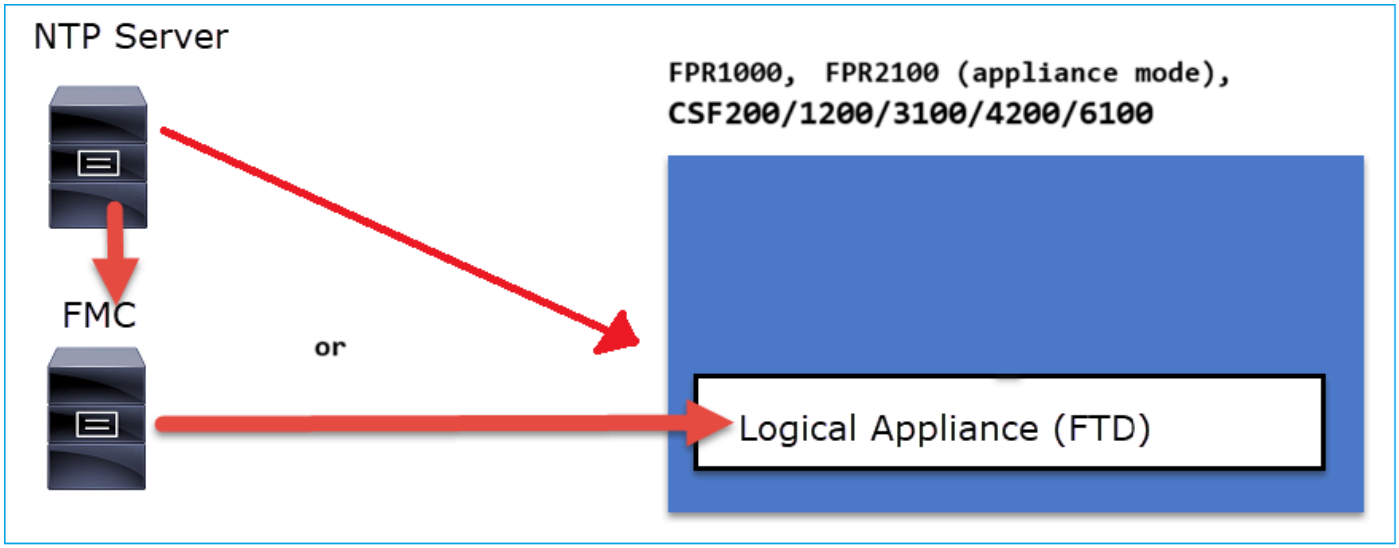
FPR4100/FPR9300、FPR2100（平台模式）

ASA或FTD时间取自机箱Firepower机箱管理器(FCM)管理输入/输出(MIO)。MIO是Firepower机箱的管理引擎。



FPR1000、FPR2100（设备模式）、CSF200/3100/4200/6100

在FTD上，时间取自FMC或NTP服务器：



对于此部署，请检查以下文档：

- 配置威胁防御的NTP时间同步
- 排除Firepower系统上的网络时间协议(NTP)问题

其它信息：
NTP用于时间同步。NTP使用UDP端口号123作为传输。

注意：NTP第4版不受正式支持。NTP版本4向后兼容NTP版本3。

配置

FPR4100/9300上的NTP

要点

- 要在FPR4100/9300设备上配置NTP，请登录到FCM并导航到Platform Settings选项卡。
- 逻辑设备（ASA或FTD）上的NTP与MIO同步。
- 无法将FTD上的NTP与防火墙管理中心(FMC)同步，即使选择该选项，FTD上的NTP也会与MIO同步。因此，强烈建议FMC和FCM使用相同的NTP服务器。
- FMC不是完整的NTP服务器。它只能通过sftunnel为其受管设备提供时间设置。因此，它不能用作FPR4100/9300机箱的NTP服务器。
- 要成功安装智能许可证，需要正确的NTP配置。

CSF200/1200/3100/4200/6100上的NTP

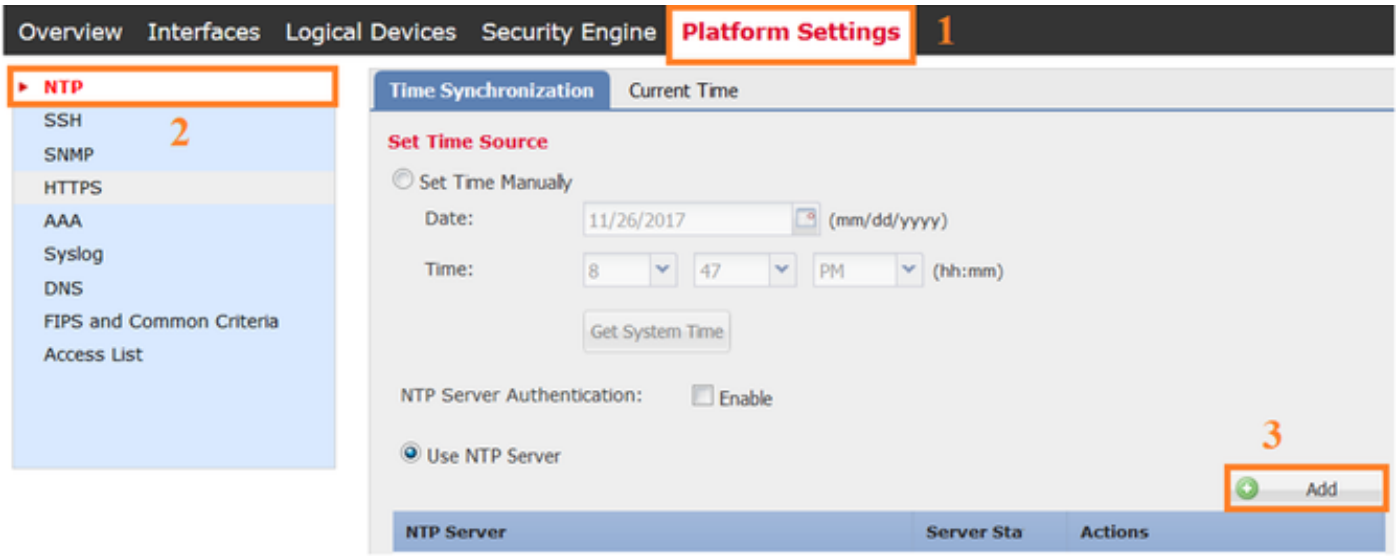
- 在逻辑应用程序本身上配置NTP设置。ASA处于设备模式，或者从防火墙设备管理器(FDM)进行FTD机上管理。
- 如果FTD由FMC（离线管理）管理，请在FMC上配置NTP。

在FPR2100/4100/9300上配置NTP

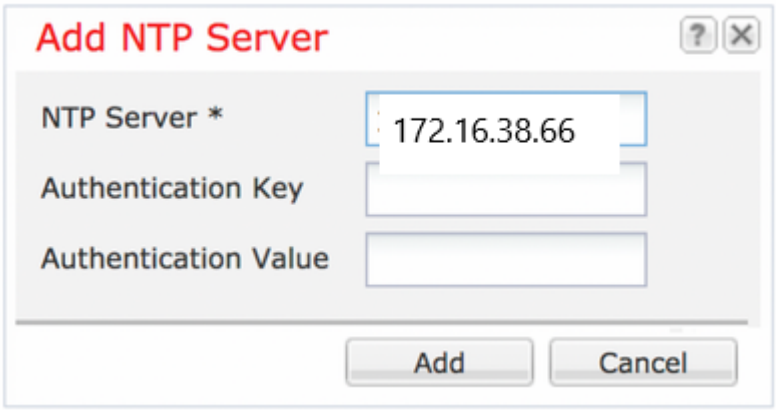
- 要在平台模式下在FPR2100设备上配置NTP，请从机箱管理器导航到平台设置选项卡。

注意：在9.13(1)后FPR2100版本上，可以运行设备模式（默认）和平台模式。设备模式允许您在ASA上配置所有设置，包括NTP。FXOS CLI仅提供高级故障排除命令。另一方面，在平台模式下，必须在机箱管理器(FCM)中配置基本设置（包括NTP）和硬件接口设置。

步骤1.使用本地用户凭证登录到机箱管理器GUI，然后导航到平台设置> NTP。选择Add按钮：



步骤2.指定NTP服务器的IP地址或主机名（如果使用主机名作为NTP服务器，则必须配置DNS服务器）。



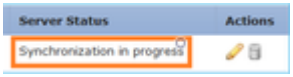
注意：最多可以配置4个NTP服务器

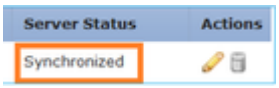
- 如果ASA处于平台模式，逻辑设备上的NTP将与MIO同步。
- 对于使用设备模式的FPR2100上的FTD，您可以在FMC上配置NTP。
- 对于使用设备模式的FPR2100上的ASA，您可以在ASA上配置NTP。

验证

验证FPR4100/9300设备上的NTP同步

监控服务器状态。





服务器状态参考

- 不可用:NTP服务器配置后立即显示的默认状态。
- 无法访问/无效：在以下情景中显示：
  - NTP协议无法访问NTP服务器IP地址或主机名时。
  - 当NTP服务器IP地址或主机名可访问，但远程主机不是NTP服务器时。
  - 其他内部故障，例如查询无法执行、引发异常、遇到未定义的时间同步状态等。
- 正在进行同步：服务器可访问且支持NTP协议，初始时间收敛仍在进行且尚未完成。
- 已同步：主机被声明为系统同步对等体，并且时间时钟与其同步。
- 应聘者：主机是候选（备用）对等体。候选NTP服务器表示它是有效服务器并且已成功与Firepower设备通信，但模块已与另一个NTP服务器同步，因此它是备用服务器。如果当前同步对等体被删除，则可以将其选为下一个同步对等体。
- 异常值：由于与其他NTP服务器相比存在显着差异（时间偏移和往返延迟）而被丢弃的NTP服务器。

验证NTP对等体状态：

<#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
```

验证NTP服务器配置和同步：

```
<#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:
```

验证NTP关联：

```
<#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
```

验证NTP系统信息：

<#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
```

其他验证：

<#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
```

验证FPR4100/9300设备上MIO和逻辑设备（刀片）之间的NTP同步

在FPR4100/9300上，NTP设置通过MIO（机箱）推送到FTD。 无法从FTD CLI或FMC UI进行NTP配置。

每个FTD刀片使用一个内部引用ID:203.0.113.126与MIO进行时间同步通信，并据此显示是否同步。FTD CLI反映了这一点。本示例中的NTP IP是内部ref-id，而不是实际NTP服务器IP。更改FCM中的NTP服务器IP不会影响此输出，因为reference-id始终相同：

<#root>

```
 >
```

show ntp

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

验证FRP2100平台模式和CSF200/1200/3100/4200/6100上的NTP配置：

```
<#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:
```

在FTD上，您还可以从CLISH模式验证NTP设置：

```
<#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)
```

如果FTD从FMC获取时间，您将看到IP地址127.0.0.2:

<#root>

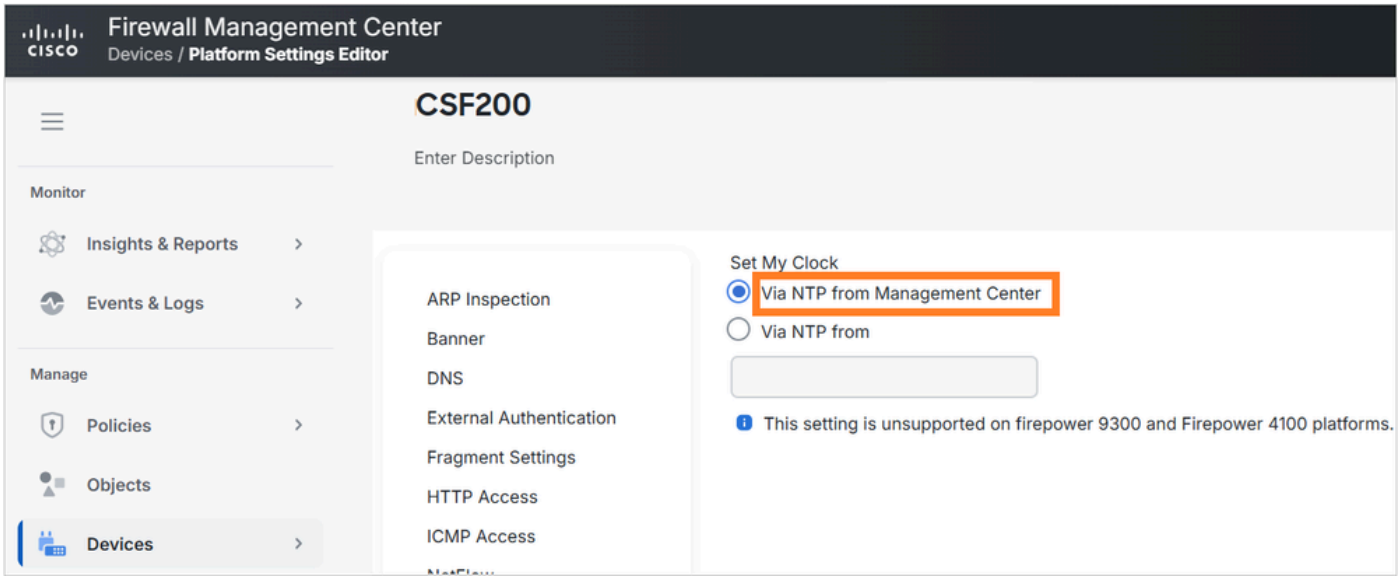
FTD220 /system/services #

show ntp-server detail expand

NTP server hostname:

Name: 127.0.0.2

Time Sync Status: Time Synchronized
Error Msg:



在本例中，您还会从CLISH看到IP地址127.0.0.2:

<#root>

>

show ntp

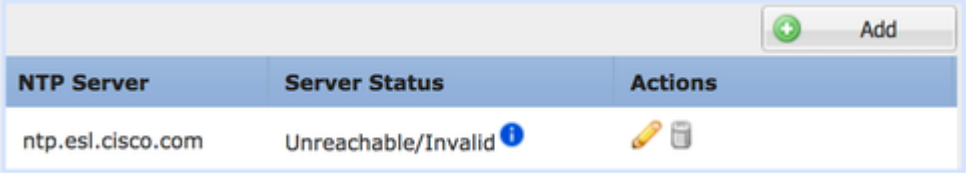
NTP Server : 127.0.0.2
Status : Being Used
Offset : +0.008 (milliseconds)
Last Update : 6 (seconds)

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

排除常见问题

1. FXOS无法解析NTP服务器主机名

FCM UI显示：



建议操作

使用ping命令验证NTP服务器主机名解析

<#root>

```
FPR4100(local-mgmt)#

ping ntp.esl.cisco.com

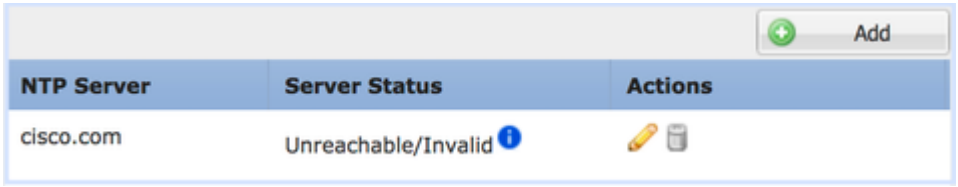
Invalid Host Name.
```

可能的原因

- 未配置DNS服务器。
- DNS服务器无法解析主机名。

2. FXOS和UDP端口123上的NTP服务器之间的连接问题

FCM UI显示：



建议操作

⚠ 警告：机箱管理接口上的Ethanalyzer捕获仅在FPR4100/9300设备上可用。

在机箱管理接口上捕获数据并验证UDP端口123上的双向通信：

<#root>

```
FPR4100(fxos)#

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

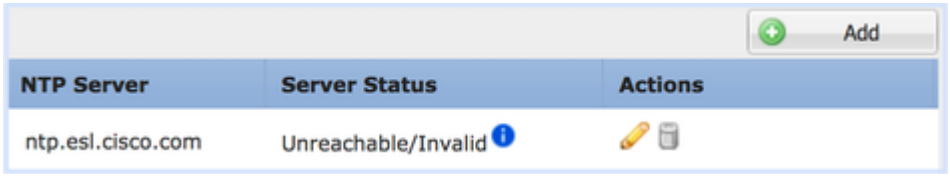
Capturing on 'eth0'
1 2020-04-30 20:09:54.150237760 10.62.148.196 → 172.16.4.161 NTP 90 NTP Version 3, client
2 2020-04-30 20:14:14.150172804 10.62.148.196 → 172.16.4.161 NTP 90 NTP Version 3, client
3 2020-04-30 20:23:13.150171682 10.62.148.196 → 172.16.4.161 NTP 90 NTP Version 3, client
```

可能的原因

- 配置的服务器不是NTP服务器。
- 路径中的设备（例如防火墙）会阻止或修改流量。

3. FXOS和NTP服务器之间的间歇性连接问题

FCM UI显示：



推荐的操作

⚠ 警告：仅适用于FPR4100/9300设备。

从FXOS CLI启动NTP同步进程

<#root>

FPR4100#

connect fxos

FPR4100(fxos)#

ntp sync-retry

使用ethanalyzer CLI命令工具获取机箱管理界面上的捕获信息。

可能的原因

- FXOS和NTP服务器之间的间歇性连接问题

相关问题

检查版本说明中是否存在已知/已修复的缺陷。

相关信息

- FXOS 配置指南
- 排除Firepower系统上的网络时间协议(NTP)问题

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。