

FirepowerアプライアンスでのNTP設定の設定とトラブルシューティング

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[FPR 41xx/9300のNTP](#)

[FPR 1xxx/2100のNTP](#)

[FPR 1xxx/2100/41xx/9300アプライアンスでのNTPの設定](#)

[確認](#)

[FPR41xx/9300アプライアンスでのNTP同期の確認](#)

[FPR41xx/9300アプライアンスでのNTP設定の確認](#)

[FPR41xx/9300アプライアンスでのMIOと論理デバイス \(ブレード \) 間のNTP同期の確認](#)

[FPR1xxx/2100アプライアンスのNTP設定の確認](#)

[一般的な問題のトラブルシューティング](#)

[1. FXOSがNTPサーバのホスト名を解決できない](#)

[2. FXOS間の接続の問題 - UDPポート123のNTPサーバ](#)

[3. FXOSとNTPサーバ間の接続が断続する問題](#)

[関連する不具合](#)

[関連情報](#)

概要

このドキュメントでは、Firepower FXOSアプライアンスでネットワークタイムプロトコル (NTP)を設定、確認、およびトラブルシューティングする方法について説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

- FXOS 2.3(1.130)および2.8(1.105)が稼働するFPR4140

- ASAプラットフォームモードを実行するFPR2110
- ASAアプライアンスモードで稼働するFPR1140

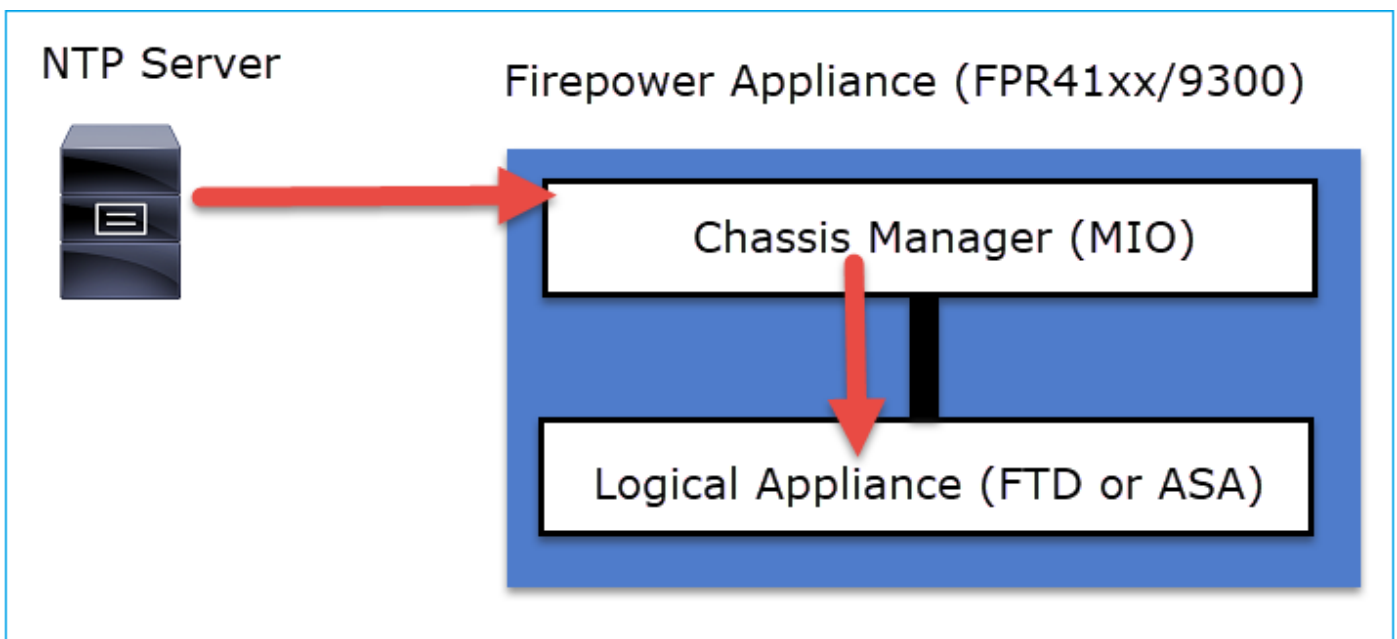
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Firepowerでは、NTPの動作はプラットフォームによって異なります。

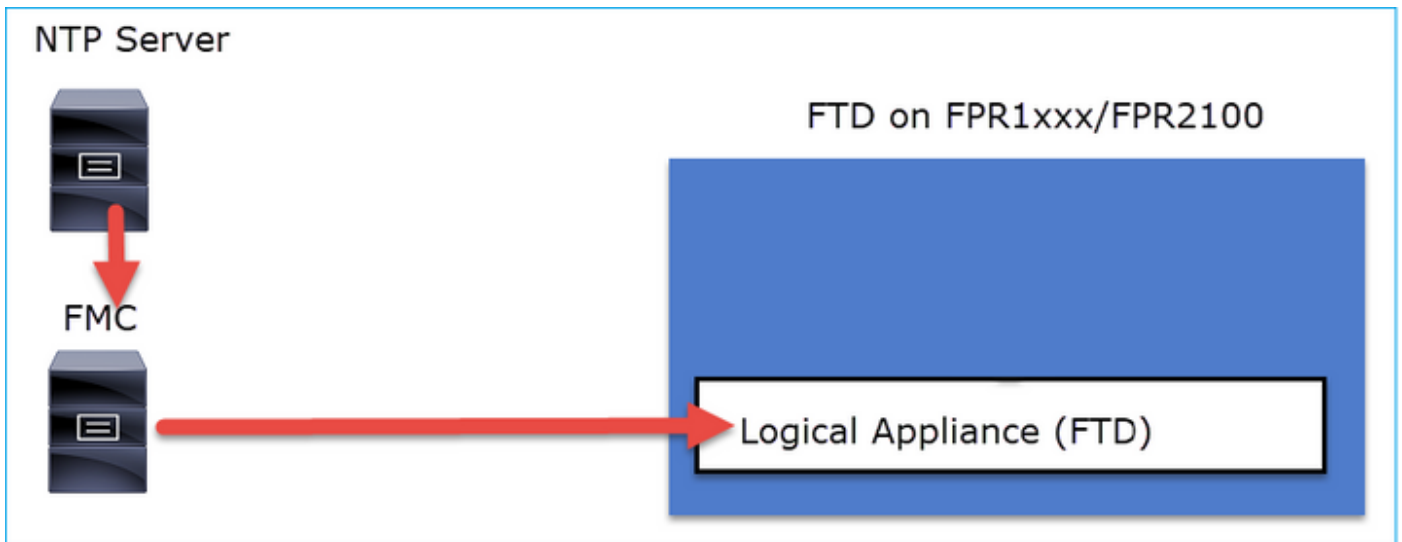
FPR41xx/FPR9300

ASAまたはFTDの時間は、シャーシのFirepower Chassis Manager (FCM) Management Input/Output (MIO) から取得されます。MIOはFirepowerシャーシのスーパーバイザです。



FPR1xxx/FPR2100

FTDでは、時間はFMCから取得されます。



この導入では、次のドキュメントを確認してください。

- [脅威対策のためのNTP時刻同期の設定](#)
- [Firepower システムの Network Time Protocol \(NTP \) に伴う問題のトラブルシューティング](#)

追加情報

NTPは時刻の同期に使用されます。NTPはUDPポート番号123をトランスポートとして使用します。

FXOSでサポートされるNTPバージョン：

- FXOS 10.2.2.7以降はNTPバージョン3を使用します
- 10.2.2.7よりも古いFXOSはNTPバージョン2を使用する

Cisco Bug ID [CSCve58269](#)により、サポートされるバージョンが変更されました。 - NTP:v2をv3に変更

注:NTPバージョン4は公式にはサポートされていません。NTPバージョン4は、NTPバージョン3と下位互換性があります。

設定

FPR 41xx/9300のNTP

要点

- Firepower 41xx/9300アプライアンスでNTPを設定するには、FCMにログインし、[Platform Settings] タブに移動します。
- 論理デバイス (ASAまたはFTD) のNTPはMIOと同期されます。
- 現在、FTDのNTPをFirepower Management Center(FMC)と同期することはできません。このオプションを選択しても、FTDのNTPはMIOと同期されます。したがって、FMCとFCMは同じNTPサーバを使用することを強く推奨します。

- FMCは本格的なNTPサーバではありません。Sftunnelを介して管理対象デバイスに時間設定を提供するだけです。したがって、Firepower 41xx/9300シャーシのNTPサーバとして使用することはできません。
- スマートライセンスを正常にインストールするには、適切なNTP設定が必要です。

FPR 1xxx/2100のNTP

- Firepower 1xxx/2100アプライアンスでNTPを設定するには、Firepower Chassis Manager(FCM)、Firepower for ASAのプラットフォームモードから[Platform Settings] タブに移動します。
- プラットフォームモードのASAの場合、論理デバイスのNTPはMIOと同期されます。
- 論理アプリケーション自体でNTP設定を行います。アプライアンスモードのASA、またはFirepower Device Manager(FDM)からのFTDオンボックス管理の場合。
- FTDがFMCによって管理されている場合 (オフボックス管理)、FMCでNTPを設定します。

注：9.13(1)以降のバージョンでは、Firepower 1xxx/2100 for ASAをアプライアンスモード (デフォルト) とプラットフォームモードのモードで実行できます。アプライアンスモードでは、NTPを含むすべての設定をASAで設定できます。FXOS CLIから使用できるのは、高度なトラブルシューティングコマンドだけです。一方、プラットフォームモードでは、Chassis Manager(FCM)で基本設定 (NTPを含む) とハードウェアインターフェイス設定を行う必要があります。

FPR 1xxx/2100/41xx/9300アプライアンスでのNTPの設定

手順 1：ローカルユーザクレデンシャルを使用してFirepower Chassis Manager(FCM)のGUIにログインし、[Platform Settings] > [NTP] に移動します。[Add] ボタンを選択します。

The screenshot shows the Firepower Chassis Manager (FCM) GUI. The top navigation bar includes 'Overview', 'Interfaces', 'Logical Devices', 'Security Engine', and 'Platform Settings' (highlighted with a red box and the number 1). The left sidebar shows a list of settings: 'NTP' (highlighted with a red box and the number 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 contains a 'Set Time Source' section with two radio buttons: 'Set Time Manually' and 'Use NTP Server' (selected). The 'Set Time Manually' section includes a 'Date' field (11/26/2017) and a 'Time' field (8:47 PM). Below this is a 'Get System Time' button. The 'Use NTP Server' section has an 'NTP Server Authentication' checkbox (unchecked) and an 'Add' button (highlighted with a red box and the number 3). At the bottom, there is a table with columns 'NTP Server', 'Server Sta', and 'Actions'.

ステップ 2：NTPサーバのIPアドレスまたはホスト名を指定します (NTPサーバにホスト名を使用する場合は、DNSサーバを設定する必要があります)。

Add NTP Server

NTP Server * 172.16.38.66

Authentication Key

Authentication Value





Add Cancel

注：最大4台のNTPサーバを設定できます

確認

FPR41xx/9300アプライアンスでのNTP同期の確認

サーバのステータスを監視します。

Server Status	Actions
Synchronization in progress	 
Synchronized	 

サーバステータスの参照

- [Not available]: NTPサーバ設定の直後に表示されるデフォルトのステータス。
- 到達不能/無効：次のシナリオで表示されます。NTPサーバのIPアドレスまたはホスト名にNTPプロトコルから到達できない場合。NTPサーバのIPアドレスまたはホスト名に到達できるが、リモートホストがNTPサーバではない場合。クエリの実行に失敗した場合、例外がスローされた場合、未定義の時刻同期ステータスが発生した場合など、その他の内部エラー。
- 同期中：サーバに到達でき、NTPプロトコルをサポートしています。初期タイムコンバージョンは継続されており、まだ完了していません。
- 同期済み：ホストはシステム同期ピアとして宣言され、タイムクロックは同期されています。
- Candidate：ホストは候補（スタンバイ）ピアです。NTPサーバ候補とは、それが有効なサーバであり、Firepowerアプライアンスとの通信は成功したが、モジュールは別のNTPサーバと同期されているため、スタンバイNTPサーバであることを意味します。現在のピアが削除されている場合は、次の同期ピアとして選択できます。
- Outlier：他のNTPサーバと大きく異なる（タイムオフセットとラウンドトリップ遅延）ために廃棄されるNTPサーバ。

FPR41xx/9300アプライアンスでのNTP設定の確認

NTPピアのステータスを確認します。

```
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
```

NTPサーバの設定と同期を確認します。

```
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:
```

NTPアソシエーションを確認します。

```
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
```

NTPのsysinfoを確認します。

```
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
```

FPR41xx/9300アプライアンスでのMIOと論理デバイス (ブレード) 間のNTP同期の確認

FPR41xx/9300では、NTP設定はMIO (シャーシ) 経由でFTDにプッシュされます。FTD CLIまたはFMC UIからのNTP設定は不可能です。

各FTDブレードは内部参照ID 203.0.113.126を使用して時刻同期のためにMIOと通信し、それに基づいて同期されているかどうかを示します。FTD CLIはこれを反映します。この例のNTP IPは、実際のNTPサーバのIPではなく、内部参照IDです。FCMでNTPサーバのIPを変更しても、reference-idは常に同じであるため、この出力には影響しません。

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

FPR1xxx/2100アプライアンスのNTP設定の確認

注意：これは、プラットフォームモードのASA用のFPR1xxx/2100アプライアンスにのみ適用されます。

```
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:
```

一般的な問題のトラブルシューティング

1. FXOSがNTPサーバのホスト名を解決できない

FCM UIには次のように表示されます。

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

推奨処置

pingコマンドを使用して、NTPサーバのホスト名解決を確認します



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

考えられる原因

- DNSサーバが設定されていません。
- DNSサーバがホスト名を解決できません。

2. FXOS間の接続の問題 – UDPポート123のNTPサーバ

FCM UIには次のように表示されます。

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

推奨処置

注意：シャーシ管理インターフェイスでのEthanalyzerキャプチャは、FPR41xx/9300アプリケーションでのみ使用できます。

シャーシ管理インターフェイスでキャプチャを取得し、UDPポート123での双方向通信を確認します。




```
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
```

考えられる原因

- 設定されたサーバはNTPサーバではありません。
- パス内のデバイス (ファイアウォールなど) は、トラフィックをブロックまたは変更します。

3. FXOSとNTPサーバ間の接続が断続する問題

FCM UIには次のように表示されます。

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

推奨処置

注意：FPR41xx/9300アプライアンスのみ。

FXOS CLIからNTP同期プロセスを開始します

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

ethalyzer CLIコマンドツールを使用して、シャーシ管理インターフェイスのキャプチャを取得します。

考えられる原因

- FXOSとNTPサーバ間の接続が断続的に発生する問題

関連する不具合

リリースノートで、既知の問題と修正済みの問題を不具合します。

関連情報

- [FXOS コンフィギュレーションガイド](#)
- [Firepower システムの Network Time Protocol \(NTP \) に伴う問題のトラブルシューティング](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。