

NTP-Einstellungen auf FirePOWER-Appliances konfigurieren und Fehlerbehebung dafür durchführen

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[NTP auf FPR 41xx/9300](#)

[NTP auf FPR 1xxx/2100](#)

[Konfigurieren des NTP auf FPR 1xxx/2100/41xx/9300-Appliances](#)

[Überprüfung](#)

[Überprüfen der NTP-Synchronisierung auf FPR41xx-/9300-Appliances](#)

[Überprüfen der NTP-Konfiguration auf FPR41xx/9300-Appliances](#)

[Überprüfen der NTP-Synchronisierung zwischen MIO und logischem Gerät \(Blade\) auf FPR41xx/9300-Appliances](#)

[Überprüfen der NTP-Konfiguration von FPR1xxx/2100-Appliances](#)

[Fehlerbehebung bei gängigen Problemen](#)

[1. FXOS konnte den NTP-Server-Hostnamen nicht auflösen](#)

[2. Verbindungsprobleme zwischen FXOS - NTP-Server auf UDP-Port 123](#)

[3. Intermittierende Verbindungsprobleme zwischen FXOS und NTP-Server](#)

[Verwandte Fehler](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie das Network Time Protocol (NTP) auf FirePOWER FXOS-Appliances konfigurieren, überprüfen und Fehler beheben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

- FPR4140 mit FXOS 2.3(1.130) und 2.8(1.105)
- FPR2110 mit ASA-Plattformmodus
- FPR1140, der den ASA Appliance-Modus ausführt

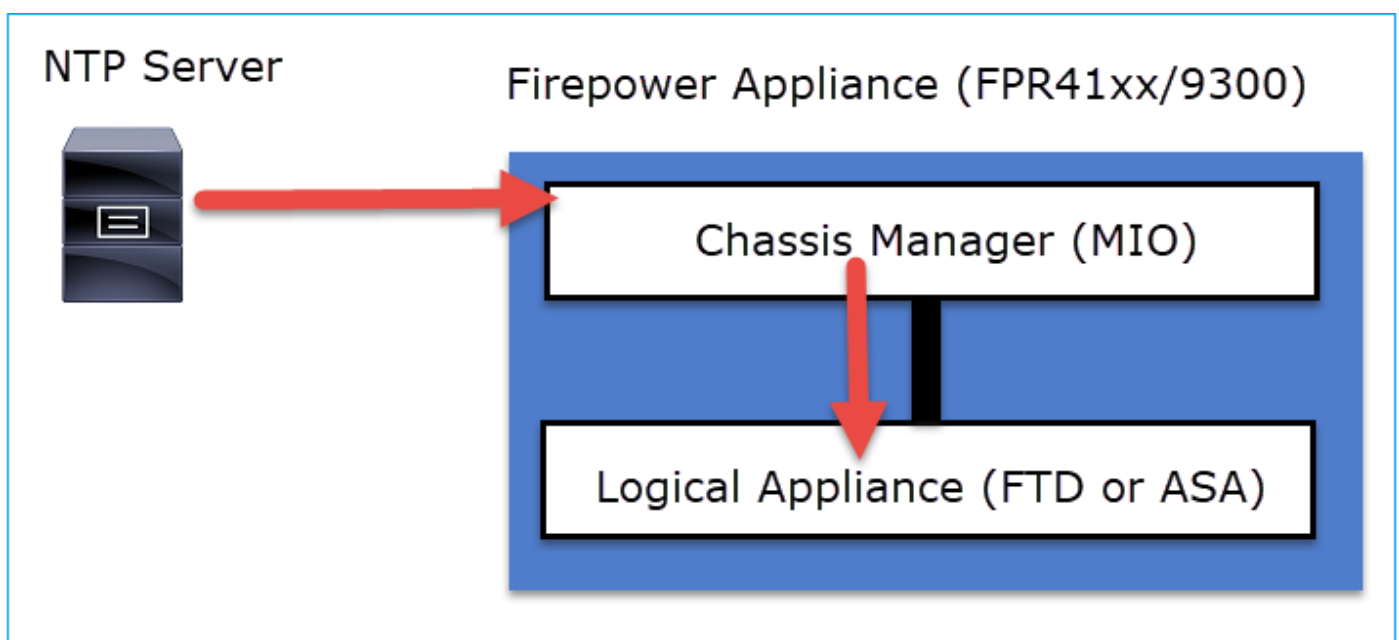
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Bei Firepower ist der NTP-Betrieb von der Plattform abhängig.

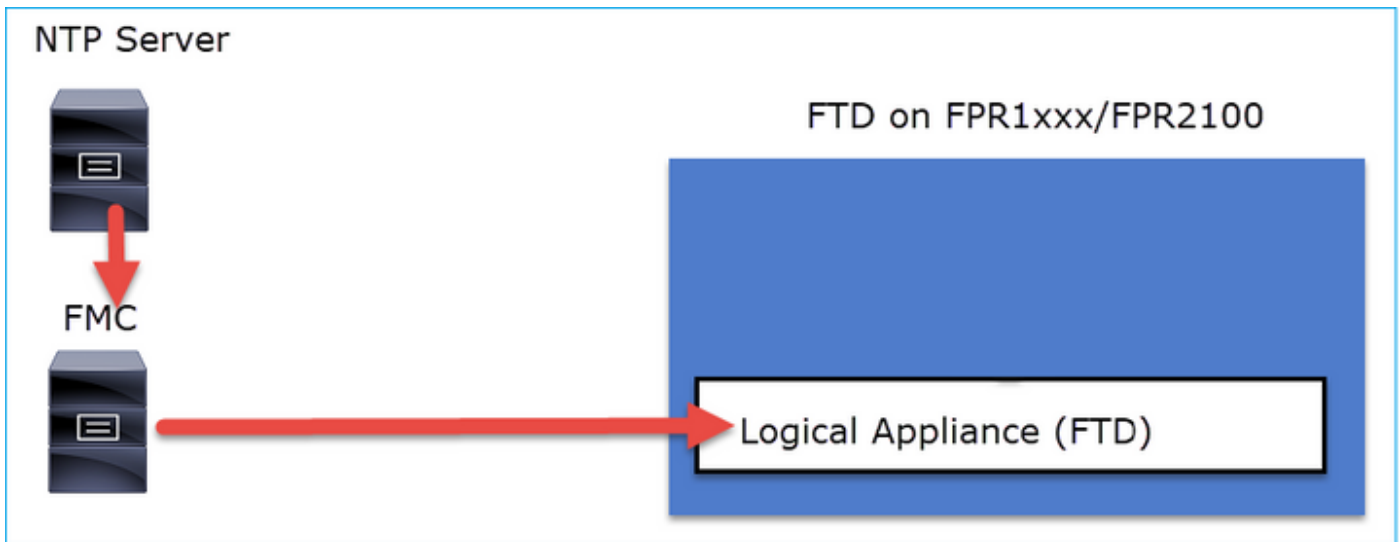
FPR 41xx/FPR 9300

Die ASA- oder FTD-Zeit wird vom Management-Eingang/Ausgang (MIO) des Firepower Chassis Managers (FCM) übernommen. MIO ist der Supervisor des Firepower-Chassis.



FPR1xxx/FPR2100

Bei FTD wird die Zeit vom FMC übernommen:



Überprüfen Sie für diese Bereitstellung die folgenden Dokumente:

- [NTP-Zeitsynchronisierung für die Abwehr von Bedrohungen konfigurieren](#)
- [Fehlerbehebung bei Problemen mit dem Network Time Protocol \(NTP\) in FirePOWER-Systemen](#)

Zusätzliche Informationen

NTP wird für die Zeitsynchronisierung verwendet. Das NTP verwendet als Transport die UDP-Portnummer 123.

Unterstützte NTP-Versionen auf FXOS:

- FXOS 10.2.2.7 und höher verwenden NTP-Version 3.
- Ältere FXOS als 10.2.2.7 verwenden NTP-Version 2

Unterstützte Version geändert aufgrund von Cisco Bug-ID [CSCve58269](#) - NTP: v2 in v3 ändern

Hinweis: NTP-Version 4 wird nicht offiziell unterstützt. NTP-Version 4 ist mit NTP-Version 3 abwärtskompatibel.

Konfigurieren

NTP auf FPR 41xx/9300

Wichtigste Punkte

- Um NTP auf einer FirePOWER 41xx/9300-Appliance zu konfigurieren, melden Sie sich bei FCM an, und navigieren Sie zur Registerkarte **Platform Settings** (Plattformeinstellungen).
- Das NTP auf den logischen Geräten (ASA oder FTD) wird mit der MIO synchronisiert.
- Derzeit besteht keine Möglichkeit, NTP auf FTD mit FirePOWER Management Center (FMC) zu synchronisieren, selbst wenn Sie diese Option auswählen, wird NTP auf FTD mit MIO synchronisiert. Es wird daher dringend empfohlen, dass FMC und FCM denselben NTP-

Server verwenden.

- Das FMC ist kein vollständiger NTP-Server. Er kann einfach Zeiteinstellungen für seine verwalteten Geräte über den Sftunnel bereitstellen. Daher kann er nicht als NTP-Server für das FirePOWER 41xx/9300-Chassis verwendet werden.
- Für eine erfolgreiche Installation der Smart-Lizenz ist eine ordnungsgemäße NTP-Konfiguration erforderlich.

NTP auf FPR 1xxx/2100

- Um NTP auf einer FirePOWER 1xxx/2100-Appliance zu konfigurieren, navigieren Sie zur Registerkarte **Plattformeinstellungen** im FirePOWER Chassis Manager (FCM), FirePOWER für ASA im Plattformmodus.
- Bei einer ASA im Plattformmodus wird das NTP auf dem logischen Gerät mit der MIO synchronisiert.
- Konfigurieren Sie die NTP-Einstellungen für die logische Anwendung selbst. Die ASA im Appliance-Modus oder bei FTD-On-Box-Management über den Firepower Device Manager (FDM).
- Falls das FTD vom FMC verwaltet wird (externes Management), konfigurieren Sie das NTP auf dem FMC.

Hinweis: In Versionen nach 9.13(1) kann Firepower 1xxx/2100 für ASA in den folgenden Modi ausgeführt werden: Appliance-Modus (Standard) und Plattform-Modus. Im Appliance-Modus können Sie alle Einstellungen auf der ASA konfigurieren, einschließlich NTP. Nur Befehle für die erweiterte Fehlerbehebung sind über die FXOS-CLI verfügbar. Andererseits müssen Sie im Plattformmodus die Grundeinstellungen (einschließlich NTP) und die Hardware-Schnittstelleneinstellungen im Chassis-Manager (FCM) konfigurieren.

Konfigurieren des NTP auf FPR 1xxx/2100/41xx/9300-Appliances

Schritt 1: Melden Sie sich mit den lokalen Benutzeranmeldeinformationen bei der Firepower Chassis Manager-GUI an, und navigieren Sie zu **Plattformeinstellungen > NTP**. Wählen Sie die Schaltfläche **Hinzufügen**:

The screenshot shows the Firepower Chassis Manager 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 'NTP' (highlighted with a red box and the number 2) and other settings like 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 has two tabs: 'Set Time Source' and 'Current Time'. Under 'Set Time Source', there are two radio buttons: 'Set Time Manually' and 'Use NTP Server' (selected). The 'Set Time Manually' section includes a date field (11/26/2017), a time field (8:47 PM), and a 'Get System Time' button. The 'Use NTP Server' section includes an 'NTP Server Authentication' checkbox (unchecked) and an 'Add' button (highlighted with a red box and the number 3). The bottom of the page has a table with columns 'NTP Server', 'Server Sta', and 'Actions'.

Schritt 2: Geben Sie die IP-Adresse oder den Hostnamen des NTP-Servers an (wenn Sie einen Hostnamen für den NTP-Server verwenden, müssen Sie einen DNS-Server konfigurieren).

Add NTP Server

NTP Server *

Authentication Key

Authentication Value

Hinweis: Sie können bis zu 4 NTP-Server konfigurieren.

Überprüfung

Überprüfen der NTP-Synchronisierung auf FPR41xx-/9300-Appliances

Überwachen des Serverstatus



Serverstatusreferenz

- Not available (Nicht verfügbar): Der Standardstatus wird unmittelbar nach der NTP-Serverkonfiguration angezeigt.
- Nicht erreichbar/Ungültig: Wird in den folgenden Szenarien angezeigt: Wenn die IP-Adresse oder der Hostname des NTP-Servers für das NTP-Protokoll nicht erreichbar ist. Wenn die IP-Adresse oder der Hostname des NTP-Servers erreichbar ist, der Remote-Host jedoch kein NTP-Server ist. Andere interne Fehler, z. B. wenn die Abfrage nicht ausgeführt werden kann, eine Ausnahme ausgelöst wird, ein undefinierter Synchronisierungsstatus auftritt usw.
- Synchronisierung läuft: Der Server ist erreichbar und unterstützt das NTP-Protokoll. Die anfängliche Zeitkonvergenz läuft noch und ist noch nicht abgeschlossen.
- Synchronized (Synchronisiert): Der Host wird als System-Synchronisierungs-Peer deklariert, und die Zeituhr wird mit diesem synchronisiert.
- Kandidat: Der Host ist der Kandidat (Standby)-Peer. Ein möglicher NTP-Server bedeutet, dass es sich um einen gültigen Server handelt und erfolgreich mit der FirePOWER-Appliance kommuniziert wurde. Das Modul wurde jedoch mit einem anderen NTP-Server synchronisiert und ist somit der Standby-Server. Er kann als nächster synchronisierter Peer ausgewählt werden, wenn der aktuelle Peer gelöscht wird.

- Ausreißer: Ein NTP-Server, der aufgrund eines großen Unterschieds (Zeitversatz und Round-Trip-Verzögerung) im Vergleich zum Rest der NTP-Server verworfen wird.

Überprüfen der NTP-Konfiguration auf FPR41xx/9300-Appliances

Überprüfen Sie den NTP-Peer-Status:

```
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
```

Überprüfen Sie die Konfiguration und Synchronisierung des NTP-Servers:

```
FPR4100-8-A# scope system
FPR4100-8-A /system # scope services
FPR4100-8-A /system/services # show ntp-server detail
NTP server hostname: Name: 172.16.38.65 Time 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:
```

Überprüfen Sie die NTP-Zuordnung:

```
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
```

Überprüfen Sie die 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
```

Überprüfen der NTP-Synchronisierung zwischen MIO und logischem Gerät (Blade) auf FPR41xx/9300-Appliances

Auf FPR41xx/9300 werden die NTP-Einstellungen über die MIO (Chassis) an FTD übermittelt. Die NTP-Konfiguration über die FTD-CLI oder die FMC-UI ist nicht möglich.

Jeder FTD-Blade nutzt die interne Referenz-ID 203.0.113.126, um zur Zeitsynchronisierung mit der MIO zu kommunizieren. Basierend darauf wird angezeigt, ob eine Synchronisierung erfolgt. Die FTD-CLI spiegelt dies wider. Die NTP-IP in diesem Beispiel ist die interne Ref-ID und nicht die tatsächliche NTP-Server-IP. Eine Änderung der IP-Adresse des NTP-Servers im FCM wirkt sich nicht auf diese Ausgabe aus, da die Referenz-ID immer dieselbe ist:

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

Überprüfen der NTP-Konfiguration von FPR1xxx/2100-Appliances

Achtung: Dies gilt nur für FPR1xxx/2100-Appliances für ASA im Plattformmodus.

```
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:
```

Fehlerbehebung bei gängigen Problemen

1. FXOS konnte den NTP-Server-Hostnamen nicht auflösen

Die FCM-Benutzeroberfläche zeigt Folgendes an:

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

Empfohlene Aktion

Verwenden Sie den Befehl ping, um die Hostnamenauflösung des NTP-Servers zu überprüfen.



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

Mögliche Ursachen

- Der DNS-Server ist nicht konfiguriert.
- Der DNS-Server kann den Hostnamen nicht auflösen.

2. Verbindungsprobleme zwischen FXOS - NTP-Server auf UDP-Port 123

Die FCM-Benutzeroberfläche zeigt Folgendes an:

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

Empfohlene Aktion

Achtung: Die Erfassung von Ethalyzer an der Chassis-Management-Schnittstelle ist nur auf FPR41xx/9300-Appliances verfügbar.

Aufnahmen an der Chassis-Managementschnittstelle und Überprüfung der bidirektionalen Kommunikation auf UDP-Port 123:

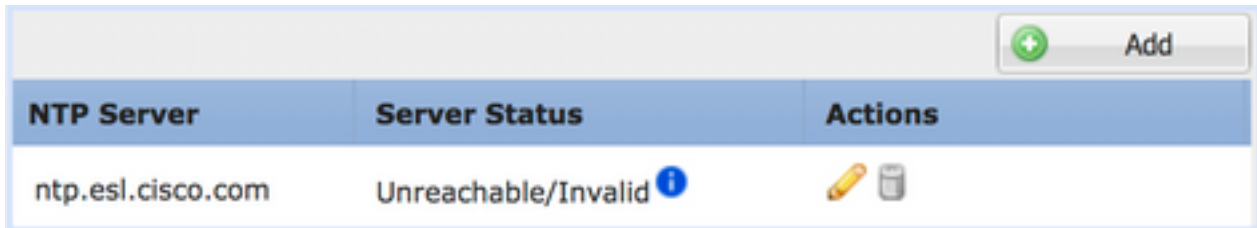
```
KSEC- FPR4100-8-A(fxos)# ethalyzer local interface mgmt capture-filter "udp port 123"
Capturing on 'eth0'
1 2020-04-30 20:09:54.150237760 10.62.148.196 172.16.4.161 NTP 90 NTP Version 3, client
2 2020-04-30 20:14:14.150172804 10.62.148.196 172.16.4.161 NTP 90 NTP Version 3, client
3 2020-04-30 20:23:13.150171682 10.62.148.196 172.16.4.161 NTP 90 NTP Version 3, client
```



Mögliche Ursachen

- Der konfigurierte Server ist kein NTP-Server.
- Ein Gerät im Pfad (z. B. die Firewall) blockiert oder ändert den Datenverkehr.

3. Intermittierende Verbindungsprobleme zwischen FXOS und NTP-Server

Die FCM-Benutzeroberfläche zeigt Folgendes an:



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

Empfohlene Maßnahmen

Achtung: Nur für FPR41xx/9300-Appliances.

Initiieren des NTP-Synchronisierungsprozesses von der FXOS-CLI aus

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

Erfassung über die Chassis-Managementschnittstelle mit dem Befehlszeilentool **ethalyzer** CLI

Mögliche Ursache

- Intermittierende Verbindungsprobleme zwischen FXOS - NTP-Server

Verwandte Fehler

Überprüfen Sie die Versionshinweise auf bekannte/behobene Fehler.

Zugehörige Informationen

- [FXOS-Konfigurationsleitfäden](#)
- [Fehlerbehebung bei Problemen mit dem Network Time Protocol \(NTP\) in FirePOWER-Systemen](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.