Fehlerbehebung bei Problemen mit Network Time Protocol (NTP) auf FireSIGHT-Systemen

Inhalt

[Einleitung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Hintergrundinformationen](#)
[Symptome](#)
[Fehlerbehebung](#)
[Schritt 1: Überprüfen der NTP-Konfiguration](#)
[Überprüfen in Version 5.4 und früheren Versionen](#)
[Überprüfen in Version 6.0 und höher](#)
[Schritt 2: Identifizieren eines Timeservers und seines Status](#)
[Schritt 3: Überprüfen der Verbindung](#)
[Schritt 4: Überprüfen der Konfigurationsdateien](#)

Einleitung

In diesem Dokument werden häufige Probleme bei der Zeitsynchronisierung auf FireSIGHT-Systemen beschrieben, und es wird beschrieben, wie diese behoben werden können.

Voraussetzungen

Anforderungen

Um die Einstellung für die Zeitsynchronisierung zu konfigurieren, benötigen Sie Zugriff auf die Admin-Ebene Ihres FireSIGHT Management Center.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

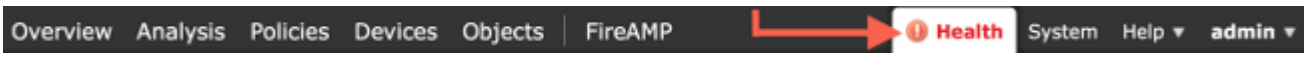
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen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

Hintergrundinformationen

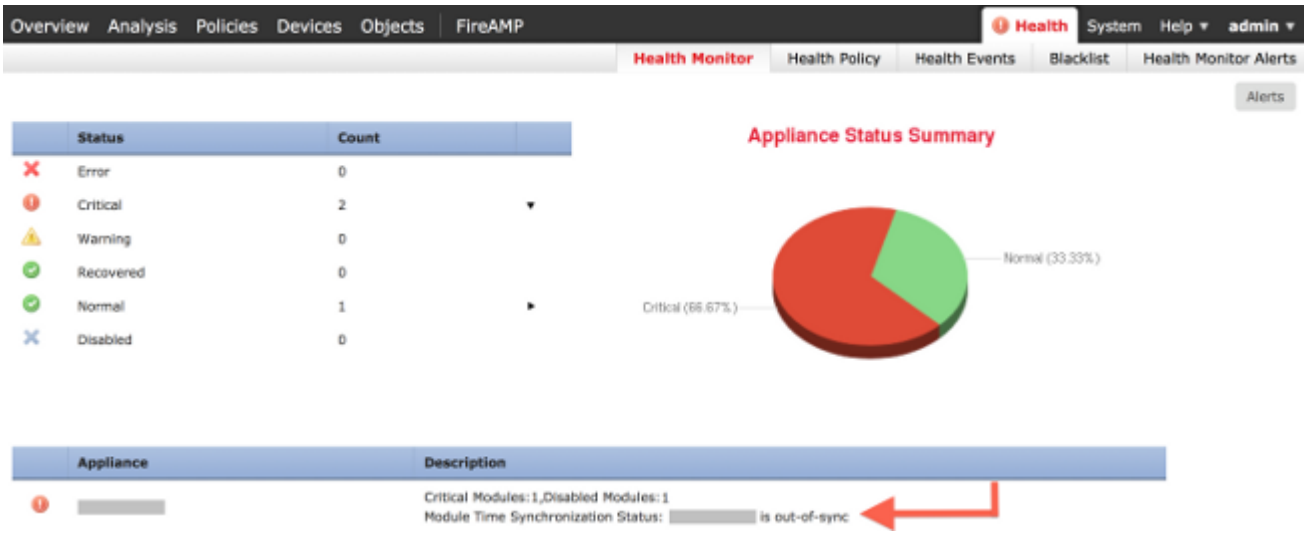
Sie können die Zeit zwischen Ihren FireSIGHT-Systemen auf drei verschiedene Arten synchronisieren, z. B. manuell mit externen NTP-Servern (Network Time Protocol) oder mit FireSIGHT Management Center, das als NTP-Server dient. Sie können ein FireSIGHT Management Center mit NTP als Zeitserver konfigurieren und dann die Zeit zwischen dem FireSIGHT Management Center und verwalteten Geräten synchronisieren.

Symptome

- FireSIGHT Management Center zeigt Statuswarnungen in der Browser-Oberfläche an.



- Auf der Seite **Integritätsmonitor** wird eine Appliance als kritisch angezeigt, da der Status des Zeitsynchronisierungsmoduls nicht synchronisiert ist.



- Wenn die Appliances nicht synchronisiert werden können, werden gelegentlich Warnmeldungen angezeigt.
- Nachdem eine Systemrichtlinie angewendet wurde, werden Integritätswarnungen angezeigt, da die Synchronisierung eines FireSIGHT Management Center und seiner verwalteten Geräte bis zu 20 Minuten dauern kann. Der Grund hierfür ist, dass ein FireSIGHT Management Center zunächst eine Synchronisierung mit dem konfigurierten NTP-Server durchführen muss, bevor die Uhrzeit an ein verwaltetes Gerät übertragen werden kann.
- Die Zeit zwischen einem FireSIGHT Management Center und einem verwalteten Gerät stimmt nicht überein.
- Am Sensor erzeugte Ereignisse können Minuten oder Stunden dauern, bis sie in einem FireSIGHT Management Center angezeigt werden.
- Wenn Sie virtuelle Appliances ausführen und die Seite **Systemüberwachung** anzeigt, dass die Uhr für Ihre virtuelle Appliance nicht synchronisiert ist, überprüfen Sie die Einstellungen für die Zeitsynchronisierung der Systemrichtlinie. Cisco empfiehlt, die virtuellen Appliances mit einem physischen NTP-Server zu synchronisieren. Synchronisieren Sie Ihre verwalteten Geräte (virtuell oder physisch) nicht mit einem virtuellen Verteidigungszentrum.

Fehlerbehebung

Schritt 1: Überprüfen der NTP-Konfiguration

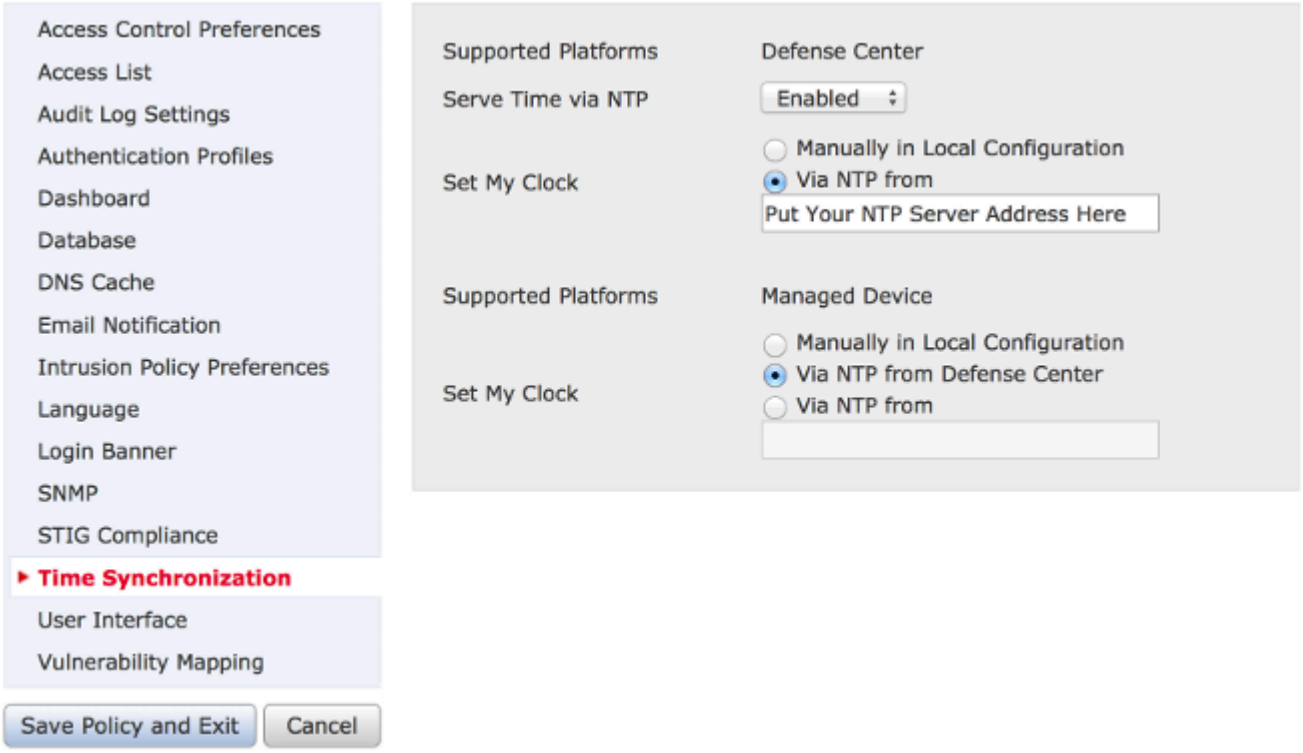
Überprüfen in Version 5.4 und früheren Versionen

Überprüfen Sie, ob NTP in der Systemrichtlinie aktiviert ist, die auf die FireSIGHT-Systeme angewendet wird. Gehen Sie wie folgt vor, um dies zu überprüfen:

1. Wählen Sie **System > Local > System Policy (System > Lokal > Systemrichtlinie)**.
2. Bearbeiten Sie die auf Ihre FireSIGHT-Systeme angewendete Systemrichtlinie.
3. Wählen Sie **Zeitsynchronisierung aus**.

Überprüfen Sie, ob für das FireSIGHT Management Center (auch Defense Center oder DC genannt) die Uhr **Via NTP von** eingestellt ist, und geben Sie die Adresse eines NTP-Servers an. Stellen Sie außerdem sicher, dass das verwaltete Gerät **über NTP vom Defense Center** auf eingestellt ist.

Wenn Sie einen externen Remote-NTP-Server angeben, muss Ihre Appliance über Netzwerkzugriff verfügen. Geben Sie keinen nicht vertrauenswürdigen NTP-Server an. Synchronisieren Sie Ihre verwalteten Geräte (virtuell oder physisch) nicht mit einem virtuellen FireSIGHT Management Center. Cisco empfiehlt, die virtuellen Appliances mit einem physischen NTP-Server zu synchronisieren.



Überprüfen in Version 6.0 und höher

In Version 6.0.0 und höher werden die Zeitsynchronisierungseinstellungen an verschiedenen Stellen im Firepower Management Center konfiguriert, obwohl sie die gleiche Logik wie die Schritte für 5.4 verfolgen.

Die Zeitsynchronisierungseinstellungen für das FirePOWER Management Center selbst finden Sie unter **System > Configuration > Time Synchronization**.

Die Zeitsynchronisierungseinstellungen für die verwalteten Geräte finden Sie unter **Geräte > Plattformeinstellungen.** Klicken Sie neben der auf das Gerät angewendeten Richtlinie für die Plattformeinstellungen auf **Bearbeiten**, und wählen Sie dann **Zeitsynchronisierung aus.**

Nachdem Sie die Konfiguration für die Zeitsynchronisierung angewendet haben (unabhängig von der Version), stellen Sie sicher, dass die Uhrzeit auf dem Management Center und den verwalteten Geräten übereinstimmt. Andernfalls kann es zu unbeabsichtigten Folgen kommen, wenn die verwalteten Geräte mit dem Management Center kommunizieren.

Schritt 2: Identifizieren eines Timeservers und seines Status

- Um Informationen über die Verbindung mit einem Zeitserver zu sammeln, geben Sie den folgenden Befehl in Ihrem FireSIGHT Management Center ein:
  <#root>

```
admin@FireSIGHT:~$
```

ntpq -pn

```
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*198.51.100.2   203.0.113.3      2 u  417 1024  377   76.814    3.458   1.992
```

Ein Sternchen "*" unter der Fernbedienung zeigt den Server an, mit dem Sie gerade synchronisiert werden. Wenn ein Eintrag mit einem Sternchen nicht verfügbar ist, wird die Uhr derzeit nicht mit ihrer Zeitquelle synchronisiert.

Auf einem verwalteten Gerät können Sie diesen Befehl in der Shell eingeben, um die Adresse Ihres NTP-Servers zu bestimmen:

<#root>

>

show ntp

```
NTP Server               : 127.0.0.2  (Cannot Resolve)
Status                   : Being Used
Offset                   : -8.344 (milliseconds)
Last Update              : 188 (seconds)
```

> **Hinweis:** Wenn ein verwaltetes Gerät so konfiguriert ist, dass es Zeit von einem FireSIGHT Management Center erhält, zeigt das Gerät eine Zeitquelle mit Loopback-Adresse an, z. B. 127.0.0.2. Diese IP-Adresse ist ein Sfipproxy-Eintrag und gibt an, dass das virtuelle Verwaltungsnetzwerk zum Synchronisieren der Zeit verwendet wird.

- Wenn eine Appliance anzeigt, dass sie eine Synchronisierung mit 127.127.1.1 durchführt, weist sie darauf hin, dass die Appliance eine Synchronisierung mit ihrer eigenen Uhr durchführt. Sie tritt auf, wenn ein in einer Systemrichtlinie konfigurierter Timeserver nicht synchronisierbar ist. Beispiele:
<#root>

```
admin@FirePOWER:~$
```

ntpq -pn

```
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 192.0.2.200     .INIT.          16 u    - 1024    0    0.000    0.000   0.000
*127.127.1.1     .SFCL.          14 l    3   64  377    0.000    0.000   0.001
```

- Wenn Sie in der Ausgabe des Befehls ntpq feststellen, dass der Wert von st (stratum) 16 ist, bedeutet dies, dass der Timeserver nicht erreichbar ist und die Appliance nicht mit diesem Timeserver synchronisiert werden kann.
- In der ntpq-Befehlsausgabe zeigt reach eine Oktalzahl an, die angibt, ob die Quelle für die letzten acht

Abfrageversuche erreicht wurde oder nicht. Wenn Sie den Wert 377 sehen, bedeutet dies, dass die letzten 8 Versuche erfolgreich waren. Alle anderen Werte können darauf hinweisen, dass einer oder mehrere der letzten acht Versuche erfolglos waren.

Schritt 3: Überprüfen der Verbindung

1. Überprüfen Sie die grundlegende Verbindung zum Zeitserver.
   <#root>

   ```
   admin@FireSIGHT:~$

   ping
   ```

2. Stellen Sie sicher, dass Port 123 auf Ihrem FireSIGHT-System offen ist.
   <#root>

   ```
   admin@FireSIGHT:~$

   netstat -an | grep 123
   ```

3. Vergewissern Sie sich, dass Port 123 auf der Firewall geöffnet ist.
4. Hardware-Uhr prüfen:
   <#root>

   ```
   admin@FireSIGHT:~$

   sudo hwclock
   ```

   Wenn die Hardwareuhr zu weit veraltet ist, kann sie nie erfolgreich synchronisiert werden. Geben Sie den folgenden Befehl ein, um die manuelle Einrichtung der Uhr über einen Zeitserver zu erzwingen:

   <#root>

   ```
   admin@FireSIGHT:~$

   sudo ntpdate -u
   ```

   Anschließend Neustart ntpd:

   <#root>

   ```
   admin@FireSIGHT:~$
   ```

```
sudo pmtool restartbyid ntpd
```

Schritt 4: Überprüfen der Konfigurationsdateien

1. Überprüfen Sie, ob die Datei sfipproxy.conf korrekt ausgefüllt wurde. Diese Datei sendet NTP-Datenverkehr über den Sftunnel.

   Ein Beispiel für die Datei /etc/sf/sfipproxy.conf auf einem verwalteten Gerät ist hier dargestellt:

   <#root>

   ```
   admin@FirePOWER:~$
   ```

   sudo cat /etc/sf/sfipproxy.conf

```
config
{
    nodaemon 1;
}
peers
{
    dbef067c-4d5b-11e4-a08b-b3f170684648
    {
        services
        {
            ntp
            {
                listen_ip 127.0.0.2;
                listen_port 123;
                protocol udp;
                timeout 20;
            }
        }
    }
}
```

   Ein Beispiel für die Datei /etc/sf/sfipproxy.conf in einem FireSIGHT Management Center ist hier dargestellt:

   <#root>

   ```
   admin@FireSIGHT:~$
   ```

   sudo cat /etc/sf/sfipproxy.conf

```
config
{
```

```
    nodaemon 1;
}
peers
{
    854178f4-4eec-11e4-99ed-8b16d263763e
    {
        services
        {
            ntp
            {
                protocol udp;
                server_ip 127.0.0.1;
                server_port 123;
                timeout 10;
            }
        }
    }
}
```

2. Stellen Sie sicher, dass der Universally Unique Identifier (UUID) unter dem Peers-Abschnitt mit der ims.conf-Datei des Peers übereinstimmt. Beispielsweise muss die UUID, die im Abschnitt Peers der Datei /etc/sf/sfipproxy.conf in einem FireSIGHT Management Center gefunden wurde, mit der UUID übereinstimmen, die in der Datei /etc/ims.conf des verwalteten Geräts gefunden wurde. Ebenso muss die UUID, die im Peers-Abschnitt der Datei /etc/sf/sfipproxy.conf auf einem verwalteten Gerät gefunden wird, mit der UUID übereinstimmen, die in der /etc/ims.conf-Datei der Management-Appliance gefunden wird.

   Sie können die UUID der Geräte mit dem folgenden Befehl abrufen:

   <#root>

   ```
   admin@FireSIGHT:~$
   ```

   sudo grep UUID /etc/sf/ims.conf

   ```
   APPLIANCE_UUID=dbef067c-4d5b-11e4-a08b-b3f170684648
   ```

   Diese müssen in der Regel automatisch von der Systemrichtlinie ausgefüllt werden, aber es gab Fälle, in denen diese Strophen verloren gingen. Wenn sie geändert werden müssen, müssen Sie sfipproxy und sftunnel wie in diesem Beispiel gezeigt neu starten:

   <#root>

   ```
   admin@FireSIGHT:~$
   ```

   sudo pmtool restartbyid sfipproxy

   ```
   admin@FireSIGHT:~$
   ```

   sudo pmtool restartbyid sftunnel

3. Überprüfen Sie, ob im Verzeichnis /etc eine Datei ntp.conf verfügbar ist.

<#root>

admin@FireSIGHT:~$

ls /etc/ntp.conf*

Wenn eine NTP-Konfigurationsdatei nicht verfügbar ist, können Sie eine Kopie der Sicherungskonfigurationsdatei erstellen. Beispiele:

<#root>

admin@FireSIGHT:~$

sudo cp /etc/ntp.conf.bak /etc/ntp.conf

4. Überprüfen Sie, ob die Datei /etc/ntp.conf richtig ausgefüllt wurde. Wenn Sie eine Systemrichtlinie anwenden, wird die Datei ntp.conf neu geschrieben.

> **Hinweis**: Die Ausgabe einer ntp.conf-Datei zeigt die Timeserver-Einstellungen an, die für eine Systemrichtlinie konfiguriert wurden. Der Zeitstempeleintrag muss die Zeit anzeigen, zu der die letzte Systemrichtlinie auf ein Gerät angewendet wurde. Der Servereintrag muss die angegebene Timeserver-Adresse enthalten.

<#root>

admin@FireSIGHT:~$

sudo cat /etc/ntp.conf

```
# automatically generated by /etc/sysconfig/configure-network ; do not edit
# Tue Oct 21 17:44:03 UTC 2014

restrict default noquery nomodify notrap nopeer
restrict 127.0.0.1
server 198.51.100.2
logfile /var/log/ntp.log
driftfile /etc/ntp.drift
```

Überprüfen Sie die NTP-Versionen auf zwei Geräten, und vergewissern Sie sich, dass dies auch der Fall ist.

Weitere Informationen zu NTP-Grundlagen finden Sie unter Best Practices für Network Time Protocol verwenden.

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.