# Problemas del Troubleshooting con el Network Time Protocol (NTP) en los sistemas de FirePOWER

## Contenido



## Introducción

Este documento describe los problemas frecuentes con la sincronización horaria en los sistemas de FireSIGHT y cómo resolverlos problemas. Usted puede elegir sincronizar el tiempo entre sus sistemas de FireSIGHT en tres maneras diferentes, tales como manualmente con los servidores externos del Network Time Protocol (NTP), o con el centro de administración de FireSIGHT que sirve como servidor NTP. Usted puede configurar un centro de administración de FireSIGHT como un Servidor de tiempo con el NTP y después lo utiliza para sincronizar el tiempo entre el centro de administración de FireSIGHT y los dispositivos administrados.

## Prerequisites

### Requisitos

Para configurar la configuración de la sincronización horaria, usted necesita el nivel `admin de` acceso en su centro de administración de FireSIGHT.

### Componentes Utilizados

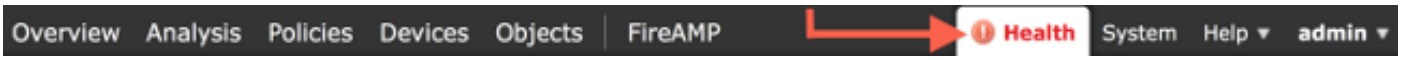
Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando,

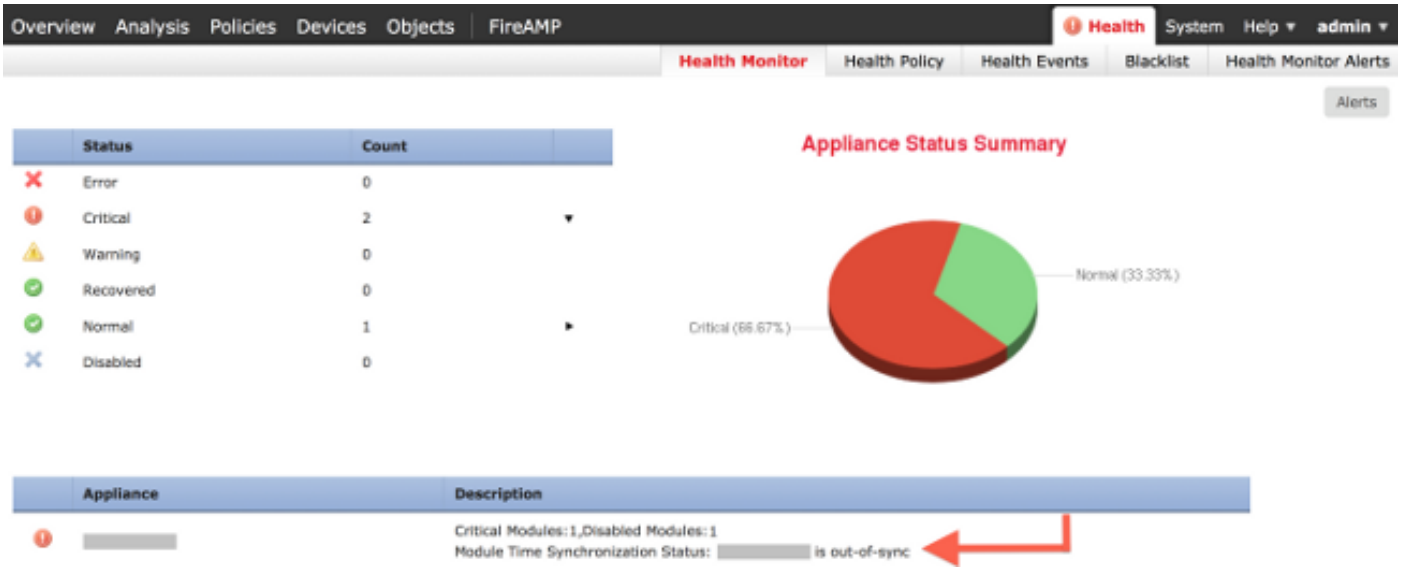
asegúrese de haber comprendido el impacto que puede tener cualquier comando.

# Síntomas

- El centro de administración de FireSIGHT visualiza las alertas de la salud en la interfaz Web.




- La página del **control de salud** muestra un dispositivo como critial, porque es el estatus del módulo de la sincronización horaria hacia fuera-de-sincronice.




- Usted puede ser que vea las alertas intermitentes de la salud si los dispositivos no pueden permanecer sincronizados.
- Después de que una política del sistema sea aplicada usted puede ser que vea las alertas de la salud, porque un centro de administración de FireSIGHT y sus dispositivos administrados podrían tomar hasta 20 minutos para completar la sincronización. Esto es porque un centro de administración de FireSIGHT debe primero sincronizar con su servidor NTP configurado antes de que pueda servir el tiempo a un dispositivo administrado.
- El tiempo entre un centro de administración de FireSIGHT y un dispositivo administrado no hace juego.
- Los eventos generados en el sensor pudieron tardar los minutos o las horas para llegar a ser visibles en un centro de administración de FireSIGHT.
- Si usted ejecuta los dispositivos virtuales y la página del **control de salud** indica que la configuración del reloj para su dispositivo virtual no está sincronizada, marque sus configuraciones de la sincronización horaria de la política del sistema. Cisco recomienda que usted sincroniza sus dispositivos virtuales a un servidor NTP físico. No sincronice sus dispositivos administrados (virtuales o físicos) a un centro virtual de la defensa.

# Troubleshooting

## Paso 1: Verifique la configuración del NTP

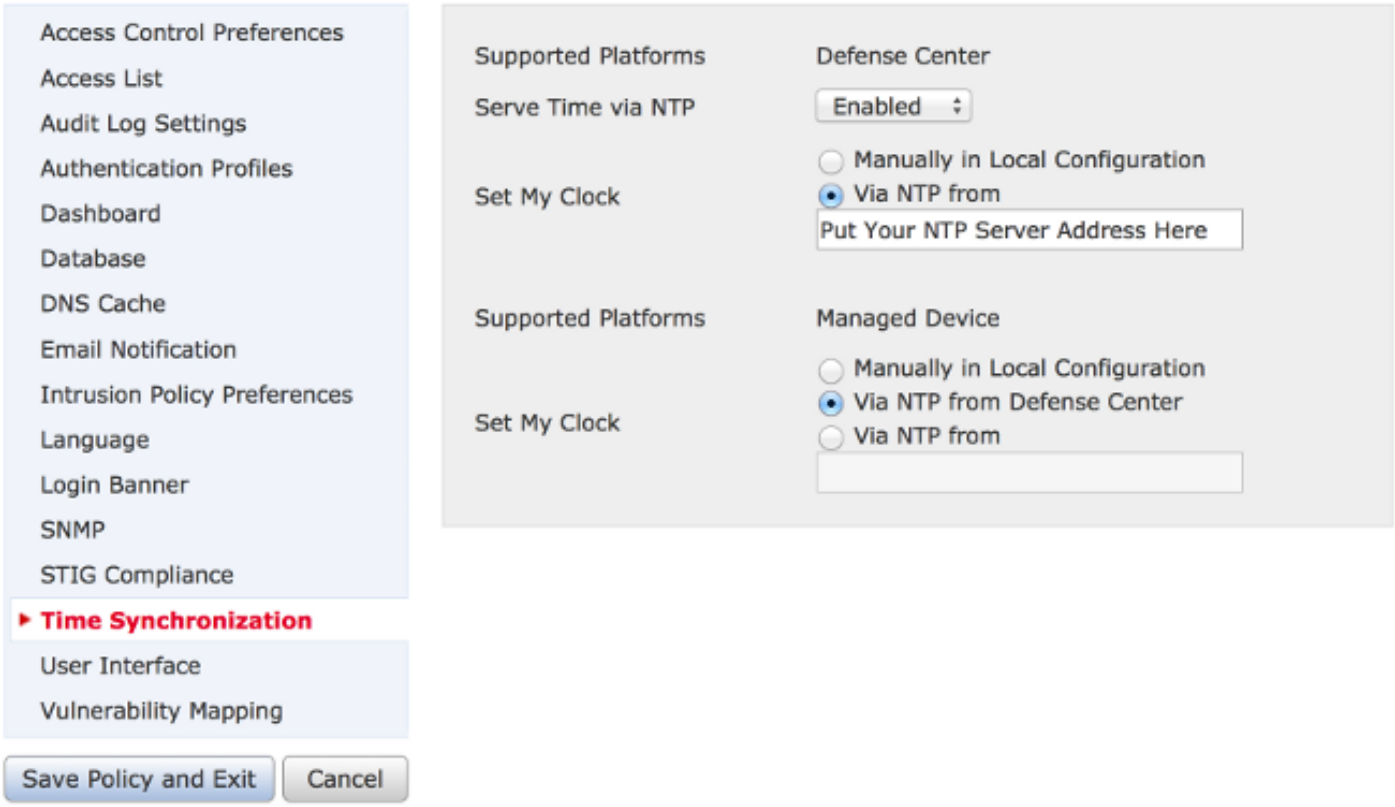
### Cómo verificar en las versiones 5.4 y anterior

Verifique que el NTP esté habilitado en la política del sistema que se aplica en los sistemas de FireSIGHT. Para verificar eso, complete estos pasos:

1. Elija el **sistema > el Local > la política del sistema**.
2. Edite la política del sistema aplicada en sus sistemas de FireSIGHT.
3. Elija la **sincronización horaria**.

Marque si el centro de administración de FireSIGHT (también conocido como el centro o DC de la defensa) tiene el reloj fijado **vía al NTP de**, y un direccionamiento de un servidor NTP se proporciona. También confirme que el dispositivo administrado está fijado **vía al NTP del centro de la defensa**.

Si usted especifica a un servidor NTP externo remoto, su dispositivo debe tener acceso a la red a él. No especifique a un servidor NTP untrusted. No sincronice sus dispositivos administrados (virtuales o físicos) a un centro de administración virtual de FireSIGHT. Cisco recomienda que usted sincroniza sus dispositivos virtuales a un servidor NTP físico.




### Cómo verificar en las versiones 6.0 y posterior

En las versiones 6.0.0 y posterior, las configuraciones de la sincronización horaria se configuran en los lugares separados en el centro de administración de FirePOWER, aunque siguen la misma lógica que los pasos para 5.4.

Las configuraciones para el centro de administración de FirePOWER sí mismo de la sincronización horaria se encuentran bajo el **sistema > la configuración > sincronización horaria**.

Las configuraciones de la sincronización horaria para los dispositivos administrados se encuentran bajo los **dispositivos > configuraciones de la plataforma.** Haga clic **editan** al lado de las configuraciones de la plataforma la directiva aplicada al dispositivo y después eligen la **sincronización horaria.**

Después de que usted aplique la configuración para la sincronización horaria (sin importar la versión), aseegurese que el tiempo en su centro de administración y coincidencias de los dispositivos administrados. Si no, las consecuencias involuntarias pudieron ocurrir cuando los dispositivos administrados comunican con el centro de administración.

## Paso 2: Identifique a un Timeserver y es estatus

- Para recopilar la información sobre la conexión a un Servidor de tiempo, ingrese este comando en su centro de administración de FireSIGHT:
  ```
  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
  ```
  Un asterisco “*” bajo el `telecontrol` indica el servidor que le sincronizan actualmente a. Si una entrada con un asterisco es inasequible, el reloj no se sincroniza actualmente con él es timesource.En un dispositivo administrado, usted puede ingresar este comando en el shell para determinar el direccionamiento de su servidor NTP:
  ```
  > show ntp

  NTP Server : 127.0.0.2 (Cannot Resolve)
  Status : Being Used
  Offset : -8.344 (milliseconds)
  Last Update : 188 (seconds)
  ```
  **Note**: Si un dispositivo administrado se configura para recibir el tiempo de un centro de administración de FireSIGHT, el dispositivo muestra un timesource con el Loopback Address, tal como `127.0.0.2`. Esta dirección IP es una entrada del sfipproxy e indica que la red virtual de la Administración se está utilizando para sincronizar el tiempo.
- Si las visualizaciones de un dispositivo que sincroniza con `127.127.1.1`, él indican que el dispositivo sincroniza con su propio reloj. Ocurre cuando un timeserver configurado en una política del sistema no es synchronizable. Por ejemplo:
  ```
  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
  ```
- En la salida de comando del `ntpq`, si usted nota el valor de `st` (estrato) es 16, él indica que el timeserver es inalcanzable y el dispositivo no puede sychronize con ese timeserver.
- En la salida de comando del `ntpq`, el `alcance` muestra un número octal que indique el éxito o el error de alcanzar la fuente para las ocho tentativas que sondean más recientes. Si usted ve el valor es 377, él significa que las tentativas del último 8 eran acertadas. Cualquier otro valor pudo indicar que uno o más de las ocho tentativas más recientes eran fracasadas.

## Paso 3: Verifique la Conectividad

1. Marque la conectividad básica al Servidor de tiempo.
   ```
   admin@FireSIGHT:~$ ping <IP_addres_of_NTP_server>
   ```
2. Asegúrese de que el puerto 123 esté abierto en su sistema de FireSIGHT.
   ```
   admin@FireSIGHT:~$ netstat -an | grep 123
   ```
3. Confirme que el puerto 123 está abierto en el Firewall.
4. Marque el reloj de hardware:
   ```
   admin@FireSIGHT:~$ sudo hwclock
   ```

Si el reloj de hardware es anticuado demasiado lejano, puede ser que sincronicen nunca con éxito. Para forzar manualmente el reloj para ser fijado con un Servidor de tiempo, ingrese este comando:

```
admin@FireSIGHT:~$ sudo ntpdate -u <IP_address_of_known_good_timesource>
```

Entonces `ntpd del` reinicio:

```
admin@FireSIGHT:~$ sudo pmtool restartbyid ntpd
```

## Paso 4: Verifique los archivos de configuración

1. Marque si el `archivo sfipproxy.conf` se puebla correctamente. Este archivo envía el tráfico NTP sobre el sftunnel.
   Un ejemplo del archivo de `/etc/sf/sfipproxy.conf` en un dispositivo administrado se muestra aquí:

```
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;
}
}
}
}
```

   Un ejemplo del archivo de `/etc/sf/sfipproxy.conf` en un centro de administración de FireSIGHT se muestra aquí:

```
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. Aseegurese que universal el Identificador único (UUID) bajo coincidencias de la sección de los `pares` con el `archivo ims.conf el` par. Por ejemplo, el UUID encontrado bajo el peerssection del `archivo de` /etc/sf/sfipproxy.conf en un centro de administración de FireSIGHT debe hacer juego con el UUID encontrado en el `archivo de` /etc/ims.conf de su dispositivo administrado. Semejantemente, el UUID encontrado bajo el peerssection del `archivo de` /etc/sf/sfipproxy.conf en un dispositivo administrado debe hacer juego con el UUID encontrado en el `archivo de` /etc/ims.conf de su dispositivo de la Administración. Usted puede extraer el UUID de los dispositivos con este comando:

```
admin@FireSIGHT:~$ sudo grep UUID /etc/sf/ims.conf

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

   Éstos se deben poblar normalmente automáticamente por la política del sistema, pero ha habido casos donde estaban que falta estas estrofas. Si necesitan ser modificadas o ser cambiadas usted necesitará recomenzar el sfipproxy y el sftunnel como sigue:

```
admin@FireSIGHT:~$ sudo pmtool restartbyid sfipproxy
admin@FireSIGHT:~$ sudo pmtool restartbyid sftunnel
```

3. Verifique si un `archivo ntp.conf` está disponible en el `directorio de` /etc.

```
admin@FireSIGHT:~$ ls /etc/ntp.conf*
```

   Si un archivo de configuración del NTP es inasequible, usted puede hacer una copia del archivo de configuración de respaldo. Por ejemplo:

```
admin@FireSIGHT:~$ sudo cp /etc/ntp.conf.bak /etc/ntp.conf
```

4. Verifique si el archivo de `/etc/ntp.conf` se puebla correctamente. Cuando usted aplica una política del sistema, se reescribe el `archivo ntp.conf`. **Note**: La salida de un `archivo ntp.conf` muestra las configuraciones del timeserver configuradas en una política del sistema. La entrada del sello de fecha/hora debe mostrar el tiempo en que la política del sistema más reciente se aplicó a un dispositivo. La Entrada de servidor muestre el direccionamiento especificado del timeserver.

```
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
```