Resolución de problemas con el protocolo de tiempo de la red (NTP) en sistemas FireSIGHT

Contenido

Introducción

Este documento describe problemas comunes con la sincronización horaria en los sistemas FireSIGHT y cómo solucionarlos.

Prerequisites

Requirements

Para configurar la configuración de sincronización horaria, necesita el nivel de acceso admin en su FireSIGHT Management Center.

Componentes Utilizados

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

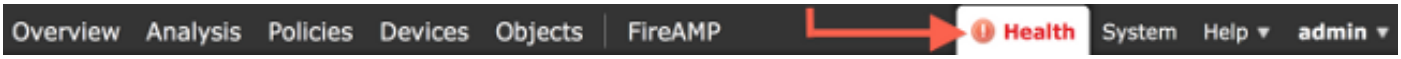
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

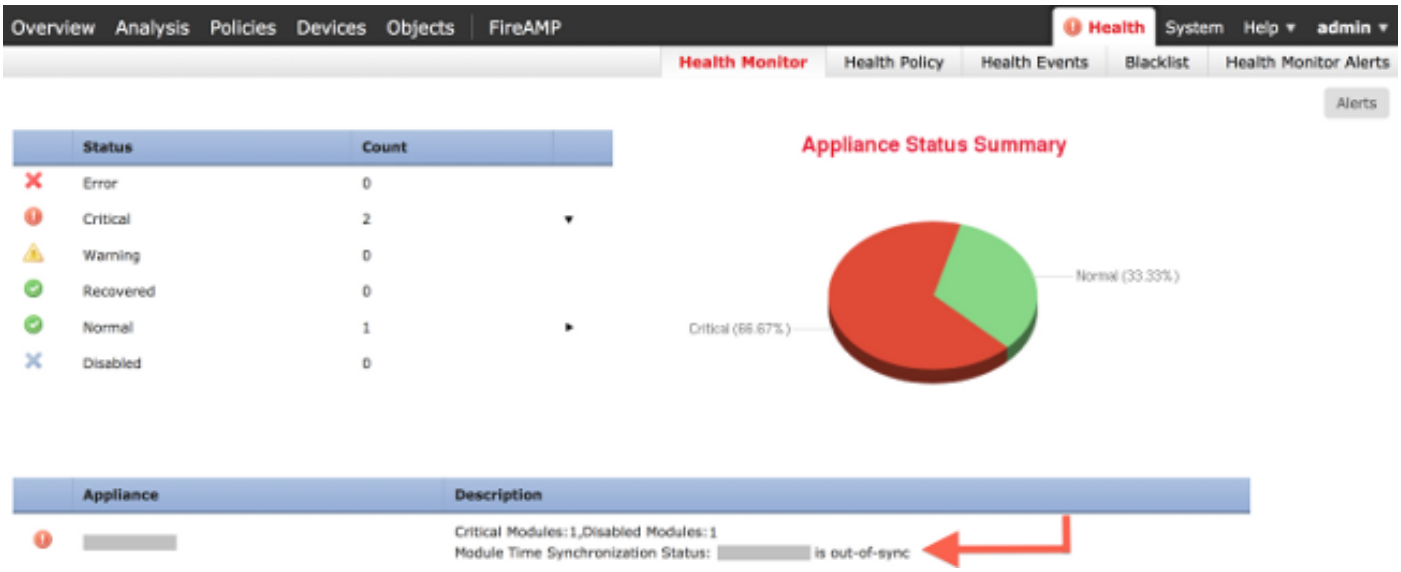
Puede optar por sincronizar la hora entre los sistemas FireSIGHT de tres formas diferentes, como manualmente con servidores externos de protocolo de tiempo de la red (NTP) o con FireSIGHT Management Center, que actúa como servidor NTP. Puede configurar FireSIGHT Management Center como servidor de hora con NTP y, a continuación, utilizarlo para sincronizar la hora entre FireSIGHT Management Center y los dispositivos administrados.

Síntomas

- FireSIGHT Management Center muestra alertas de estado en la interfaz del navegador.



- La página Health Monitor muestra un dispositivo como crítico, porque el estado del módulo de sincronización horaria no está sincronizado.



- Puede ver alertas de estado intermitentes si los dispositivos no se mantienen sincronizados.
- Después de aplicar una política del sistema, puede ver las alertas de estado, ya que FireSIGHT Management Center y sus dispositivos administrados podrían tardar hasta 20 minutos en completar la sincronización. Esto se debe a que FireSIGHT Management Center debe sincronizarse primero con su servidor NTP configurado antes de poder dedicar tiempo a un dispositivo administrado.
- El tiempo entre un FireSIGHT Management Center y un dispositivo administrado no coincide.
- Los eventos generados en el sensor pueden tardar minutos u horas en hacerse visibles en un FireSIGHT Management Center.
- Si ejecuta dispositivos virtuales y la página Health Monitor indica que la configuración del reloj del dispositivo virtual no está sincronizada, compruebe la configuración de sincronización horaria de la directiva del sistema. Cisco recomienda que sincronice los dispositivos virtuales con un servidor NTP físico. No sincronice los dispositivos administrados (virtuales o físicos) con un Virtual Defense Center.

Troubleshoot

Paso 1: Verificar la configuración de NTP

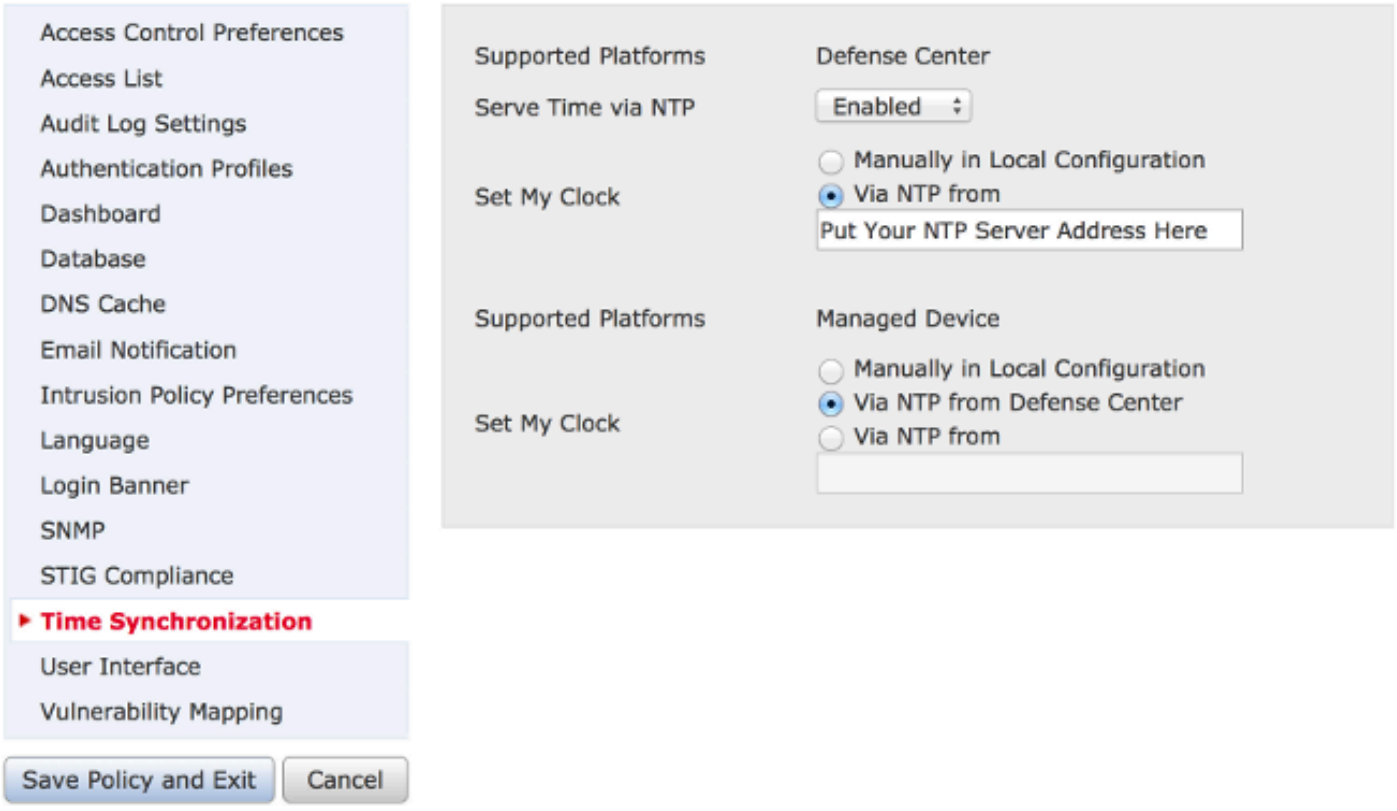
Cómo verificar en las versiones 5.4 y anteriores

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

1. Elija System > Local > System Policy.
2. Edite la política del sistema aplicada en sus sistemas FireSIGHT.
3. Elija Sincronización horaria.

Verifique si FireSIGHT Management Center (también conocido como Defense Center o DC) tiene el reloj configurado en Via NTP from, y si se proporciona una dirección de un servidor NTP. Confirme también que el dispositivo administrado se ha establecido en a través de NTP desde el centro de defensa.

Si especifica un servidor NTP externo remoto, el dispositivo debe tener acceso de red al mismo. No especifique un servidor NTP no confiable. No sincronice los dispositivos administrados (virtuales o físicos) con un FireSIGHT Management Center virtual. Cisco recomienda que sincronice los dispositivos virtuales con un servidor NTP físico.



Cómo verificar en las versiones 6.0 y posteriores

En las versiones 6.0.0 y posteriores, los ajustes de sincronización horaria se configuran en lugares separados en Firepower Management Center, aunque siguen la misma lógica que los pasos de la versión 5.4.

Los ajustes de sincronización horaria para el propio Firepower Management Center se encuentran en System > Configuration > Time Synchronization.

La configuración de sincronización horaria para los dispositivos administrados se encuentra en Dispositivos > Configuración de plataforma. Haga clic en editar junto a la directiva Configuración de la plataforma aplicada al dispositivo y, a continuación, seleccione Sincronización horaria.

Después de aplicar la configuración para la sincronización horaria (independientemente de la versión), asegúrese de que la hora de Management Center y de los dispositivos gestionados coincide. De lo contrario, pueden producirse consecuencias no deseadas cuando los dispositivos administrados se comunican con Management Center.

Paso 2: Identificar un servidor de tiempo y su estado

- Para recopilar información sobre la conexión a un servidor de hora, introduzca este comando en FireSIGHT Management Center:
  <#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
  ```

  Un asterisco '*' debajo del mando a distancia indica el servidor con el que está actualmente sincronizado. Si una entrada con un asterisco no está disponible, el reloj no está sincronizado con su origen de tiempo.

  En un dispositivo administrado, puede ingresar este comando en el shell para determinar la dirección de su servidor NTP:

  <#root>

  ```
  >

  show ntp


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

Nota: Si un dispositivo administrado se configura para recibir tiempo desde un FireSIGHT Management Center, el dispositivo muestra un recurso de tiempo con dirección de loopback, como 127.0.0.2. Esta dirección IP es una entrada sfipproxy e indica que la red virtual de administración se utiliza para sincronizar la hora.

- Si un dispositivo muestra que se sincroniza con 127.127.1.1, indica que el dispositivo se sincroniza con su propio reloj. Se produce cuando un servidor de tiempo configurado en una directiva del sistema no es sincronizable. Por ejemplo:
  <#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
  ```

- En el resultado del comando ntpq, si observa que el valor de st (stratum) es 16, indica que el servidor de tiempo es inalcanzable y que el dispositivo no puede sincronizarse con ese servidor de tiempo.
- En el resultado del comando ntpq, reach muestra un número octal que indica éxito o fracaso en alcanzar el origen para los ocho intentos de sondeo más recientes. Si el valor es 377, significa que los últimos 8 intentos se realizaron correctamente. Cualquier otro valor puede indicar que uno o más de los últimos ocho intentos no tuvieron éxito.

Paso 3: Verificación de la conectividad

1. Compruebe la conectividad básica con el servidor de hora.
   <#root>

   ```
   admin@FireSIGHT:~$

   ping
   ```

2. Asegúrese de que el puerto 123 está abierto en su sistema FireSIGHT.
   <#root>

   ```
   admin@FireSIGHT:~$

   netstat -an | grep 123
   ```

3. Confirme que el puerto 123 esté abierto en el firewall.
4. Compruebe el reloj del hardware:

<#root>

admin@FireSIGHT:~$

sudo hwclock

Si el reloj de hardware está demasiado desactualizado, nunca se podrá sincronizar correctamente. Para forzar manualmente que el reloj se establezca con un servidor de hora, ingrese este comando:

<#root>

admin@FireSIGHT:~$

sudo ntpdate -u

A continuación, reinicie ntpd:

<#root>

admin@FireSIGHT:~$

sudo pmtool restartbyid ntpd

Paso 4: Verificación de los archivos de configuración

1. Verifique si el archivo sfipproxy.conf se ha llenado correctamente. Este archivo envía tráfico NTP a través del sftunnel.

Aquí se muestra un ejemplo del archivo /etc/sf/sfipproxy.conf en un dispositivo administrado:

<#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;
            }
        }
    }
}
```

Aquí se muestra un ejemplo del archivo /etc/sf/sfipproxy.conf en un FireSIGHT Management Center:

<#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. Asegúrese de que el Identificador único universal (UUID) de la sección peers coincida con el archivo ims.conf del peer. Por ejemplo, el UUID que se encuentra en la sección peers del archivo /etc/sf/sfipproxy.conf en un FireSIGHT Management Center debe coincidir con el UUID que se encuentra en el archivo /etc/ims.conf de su dispositivo administrado. De manera similar, el UUID encontrado en la sección peers del archivo /etc/sf/sfipproxy.conf en un dispositivo administrado debe coincidir con el UUID encontrado en el archivo /etc/ims.conf de su dispositivo de administración.

   Puede recuperar el UUID de los dispositivos con este comando:

   <#root>

   admin@FireSIGHT:~$

   sudo grep UUID /etc/sf/ims.conf

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

   Normalmente, la política del sistema debe cumplimentar estos campos de forma automática, pero ha habido casos en los que se han perdido estas estrofas. Si es necesario modificarlos o cambiarlos, debe reiniciar sfipproxy y sftunnel, como se muestra en este ejemplo:

   <#root>

   admin@FireSIGHT:~$

   sudo pmtool restartbyid sfipproxy

   admin@FireSIGHT:~$

   sudo pmtool restartbyid sftunnel

3. Verifique si un archivo ntp.conf está disponible en el directorio /etc.
   <#root>

   admin@FireSIGHT:~$

   ls /etc/ntp.conf*

   Si un archivo de configuración NTP no está disponible, puede realizar una copia desde el archivo de configuración de copia de seguridad. Por ejemplo:

   <#root>

   admin@FireSIGHT:~$

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

4. Verifique si el archivo /etc/ntp.conf se ha llenado correctamente. Cuando se aplica una política del sistema, se reescribe el archivo ntp.conf.

> Nota: La salida de un archivo ntp.conf muestra la configuración del servidor de tiempo configurada en una política del sistema. La entrada de marca de tiempo debe mostrar la hora a la que se aplicó la última política del sistema a un dispositivo. La entrada del servidor debe mostrar la dirección del servidor de hora especificada.

<#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
```

Verifique las versiones de NTP en dos dispositivos y asegúrese de que también sean iguales.

Para obtener detalles sobre los fundamentos de NTP, consulte Uso de Prácticas Recomendadas para el Protocolo de Tiempo de Red.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).