Solucionar problemas com o Network Time Protocol (NTP) em sistemas FireSIGHT

Contents

- Introdução
- Pré-requisitos
  - Requisitos
  - Componentes Utilizados
- Informações de Apoio
- Sintomas
- Troubleshooting
  - Etapa 1: Verifique a configuração do NTP
    - Como verificar nas versões 5.4 e anteriores
    - Como verificar nas versões 6.0 e posteriores
  - Etapa 2: Identificar um Servidor de Tempo e seu Status
  - Etapa 3: Verifique a conectividade
  - Etapa 4: Verifique os arquivos de configuração

Introdução

Este documento descreve problemas comuns com sincronização de tempo em sistemas FireSIGHT e como solucioná-los.

Pré-requisitos

Requisitos

Para definir a configuração de sincronização de horário, você precisa do nível de acesso admin em seu FireSIGHT Management Center.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

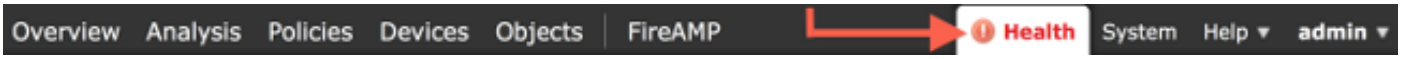
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

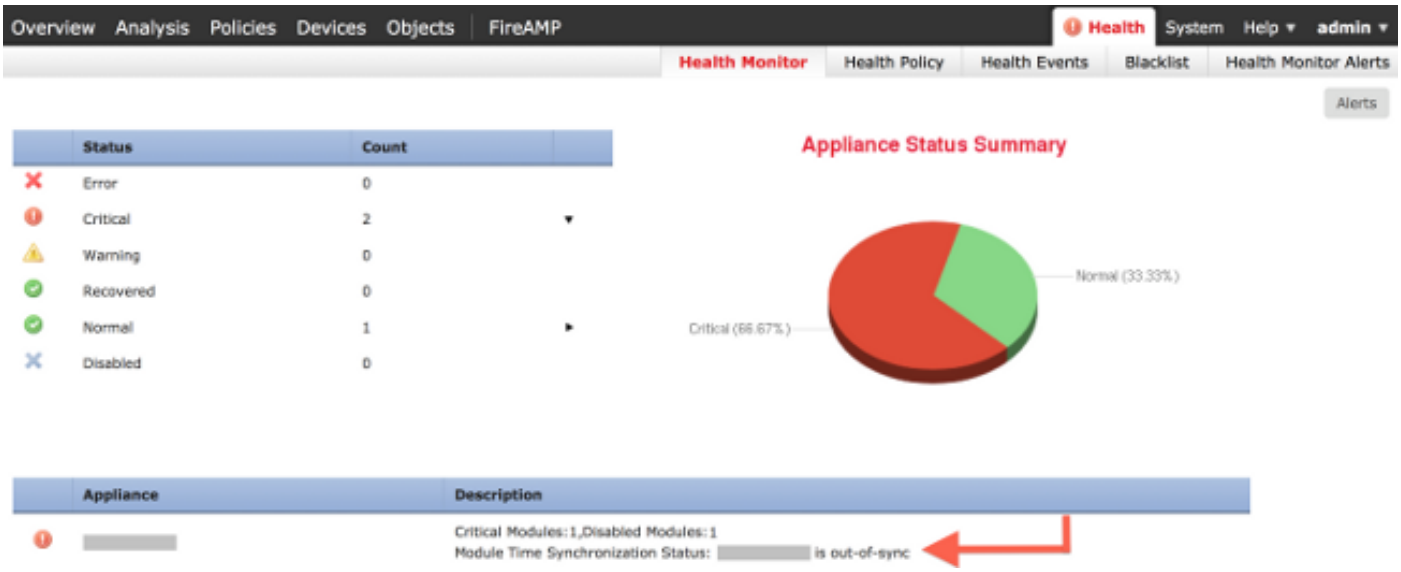
Você pode optar por sincronizar o tempo entre seus FireSIGHT Systems de três maneiras diferentes, como manualmente com servidores NTP (Network Time Protocol) externos ou com o FireSIGHT Management Center, que funciona como um servidor NTP. Você pode configurar um FireSIGHT Management Center como um servidor de horário com NTP e, em seguida, usá-lo para sincronizar o horário entre o FireSIGHT Management Center e os dispositivos gerenciados.

Sintomas

- O FireSIGHT Management Center exibe alertas de integridade na interface do navegador.



- A página Health Monitor mostra um equipamento como crítico, pois o status do Time Synchronization Module está fora de sincronia.



- Você pode ver alertas de integridade intermitentes se os dispositivos não ficarem sincronizados.
- Depois que uma política do sistema é aplicada, você pode ver alertas de integridade, pois um FireSIGHT Management Center e seus dispositivos gerenciados podem levar até 20 minutos para concluir a sincronização. Isso ocorre porque um FireSIGHT Management Center deve primeiro sincronizar com seu servidor NTP configurado para poder atender o tempo de um dispositivo gerenciado.
- O tempo entre um FireSIGHT Management Center e um dispositivo gerenciado não corresponde.
- Os eventos gerados no sensor podem levar minutos ou horas para se tornarem visíveis em um FireSIGHT Management Center.
- Se você executar aplicativos virtuais e a página Monitor de integridade indicar que a configuração do relógio do seu aplicativo virtual não está sincronizada, verifique as configurações de sincronização de horário da política do sistema. A Cisco recomenda que você sincronize seus dispositivos virtuais com um servidor NTP físico. Não sincronize seus dispositivos gerenciados (virtuais ou físicos) com um Centro de Defesa Virtual.

Troubleshooting

Etapa 1: Verifique a configuração do NTP

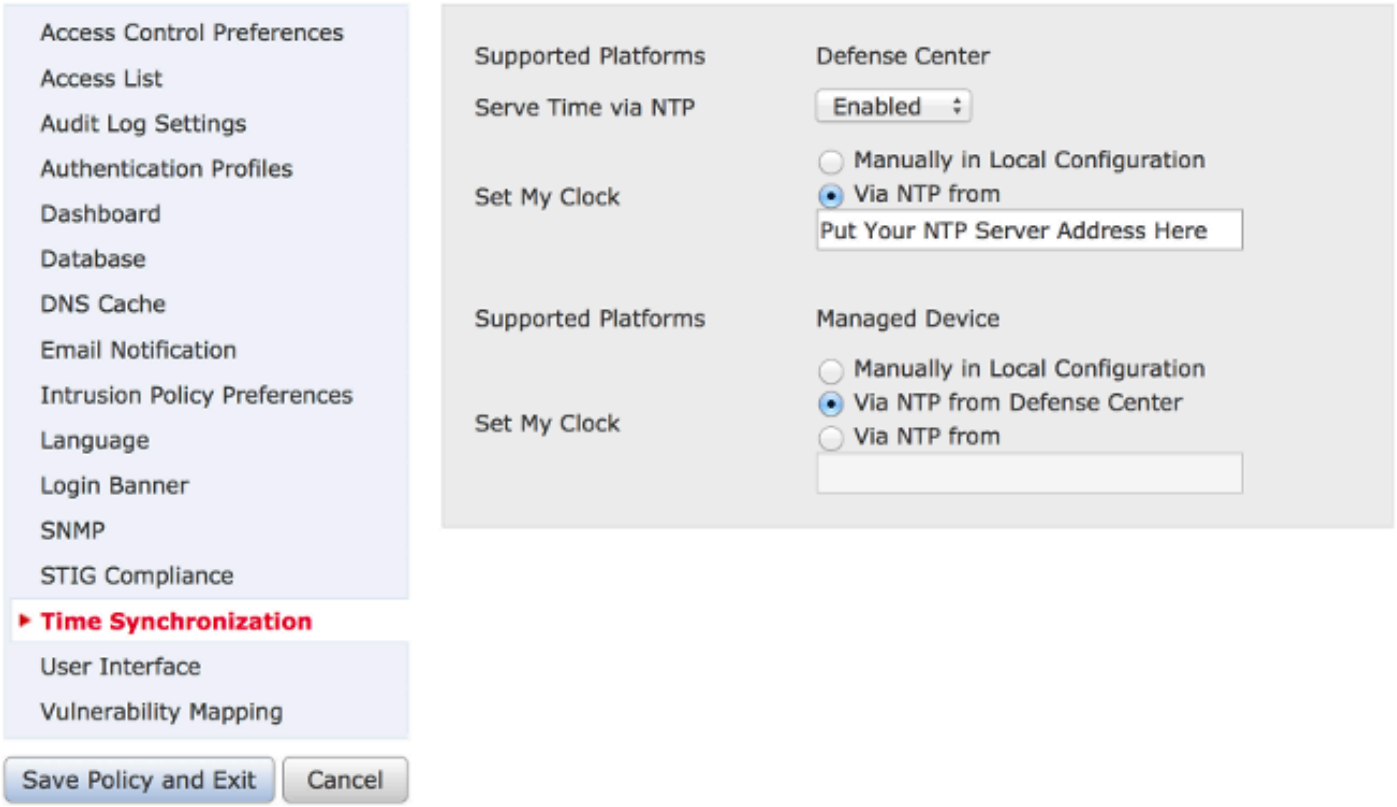
Como verificar nas versões 5.4 e anteriores

Verifique se o NTP está ativado na política do sistema que é aplicada nos sistemas FireSIGHT. Para verificar isso, conclua estas etapas:

1. Escolha System > Local > System Policy.
2. Edite a política do sistema aplicada aos sistemas FireSIGHT.
3. Escolha Sincronização de horário.

Verifique se o FireSIGHT Management Center (também conhecido como Defense Center ou DC) tem o relógio definido como Via NTP from, e se um endereço de um servidor NTP é fornecido. Confirme também se o dispositivo gerenciado está definido como via NTP do Defense Center.

Se você especificar um servidor NTP externo remoto, seu equipamento deverá ter acesso de rede a ele. Não especifique um servidor NTP não confiável. Não sincronize seus dispositivos gerenciados (virtuais ou físicos) com um Virtual FireSIGHT Management Center. A Cisco recomenda que você sincronize seus dispositivos virtuais com um servidor NTP físico.



Como verificar nas versões 6.0 e posteriores

Nas versões 6.0.0 e posteriores, as configurações de sincronização de tempo são definidas em

locais separados no Firepower Management Center, embora rastreiem a mesma lógica das etapas do 5.4.

As configurações de sincronização de horário do próprio Firepower Management Center são encontradas em System > Configuration > Time Synchronization.

As configurações de sincronização de horário para os dispositivos gerenciados são encontradas em Devices > Platform Settings. Clique em editar ao lado da política Configurações de plataforma aplicada ao dispositivo e escolha Sincronização de tempo.

Depois de aplicar a configuração para sincronização de horário (independentemente da versão), certifique-se de que a hora no Centro de gerenciamento e nos dispositivos gerenciados seja correspondente. Caso contrário, consequências não intencionais podem ocorrer quando os dispositivos gerenciados se comunicam com o Management Center.

Etapa 2: Identificar um Servidor de Tempo e seu Status

- Para coletar informações sobre a conexão com um servidor de horário, digite este comando no 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
  ```

  Um asterisco '*' sob o remoto indica o servidor para o qual você está sincronizado no momento. Se uma entrada com um asterisco não estiver disponível, o relógio não está sincronizado com sua fonte de tempo.

  Em um dispositivo gerenciado, você pode inserir este comando no shell para determinar o endereço do seu servidor NTP:

  <#root>

  ```
  >
  ```

  show ntp

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

> Observação: se um dispositivo gerenciado estiver configurado para receber tempo de um FireSIGHT Management Center, o dispositivo mostrará uma fonte de tempo com endereço de loopback, como 127.0.0.2. Esse endereço IP é uma entrada sfipproxy e indica que a Rede Virtual de Gerenciamento é usada para sincronizar o tempo.

- Se um equipamento mostrar que está sincronizado com 127.127.1.1, ele indicará que o equipamento está sincronizado com seu próprio relógio. Ocorre quando um servidor de tempo configurado em uma política do sistema não é sincronizável. Por exemplo:
  <#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
  ```

- Na saída do comando ntpq, se você observar que o valor de st (stratum) é 16, isso indica que o servidor de tempo está inacessível e o equipamento não pode sincronizar com esse servidor de tempo.
- Na saída do comando ntpq, reach mostra um número octal que indica sucesso ou falha ao alcançar a origem para as oito tentativas de sondagem mais recentes. Se o valor for 377, significa que as 8 últimas tentativas foram bem-sucedidas. Qualquer outro valor pode indicar que uma ou mais das últimas oito tentativas não tiveram êxito.

Etapa 3: Verifique a conectividade

1. Verifique a conectividade básica com o servidor de horário.
   <#root>

   ```
   admin@FireSIGHT:~$

   ping
   ```

2. Verifique se a porta 123 está aberta no sistema FireSIGHT.
   <#root>

   ```
   admin@FireSIGHT:~$

   netstat -an | grep 123
   ```

3. Confirme se a porta 123 está aberta no firewall.

4. Verifique o relógio do hardware:
   <#root>

   ```
   admin@FireSIGHT:~$

   sudo hwclock
   ```

   Se o relógio do hardware estiver muito desatualizado, ele nunca poderá ser sincronizado com êxito. Para forçar manualmente o relógio a ser definido com um servidor de hora, insira este comando:

   <#root>

   ```
   admin@FireSIGHT:~$

   sudo ntpdate -u
   ```

   Em seguida, reinicie ntpd:

   <#root>

   ```
   admin@FireSIGHT:~$

   sudo pmtool restartbyid ntpd
   ```

Etapa 4: Verifique os arquivos de configuração

1. Verifique se o arquivo sfipproxy.conf foi preenchido corretamente. Esse arquivo envia o tráfego NTP pelo sftunnel.

   Um exemplo do arquivo /etc/sf/sfipproxy.conf em um dispositivo gerenciado é mostrado aqui:

   <#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;
            }
        }
    }
}
```

Um exemplo do arquivo /etc/sf/sfipproxy.conf em um FireSIGHT Management Center é mostrado aqui:

<#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. Certifique-se de que o Universally Unique Identifier (UUID) na seção peers corresponda ao

arquivo ims.conf do peer. Por exemplo, o UUID encontrado na seção peers do arquivo /etc/sf/sfipproxy.conf em um FireSIGHT Management Center deve corresponder ao UUID encontrado no arquivo /etc/ims.conf de seu dispositivo gerenciado. Da mesma forma, o UUID encontrado na seção peers do arquivo /etc/sf/sfipproxy.conf em um dispositivo gerenciado deve corresponder ao UUID encontrado no arquivo /etc/ims.conf de seu dispositivo de gerenciamento.

Você pode recuperar o UUID dos dispositivos com este comando:

```
<#root>

admin@FireSIGHT:~$

sudo grep UUID /etc/sf/ims.conf


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

Normalmente, eles devem ser preenchidos automaticamente pela política do sistema, mas houve casos em que essas estrofes foram perdidas. Se eles precisarem ser modificados ou alterados, será necessário reiniciar o sfipproxy e o sftunnel conforme visto neste exemplo:

```
<#root>

admin@FireSIGHT:~$

sudo pmtool restartbyid sfipproxy

admin@FireSIGHT:~$

sudo pmtool restartbyid sftunnel
```

3. Verifique se um arquivo ntp.conf está disponível no diretório /etc.

```
<#root>

admin@FireSIGHT:~$

ls /etc/ntp.conf*
```

Se um arquivo de configuração NTP não estiver disponível, você poderá fazer uma cópia a partir do arquivo de configuração de backup. Por exemplo:

```
<#root>

admin@FireSIGHT:~$

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

4. Verifique se o arquivo /etc/ntp.conf foi preenchido corretamente. Quando você aplica uma política do sistema, o arquivo ntp.conf é regravado.

> Observação: a saída de um arquivo ntp.conf mostra as configurações do servidor de tempo definidas em uma política do sistema. A entrada do carimbo de data/hora deve mostrar a hora em que a última política do sistema foi aplicada a um dispositivo. A entrada do servidor deve mostrar o endereço do servidor de tempo especificado.

```
<#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 as versões do NTP em dois dispositivos e certifique-se de que também sejam iguais.

Para obter detalhes sobre os conceitos básicos de NTP, consulte Usar as Melhores Práticas para o Network Time Protocol.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.