Pesquise defeitos edições com o Network Time Protocol (NTP) em sistemas de FirePOWER

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Sintomas
Troubleshooting
Passo 1: Verifique a configuração de NTP
Como verificar nas versões 5.4 e anterior
Como verificar nas versões 6.0 e mais recente
Passo 2: Identifique um Timeserver e é estado
Passo 3: Verifique a Conectividade
Passo 4: Verifique arquivos de configuração

Introdução

Este documento descreve problemas comuns com a sincronização de tempo em sistemas de FireSIGHT e como pesquisá-los defeitos. Você pode escolher sincronizar o tempo entre seus sistemas de FireSIGHT em três maneiras diferentes, tais como manualmente com os server externos do Network Time Protocol (NTP), ou com centro de gerenciamento de FireSIGHT que serve como um servidor de NTP. Você pode configurar um centro de gerenciamento de FireSIGHT como um Time Server com NTP e o usa então para sincronizar o tempo entre o centro de gerenciamento de FireSIGHT e os dispositivos gerenciado.

Pré-requisitos

Requisitos

A fim configurar o ajuste da sincronização de tempo, você precisa o nível `admin do` acesso em seu centro de gerenciamento de FireSIGHT.

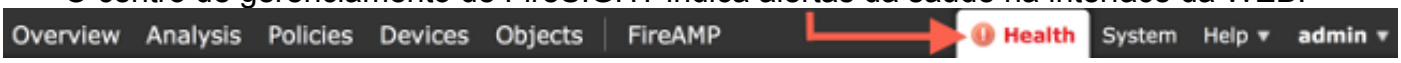
Componentes Utilizados

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

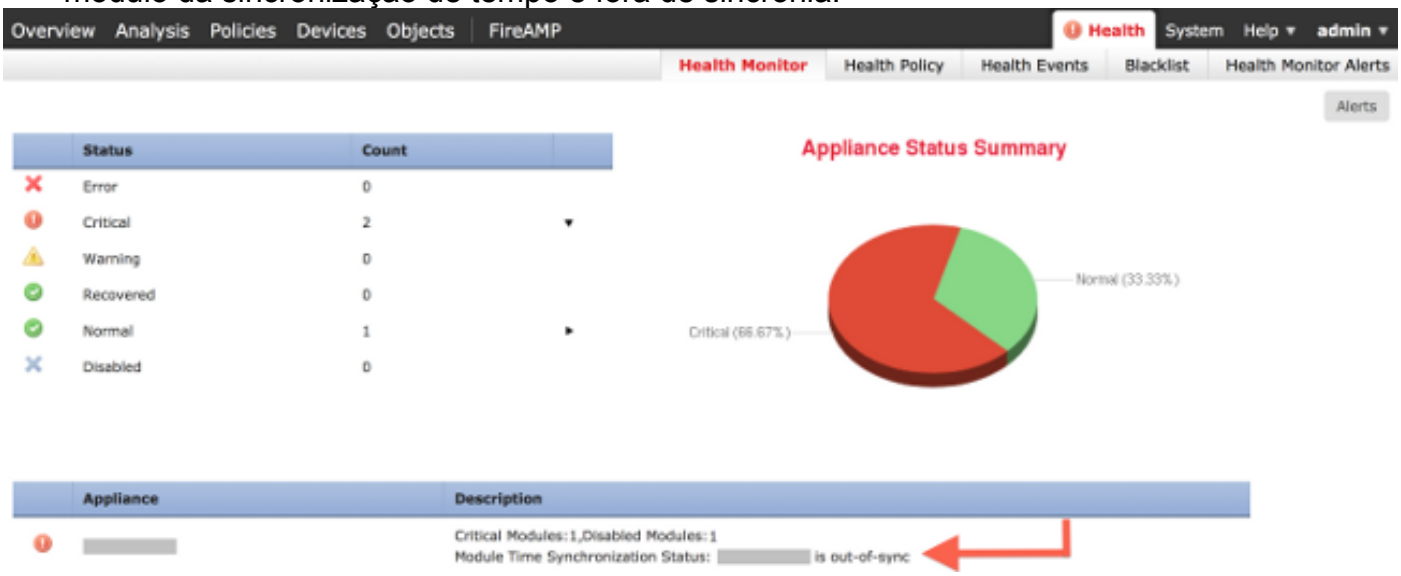
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer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

Sintomas

- O centro de gerenciamento de FireSIGHT indica alertas da saúde na interface da WEB.



- A página do **monitor de funcionamento** mostra um dispositivo como critial, porque o estado do módulo da sincronização de tempo é fora de sincronia.



- Você pôde ver alertas intermitentes da saúde se os dispositivos não ficam sincronizados.
- Depois que uma política de sistema é aplicada você pôde ver alertas da saúde, porque um centro de gerenciamento de FireSIGHT e seus dispositivos gerenciado poderiam tomar até 20 minutos para terminar a sincronização. Isto é porque um centro de gerenciamento de FireSIGHT deve primeiramente sincronizar com seu servidor de NTP configurado antes que possa servir o tempo a um dispositivo gerenciado.
- O tempo entre um centro de gerenciamento de FireSIGHT e um dispositivo gerenciado não combina.
- Os eventos gerados no sensor puderam tomar minutos ou horas para tornar-se visíveis em um centro de gerenciamento de FireSIGHT.
- Se você executa dispositivos virtuais e a página do **monitor de funcionamento** indica que a instalação do pulso de disparo para seu dispositivo virtual não está sincronizada, verifique seus ajustes da sincronização de tempo da política de sistema. Cisco recomenda que você sincroniza seus dispositivos virtuais a um servidor de NTP físico. Não sincronize seus dispositivos gerenciado (virtuais ou físicos) a um centro virtual da defesa.

Troubleshooting

Passo 1: Verifique a configuração de NTP

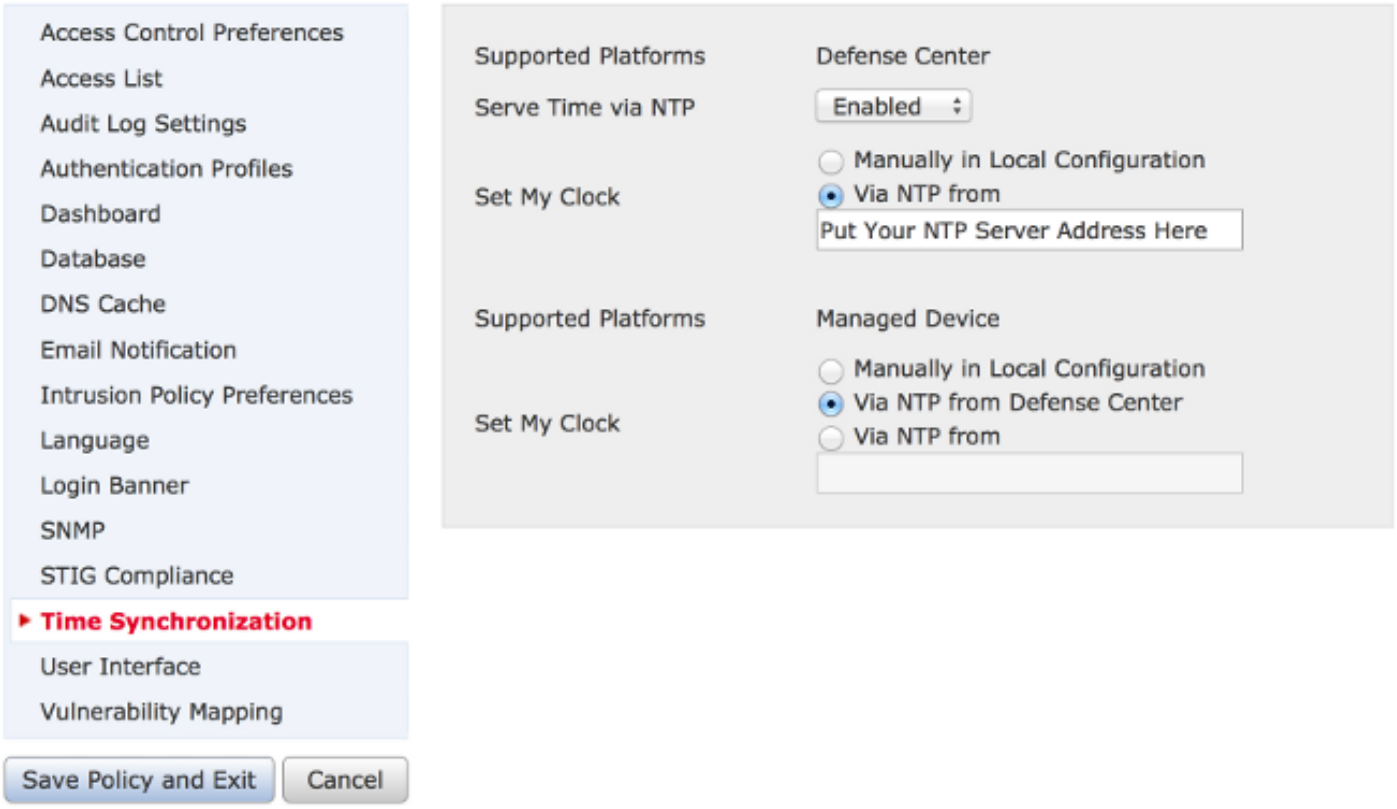
Como verificar nas versões 5.4 e anterior

Verifique que o NTP está permitido na política de sistema que é aplicada nos sistemas de FireSIGHT. A fim verificar isso, termine estas etapas:

1. Escolha o **sistema > o Local > a política de sistema**.
2. Edite a política de sistema aplicada em seus sistemas de FireSIGHT.
3. Escolha a **sincronização de tempo**.

Verifique se o centro de gerenciamento de FireSIGHT (igualmente conhecido como o centro da defesa ou o DC) tem o pulso de disparo ajustado **através do NTP de**, e um endereço de um servidor de NTP está fornecido. Igualmente confirme que o dispositivo gerenciado está ajustado **através do NTP do centro da defesa**.

Se você especifica um servidor externo NTP remoto, seu dispositivo deve ter-lhe o acesso de rede. Não especifique um servidor de NTP não confiável. Não sincronize seus dispositivos gerenciado (virtuais ou físicos) a um centro de gerenciamento virtual de FireSIGHT. Cisco recomenda que você sincroniza seus dispositivos virtuais a um servidor de NTP físico.



Como verificar nas versões 6.0 e mais recente

Nas versões 6.0.0 e mais recente, os ajustes da sincronização de tempo são configurados em lugares separados no centro de gerenciamento de FirePOWER, embora seguem a mesma lógica que as etapas para 5.4.

Os ajustes para o centro de gerenciamento de FirePOWER próprios da sincronização de tempo são encontrados sob o **sistema > a configuração > a sincronização de tempo**.

Os ajustes da sincronização de tempo para os dispositivos gerenciado são encontrados sob **dispositivos > ajustes da plataforma.** Clique **editam** ao lado dos ajustes da plataforma a política aplicada ao dispositivo e escolhem então a **sincronização de tempo.**

Depois que você aplica a configuração para a sincronização de tempo (apesar da versão), certifique-se de que o tempo em seus centro de gerenciamento e fósforos dos dispositivos gerenciado. Se não, as consequências sem intenção puderam ocorrer quando os dispositivos gerenciado se comunicam com o centro de gerenciamento.

Passo 2: Identifique um Timeserver e é estado

- A fim recolher a informação sobre a conexão a um Time Server, incorpore este comando em seu centro de gerenciamento 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
```
Um asterisco "*" sob o `telecontrole` indica o server que você é sincronizado atualmente a. Se uma entrada com um asterisco é não disponível, o pulso de disparo não está sincronizado atualmente com ele é timesource.Em um dispositivo gerenciado, você pode incorporar este comando no shell a fim determinar o endereço de seu servidor de NTP:
```
> show ntp

NTP Server : 127.0.0.2 (Cannot Resolve)
Status : Being Used
Offset : -8.344 (milliseconds)
Last Update : 188 (seconds)
```
Note: Se um dispositivo gerenciado é configurado para receber o tempo de um centro de gerenciamento de FireSIGHT, o dispositivo mostra um timesource com endereço de loopback, tal como `127.0.0.2`. Este endereço IP de Um ou Mais Servidores Cisco ICM NT é uma entrada do sfipproxy e indica que a rede virtual do Gerenciamento está sendo usada para sincronizar o tempo.
- Se indicadores de um dispositivo que sincronizações com `127.127.1.1`, ele indicam que as sincronizações do dispositivo com seu próprio pulso de disparo. Ocorre quando um timeserver configurado em uma política de sistema não é synchronizable. Por exemplo:
```
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 do `ntpq`, se você observa o valor de `st` (estrato) é 16, ele indica que o timeserver é inacessível e o dispositivo não pode sychronize com esse timeserver.
- Na saída do comando do `ntpq`, o `alcance` mostra um número octal que indique o sucesso ou a falha alcançar a fonte para as oito tentativas de vatação as mais recentes. Se você vê o valor é 377, ele significa que as últimas 8 tentativas eram bem sucedidas. Todos os outros valores puderam indicar que umas ou várias das últimas oito tentativas eram mal sucedidas.

Passo 3: Verifique a Conectividade

1. Verifique a conectividade básica ao Time Server.
```
admin@FireSIGHT:~$ ping <IP_addres_of_NTP_server>
```
2. Assegure-se de que a porta 123 esteja aberta em seu sistema de FireSIGHT.
```
admin@FireSIGHT:~$ netstat -an | grep 123
```
3. Confirme que a porta 123 está aberta no Firewall.
4. Verifique o relógio de hardware:
```
admin@FireSIGHT:~$ sudo hwclock
```

   Se o relógio de hardware é expirado demasiado distante, puderam nunca com sucesso sincronização. A fim forçar manualmente o pulso de disparo para ser ajustado com um Time Server, incorpore este comando:

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

Então `ntpd do` reinício:

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

Passo 4: Verifique arquivos de configuração

1. Verifique se o `arquivo sfipproxy.conf` é povoado corretamente. Este arquivo envia o tráfego NTP sobre o sftunnel.
   Um exemplo do arquivo de `/etc/sf/sfipproxy.conf em um` dispositivo gerenciado é mostrado aqui:

```
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 de `/etc/sf/sfipproxy.conf em um` centro de gerenciamento de FireSIGHT é mostrado aqui:

```
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 universalmente o identificador exclusivo (UUID) sob os fósforos da

seção dos pares com o arquivo ims.conf o par. Por exemplo, o UUID encontrado sob o peerssection do arquivo de /etc/sf/sfipproxy.conf em um centro de gerenciamento de FireSIGHT deve combinar com o UUID encontrado no arquivo de /etc/ims.conf de seu dispositivo gerenciado. Similarmente, o UUID encontrado sob o peerssection do arquivo de /etc/sf/sfipproxy.conf em um dispositivo gerenciado deve combinar com o UUID encontrado no arquivo de /etc/ims.conf de seu dispositivo do Gerenciamento. Você pode recuperar o UUID dos dispositivos com este comando:

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

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

Estes devem normalmente automaticamente ser povoados pela política de sistema, mas houve os casos onde estas estâncias faltavam. Se precisam de ser alterados ou mudado você precisará de reiniciar o sfipproxy e o sftunnel como segue:

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

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

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

Se um arquivo de configuração de NTP é não disponível, você pode fazer uma cópia do arquivo de configuração de backup. Por exemplo:

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

4. Verifique se o arquivo de /etc/ntp.conf é povoado corretamente. Quando você aplica uma política de sistema, o arquivo ntp.conf está reescrito. **Note**: A saída de um arquivo ntp.conf mostra os ajustes do timeserver configurados em uma política de sistema. A entrada do selo de tempo deve mostrar o tempo em que a última política de sistema se aplicou a um dispositivo. A entrada de servidor mostre o endereço especificado do 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
```