

排除故障与网络时间协议(NTP)的问题在Firepower系统

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[症状](#)

[故障排除](#)

[步骤 1：验证NTP配置](#)

[如何验证在版本5.4和以下](#)

[如何验证在版本6.0和以上](#)

[步骤 2：识别趋炎附势者，并且它是状态](#)

[步骤 3：检验连通性](#)

[步骤 4：验证配置文件](#)

简介

本文描述与时间同步的常见问题在FireSIGHT系统和如何排除故障他们。您能用外部网络时间协议(NTP)服务器选择您的FireSIGHT系统之间的同步时间用三个不同的方式，例如手工，或者有担当Ntp server的FireSIGHT管理中心的。您能配置FireSIGHT管理中心作为有NTP的一时间服务器然后使用它FireSIGHT管理中心和受管理设备之间的同步时间。

先决条件

要求

为了配置时间同步设置，您需要admin级在您的FireSIGHT管理中心的访问。

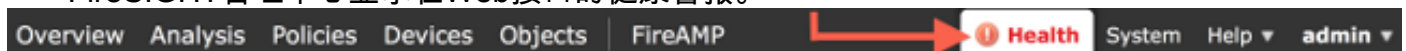
使用的组件

本文档不限于特定的软件和硬件版本。

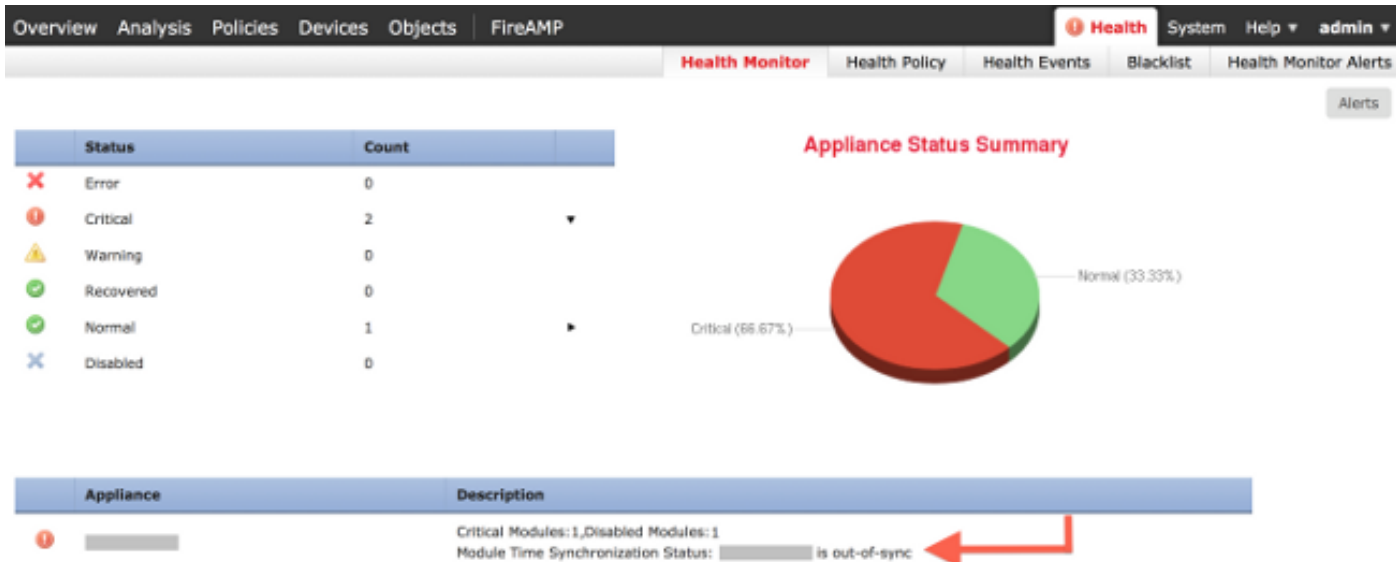
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

症状

- FireSIGHT管理中心显示在Web接口的健康警报。



- 因为时间同步模块状况是失调的，健康监控页显示设备如critical。



- 如果设备不能坚持同步，您也许发现断断续续健康警报。
- 在系统策略应用后您也许发现健康警报，因为FireSIGHT管理中心和其受管理设备可能花费20分钟完成同步。这是因为FireSIGHT管理中心必须与其已配置的Ntp server首先同步，在能为时间服务到受管理设备前。
- FireSIGHT管理中心和受管理设备之间的时间不配比。
- 事件生成在传感器也许耗费分钟或几小时变得可视在FireSIGHT管理中心。
- 如果运行虚拟设备，并且**健康监控**页表明您的虚拟设备的时钟设置没有同步，请检查您的系统策略时间同步设置。思科建议您同步您的虚拟设备对一物理Ntp server。请勿同步您的受管理设备(虚拟或物理)到一虚拟防御中心。

故障排除

步骤 1：验证NTP配置

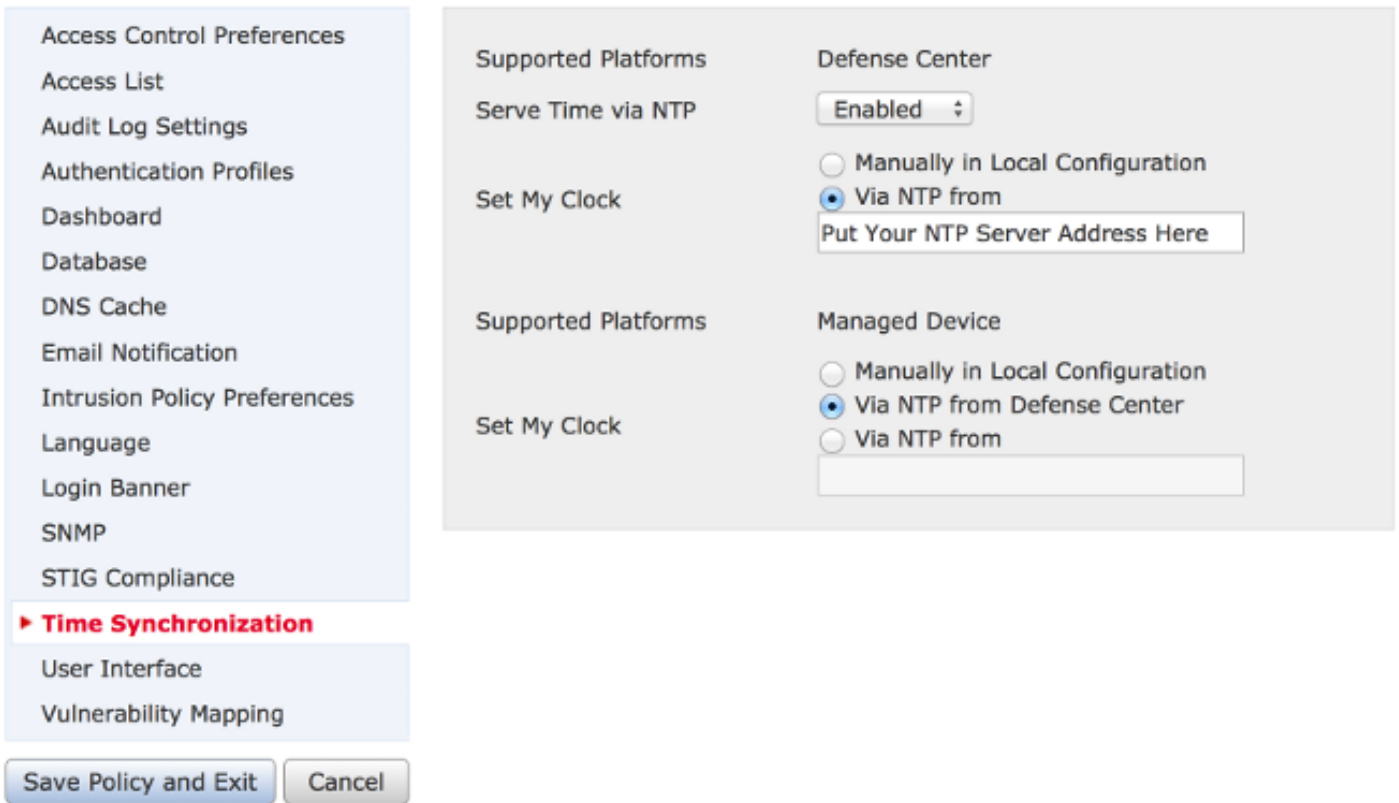
如何验证在版本5.4和以下

验证NTP在FireSIGHT系统应用的系统策略启用。为了验证那，请完成这些步骤：

1. 选择**系统>本地>System策略**。
2. 编辑在您的FireSIGHT系统应用的系统策略。
3. 选择**时间同步**。

检查FireSIGHT管理中心(亦称防御中心或DC)是否有clock set对**通过NTP从**，并且提供Ntp server的地址。并且请确认受管理设备设置为**通过从防御中心的NTP**。

如果指定远程外部Ntp server，您的设备必须访问网络访问它。请勿指定一不信任Ntp server。请勿同步您的受管理设备(虚拟或物理)对一个虚拟FireSIGHT管理中心。思科建议您同步您的虚拟设备对一物理Ntp server。



如何验证在版本6.0和以上

在版本6.0.0和以上，时间同步设置在Firepower管理中心的独立的地方配置，虽然他们按照逻辑和5.4的步骤一样。

Firepower管理中心的时间同步设置被找到在**系统 > Configuration > 时间同步**下。

受管理设备的时间同步设置被找到在**设备 > 平台设置**下。单击在平台设置旁边**编辑策略应用**对设备然后选择**时间同步**。

在您申请配置时间同步(不管版本)后，请确保在您的管理中心和受管理设备匹配的时间。否则，当受管理设备连通与管理中心时，不愿意的结果也许发生。

步骤 2：识别趋炎附势者，并且它是状态

- 为了关于连接的收集信息对时间服务器，输入此on命令您的FireSIGHT管理中心：

```
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
```

在星号 '*' 指示您当前同步的服务器。如果与星号的一个条目不可用，时钟没有与它当前同步是 timesource。在受管理设备上，您能输入此on命令shell为了确定您的Ntp server地址：

```
> show ntp
```

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

Note: 如果受管理设备配置接收从FireSIGHT管理中心的时间，设备显示与环回地址的一 timesource，例如127.0.0.2。此IP地址是sfiproxy条目并且表明使用管理虚拟网络同步时间

-
- 如果它同步与127.127.1.1设备显示，它表明设备用其自己的时钟同步。当在系统策略配置的趋炎附势者不synchronizable，它发生。例如：

```
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

```

- 在ntpq命令输出，如果注意值st (层)是16，它表明趋炎附势者是不可得到的，并且设备不能synchronize与该趋炎附势者。
- 在ntpq命令输出，显示指示成功或疏忽到达最最近的八轮询的尝试的来源的八进制数。如果看到值是377，它含义最后8尝试是成功的。所有其他值也许表明一个或很多最后八尝试不成功。

步骤 3：检验连通性

1. 检查基本连通性到时间服务器。

```
admin@FireSIGHT:~$ ping <IP_address_of_NTP_server>
```

2. 保证端口123是开放的在您的FireSIGHT系统。

```
admin@FireSIGHT:~$ netstat -an | grep 123
```

3. 确认端口123是开放的在防火墙。

4. 检查硬件时钟：

```
admin@FireSIGHT:~$ sudo hwclock
```

如果硬件时钟是太更过时的，他们也许从未顺利地同步。为了手工强制时钟设置时间服务器，请输入此命令：

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

然后重新启动ntpd：

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

步骤 4：验证配置文件

1. 检查sfiproxy.conf是否正确地填充。此文件发送在sftunnel的NTP流量。
/etc/sf/sfiproxy.conf文件的示例在受管理设备的显示此处：

```
admin@FirePOWER:~$ sudo cat /etc/sf/sfiproxy.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;
}
}
}
```

/etc/sf/sfiproxy.conf文件的示例在FireSIGHT管理中心的显示此处：

```
admin@FireSIGHT:~$ sudo cat /etc/sf/sfiproxy.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. 确保唯一标识符(UUID)在部分下用ims.conf全体地匹配对等体。例如，UUID被找到在/etc/sf/sfiproxy.confpeerssection下在FireSIGHT管理中心的应该配比与在其受管理设备/etc/ims.conf找到的UUID。同样地，UUID被找到在/etc/sf/sfiproxy.confpeerssection下在受管理设备的应该配比与在其管理设备/etc/ims.conf找到的UUID。您能获取设备的UUID用此命令：

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

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

应该由系统策略自动地通常填充这些，但是有这些节未命中的案件。如果需要修改他们或更改您将需要重新启动sfiproxy和sftunnel如下：

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

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

3. 如果ntp.conf是可用的在/etc验证。

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

如果NTP配置文件不可用，您能由备份配置文件做复制。例如：

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

4. 如果/etc/ntp.conf文件正确地，填充请验证。当您运用系统策略时，ntp.conf重写。

Note:ntp.conf输出显示在系统策略配置的趋炎附势者设置。当最后系统策略应用到设备，时间戳条目应该显示时候。服务器项应该应该请显示指定的趋炎附势者地址。

```
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