排除FireSIGHT系统上的网络时间协议(NTP)问题

目录

简介

本文档介绍FireSIGHT系统上的时间同步的常见问题以及如何解决这些问题。

先决条件

要求

要配置时间同步设置，您需要FireSIGHT管理中心上的admin级别的访问权限。

使用的组件

本文档不限于特定的软件和硬件版本。

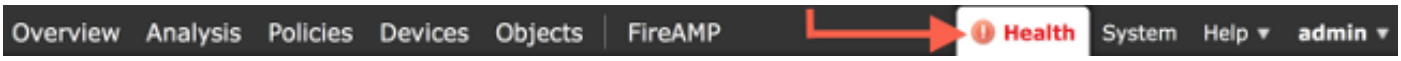
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

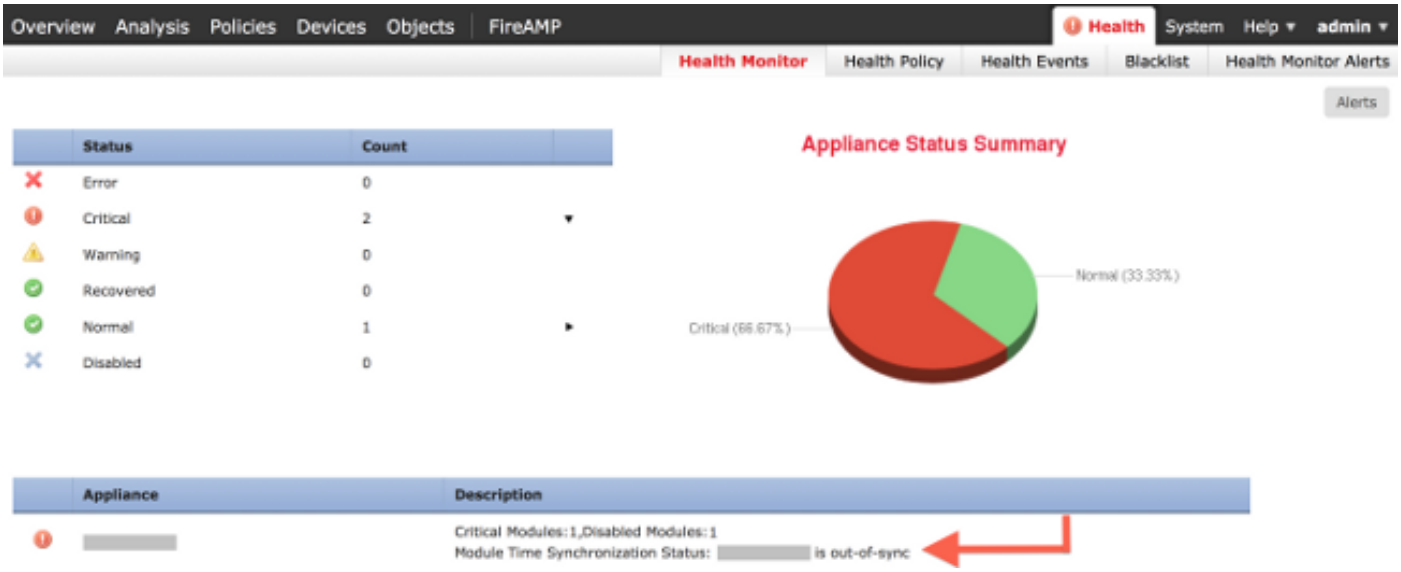
您可以选择以三种不同方式在FireSIGHT系统之间同步时间，例如使用外部网络时间协议(NTP)服务器手动同步，或者使用充当NTP服务器的FireSIGHT管理中心同步。您可以将FireSIGHT管理中心配置为具有NTP的时间服务器，然后使用它来同步FireSIGHT管理中心和受管设备之间的时间。

症状

- FireSIGHT管理中心在浏览器界面上显示运行状况警报。



- Health Monitor页面将设备显示为关键设备，因为时间同步模块的状态不同步。



- 如果设备无法保持同步，您可以看到间歇性运行状况警报。
- 应用系统策略后，您可以看到运行状况警报，因为FireSIGHT管理中心及其受管设备可能最多需要20分钟才能完成同步。这是因为，FireSIGHT管理中心必须先与其配置的NTP服务器同步，然后才能为受管设备提供时间。
- FireSIGHT管理中心与受管设备之间的时间不匹配。
- 在传感器上生成的事件可能需要几分钟或几小时才能在FireSIGHT管理中心上可见。
- 如果运行虚拟设备并且Health Monitor页面指示虚拟设备的时钟设置未同步，请检查系统策略时间同步设置。思科建议您将虚拟设备同步到物理NTP服务器。请勿将受管设备（虚拟或物理）与虚拟防御中心同步。

故障排除

第1步：检验NTP配置

如何在版本5.4及更低版本中验证

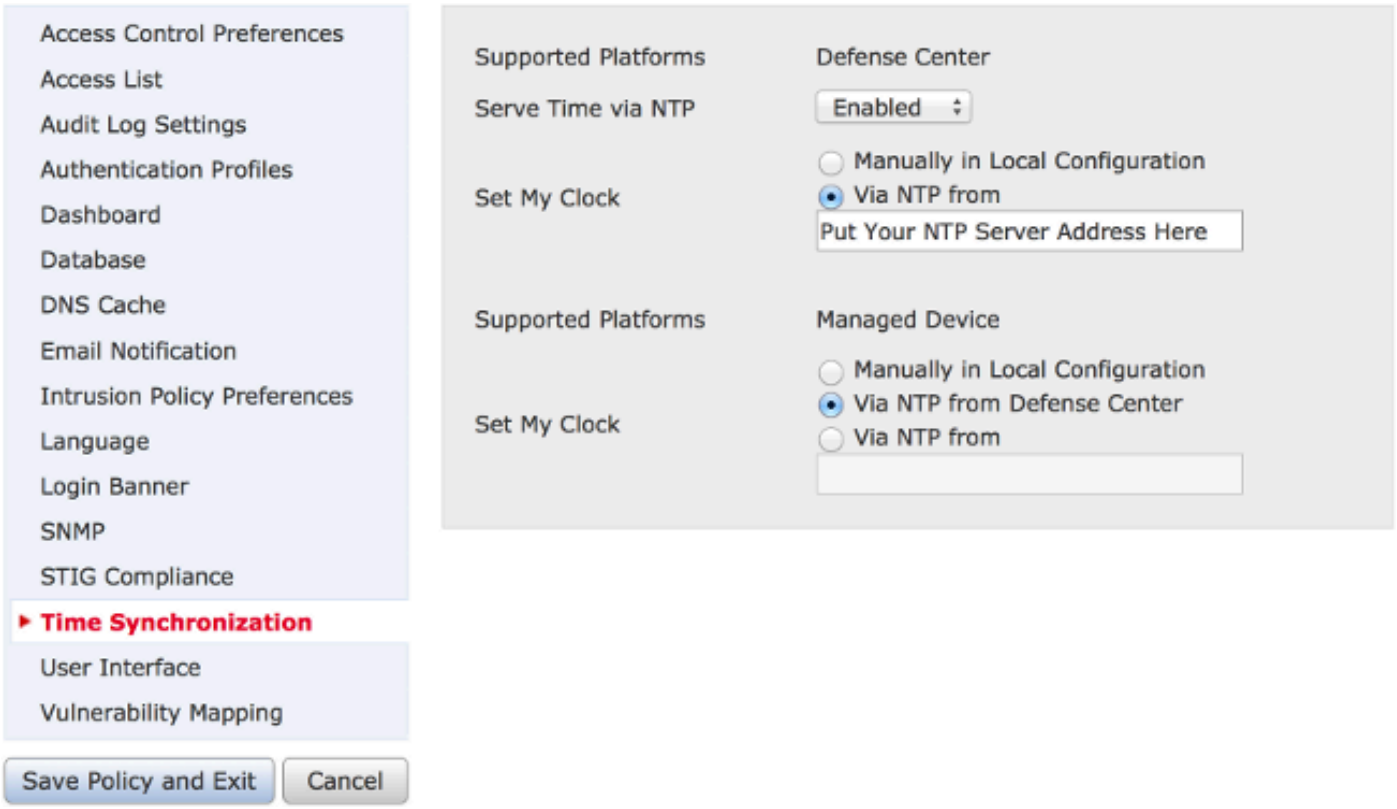
验证在应用于FireSIGHT系统的系统策略上启用了NTP。要验证这一点，请完成以下步骤：

1. 选择System > Local > System Policy。
2. 编辑应用于FireSIGHT系统的系统策略。
3. 选择时间同步。

检查FireSIGHT管理中心（也称为防御中心或DC）是否将时钟设置为Via NTP from，并提供NTP服务器的地址。另请确认受管设备已设置为通过NTP从防御中心。

如果指定远程外部NTP服务器，则设备必须能够对其进行网络访问。请勿指定不受信任的NTP服务器。请勿将受管设备（虚拟或物理）与虚拟FireSIGHT管理中心同步。思科建议您将虚拟设备同步

到物理NTP服务器。



如何在版本6.0及更高版本中验证

在版本6.0.0及更高版本中，时间同步设置在Firepower管理中心的不同位置进行配置，尽管它们遵循的逻辑与5.4的步骤相同。

Firepower管理中心本身的时间同步设置位于System > Configuration > Time Synchronization下。

受管设备的时间同步设置位于Devices > Platform Settings下。点击应用到设备的平台设置策略旁的edit，然后选择时间同步。

应用时间同步配置后（无论版本如何），请确保管理中心和受管设备上的时间匹配。否则，当受管设备与管理中心通信时，可能会出现意外后果。

第2步：确定时间服务器及其状态

- 要收集有关连接到时间服务器的信息，请在FireSIGHT管理中心输入以下命令：
  <#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
```

remote下的星号“*”表示您当前同步到的服务器。如果带星号的条目不可用，则时钟当前未与其时间源同步。

在受管设备上，可以在shell中输入以下命令以确定NTP服务器的地址：

<#root>

>

show ntp

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

注意：如果受管设备配置为从FireSIGHT管理中心接收时间，则该设备显示具有环回地址的时间源，例如127.0.0.2。此IP地址是一个sfipproxy条目，表示管理虚拟网络用于同步时间。

- 如果设备显示它与127.127.1.1同步，则表示设备与自己的时钟同步。当在系统策略上配置的时间服务器无法同步时会发生这种情况。例如：
  <#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
```

- 在ntpq命令输出中，如果您注意到st（层）的值是16，则表明无法访问时间服务器，并且设备无法与该时间服务器同步。
- 在ntpq命令输出中，reach显示一个八进制数字，表示在最近八次轮询尝试中成功或未能到达源。如果看到值为377，则表示最后8次尝试成功。任何其他值都可能表示最近八次尝试中的一次或多次不成功。

第3步：检验连接

1. 检查与时间服务器的基本连通性。
   <#root>

   admin@FireSIGHT:~$

```
ping
```

2. 确保FireSIGHT系统上的端口123处于打开状态。
   <#root>

   ```
   admin@FireSIGHT:~$
   ```

   ```
   netstat -an | grep 123
   ```

3. 确认防火墙上的端口123已打开。
4. 检查硬件时钟：
   <#root>

   ```
   admin@FireSIGHT:~$
   ```

   ```
   sudo hwclock
   ```

   如果硬件时钟太过时，则无法成功同步。要手动强制使用时间服务器设置时钟，请输入以下命令：

   <#root>

   ```
   admin@FireSIGHT:~$
   ```

   ```
   sudo ntpdate -u
   ```

   然后重新启动 ntpd:

   <#root>

   ```
   admin@FireSIGHT:~$
   ```

   ```
   sudo pmtool restartbyid ntpd
   ```

第4步：检验配置文件

1. 检查sfipproxy.conf文件是否已正确填充。此文件通过sftunnel发送NTP流量。

受管设备上的/etc/sf/sfipproxy.conf文件示例如下所示：

<#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;
            }
        }
    }
}
```

FireSIGHT管理中心上的/etc/sf/sfipproxy.conf文件示例如下所示：

<#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. 确保peers部分下的通用唯一标识符(UUID)与对等体的ims.conf文件匹配。例如，FireSIGHT管理中心上/etc/sf/sfipproxy.conf文件的peers部分下找到的UUID必须与其受管设备的/etc/ims.conf文件上找到的UUID匹配。同样，受管设备上/etc/sf/sfipproxy.conf文件的peers部分下找到的UUID必须与其管理设备/etc/ims.conf文件上找到的UUID匹配。

   您可以使用以下命令检索设备的UUID:

   <#root>

   admin@FireSIGHT:~$

   sudo grep UUID /etc/sf/ims.conf

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

   这些标准通常必须由系统策略自动填充，但有时这些标准会丢失。如果需要修改或更改它们，您需要重新启动sfipproxy和sftunnel，如下例所示：

   <#root>

   admin@FireSIGHT:~$

   sudo pmtool restartbyid sfipproxy

   admin@FireSIGHT:~$

   sudo pmtool restartbyid sftunnel

3. 验证/etc目录上是否有ntp.conf文件。

   <#root>

   admin@FireSIGHT:~$

   ls /etc/ntp.conf*

如果NTP配置文件不可用，您可以从备份配置文件创建副本。例如：

```
<#root>

admin@FireSIGHT:~$

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

4. 验证/etc/ntp.conf文件是否已正确填充。当您应用系统策略时，ntp.conf文件将被重写。

> 注意:ntp.conf文件的输出显示在系统策略上配置的时间服务器设置。时间戳条目必须显示上一次系统策略应用于设备的时间。服务器条目必须显示指定的时间服务器地址。

```
<#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
```

验证两台设备上的NTP版本，并确保其版本相同。

有关NTP基础的详细信息，请参阅使用网络时间协议的最佳实践。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。