用在Firepower系统的网络时间协议(NTP)排除问题故障

Contents

Introduction

本文描述与时间同步的常见问题在FireSIGHT系统和如何排除他们故障。您能选择与外部网络时间协议(NTP)服务器同步您的FireSIGHT系统之间的时间用三个不同的方式，例如手工，或者与FireSIGHT担当Ntp server的管理中心。您能用NTP配置FireSIGHT管理中心，时间服务器然后使用它同步FireSIGHT管理中心和可管理的设备之间的时间。

Prerequisites

Requirements

为了配置时间同步设置，您需要访问的`admin`级别在您的FireSIGHT管理中心的。

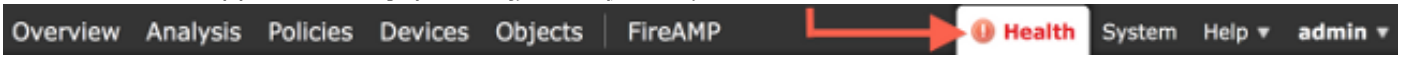
Components Used

This document is not restricted to specific software and hardware versions.

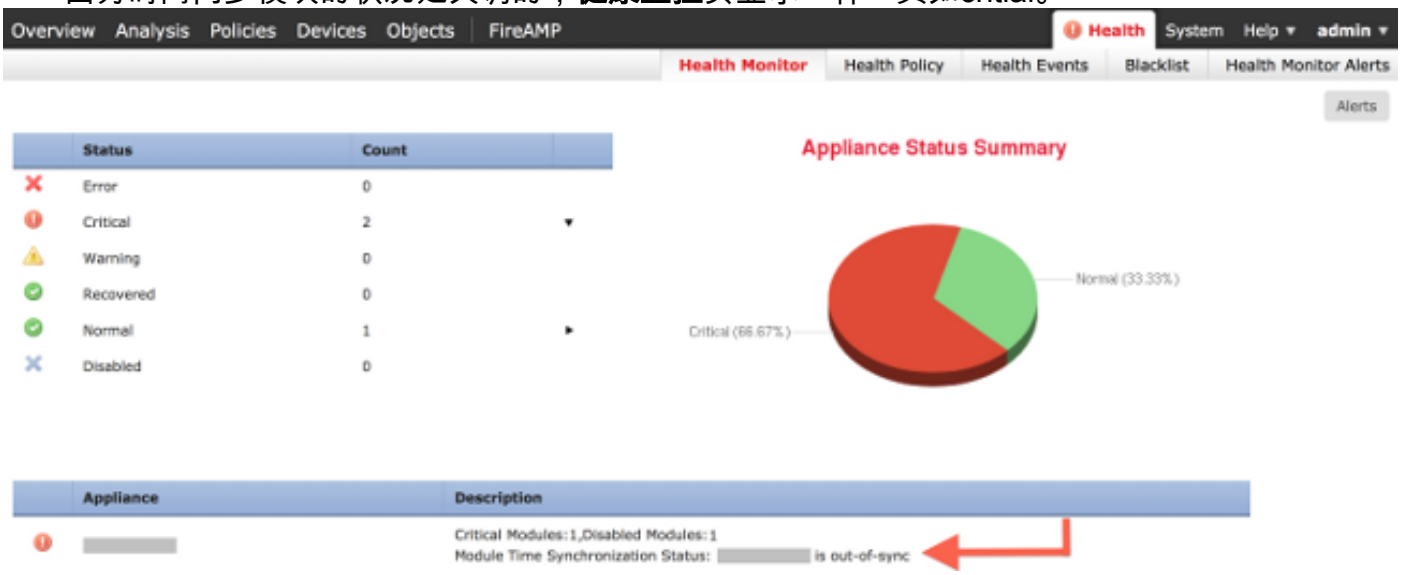
The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

症状

- FireSIGHT管理中心显示在Web接口的健康戒备。



- 因为时间同步模块的状况是失调的，**健康监控**页显示一种工具如critial。



- 如果工具不能坚持同步，您也许发现断断续续的健康戒备。
- 在系统策略适用后您也许发现健康戒备，因为FireSIGHT管理中心和其可管理的设备可能花费20分钟完成同步。这是因为FireSIGHT管理中心必须与其被配置的Ntp server首先同步，在能为时间服务到一个可管理的设备前。
- FireSIGHT管理中心和一个可管理的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。
- 如果运行虚拟工具，并且**健康监控**页表明您的虚拟工具的时钟设置没有同步，请检查您的系统策略时间同步设置。Cisco建议您同步您的虚拟工具对一物理Ntp server。请勿同步您的可管理的设备(虚拟或物理)对一个虚拟防御中心。

Troubleshoot

步骤 1：验证NTP配置

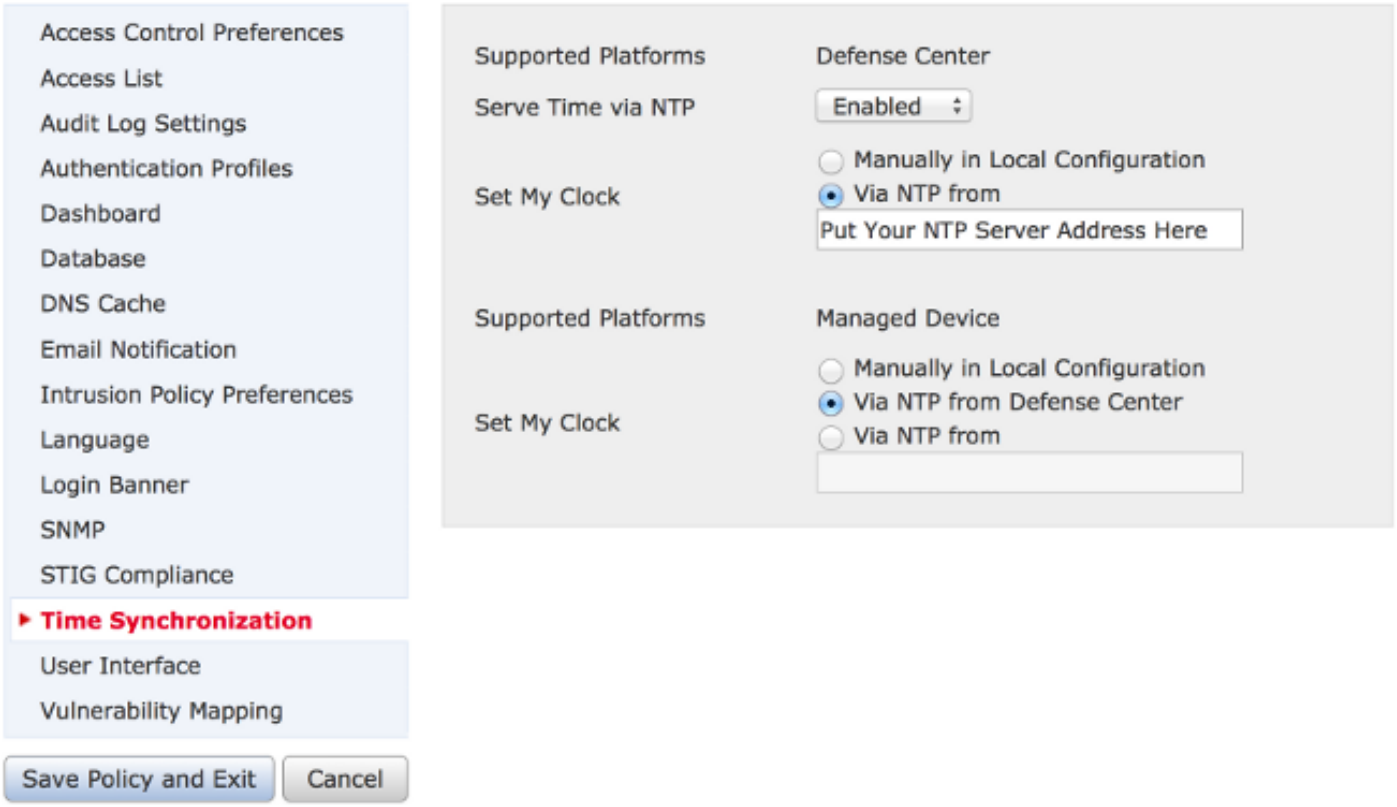
如何验证在版本5.4和以下

验证NTP在FireSIGHT系统被运用的系统策略被启用。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系统运用的系统策略。
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。并且请确认可管理的设备设置为**通过从防御中心的NTP**。

如果指定遥控外部Ntp server，您的工具必须有对它的网络访问。请勿指定一不信任的Ntp server。请勿同步您的可管理的设备(虚拟或物理)对一个虚拟FireSIGHT管理中心。Cisco建议您同步您的虚拟工具对一物理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被配置，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。

可管理的设备的时间同步设置被找到在**设备>平台设置下。**点击在平台设置旁边**编辑**策略适用于设备然后选择**时间同步。**

在您运用时间同步的配置(不管版本)后，请切记在您的管理中心和可管理的设备匹配的时间。否则，当可管理的设备与管理中心时，连通不愿意的后果也许发生。

步骤 2：识别一位趋炎附势者，并且它是状态

- 为了关于连接的收集信息与时间服务器，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是未提供的，时钟没有与它当前同步是timesource。在一个可管理的设备上，您能输入此on命令shell为了确定您的Ntp server的地址：

```
> show ntp

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

Note:如果配置一个可管理的设备从FireSIGHT管理中心接受时间，设备显示与环回地址的一

timesource，例如127.0.0.2。此IP地址是sfipproxy条目并且表明管理虚拟网络用于同步时间。

- 如果工具显示同步与127.127.1.1，表明工具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st (层)的值是16，它表明趋炎附势者是不可得到的，并且工具不能sychronize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近八个轮询的尝试的来源的八进制数。如果看到值是377，它意味着前8个尝试是成功的。所有其他值也许表明一个或很多前八个尝试是不成功的。

步骤 3：验证连接

1. 检查基本连通性到时间服务器。

```
admin@FireSIGHT:~$ ping <IP_addres_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sfipproxy.conf是否正确地被填充。此文件发送在sftunnel的NTP流量。/etc/sf/sfipproxy.conf文件的示例在一个可管理的设备的显示得这里：

```
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;
}
}
}
}
```

/etc/sf/sfipproxy.conf文件的示例在FireSIGHT管理中心的显示得这里：

```
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. 切记唯一标识符(UUID)在全体地区分与ims.conf匹配对等体。例如， UUID被找到在/etc/sf/sfipproxy.confpeerssection下在FireSIGHT管理中心的应该与在其可管理的设备/etc/ims.conf找到的UUID配比。同样地， UUID被找到在/etc/sf/sfipproxy.confpeerssection下在一个可管理的设备的应该与在其管理工具/etc/ims.conf找到的UUID配比。 您能检索设备的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，但是有这些节失踪的案件。如果需要修改或更改他们您将需要重新启动sfipproxy和sftunnel如下：

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

3. 验证ntp.conf是否是可用的在/etc。

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

如果NTP配置文件是未提供的，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. 验证/etc/ntp.conf文件是否正确地被填充。当您运用一个系统策略时， 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。当最后系统策略适用于设备，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
```