Troubleshoot Issues with Network Time Protocol (NTP) on FireSIGHT Systems

Contents

Introduction

This document describes common issues with time synchronization on FireSIGHT Systems and how to troubleshoot them.

Prerequisites

Requirements

In order to configure the time synchronization setting, you need admin level of access on your FireSIGHT Management Center.

Components Used

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

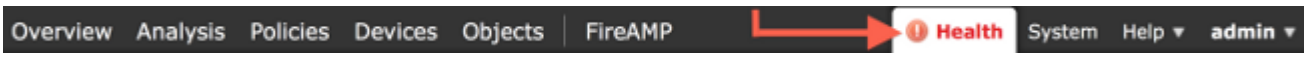
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

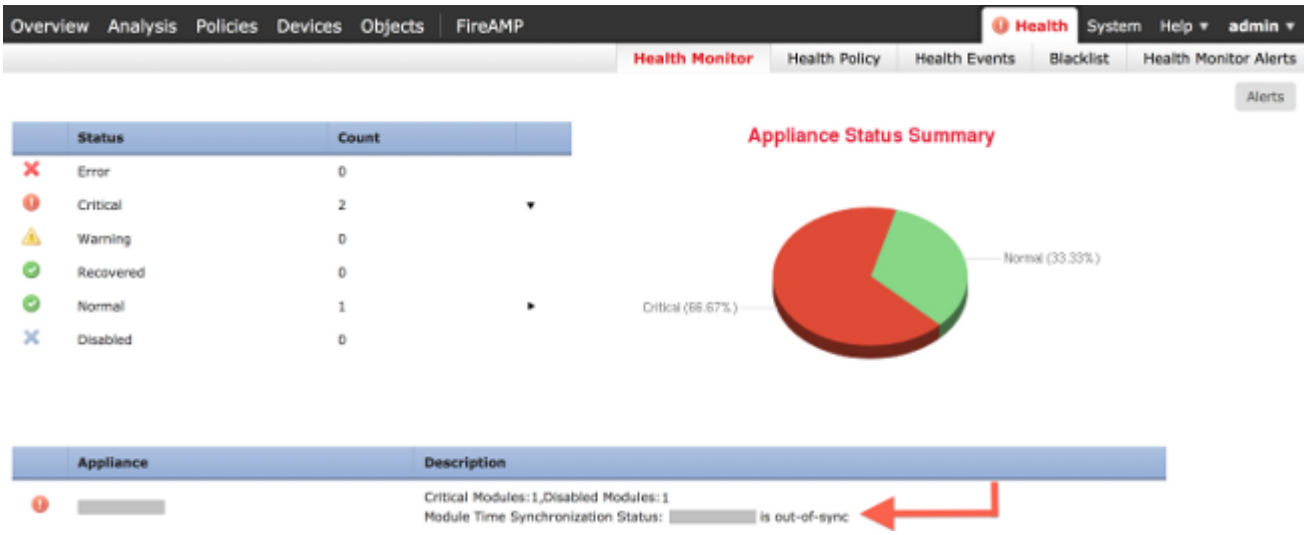
You can choose to synchronize time between your FireSIGHT Systems in three different ways, such as manually with external Network Time Protocol (NTP) servers, or with FireSIGHT Management Center which serves as an NTP server. You can configure a FireSIGHT Management Center as a time server with NTP and then use it to synchronize time between the FireSIGHT Management Center and managed devices.

Symptoms

- FireSIGHT Management Center displays health alerts on the browser interface.



- The **Health Monitor** page shows an appliance as critial, because the status of Time Synchronization Module is out-of-sync.



- You can see intermittent health alerts if the appliances fail to stay synchronized.
- After a system policy is applied you can see health alerts, because a FireSIGHT Management Center and its managed devices could take up to 20 minutes to complete synchronization. This is because a FireSIGHT Management Center must first synchronize with its configured NTP server before it can serve time to a managed device.
- The time between a FireSIGHT Management Center and a managed device does not match.
- Events generated at the sensor can take minutes or hours to become visible on a FireSIGHT Management Center.
- If you run virtual appliances and the **Health Monitor** page indicates that the clock setup for your virtual appliance is not synchronized, check your system policy time synchronization settings. Cisco recommends that you synchronize your virtual appliances to a physical NTP server. Do not synchronize your managed devices (virtual or physical) to a Virtual Defense Center.

Troubleshoot

Step 1: Verify NTP Configuration

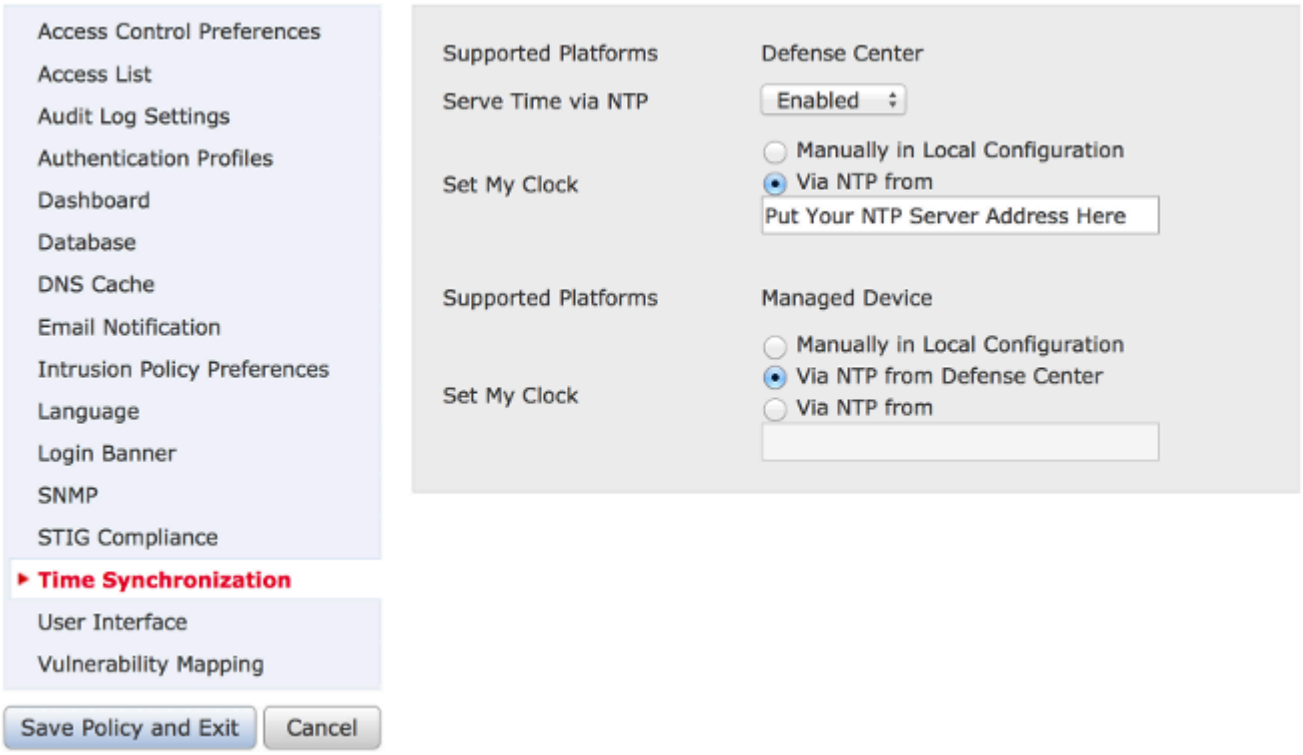
How to Verify in Versions 5.4 and Earlier

Verify that NTP is enabled on the system policy that is applied on the FireSIGHT Systems. In order to verify that, complete these steps:

1. Choose **System > Local > System Policy**.
2. Edit the system policy applied on your FireSIGHT Systems.
3. Choose **Time Synchronization**.

Check if the FireSIGHT Management Center (also known as Defense Center or DC) has the clock set to **Via NTP from**, and an address of an NTP server is provided. Also confirm that the Managed Device is set to **via NTP from Defense Center**.

If you specify a remote external NTP server, your appliance must have network access to it. Do not specify an untrusted NTP server. Do not synchronize your managed devices (virtual or physical) to a Virtual FireSIGHT Management Center. Cisco recommends that you synchronize your virtual appliances to a physical NTP server.



How to Verify in Versions 6.0 and Later

In versions 6.0.0 and later, the time synchronization settings are configured in separate places on the Firepower Management Center, though they trace the same logic as the steps for 5.4.

The time synchronization settings for the Firepower Management Center itself are found under **System > Configuration > Time Synchronization**.

The time synchronization settings for the managed devices are found under **Devices > Platform Settings.** Click **edit** next to the Platform Settings policy applied to the device and then choose **Time Synchronization.**

After you apply the configuration for time synchronization (regardless of version), make sure that the time on your Management Center and managed devices matches. Otherwise, unintended consequences can occur when the managed devices communicate with the Management Center.

Step 2: Identify a Timeserver and Its Status

- In order to gather information about the connection to a time server, enter this command on your 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
```

An asterisk '*' under the remote indicates the server you are currently synchronized to. If an entry with an asterisk is unavailable, the clock is currently not synchronised with its timesource.

On a managed device, you can enter this command on shell in order to determine the address of your NTP server:

<#root>

>

show ntp

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

> **Note**: If a managed device is configured to receive time from a FireSIGHT Management Center, the device shows a timesource with loopback address, such as 127.0.0.2. This IP address is an sfipproxy entry and indicates that the Managment Virtual Network is used to synchronize time.

- If an appliance displays that it syncs with 127.127.1.1, it indicates that the appliance syncs with its own clock. It occurs when a timeserver configured on a system policy is not synchronizable. For example:
<#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
```

- On the ntpq command output, if you notice the value of st (stratum) is 16, it indicates that the timeserver is unreachable and the appliance is not able to sychronize with that timeserver.
- On the ntpq command output, reach shows an octal number that indicates success or failure to reach source for the most recent eight polling attempts. If you see the value is 377, it means the last 8 attempts were successful. Any other values can indicate that one or more of the last eight attempts were unsuccessful.

Step 3: Verify Connectivity

1. Check the basic connectivity to the time server.
   <#root>

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

   ping <*IP_addres_of_NTP_server*>

2. Ensure that port 123 is open on your FireSIGHT System.
   <#root>

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

   netstat -an | grep 123

3. Confirm that port 123 is open on the firewall.
4. Check the hardware clock:
   <#root>

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

   sudo hwclock

   If the hardware clock is too far out of date, they can never successfully sync. In order to manually force the clock to be set with a time server, enter this command:

   <#root>

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

   sudo ntpdate -u <*IP_address_of_known_good_timesource*>

   Then restart ntpd:

   <#root>

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

   sudo pmtool restartbyid ntpd

Step 4: Verify Configuration Files

1. Check if the sfipproxy.conf file is populated correctly. This file sends NTP traffic over the sftunnel.

   An example of the /etc/sf/sfipproxy.conf file on a managed device is shown here:

<#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;
            }
        }
    }
}
```

An example of the /etc/sf/sfipproxy.conf file on a FireSIGHT Management Center is shown here:

<#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. Make sure that the Universally Unique Identifier (UUID) under the peers section matches with the ims.conf file the peer. For example, the UUID found under the peers section of the /etc/sf/sfipproxy.conf file on a FireSIGHT Management Center must match with the UUID found on the /etc/ims.conf file of its managed device. Similarly, the UUID found under the peers section of the /etc/sf/sfipproxy.conf file on a managed device must match with the UUID found on the /etc/ims.conf file of its management appliance.

   You can retrieve the UUID of the devices with this command:

   <#root>

   admin@FireSIGHT:~$

   sudo grep UUID /etc/sf/ims.conf

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

   These must normally be automatically populated by the system policy, but there have been cases where these stanzas were lost. If they need to be modified or changed you need to restart sfipproxy and sftunnel as seen in this example:

   <#root>

   admin@FireSIGHT:~$

   sudo pmtool restartbyid sfipproxy

   admin@FireSIGHT:~$

   sudo pmtool restartbyid sftunnel

3. Verify if a ntp.conf file is available on the /etc directory.
   <#root>

   admin@FireSIGHT:~$

   ls /etc/ntp.conf*

   If an NTP configuration file is unavailable, you can make a copy from the backup configuration file. For example:

   <#root>

   admin@FireSIGHT:~$

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

4. Verify if the /etc/ntp.conf file is populated correctly. When you apply a system policy, the ntp.conf file is rewritten.

> **Note**: The output of an ntp.conf file shows the timeserver settings configured on a system policy. The time stamp entry must show the time when the last system policy applied to a device. The server entry must must show the specified timeserver address.

<#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
```

Verify NTP versions on two devices and make sure its same as well.

For details on NTP basics, refer to Use Best Practices for Network Time Protocol.