

# 排除FireSIGHT系統上的網路時間協定(NTP)問題

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[症狀](#)

[疑難排解](#)

[第1步：驗證NTP配置](#)

[如何在5.4及更低版本中驗證](#)

[如何在6.0及更新版本中驗證](#)

[第2步：確定時間伺服器及其狀態](#)

[第3步：檢驗連線](#)

[第4步：驗證配置檔案](#)

---

## 簡介

本文檔介紹FireSIGHT系統上的時間同步常見問題以及如何解決這些問題。

## 必要條件

### 需求

要配置時間同步設定，您需要對FireSIGHT管理中心具有管理員級別的訪問許可權。

### 採用元件

本文件所述內容不限於特定軟體和硬體版本。

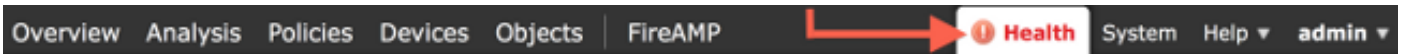
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

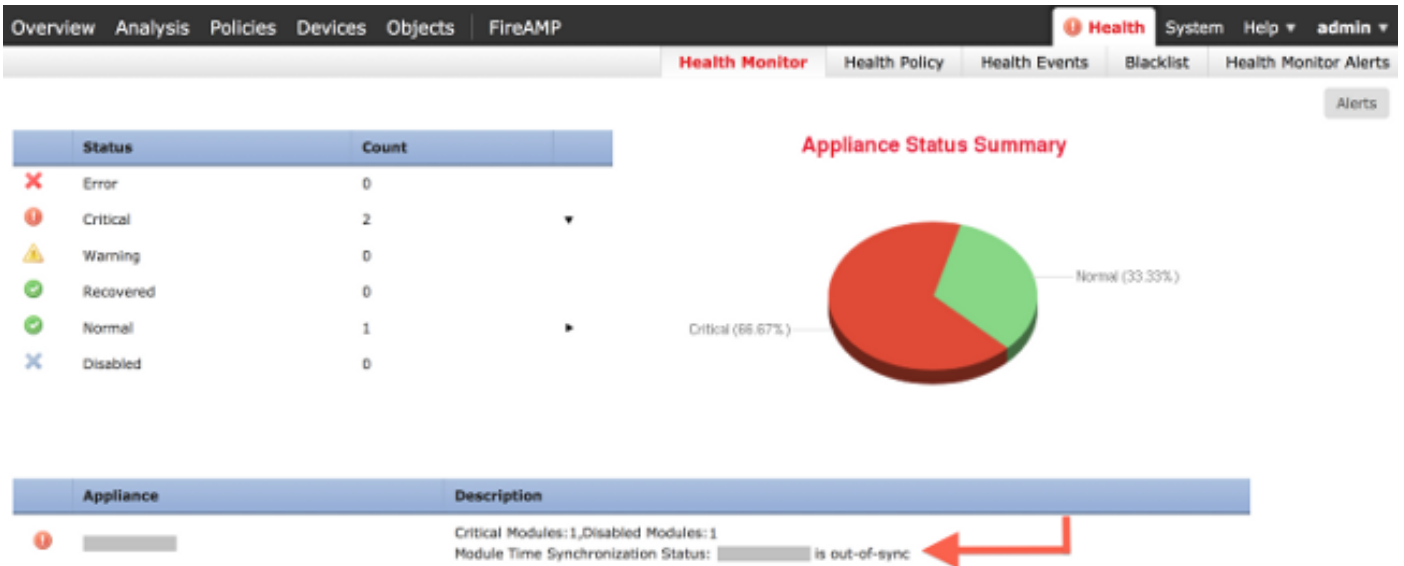
您可以選擇以三種不同方式在FireSIGHT系統之間同步時間，例如手動與外部網路時間協定(NTP)伺服器同步，或者與充當NTP伺服器的FireSIGHT管理中心同步。您可以使用NTP將FireSIGHT管理中心配置為時間伺服器，然後使用它來同步FireSIGHT管理中心和受管裝置之間的時間。

## 症狀

- FireSIGHT管理中心在瀏覽器介面上顯示運行狀況警報。



- Health Monitor頁面將裝置顯示為關鍵裝置，因為時間同步模組的狀態不同步。



- 如果裝置無法保持同步，您可以看到間歇性運行狀況警報。
- 應用系統策略後，您可以看到運行狀況警報，因為FireSIGHT管理中心及其受管裝置可能需要20分鐘才能完成同步。這是因為FireSIGHT管理中心必須先與其配置的NTP伺服器同步，然後才能為受管裝置提供時間。
- FireSIGHT管理中心與受管裝置之間的時間不匹配。
- 在感測器上生成的事件可能需要幾分鐘或幾小時才能在FireSIGHT管理中心上可見。
- 如果運行虛擬裝置，並且Health Monitor頁面指示虛擬裝置的時鐘設定未同步，請檢查系統策略時間同步設定。思科建議您將虛擬裝置同步到物理NTP伺服器。請勿將受管裝置（虛擬或物理）同步到Virtual Defense Center。

## 疑難排解

### 第1步：驗證NTP配置

如何在5.4及更低版本中驗證

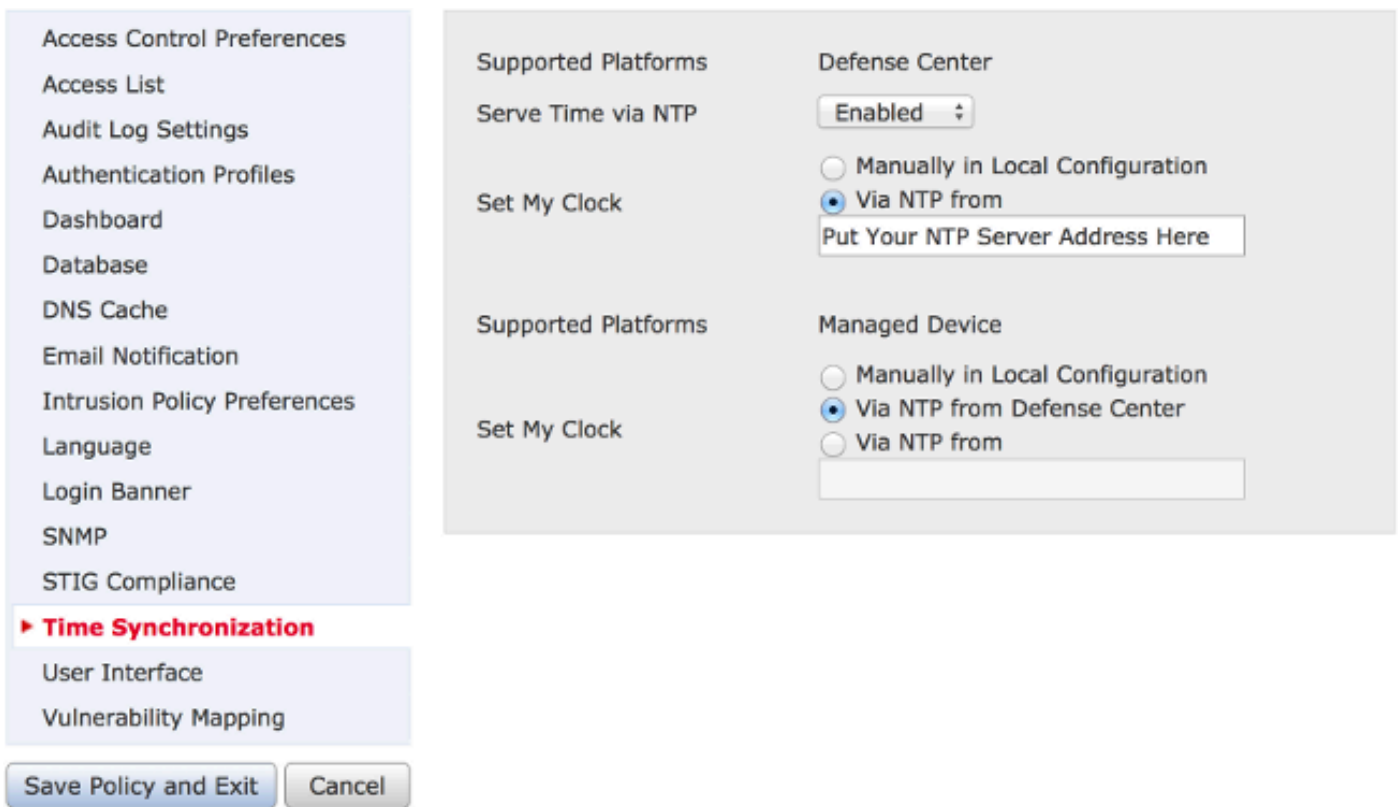
驗證在FireSIGHT系統上應用的系統策略上是否啟用了NTP。若要驗證這一點，請完成以下步驟：

1. 選擇System > Local > System Policy。
2. 編輯應用於FireSIGHT系統的系統策略。
3. 選擇Time Synchronization。

檢查FireSIGHT管理中心（也稱為防禦中心或DC）是否已將時鐘設定為Via NTP from，並提供NTP伺服器的地址。此外，請確認受管裝置已設定為通過防禦中心的NTP。

如果指定遠端外部NTP伺服器，則裝置必須擁有對該伺服器的網路訪問許可權。請勿指定不受信任的NTP伺服器。請勿將受管裝置（虛擬或物理）與虛擬FireSIGHT管理中心同步。思科建議您將虛

擬裝置同步到物理NTP伺服器。



如何在6.0及更新版本中驗證

在6.0.0及更高版本中，時間同步設定在Firepower管理中心的不同位置進行配置，儘管它們跟蹤的邏輯與5.4的步驟相同。

Firepower管理中心本身的時間同步設定位於System > Configuration > Time Synchronization下。

在Devices > Platform Settings下找到受管裝置的時間同步設定。按一下應用於裝置的「平台設定」策略旁邊的編輯，然後選擇時間同步。

應用時間同步配置後（無論版本如何），請確保管理中心和受管裝置上的時間匹配。否則，當受管裝置與管理中心通訊時，可能會出現意外後果。

## 第2步：確定時間伺服器及其狀態

- 若要收集有關連線到時間伺服器的資訊，請在FireSIGHT管理中心輸入以下命令：

```
<#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下的星號「\*」表示您當前同步到的伺服器。如果帶星號的條目不可用，則時鐘當前未與其時間源同步。

在受管裝置上，可以在shell中輸入以下命令以確定NTP伺服器的地址：

```
<#root>
>
show ntp

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

---

 註：如果受管裝置配置為從FireSIGHT管理中心接收時間，則該裝置顯示具有環回地址的時間源，如127.0.0.2。此IP地址是一個sfiproxy條目，表示管理虛擬網路用於同步時間。

---

- 如果裝置顯示其與127.127.1.1同步，則表示裝置與自己的時鐘同步。當系統策略上配置的時間伺服器無法同步時會發生這種情況。舉例來說：

```
<#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命令輸出中，如果您注意到st ( 層 ) 的值是16，則表示無法訪問時間伺服器，並且裝置無法與該時間伺服器同步。
- 在ntpq命令輸出中，reach顯示一個八進位制數，表示在最近八次輪詢嘗試中到達源成功或失敗。如果您看到值為377，則表示最後8次嘗試成功。任何其他值都可以表示最近八次嘗試中的一次或多次嘗試失敗。

### 第3步：檢驗連線

1. 檢查與時間伺服器的基本連線。

```
<#root>
admin@FireSIGHT:~$
```

```
ping
```

2. 確保FireSIGHT系統上的埠123處於開啟狀態。

```
<#root>
```

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

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

3. 確認防火牆上的埠123已開啟。

4. 檢查硬體時鐘：

```
<#root>
```

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

```
sudo hwclock
```

如果硬體時鐘太過「過時」，則它們永遠無法成功同步。若要手動強制使用時間伺服器設定時鐘，請輸入以下命令：

```
<#root>
```

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

```
sudo ntpdate -u
```

然後重新啟動 ntpd:

```
<#root>
```

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

```
sudo pmtool restartbyid ntpd
```

## 第4步：驗證配置檔案

1. 檢查sfiproxy.conf檔案是否已正確填充。此檔案通過sftunnel傳送NTP流量。

受管裝置上/etc/sf/sfiproxy.conf檔案的示例如下所示：

```
<#root>
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;
            }
        }
    }
}
}
```

FireSIGHT管理中心上的/etc/sf/sfiproxy.conf檔案的示例如下所示：

```
<#root>
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. 確保peers部分下的通用唯一識別符號(UUID)與對等體的ims.conf檔案匹配。例如，在FireSIGHT管理中心上/etc/sf/sfiproxy.conf檔案的peers部分下找到的UUID必須與其受管裝置的/etc/ims.conf檔案上的UUID匹配。同樣，在受管裝置的/etc/sf/sfiproxy.conf檔案的peers部分下找到的UUID必須與其管理裝置的/etc/ims.conf檔案上的UUID匹配。

您可以使用以下命令檢索裝置的UUID:

```

<#root>
admin@FireSIGHT:~$
sudo grep UUID /etc/sf/ims.conf

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

```

這些標準通常必須由系統策略自動填充，但有時會丟失這些標準。如果需要修改或更改它們，您需要重新啟動sfiproxy和sftunnel，如以下示例所示：

```

<#root>
admin@FireSIGHT:~$
sudo pmtool restartbyid sfiproxy
admin@FireSIGHT:~$
sudo pmtool restartbyid sftunnel

```

3. 驗證ntp.conf檔案在/etc目錄上是否可用。

```

<#root>
admin@FireSIGHT:~$
ls /etc/ntp.conf*


```

如果NTP配置檔案不可用，您可以從備份配置檔案建立副本。舉例來說：

```
<#root>
admin@FireSIGHT:~$
sudo cp /etc/ntp.conf.bak /etc/ntp.conf
```

#### 4. 驗證/etc/ntp.conf檔案是否已正確填充。應用系統策略時，會重寫ntp.conf檔案。

---

 註:ntp.conf檔案的輸出顯示在系統策略上配置的時間伺服器設定。時間戳條目必須顯示上一次系統策略應用於裝置的時間。伺服器條目必須顯示指定的時間伺服器地址。

---

```
<#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
```

檢驗兩台裝置上的NTP版本，並確保其相同。

有關NTP基礎的詳細資訊，請參閱[使用網路時間協定的最佳實踐。](#)



## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。