Firepower システムのネットワーク タイム プロトコル（NTP）で問題を解決して下さい

目次

概要

このドキュメントでは、FireSIGHT システムでの時刻の同期に関する一般的な問題とそのトラブルシューティング方法を説明します。 または NTP サーバとして動作する FireSIGHT Management Center 外部ネットワーク タイム プロトコル（NTP）サーバによっての SireSIGHT システム間の時間を 3 つのさまざまな方法の、手動でのような同期することを選択できます。 NTP で FireSIGHT Management Center をようにタイム サーバ設定でき、次に FireSIGHT Management Center と管理対象装置間の時間を同期するのにそれを使用する。

前提条件

要件

時刻の同期を設定するには、FireSIGHT Management Center で admin アクセス レベルが必要です。

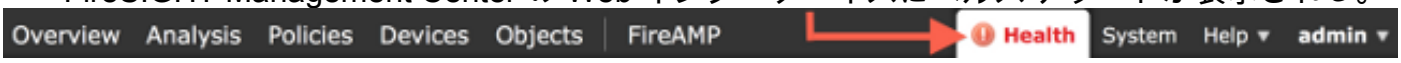
使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

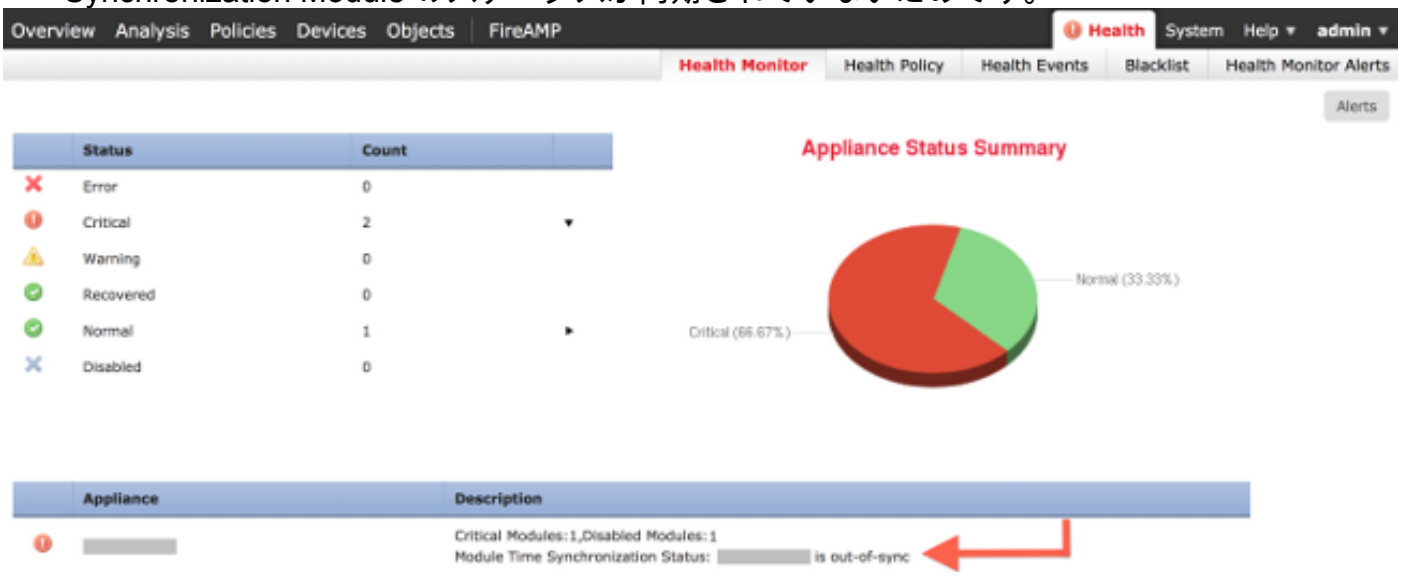
本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

症状

- FireSIGHT Management Center の Web インターフェイスにヘルス アラートが表示される。



- [Health Monitor] ページにアプライアンスが Critical として表示される。これは、Time Synchronization Module のステータスが同期されていないためです。



- アプライアンスが同期されてとどまらない場合断続的な健全性アラートを見るかもしれません。
- システム ポリシーが適用した後同期を完了するために FireSIGHT Management Center および管理対象装置が 20 分程かかる可能性があるので健全性アラートを見るかもしれません。これは、FireSIGHT Management Center が、管理対象デバイスに時刻を提供する前に、設定された NTP サーバとまず同期する必要があるためです。
- FireSIGHT Management Center と管理対象デバイスの時刻が一致していない。
- センサーで生成されるイベントは FireSIGHT Management Center で目に見えるようになるために分か時間がかかるかもしれません。
- バーチャル機器のためのクロック設定は同期されないことをバーチャル機器を実行したらおよび**ヘルス モニタ** ページが示したら、システム ポリシー時刻の同期設定をチェックして下さい。 シスコ では、仮想アプライアンスを物理 NTP サーバに同期することを推奨しています。（仮想または物理）管理対象デバイスを Virtual Defense Center と同期しないでください。

トラブルシューティング

ステップ 1： NTP 設定の確認

バージョン 5.4 および それ 以前で確認する方法

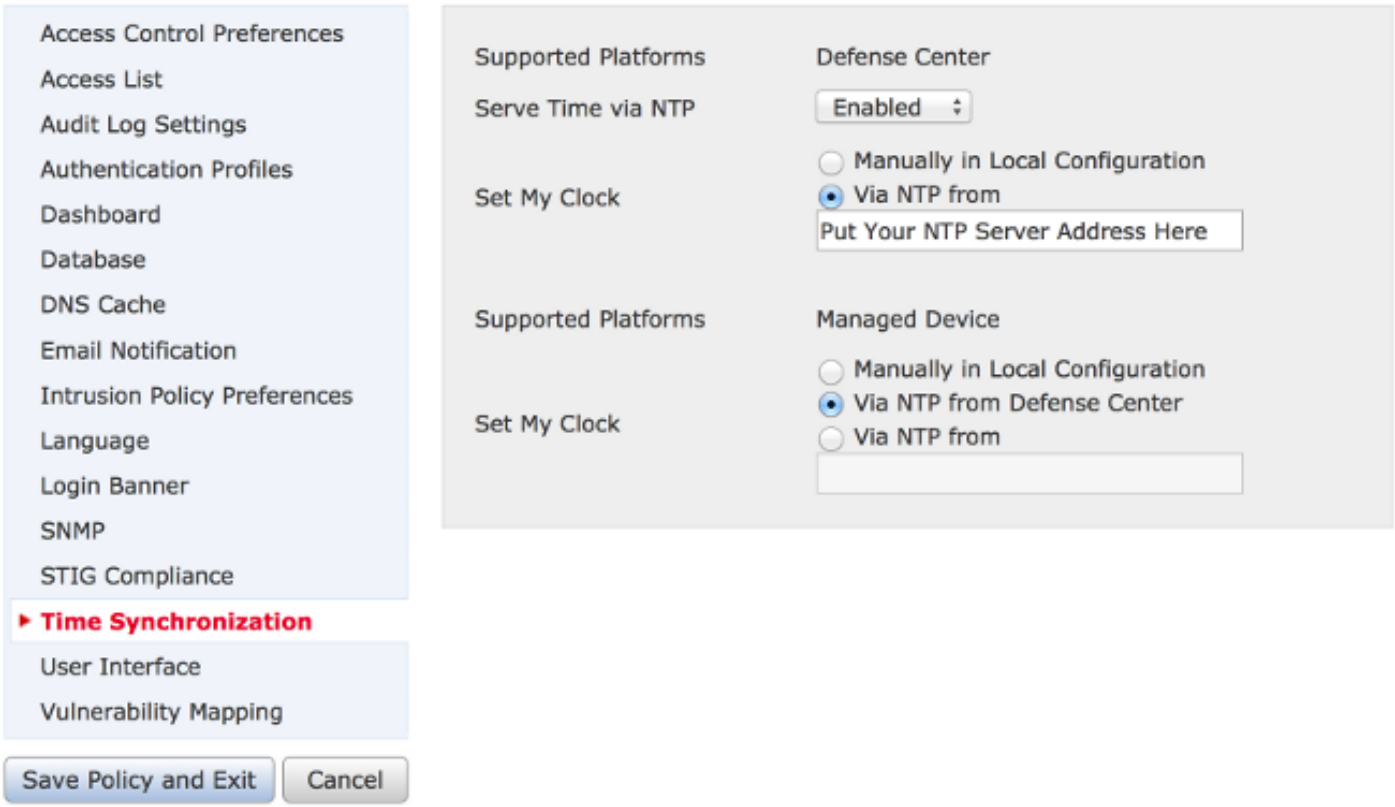
FireSIGHT システムに適用されているシステム ポリシーで NTP が有効になっていることを確認します。 それを確認するために、これらのステップを完了して下さい:

1. **システム > ローカル > システム ポリシー**を選択して下さい。
2. FireSIGHT システムに適用されているシステム ポリシーを編集します。
3. **時刻の同期**を選択して下さい。

FireSIGHT Management Center（Defense Center（DC）とも呼ばれます）でクロックが [Via

NTP from] に設定されており、NTP サーバのアドレスが指定されていることを確認します。 また、[Managed Device] が [via NTP from Defense Center] に設定されていることを確認します。

リモート外部 NTP サーバを規定 する場合、アプライアンスはそれにネットワーク アクセスをアクセスできなければなりません。 信頼できない NTP サーバを規定 しない で下さい。 バーチャル FireSIGHT Management Center に管理対象装置を (バーチャルか物理的な) 同期しないで下さい。 シスコ では、仮想アプライアンスを物理 NTP サーバに同期することを推奨しています。



バージョン 6.0 および それ 以降で確認する方法

バージョン 6.0.0 および それ 以降では、時刻の同期設定は Firepower Management Center の別々の場所で 5.4 のためのステップと同じ論理に従うけれども、行われます。

Firepower Management Center の時刻の同期設定自体は**システム > 設定 > 時刻の同期**の下にあります。

管理対象装置の時刻の同期設定は**デバイス > プラットフォーム設定**の下にあります。 デバイスに適用されるプラットフォーム設定ポリシーの隣で『Edit』 をクリック し、次に**時刻の同期を**選択して下さい。

時刻の同期のための設定を (バージョンに関係なく) 適用した後、ことを管理センターおよび管理対象装置一致の時間確かめて下さい。 さもなければ、故意ではない結果は管理対象装置が管理センターと交信を行うとき発生するかもしれません。

ステップ 2： タイム サーバとそのステータスの確認

- タイム サーバへの接続についての情報を収集するために、FireSIGHT Management Center のこのコマンドを入力して下さい:

```
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 の下のアスタリスク '*' は、現在同期しているサーバを示します。 アスタリスクが付いたエントリがない場合は、クロックは現在その時刻源と同期していません。管理対象装置で、NTP サーバのアドレスを確認するためにシェルのこのコマンドを入力できます:

```
> show ntp

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

注: FireSIGHT Management Center から時刻を受信するように管理対象デバイスが設定されている場合、そのデバイスは時刻源をループバック アドレス (127.0.0.2 など) で表示します。 この IP アドレスは sfipproxy エントリであり、時刻の同期に管理仮想ネットワークが使用されていることを示します。

- 127.127.1.1 と同期することアプライアンスが表示すれば、アプライアンスが自身のクロックによって同期することを示します。 これは、システム ポリシーで設定されているタイムサーバが同期可能ではない場合に発生します。 次に、例を示します。

```
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
```

- ntpq コマンド 出力で、注意すれば st (層) の値はタイムサーバーが到達不能であり、アプライアンスがそのタイムサーバーと sychronize できないことを 16、それ示しますです。
- ntpq コマンド 出力で、最新 8 つのポーリング試みにおけるソースに達する成功か失敗を示す 8 進数を示します。 見れば値は最後の 8 つの試みが正常だったことを 377、それ意味しますです。 他のどの値も最後の 8 つの試みの何れか一つ以上が不成功だったことを示すかもしれません。

ステップ3： 接続の確認

1. タイム サーバへの基本接続を確認します。

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

2. ポート 123 が SireSIGHT システムで開いていることを確認して下さい。

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

3. ファイアウォールでポート 123 が開いていることを確認します。
4. ハードウェア クロックを確認します。

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

ハードウェア クロックが正常に同期するには余りにも遠い旧式である場合、それらは決してかもしれませんでした。 手動でクロックをタイム サーバによって設定されるために強制するようにこのコマンドを入力して下さい:

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

次に ntpd を再起動します。

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

ステップ 4： コンフィギュレーション ファイルの確認

1. sfipproxy.conf ファイルに正しくデータが取り込まれているかどうかを確認します。 このファイルは sftunnel 上の NTP トラフィックを送信 します。
   管理対象装置の /etc/sf/sfipproxy.conf ファイルの例はここに示されています:

```
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 Management Center の /etc/sf/sfipproxy.conf ファイルの例はここに示されています:

```
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. peers セクションの下にある汎用一意識別子（UUID）が、ピアの ims.conf ファイルと一致していることを確認します。 たとえば、FireSIGHT Management Center の /etc/sf/sfipproxy.conf の peerssection の下で見つけられる UUID は管理対象装置の /etc/ims.conf で見つけられる UUID と一致する必要があります。 同様に、管理対象装置の /etc/sf/sfipproxy.conf の peerssection の下で見つけられる UUID は管理アプライアンスの /etc/ims.conf で見つけられる UUID と一致する必要があります。 このコマンドでデバイスの UUID を取得できます:

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

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

通常これらはシステム ポリシーにより自動的に設定されますが、これらのスタンザが欠落していることがあります。 変更する必要がある場合は、次のように sfipproxy および sftunnel を再起動する必要があります。

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

3. ntp.conf /etc で利用できるかどうか確認して下さい。

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

NTP コンフィギュレーション ファイルがない場合、バックアップ コンフィギュレーション ファイルからコピーを作成できます。 次に、例を示します。

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

4. /etc/ntp.conf ファイルにデータが正しく取り込まれているかどうかを確認します。 システム ポリシーを適用するとき、ntp.conf 書き換えられます。 **注:** ntp.conf ファイルの出力に、システム ポリシーで設定されているタイム サーバ設定が示されます。 タイムスタンプ エントリは、最後にシステム ポリシーがデバイスに適用された時刻を示している必要があります。 サーバ エントリは、指定されたタイム サーバのアドレスを示している必要があります。

```
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
```