

FireSIGHT システムのネットワーク タイム プロトコル (NTP) の問題のトラブルシューティング

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[症状](#)

[トラブルシュート](#)

[ステップ1:NTP設定の確認](#)

[バージョン5.4以前での確認方法](#)

[バージョン6.0以降での確認方法](#)

[手順2: タイムサーバとそのステータスを特定する](#)

[ステップ3: 接続の確認](#)

[ステップ4: コンフィギュレーションファイルの確認](#)

はじめに

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。

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

このドキュメントの内容は、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。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

外部のネットワークタイムプロトコル(NTP)サーバを手動で使用方法や、NTPサーバとして機能するFireSIGHT Management Centerを使用する方法など、3つの方法でFireSIGHTシステム間で時刻を同期することができます。FireSIGHT Management CenterをNTPを備えたタイムサーバとして設定し、それを使用してFireSIGHT Management Centerと管理対象デバイス間で時刻を同期できます。

症状

- FireSIGHT Management Centerは、ブラウザインターフェイスにヘルスアラートを表示します。



- [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。



Status	Count
✖ Error	0
❗ Critical	2
⚠ Warning	0
✅ Recovered	0
✅ Normal	1
❌ Disabled	0

Appliance Status Summary



Appliance	Description
❗	Critical Modules: 1, Disabled Modules: 1 Module Time Synchronization Status: is out-of-sync

- アプライアンスが同期を維持できない場合、断続的なヘルスアラートが表示される場合があります。
- システムポリシーを適用すると、FireSIGHT Management Centerとその管理対象デバイスの同期が完了するまでに最大20分かかることがあるため、ヘルスアラートを確認できます。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たイベントがFireSIGHT Management Centerに表示されるまでに数分または数時間かかることがあります。
- 仮想アプライアンスを実行していて、ヘルスマニタページに仮想アプライアンスのクロック設定が同期されていないことが表示される場合は、システムポリシーの時刻の同期設定を確認してください。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。

トラブルシュート

ステップ1:NTP設定の確認

バージョン5.4以前での確認方法

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。これを確認するには、次の手順を実行します。

1. System > Local > System Policyの順に選択します。
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. Time Synchronizationを選択します。

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。

リモートの外部NTPサーバを指定する場合、アプライアンスはサーバにネットワークアクセスできる必要があります。信頼できないNTPサーバは指定しないでください。管理対象デバイス (仮想または物理) を仮想FireSIGHT Management Centerと同期しないでください。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。

Access Control Preferences
Access List
Audit Log Settings
Authentication Profiles
Dashboard
Database
DNS Cache
Email Notification
Intrusion Policy Preferences
Language
Login Banner
SNMP
STIG Compliance
▶ Time Synchronization
User Interface
Vulnerability Mapping

Supported Platforms Defense Center
Serve Time via NTP Enabled
Set My Clock
Manually in Local Configuration
 Via NTP from
Put Your NTP Server Address Here

Supported Platforms Managed Device
Set My Clock
Manually in Local Configuration
 Via NTP from Defense Center
 Via NTP from

Save Policy and Exit Cancel

バージョン6.0以降での確認方法

バージョン6.0.0以降では、時刻の同期設定はFirepower Management Centerの別の場所で設定されていますが、5.4の手順と同じロジックをトレースします。

firepower Management Center自体の時刻同期設定は、System > Configuration > Time Synchronizationの下にあります。

管理対象デバイスの時刻同期設定は、Devices > Platform Settings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横にあるeditをクリックし、Time Synchronizationを選択します。

時刻の同期の設定を（バージョンに関係なく）適用した後、Management Centerと管理対象デバイスの時刻が一致していることを確認します。そうしないと、管理対象デバイスがManagement Centerと通信するときに、意図しない結果が発生する可能性があります。

手順2：タイムサーバとそのステータスを特定する

- タイムサーバへの接続に関する情報を収集するには、FireSIGHT Management Centerで次のコマンドを入力します。

```
<#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 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使用できない場合、クロックは現在その時刻源と同期していません。


管理対象デバイスでは、シェルで次のコマンドを入力して、NTPサーバのアドレスを判別できます。

```
<#root>
```

```
>
```

```
show ntp
```

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

 注：管理対象デバイスがFireSIGHT Management Centerから時刻を受信するように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sfiproxyエントリであり、管理仮想ネットワーク(MVS)が時刻の同期に使用されることを示します。

- アプライアンスで127.127.1.1と同期していることが表示される場合は、そのアプライアンスが自身のクロックと同期していることを示しています。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。例：

```
<#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

- ntpqコマンド出力で、st(stratum)の値が16の場合、タイムサーバに到達できず、アプライアンスがそのタイムサーバと同期できないことを示しています。
- ntpqコマンドの出力では、reachは直近の8回のポーリング試行における送信元への到達の成功または失敗を示す8進数を示します。値が377の場合は、最後の8回の試行が成功したことを意味します。その他の値は、最後の8回の試行のうち1回以上が失敗したことを示す可能性があります。

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。

```
<#root>
```

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

```
ping
```

2. FireSIGHTシステムでポート123が開いていることを確認します。

```
<#root>
```

```
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。

```
<#root>
```

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

```
sudo hwclock
```

ハードウェアクロックが非常に古い場合は、正常に同期できません。タイムサーバを使用してクロックを手動で強制的に設定するには、次のコマンドを入力します。

```
<#root>
```

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

```
sudo ntpdate -u
```

その後、再起動します `ntpd`:

```
<#root>
```

```
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. `sfiproxy.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`経由でNTPトラフィックを送信します。

管理対象デバイス上の`/etc/sf/sfiproxy.conf`ファイルの例を次に示します。

```
<#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 Management Centerの/etc/sf/sfiproxy.confファイルの例を次に示します。

```
<#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. 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/sfiproxy.confファイルのpeersセクションにあるUUIDは、管理対象デバイスの /etc/ims.confファイルにあるUUIDと一致する必要があります。同様に、管理対象デバイスの /etc/sf/sfiproxy.confファイルのpeersセクションにあるUUIDは、管理アプライアンスの

/etc/ims.confファイルにあるUUIDと一致する必要があります。

次のコマンドを使用して、デバイスのUUIDを取得できます。

```
<#root>
```

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

```
sudo grep UUID /etc/sf/ims.conf
```

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

これらは通常、システムポリシーによって自動的に入力される必要がありますが、これらのスタanzasが失われた場合があります。これらを変更する必要がある場合は、次の例に示すようにsfiproxyとsftunnelを再起動する必要があります。

```
<#root>
```

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

```
sudo pmtool restartbyid sfiproxy
```

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

```
sudo pmtool restartbyid sftunnel
```

3. ntp.confファイルが/etcディレクトリにあるかどうかを確認します。

```
<#root>
```

```
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。例：

```
<#root>
```

```
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、ntp.confファイルが書き換えられます。

 注:ntp.confファイルの出力には、システムポリシーで設定されたタイムサーバ設定が示されます。タイムスタンプのエントリには、最後にシステムポリシーがデバイスに適用された時刻が示されている必要があります。サーバエントリには、指定したタイムサーバアドレスが表示されている必要があります。

<#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
```

2台のデバイスでNTPバージョンを確認し、同じものであることを確認します。

NTPの基本の詳細については、『[ネットワークタイムプロトコルのベストプラクティスの使用](#)』を参照してください。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。