FireSIGHT 시스템의 NTP(Network Time Protocol) 문제 해결

목차

소개

이 문서에서는 FireSIGHT Systems에서 시간 동기화와 관련된 일반적인 문제와 문제 해결 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

시간 동기화 설정을 구성하려면 FireSIGHT Management Center에서 관리자 레벨의 액세스 권한이 필요합니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

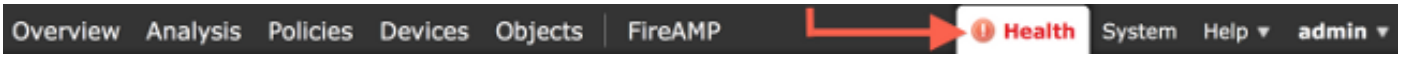
배경 정보

외부 NTP(Network Time Protocol) 서버 또는 NTP 서버 역할을 하는 FireSIGHT Management

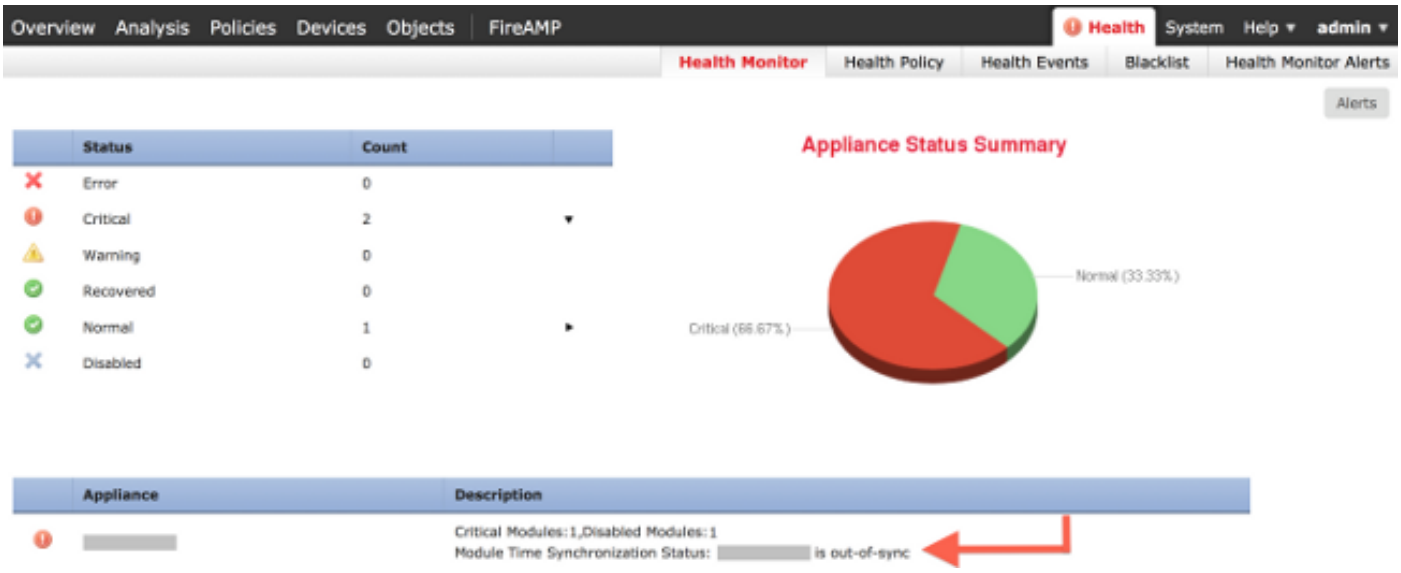
Center와 같은 세 가지 방법으로 FireSIGHT 시스템 간의 시간을 동기화하도록 선택할 수 있습니다. FireSIGHT Management Center를 NTP와 함께 시간 서버로 구성한 다음 이를 사용하여 FireSIGHT Management Center와 관리되는 디바이스 간의 시간을 동기화할 수 있습니다.

증상

- FireSIGHT Management Center는 브라우저 인터페이스에 상태 알림을 표시합니다.



- Time Synchronization Module의 상태가 동기화되지 않았기 때문에 Health Monitor 페이지에 어플라이언스가 중요한 것으로 표시됩니다.



- 어플라이언스가 동기화 상태를 유지하지 못할 경우 간헐적인 상태 알림을 볼 수 있습니다.
- 시스템 정책이 적용되면 상태 알림을 볼 수 있습니다. FireSIGHT Management Center 및 관리되는 디바이스가 동기화를 완료하는 데 최대 20분이 소요될 수 있기 때문입니다. 이는 FireSIGHT Management Center가 관리되는 디바이스에 시간을 제공하기 전에 먼저 구성된 NTP 서버와 동기화해야 하기 때문입니다.
- FireSIGHT Management Center와 관리되는 디바이스 간의 시간이 일치하지 않습니다.
- 센서에서 생성되는 이벤트가 FireSIGHT Management Center에 표시되는 데 몇 분 또는 몇 시간이 걸릴 수 있습니다.
- 가상 어플라이언스를 실행하고 Health Monitor 페이지에 가상 어플라이언스의 클럭 설정이 동기화되지 않은 것으로 표시되면 시스템 정책 시간 동기화 설정을 확인하십시오. 가상 어플라이언스를 물리적 NTP 서버와 동기화하는 것이 좋습니다. 관리되는 디바이스(가상 또는 물리적)를 Virtual Defense Center에 동기화하지 마십시오.

문제 해결

1단계: NTP 컨피그레이션 확인

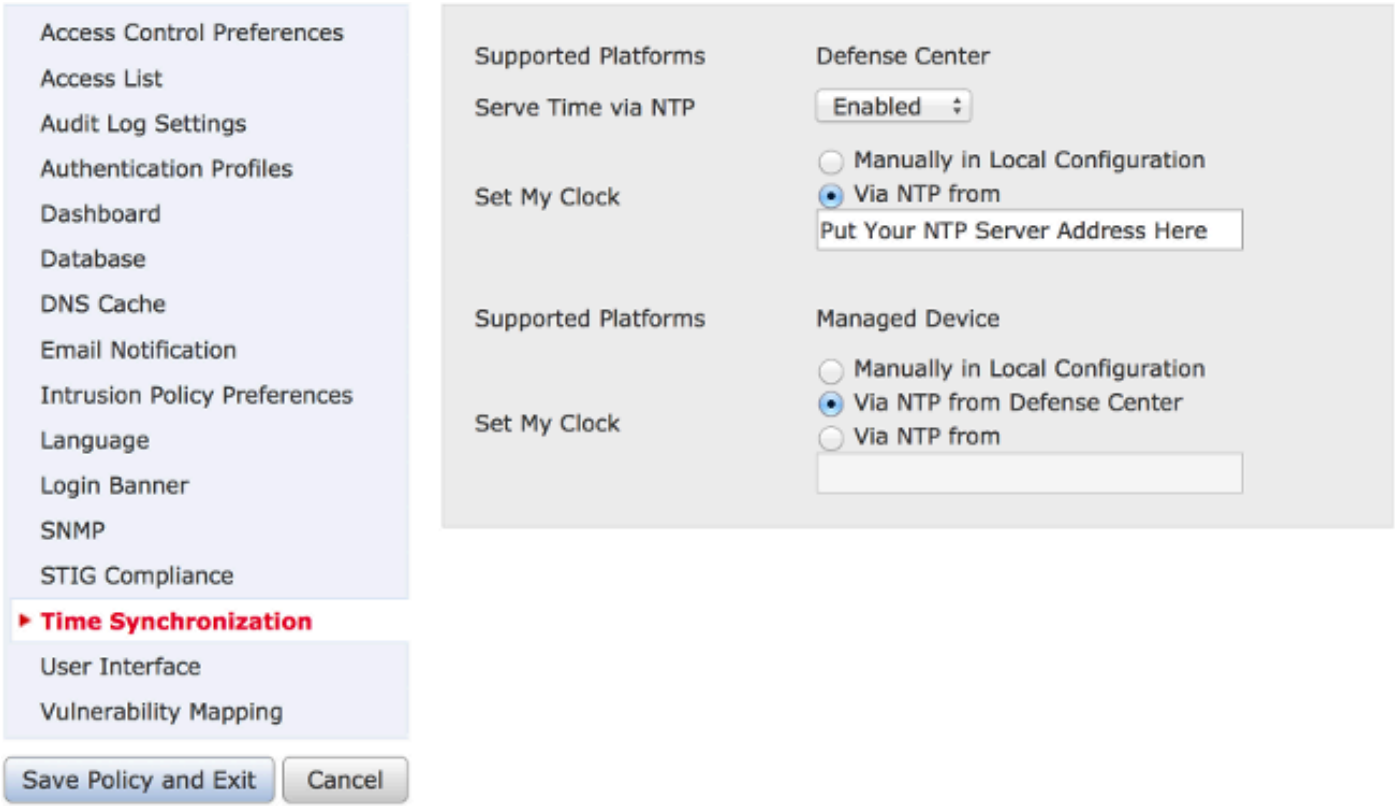
버전 5.4 이하에서 확인하는 방법

FireSIGHT 시스템에 적용된 시스템 정책에서 NTP가 활성화되었는지 확인합니다. 이를 확인하려면 다음 단계를 완료하십시오.

1. System(시스템) > Local(로컬) > System Policy(시스템 정책)를 선택합니다.
2. FireSIGHT 시스템에 적용된 시스템 정책을 수정합니다.
3. Time Synchronization을 선택합니다.

FireSIGHT Management Center(Defense Center 또는 DC라고도 함)의 시계가 Via NTP from으로 설정되어 있고 NTP 서버의 주소가 제공되는지 확인합니다. 또한 Managed Device(관리되는 디바이스)가 Defense Center에서 NTP를 통해 설정되었는지 확인합니다.

원격 외부 NTP 서버를 지정하는 경우 어플라이언스에 대한 네트워크 액세스 권한이 있어야 합니다. 신뢰할 수 없는 NTP 서버를 지정하지 마십시오. 관리되는 디바이스(가상 또는 물리적)를 가상 FireSIGHT Management Center에 동기화하지 마십시오. 가상 어플라이언스를 물리적 NTP 서버와 동기화하는 것이 좋습니다.



버전 6.0 이상에서 확인하는 방법

버전 6.0.0 이상에서는 시간 동기화 설정이 5.4의 단계와 동일한 로직을 추적하지만 Firepower Management Center의 개별 위치에서 구성됩니다.

Firepower Management Center 자체에 대한 시간 동기화 설정은 System > Configuration > Time Synchronization에 있습니다.

관리되는 디바이스에 대한 시간 동기화 설정은 Devices(디바이스) > Platform Settings(플랫폼 설정)에서 확인할 수 있습니다. 디바이스에 적용된 플랫폼 설정 정책 옆에 있는 수정을 클릭한 다음 시간 동기화 를 선택합니다.

시간 동기화를 위해 컨피그레이션을 적용한 후(버전에 상관없이) Management Center 및 관리되는 디바이스의 시간이 일치하는지 확인합니다. 그렇지 않으면 관리되는 디바이스가 Management Center와 통신할 때 의도하지 않은 결과가 발생할 수 있습니다.

2단계: Timeserver 및 해당 상태 확인

- 시간 서버 연결에 대한 정보를 수집하려면 FireSIGHT Management Center에서 다음 명령을 입력합니다.
  <#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
  ```

  원격 아래의 별표 '*'는 현재 동기화되어 있는 서버를 나타냅니다. 별표가 있는 항목을 사용할 수 없는 경우 현재 시계가 해당 시간 원본과 동기화되지 않습니다.

  관리되는 디바이스에서 NTP 서버의 주소를 확인하기 위해 셸에 이 명령을 입력할 수 있습니다.

  <#root>

  ```
  >

  show ntp


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

  참고: 관리되는 디바이스가 FireSIGHT Management Center에서 시간을 수신하도록 구성된 경우 디바이스에는 루프백 주소(예: 127.0.0.2)가 있는 시간 소스가 표시됩니다. 이 IP 주소는 sfipproxy 항목이며, 관리 가상 네트워크가 시간 동기화에 사용됨을 나타냅니다.

- 어플라이언스가 127.127.1.1과 동기화됨을 표시하는 경우 어플라이언스가 자체 클럭과 동기화됨을 나타냅니다. 이 오류는 시스템 정책에 구성된 시간 서버를 동기화할 수 없을 때 발생합니다. 예를 들면 다음과 같습니다.
  <#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 명령 출력에서 st(stratum) 값이 16인 경우 이는 timeserver에 연결할 수 없으며 어플라이언스가 해당 timeserver와 동기화할 수 없음을 나타냅니다.
- ntpq 명령 출력에서 reach는 최근 8번의 폴링 시도에 대한 소스 도달 성공 또는 실패를 나타내는 8진수를 표시합니다. 값이 377이면 마지막 8번의 시도가 성공했음을 의미합니다. 다른 값은 마지막 8개 시도 중 하나 이상이 실패했음을 나타낼 수 있습니다.

3단계: 연결 확인

1. 시간 서버에 대한 기본 연결을 확인합니다.
   <#root>

   admin@FireSIGHT:~$

   ping

2. FireSIGHT 시스템에서 포트 123이 열려 있는지 확인합니다.
   <#root>

   admin@FireSIGHT:~$

   netstat -an | grep 123

3. 방화벽에서 포트 123이 열려 있는지 확인합니다.
4. 하드웨어 시계를 확인합니다.
   <#root>

   admin@FireSIGHT:~$

   sudo hwclock

   하드웨어 시계가 너무 오래된 경우 성공적으로 동기화할 수 없습니다. 시계에 시간 서버를 수동으로 설정하려면 다음 명령을 입력합니다.

   <#root>

```
admin@FireSIGHT:~$
sudo ntpdate -u
```

그런 다음 다시 시작 ntpd:

```
<#root>
admin@FireSIGHT:~$
sudo pmtool restartbyid ntpd
```

4단계: 컨피그레이션 파일 확인

1. sfipproxy.conf 파일이 올바르게 입력되었는지 확인합니다. 이 파일은 sftunnel을 통해 NTP 트래픽을 전송합니다.

관리되는 디바이스의 /etc/sf/sfipproxy.conf 파일의 예는 다음과 같습니다.

```
<#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;
            }
        }
    }
```

```
}
```

FireSIGHT Management Center의 /etc/sf/sfipproxy.conf 파일의 예는 다음과 같습니다.

<#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. peers(피어) 섹션의 UUID(Universally Unique Identifier)가 피어의 ims.conf 파일과 일치하는지 확인합니다. 예를 들어, FireSIGHT Management Center의 /etc/sf/sfipproxy.conf 파일 피어 섹션에 있는 UUID는 관리되는 디바이스의 /etc/ims.conf 파일에 있는 UUID와 일치해야 합니다. 마찬가지로, 관리되는 디바이스의 /etc/sf/sfipproxy.conf 파일의 피어 섹션에 있는 UUID는 관리 어플라이언스의 /etc/ims.conf 파일에 있는 UUID와 일치해야 합니다.

   다음 명령을 사용하여 디바이스의 UUID를 검색할 수 있습니다.

<#root>

```
admin@FireSIGHT:~$

sudo grep UUID /etc/sf/ims.conf



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

이러한 스탠자는 일반적으로 시스템 정책에 의해 자동으로 채워져야 하지만 이러한 스탠자가 손실된 경우가 있었습니다. 수정하거나 변경해야 하는 경우 다음 예에 표시된 대로 sfipproxy 및 sftunnel을 다시 시작해야 합니다.

<#root>

admin@FireSIGHT:~$

sudo pmtool restartbyid sfipproxy

admin@FireSIGHT:~$

sudo pmtool restartbyid sftunnel

3. /etc 디렉토리에서 ntp.conf 파일을 사용할 수 있는지 확인합니다.
<#root>

admin@FireSIGHT:~$

ls /etc/ntp.conf*

NTP 컨피그레이션 파일을 사용할 수 없는 경우 백업 컨피그레이션 파일에서 복사본을 만들 수 있습니다. 예를 들면 다음과 같습니다.

<#root>

admin@FireSIGHT:~$

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

4. /etc/ntp.conf 파일이 올바르게 입력되었는지 확인합니다. 시스템 정책을 적용하면 ntp.conf 파일이 다시 작성됩니다.

참고: ntp.conf 파일의 출력에는 시스템 정책에 구성된 시간 서버 설정이 표시됩니다. 타임 스탬프 항목은 디바이스에 마지막으로 시스템 정책이 적용된 시간을 표시해야 합니다. 서버 항목에는 지정된 시간 서버 주소가 표시되어야 합니다.

<#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
```

두 디바이스에서 NTP 버전을 확인하고, 해당 버전도 동일한지 확인합니다.

NTP 기본 사항에 대한 자세한 내용은 Use Best Practices for Network Time Protocol을 참조하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.