Решите проблемы с протоколом NTP в системах FireSIGHT

Содержание

Введение

Можно принять решение синхронизировать время между Системами FireSIGHT тремя другими способами, такой как вручную, с помощью внешних серверов NTP, или с помощью Центра управления FireSIGHT (служащий сервером NTP). Можно настроить Центр управления FireSIGHT как временной сервер с помощью NTP и затем использовать его для синхронизации времени между Центром управления FireSIGHT и управляемыми устройствами. Этот документ описывает общие проблемы с временной синхронизацией в Системах FireSIGHT и как устранить неполадки их.

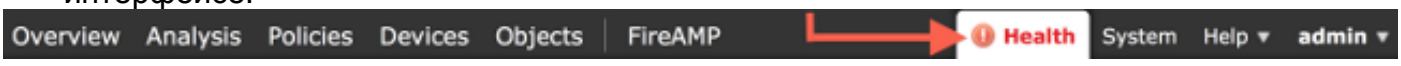
Предварительные условия

Для настройки значения временной синхронизации вам нужен уровень `admin` доступа на вашем Центре управления FireSIGHT.

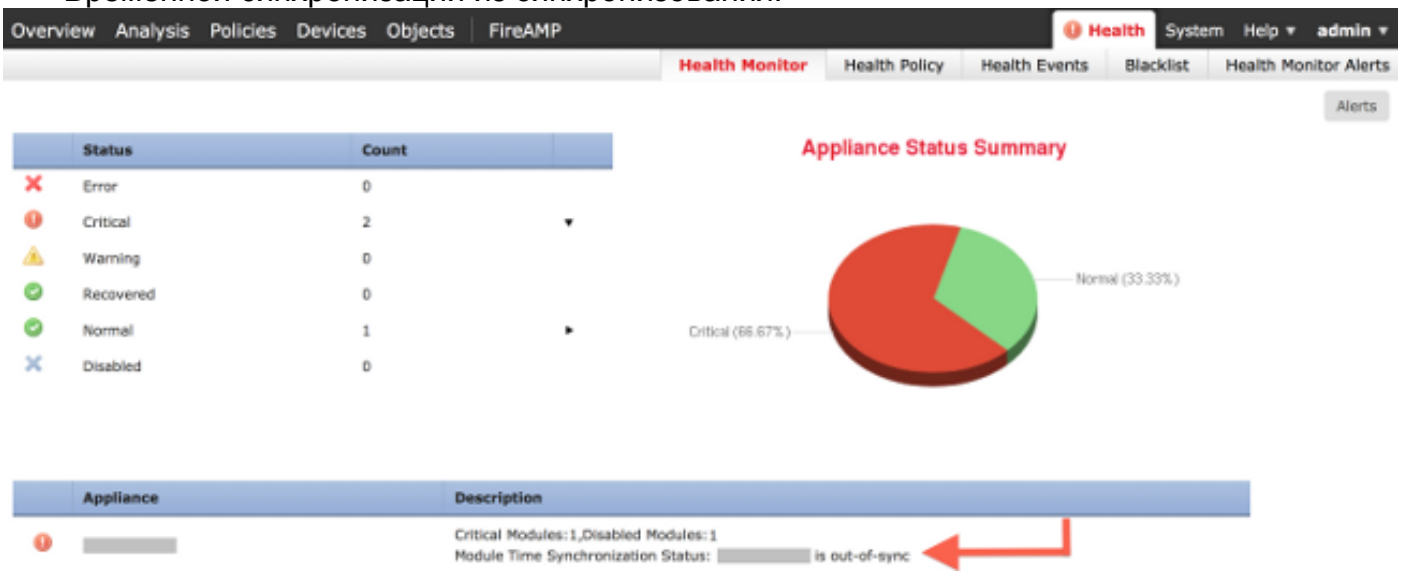
> **Примечание:** Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Признаки

- Центр управления FireSIGHT отображает предупреждения состояния на веб-интерфейсе.



- Страница **Health Monitor** показывает устройство как critial, потому что статус Модуля Временной синхронизации из синхронизования.



- Если устройства не в состоянии оставаться синхронизируемыми, можно видеть неустойчивые предупреждения состояния.
- После применения системной политики можно видеть предупреждения состояния, becasue Центр управления FireSIGHT, и его управляемые устройства могут занять до 20 минут для завершения синхронизации. Это вызвано тем, что Центр управления FireSIGHT должен сначала синхронизироваться с его настроенным сервером NTP, прежде чем он сможет отбыть срок службы к управляемому устройству.
- Время между Центром управления FireSIGHT и управляемым устройством не совпадает.
- События, генерируемые в датчике, могут занять минуты или часы для становления видимыми на Центре управления FireSIGHT.
- Если вы выполняете виртуальные устройства, и страница **Health Monitor** указывает, что настройка часов для вашего виртуального устройства "not synchronized", проверьте свои параметры настройки временной синхронизации системной политики. Cisco рекомендует синхронизировать виртуальные устройства с физическим сервером NTP. Не синхронизируйте свои управляемые устройства (действительный или физический) к Действительному Центру Защиты.

Устранение неисправностей

Шаг 1: Проверьте конфигурацию NTP

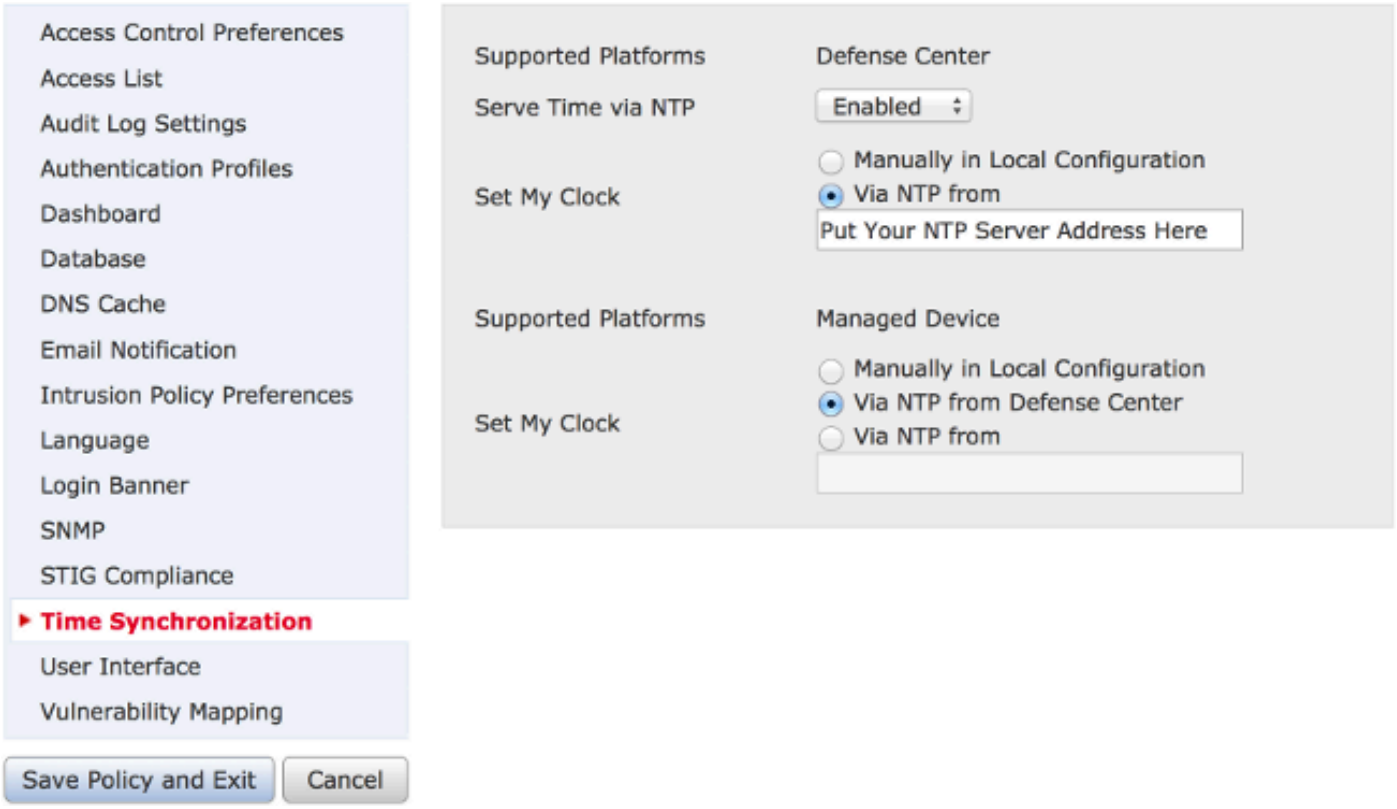
Проверьте, что NTP включен на системной политике, которая применена на Системы FireSIGHT. Чтобы проверить, что, выполните действия ниже:

- Перейдите к **Системе> Локальный> Системная политика**.
- Отредактируйте системную политику, примененную на ваши Системы FireSIGHT.
- Выберите **Time Synchronization**.

Проверьте, имеет ли Центр управления FireSIGHT (также известный как Центр Защиты или

DC) clock set к **Через NTP от**, и адрес сервера NTP предоставлен. Также подтвердите, что Управляемое устройство установлено в **через NTP от Центра Защиты**.

При определении удаленного внешнего сервера NTP устройство должно иметь доступ к сети к нему. Не задавайте недоверяемый сервер NTP. Не синхронизируйте свои управляемые устройства (действительный или физический) к Действительному Центру управления FireSIGHT. Cisco рекомендует синхронизировать виртуальные устройства с физическим сервером NTP.



После применения конфигурации для временной синхронизации удостоверьтесь, что совпадает время на Центре управления и управляемых устройствах. В противном случае, когда управляемые устройства связываются с Центром управления, непреднамеренные последствия могли бы произойти.

Шаг 2: Определите Timeserver, и это - статус

1. Для сбора информации о соединении с временным сервером выполните следующую команду на Центре управления FireSIGHT:

```
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
```

Звездочка '*' под `удаленным` указывает на сервер, с которым вы в настоящее время синхронизируетесь. Если запись со звездочкой недоступна, часы в настоящее время не синхронизируются с, он - timesource.

На управляемом устройстве можно выполнить следующую команду на оболочке для

определения адреса сервера NTP:

```
> show ntp

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

> **Примечание:** Если управляемое устройство настроено для получения времени от Центра управления FireSIGHT, устройство показывает timesource с адресом обратной связи, такой как `127.0.0.2`. Этот IP-адрес является sfipproxy записью и указывает, что Виртуальная сеть Managment используется для синхронизации времени.

2. Если устройство отображает это, оно синхронизирует с `127.127.1.1`, оно указывает, что устройство синхронизирует с его собственными часами. Когда сервер времени, настроенный на системной политике, не synchronizable, происходит. Пример:

```
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
```

3. На `ntpq` выходных данных команды, если вы замечаете, значение `Св.` (страта) равняется 16, это указывает, что сервер времени недостижим, и устройство не будет в состоянии к sychronize с тем сервером времени.

4. На `ntpq` выходных данных команды `достигните`, показывает восьмеричное число, которое указывает на успешность или неуспешность для достижения источника для новых 8 попыток опроса. Если вы видите, что значение 377, это означает, что последние 8 попыток были успешны. Любые другие значения могут указать, что тот или больше последних 8 попыток были неуспешны.

Шаг 3: Проверьте подключение

1. Проверьте основное подключение к временному серверу.

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

2. Гарантируйте, что порт 123 открыт в ваших Системах FireSIGHT.

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

3. Подтвердите, что порт 123 открыт на межсетевом экране.

4. Проверьте аппаратные часы:

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

Если аппаратные часы слишком далеко устарели, они никогда могут не успешно синхронизировать. Чтобы вручную вынудить часы быть установленными с временным сервером, выполните следующую команду:

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

Затем перезапуск `ntpd`:

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

Шаг 4. : Проверьте файлы конфигурации

1. Проверьте, заполнен ли `sfipproxy.conf` файл правильно. Этот файл ответственен за передачу трафика NTP по sftunnel.

Пример`/etc/sf/sfipproxy.conf` файла на управляемом устройстве ниже:

```
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;
}
}
}
}
```

Пример`/etc/sf/sfipproxy.conf` файла на Центре управления FireSIGHT ниже:

```
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. Удостоверьтесь, что Универсально Уникальный идентификатор (UUID) под `узлами` разделяет соответствия с `ims.conf` файлом узел. Например, UUID, найденный под `одноранговым` разделом`/etc/sf/sfipproxy.conf` файла на Центре управления

FireSIGHT, должен совпасть с UUID, найденным на`/etc/ims.conf` файле его управляемого устройства. Точно так же UUID, найденный под `одноранговым` разделом`/etc/sf/sfipproxy.conf` файла на управляемом устройстве, должен совпасть с UUID, найденным на`/etc/ims.conf` файле его устройства управления.

Можно получить UUID устройств с командой ниже:

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

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

Они должны обычно автоматически заполняться системной политикой, но были случаи, где отсутствовали эти строфы. Если они должны модифицироваться или изменились, необходимо будет перезапустить sfipproxy и sftunnel следующим образом:

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

3. Проверьте, доступен ли `ntp.conf` файл на `/ и т.д.` каталог.

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

Если файл конфигурации NTP недоступен, можно сделать копию с резервного файла конфигурации. Пример:

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

4. Проверьте, заполнен ли`/etc/ntp.conf` файл правильно. При применении системной политики `ntp.conf` файл переписан.

> **Примечание:** Выходные данные `ntp.conf` файла показывают параметры настройки сервера времени, настроенные на системной политике. Когда последняя системная политика применилась к устройству, запись штампа времени должна показать время. Серверная запись должна, должен показать указанный адрес сервера времени.

```
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
```