أستكشاف أخطاء الشبكة الزمنية (NTP) وإصلاحها على أنظمة FireSIGHT

المحتويات

المقدمة

يصف هذا المستند المشكلات الشائعة المتعلقة بمزامنة الوقت على أنظمة FireSIGHT وكيفية أستكشاف الأخطاء وإصلاحها.

المتطلبات الأساسية

المتطلبات

لتكوين إعداد مزامنة الوقت، تحتاج إلى مستوى وصول المسؤول على مركز إدارة FireSIGHT.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

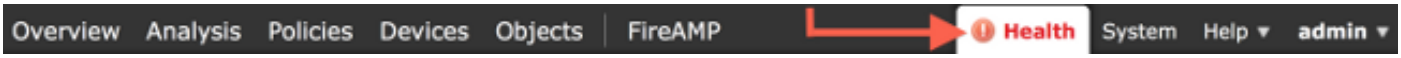
معلومات أساسية

يمكنك إختيار مزامنة الوقت بين أنظمة FireSIGHT لديك بثلاث طرق مختلفة، مثل يدوي، مع خوادم بروتوكول وقت الشبكة الخارجية (NTP)، أو مع مركز إدارة FireSIGHT الذي يعمل كخادم

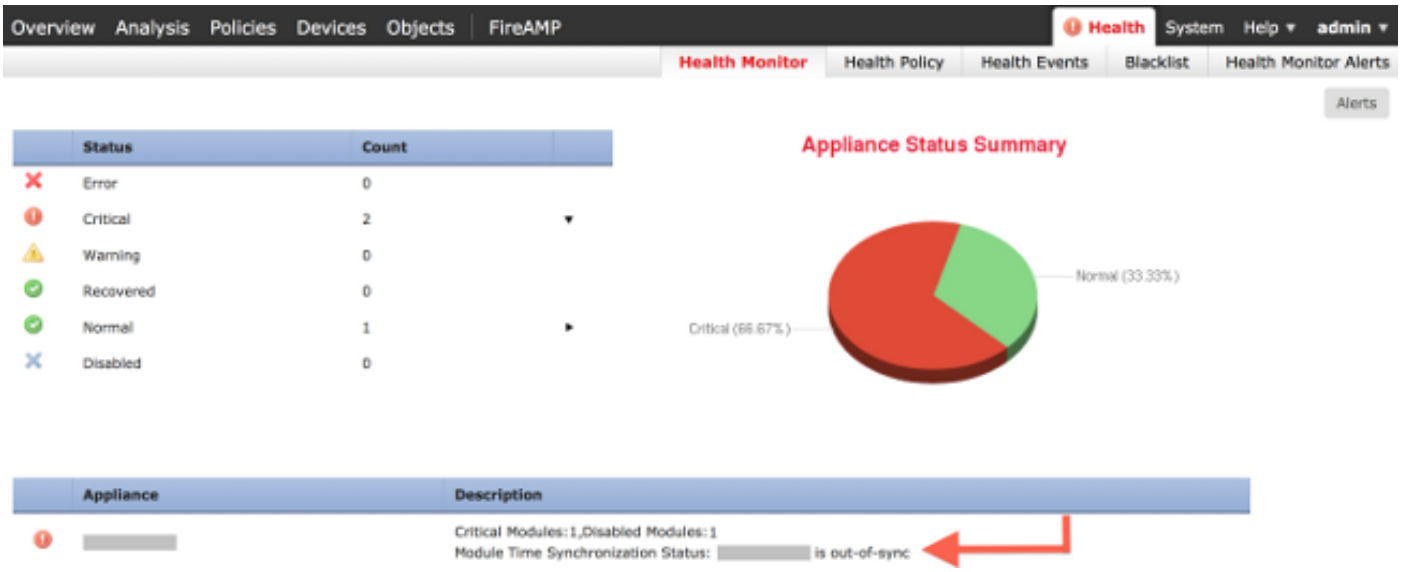
NTP. يمكنك تكوين مركز إدارة FireSIGHT كخادم وقت مع NTP ثم إستخدامه لمزامنة الوقت بين مركز إدارة FireSIGHT والأجهزة المدارة.

الأعراض

- يعرض FireSIGHT Management Center تنبيهات الحماية على واجهة المستعرض.



- تظهر صفحة Health Monitor جهاز كأمر ضروري، نظرا لأن حالة وحدة مزامنة الوقت غير متزامنة.



- يمكنك مشاهدة تنبيهات الحماية المتقطعة في حالة فشل الأجهزة في الاستمرار في المزامنة.
- بعد تطبيق نهج النظام، يمكنك مشاهدة تنبيهات الحماية، لأن مركز إدارة FireSIGHT والأجهزة المدارة الخاصة به قد يستغرق ما يصل إلى 20 دقيقة للإكمال المزامنة. وذلك لأنه يجب على مركز إدارة FireSIGHT المزامنة أولا مع خادم NTP الذي تم تكوينه قبل أن يتمكن من خدمة الوقت لجهاز مدار.
- لا يتطابق الوقت بين FireSIGHT Management Center والجهاز المدار.
- قد تستغرق الأحداث التي يتم إنشاؤها عند المستشعر دقائق أو ساعات حتى تصبح مرئية في مركز إدارة FireSIGHT.
- إذا قمت بتشغيل الأجهزة الظاهرية وتشير صفحة مراقبة الصحة إلى عدم مزامنة إعداد الساعة للجهاز الظاهري، فتحقق من إعدادات مزامنة الوقت لنهج النظام. توصي Cisco بمزامنة الأجهزة الظاهرية لديك مع خادم NTP مادي. ال تقم بمزامنة أجهزتك المدارة (الافتراضية أو المادية) مع مركز الدفاع الظاهري.

استكشاف الأخطاء وإصلاحها

الخطوة 1: التحقق من تكوين NTP

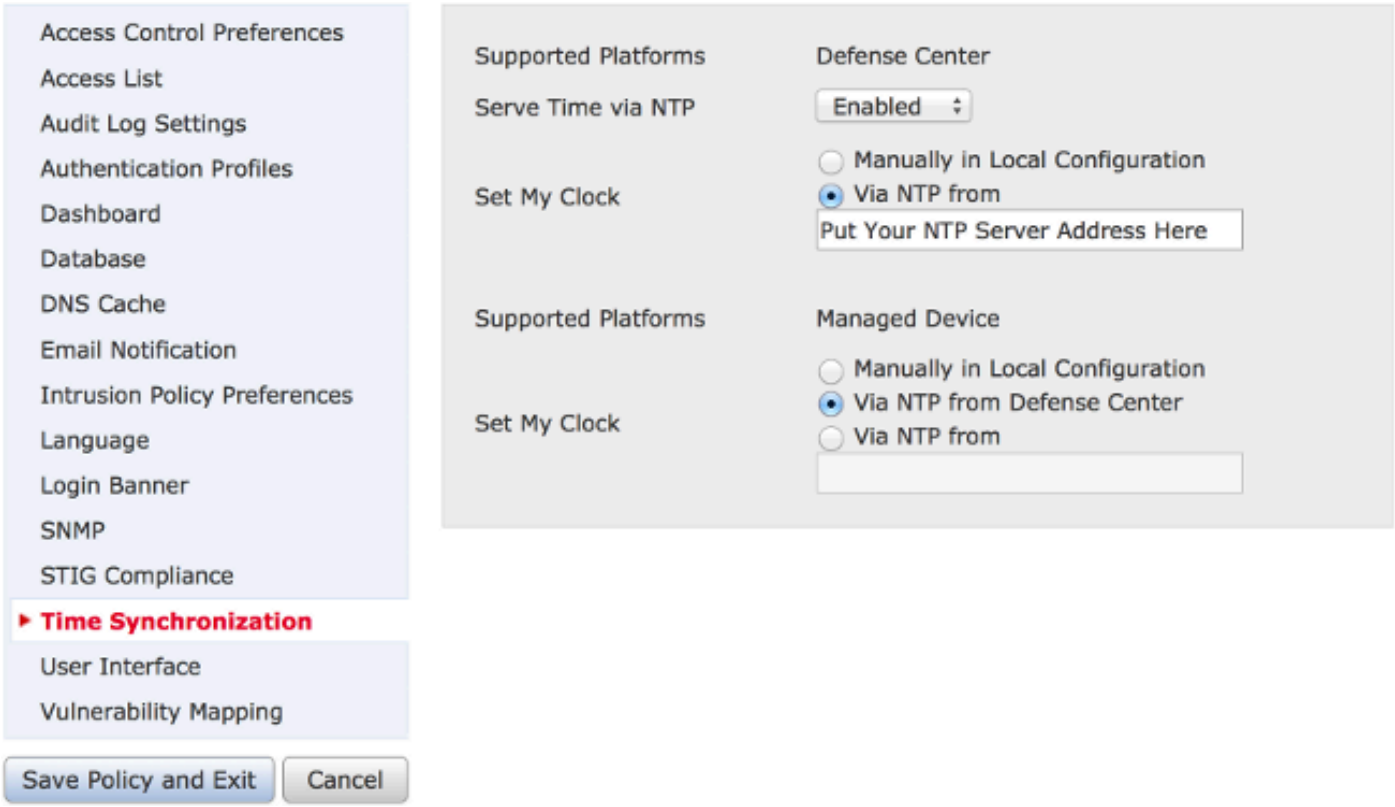
كيفية التحقق في الإصدارات 5.4 والإصدارات الأقدم

تحقق من تمكين NTP على نمط النظام المطبق على أنظمة FireSIGHT. أتمت in order to دقق أن، اذه steps:

1. أختر نظام > محلي > سياسة النظام.
2. قم بتحرير نمط النظام المطبق على أنظمة FireSIGHT.
3. أختر مزامنة الوقت.

تحقق مما إذا كان FireSIGHT Management Center (المعروف أيضا باسم Defense Center أو DC) لديه السماعة المعينة إلى عبر NTP من، وتم توفير عنوان لخادم NTP. تأكد أيضا من تعيين الجهاز المدار على عبر NTP من مركز الدفاع.

إذا قمت بتحديد خادم NTP خارجي بعيد، فيجب أن يكون لدى الجهاز الخاص بك حق وصول إلى الشبكة. عدم تحديد خادم NTP غير موثوق به. ال تقم بمزامنة أجهزتك المدارة (الافتراضية أو المادية) إلى مركز إدارة FireSIGHT ظاهري. توصي Cisco بمزامنة الأجهزة الظاهرية لديك مع خادم NTP مادي.



كيفية التحقق في الإصدارات 6.0 والإصدارات الأحدث

في الإصدارات 6.0.0 والإصدارات الأحدث، يتم تكوين إعدادات مزامنة الوقت في أماكن منفصلة على مركز إدارة Firepower، رغم أنها تتبع نفس المنطق الموجود في الخطوات الخاصة ب 5.4.

تم العثور على إعدادات مزامنة الوقت لمركز إدارة Firepower نفسه ضمن النظام > التكوين > مزامنة الوقت.

تم العثور على إعدادات مزامنة الوقت للأجهزة المدارة ضمن الأجهزة > إعدادات النظام الأساسي. انقر فوق تحرير بجوار نمط إعدادات النظام الأساسي المطبق على الجهاز ثم أختر مزامنة الوقت.

بعد تطبيق التكوين لمزامنة الوقت (بغض النظر عن الإصدار)، تأكد من تطابق الوقت في مركز الإدارة والأجهزة المدارة. وإلا، يمكن أن تحدث عواقب غير مقصودة عند اتصال الأجهزة المدارة بمركز الإدارة.

الخطوة 2: تحديد برنامج زمني وحالته

- لتجميع معلومات حول الاتصال بخادم وقت، أدخل هذا الأمر على مركز إدارة FireSIGHT الخاص بك:
<#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
```

تشير علامة نجمية '*' تحت البعيد إلى الخادم الذي تتم مزامنته حاليا. إذا لم يتوفر إدخال ذي علامة نجمية، فلا تتم مزامنة الساعة حاليا مع مصدر الوقت الخاص بها.

على جهاز تتم إدارته، يمكنك إدخال هذا الأمر على طبقة لتحديد عنوان خادم NTP الخاص بك:

<#root>

```
>
```

show ntp

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

ملاحظة: إذا تم تكوين جهاز مدار لتلقي الوقت من مركز إدارة FireSIGHT، فسيقوم عنوان IP هذا بعرض مصدر وقت بعنوان الاسترجاع، مثل 127.0.0.2. لا يشير إلى استخدام شبكة الإدارة الظاهرية لتزامن الوقت وليس إلى إدخال وكيل صغير.

- إذا عرض جهاز ما أنه يقوم بمزامنته مع 127.127.1.1، فإنه يشير إلى أن مزامنة الجهاز مع ساعته الخاصة. يحدث ذلك عندما يكون أحد الجداول الزمنية التي تم تكوينها على نحو النظام غير قابل للمزامنة. على سبيل المثال:
<#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
```

- في إخراج الأمر ntpq، إذا لاحظت أن قيمة st (stratum) هي 16، فإنها تشير إلى أن الوقت غير قابل للوصول وأن الجهاز غير قادر على التزامن باستخدام هذا الوقت.
- في إخراج أمر ntpq، يظهر Reach رقم ثماني يشير إلى النجاح أو الفشل في الوصول إلى المصدر لمحاولات الاقتراع الثماني الأخيرة. إذا كنت ترى القيمة هي 377، فهذا يعني أن 8 محاولات آخر كانت ناجحة. يمكن أن تشير أي قيم أخرى إلى أن محاولة أو أكثر من المحاولات الثماني الأخيرة كانت غير ناجحة.

الخطوة 3: التحقق من الاتصال

1. تحقق من الاتصال الأساسي بخادم الوقت.
   <#root>

   admin@FireSIGHT:~$

   ping

2. تأكد من أن المنفذ 123 مفتوح على نظام FireSIGHT لديك.
   <#root>

   admin@FireSIGHT:~$

   netstat -an | grep 123

3. تأكد من أن المنفذ 123 مفتوح على جدار الحماية.
4. تحقق من ساعة الأجهزة:
   <#root>

   admin@FireSIGHT:~$

   sudo hwclock

   إذا كانت ساعة الأجهزة قديمة جدا، فلن تتمكن هذه الساعات من المزامنة بنجاح. لفرض تعيين الساعة يدويا باستخدام خادم الوقت، أدخل هذا الأمر:

   <#root>

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

ثم أعد التشغيل ntpd:

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

الخطوة 4: التحقق من ملفات التكوين

1. تحقق مما إذا كان ملف sfipproxy.conf تم تعبئته بشكل صحيح. يرسل هذا الملف حركة مرور NTP عبر SFTUNNEL.

يتم عرض مثال على الملف /etc/sf/sfipproxy.conf على جهاز مدار هنا:

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

```
}
```

يتم عرض مثال على ملف /etc/sf/sfipproxy.conf في FireSIGHT Management Center هنا:

<#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. تأكد من أن المعرف الفريد العالمي (UUID) تحت قسم الأقران يتطابق مع ملف ims.conf النظير. على سبيل المثال، يجب أن تتطابق UUID التي تم العثور عليها ضمن قسم الأقران من الملف /etc/sf/sfipproxy.conf الموجود في "مركز إدارة FireSIGHT" مع UID الذي تم العثور عليه في الملف /etc/ims.conf الخاص بالجهاز الذي تتم إدارته. بالمثل، ال UUID الموجود تحت ال نظير قسم من /etc/sf/sfipproxy.conf مبرد على أداة مدار ينبغي تطابقت ال UUID يوجد على /etc/ims.conf مبرد من الإدارة أداة.

أنت يستطيع إسترددت ال UID من الأداة مع هذا أمر:

<#root>

```
admin@FireSIGHT:~$

sudo grep UUID /etc/sf/ims.conf


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

يجب أن يتم علم هذه التلقائي من قبل نهج النظام، ولكن هناك حالات تم فيها فقد هذه السلازن. إذا كانت بحاجة إلى التعديل أو التغيير، فأنت بحاجة إلى إعادة تشغيل sfTunnel و FastProxy كما هو موضح في هذا المثال:

```
<#root>

admin@FireSIGHT:~$

sudo pmtool restartbyid sfipproxy

admin@FireSIGHT:~$

sudo pmtool restartbyid sftunnel
```

3. دقق إن ntp.conf يتوفر مبرد على ال /etc دليل.

```
<#root>

admin@FireSIGHT:~$

ls /etc/ntp.conf*
```

إذا كان ملف تكوين NTP غير متوفر، فيمكنك إجراء نسخة من ملف تكوين النسخ الاحتياطي. على سبيل المثال:

```
<#root>

admin@FireSIGHT:~$

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

4. تحقق مما إذا كان الملف /etc/ntp.conf قد تم ملؤه بشكل صحيح. عندما توقم بتطبيق سياسة نظام، يتم إعادة كتابة ملف ntp.conf.

> ملاحظة: يظهر إخراج ملف ntp.conf إعدادات TimeServer التي تم تكوينها على نهج النظام. يجب أن يظهر إدخال الطابع الزمني الوقت الوقت الذي تم فيه تطبيق آخر نهج نظام على الجهاز. يجب أن يعرض إدخال الخادم عنوان TimeErver المحدد.

```
<#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
```

تحقق من إصدارات NTP على جهازين وتأكد من أنها مماثلة أيضا.

للحصول على تفاصيل حول أساسيات NTP، راجع إلى أفضل الممارسات لبروتوكول استخدام وقت الشبكة.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).