Résolution des problèmes liés au protocole NTP (Network Time Protocol) sur les systèmes FireSIGHT

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Symptômes

Dépannage

- Étape 1 : Vérification de la configuration NTP
  - Comment vérifier dans les versions 5.4 et antérieures
  - Vérification dans les versions 6.0 et ultérieures
- Étape 2 : Identifier un serveur de temps et son état
- Étape 3 : Vérifier la connectivité
- Étape 4 : Vérifier les fichiers de configuration

Introduction

Ce document décrit les problèmes courants de synchronisation temporelle sur les systèmes FireSIGHT et comment les résoudre.

Conditions préalables

Exigences

Pour configurer le paramètre de synchronisation horaire, vous devez disposer d'un niveau d'accès admin sur votre FireSIGHT Management Center.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

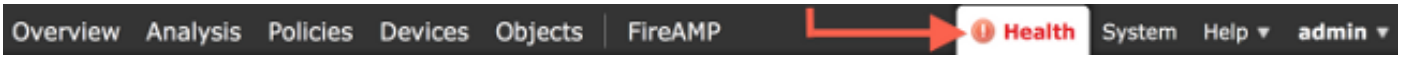
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

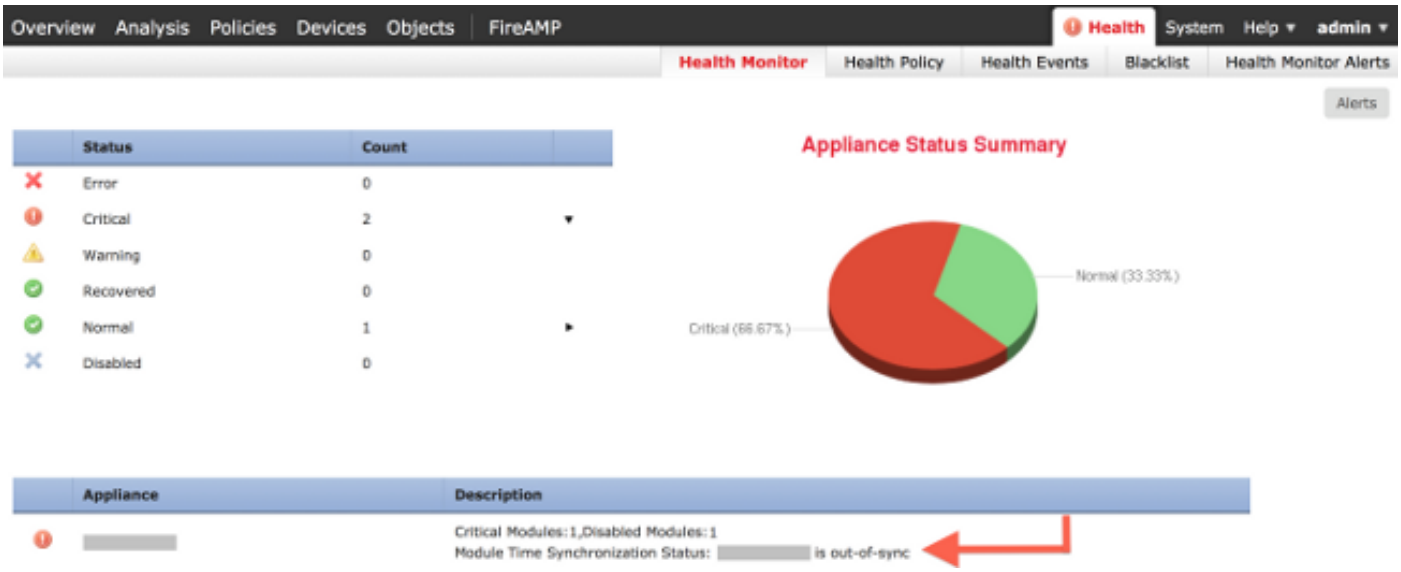
Vous pouvez choisir de synchroniser l'heure entre vos systèmes FireSIGHT de trois manières différentes, par exemple manuellement avec des serveurs NTP (Network Time Protocol) externes ou avec FireSIGHT Management Center qui fait office de serveur NTP. Vous pouvez configurer FireSIGHT Management Center en tant que serveur de temps avec NTP, puis l'utiliser pour synchroniser l'heure entre FireSIGHT Management Center et les périphériques gérés.

Symptômes

- FireSIGHT Management Center affiche des alertes d'intégrité sur l'interface du navigateur.



- La page Health Monitor indique qu'une appliance est critique, car l'état du module de synchronisation temporelle est désynchronisé.



- Vous pouvez voir des alertes d'intégrité intermittentes si les appliances ne parviennent pas à rester synchronisées.
- Après l'application d'une stratégie système, vous pouvez voir les alertes d'intégrité, car la synchronisation d'un FireSIGHT Management Center et de ses périphériques gérés peut prendre jusqu'à 20 minutes. En effet, FireSIGHT Management Center doit d'abord se synchroniser avec son serveur NTP configuré avant de pouvoir servir du temps à un périphérique géré.
- L'intervalle de temps entre FireSIGHT Management Center et un périphérique géré ne correspond pas.
- Les événements générés au niveau du capteur peuvent prendre des minutes ou des heures avant d'être visibles sur FireSIGHT Management Center.
- Si vous exécutez des appareils virtuels et que la page Health Monitor indique que la configuration de l'horloge de votre appareil virtuel n'est pas synchronisée, vérifiez les paramètres de synchronisation de l'heure de votre stratégie système. Cisco vous recommande de synchroniser vos appliances virtuelles avec un serveur NTP physique. Ne synchronisez pas vos périphériques gérés (virtuels ou physiques) avec un centre de défense virtuel.

Dépannage

Étape 1 : Vérification de la configuration NTP

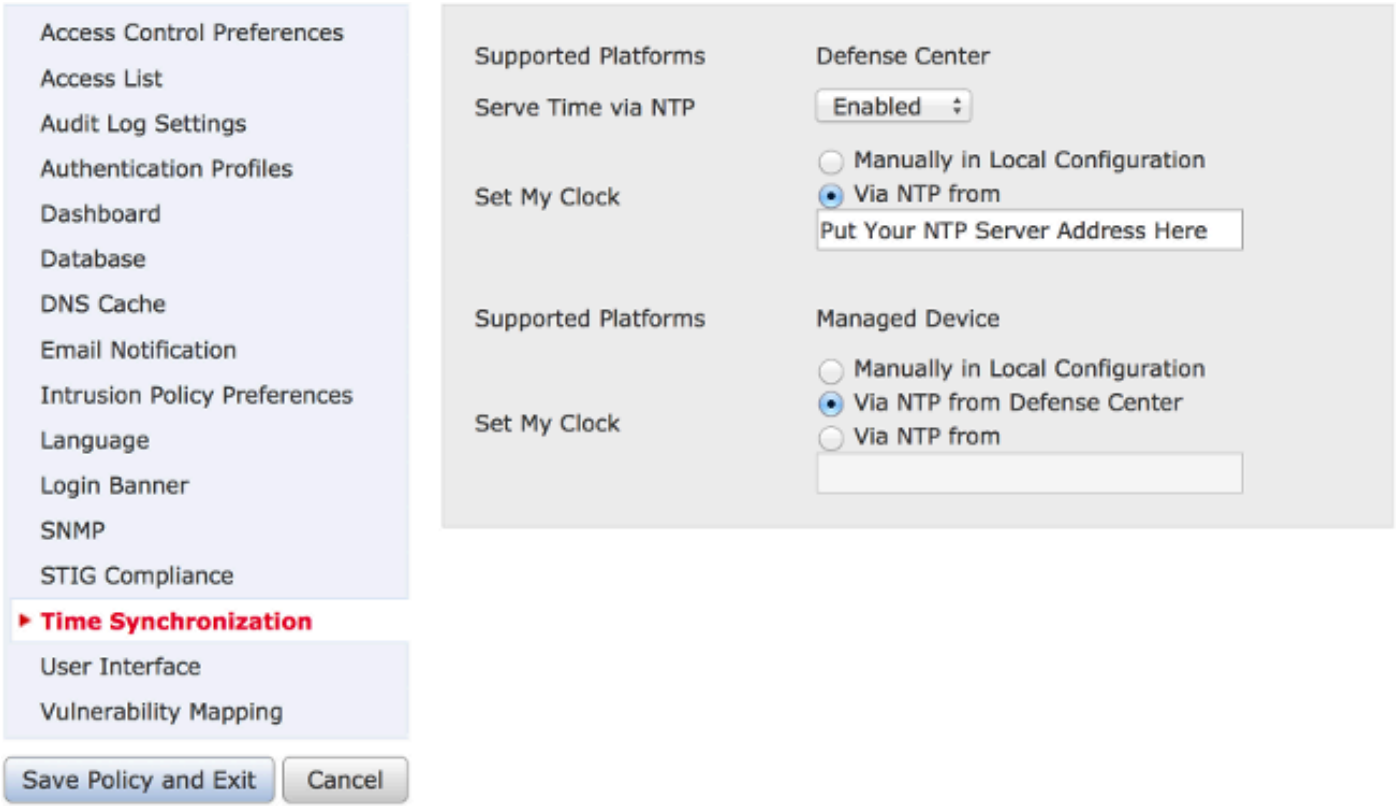
Comment vérifier dans les versions 5.4 et antérieures

Vérifiez que le protocole NTP est activé sur la stratégie système appliquée aux systèmes FireSIGHT. Afin de vérifier cela, complétez ces étapes :

1. Choisissez System > Local > System Policy.
2. Modifiez la stratégie système appliquée à vos systèmes FireSIGHT.
3. Sélectionnez Synchronisation temporelle.

Vérifiez si FireSIGHT Management Center (également appelé Defense Center ou DC) a l'horloge définie sur Via NTP from, et si une adresse d'un serveur NTP est fournie. Vérifiez également que le périphérique géré est défini sur via NTP à partir de Defense Center.

Si vous spécifiez un serveur NTP externe distant, votre appliance doit avoir un accès réseau à celui-ci. Ne spécifiez pas de serveur NTP non approuvé. Ne synchronisez pas vos périphériques gérés (virtuels ou physiques) avec un FireSIGHT Management Center virtuel. Cisco vous recommande de synchroniser vos appliances virtuelles avec un serveur NTP physique.



Vérification dans les versions 6.0 et ultérieures

Dans les versions 6.0.0 et ultérieures, les paramètres de synchronisation de l'heure sont

configurés à des emplacements distincts sur Firepower Management Center, bien qu'ils suivent la même logique que les étapes de la version 5.4.

Les paramètres de synchronisation de l'heure pour Firepower Management Center se trouvent sous System > Configuration > Time Synchronization.

Les paramètres de synchronisation de l'heure pour les périphériques gérés se trouvent sous Périphériques > Paramètres de la plate-forme. Cliquez sur edit en regard de la stratégie Platform Settings appliquée au périphérique, puis choisissez Time Synchronization.

Après avoir appliqué la configuration pour la synchronisation de l'heure (quelle que soit la version), assurez-vous que l'heure de votre Management Center et des périphériques gérés correspond. Dans le cas contraire, des conséquences imprévues peuvent se produire lorsque les périphériques gérés communiquent avec le Management Center.

Étape 2 : Identifier un serveur de temps et son état

- Afin de recueillir des informations sur la connexion à un serveur de temps, entrez cette commande sur votre FireSIGHT Management Center :
  <#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
  ```

  Un astérisque '*' sous la télécommande indique le serveur sur lequel vous êtes actuellement synchronisé. Si une entrée avec un astérisque n'est pas disponible, l'horloge n'est pas synchronisée avec sa source temporelle.

  Sur un périphérique géré, vous pouvez entrer cette commande sur le shell afin de déterminer l'adresse de votre serveur NTP :

  <#root>

  ```
  >
  ```

  show ntp

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

Remarque : Si un périphérique géré est configuré pour recevoir l'heure d'un FireSIGHT Management Center, le périphérique affiche une source de temps avec une adresse de bouclage, telle que 127.0.0.2. Cette adresse IP est une entrée sfipproxy et indique que le réseau virtuel de gestion est utilisé pour synchroniser l'heure.

- Si une appliance affiche qu'elle est synchronisée avec 127.127.1.1, elle indique que l'appliance est synchronisée avec sa propre horloge. Elle se produit lorsqu'un serveur de temps configuré sur une stratégie système n'est pas synchronisable. Exemple :
  <#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
```

- Dans la sortie de la commande ntpq, si vous remarquez que la valeur de st (strate) est 16, elle indique que le serveur de temps est inaccessible et que l'appliance ne peut pas se synchroniser avec ce serveur de temps.
- Dans le résultat de la commande ntpq, reach indique un nombre octal indiquant que la source a réussi ou échoué pour les huit tentatives d'interrogation les plus récentes. Si vous voyez la valeur 377, cela signifie que les 8 dernières tentatives ont réussi. Toute autre valeur peut indiquer qu'une ou plusieurs des huit dernières tentatives ont échoué.

Étape 3 : Vérifier la connectivité

1. Vérifiez la connectivité de base au serveur de temps.
   <#root>

```
admin@FireSIGHT:~$

ping
```

2. Assurez-vous que le port 123 est ouvert sur votre système FireSIGHT.
   <#root>

```
admin@FireSIGHT:~$

netstat -an | grep 123
```

3. Vérifiez que le port 123 est ouvert sur le pare-feu.

4. Vérifiez l'horloge matérielle :
   <#root>

   ```
   admin@FireSIGHT:~$

   sudo hwclock
   ```

   Si l'horloge matérielle est trop obsolète, elle ne pourra jamais se synchroniser correctement. Afin de forcer manuellement la configuration de l'horloge avec un serveur de temps, entrez cette commande :

   <#root>

   ```
   admin@FireSIGHT:~$

   sudo ntpdate -u
   ```

   Redémarrez ensuite ntpd:

   <#root>

   ```
   admin@FireSIGHT:~$

   sudo pmtool restartbyid ntpd
   ```

Étape 4 : Vérifier les fichiers de configuration

1. Vérifiez si le fichier sfipproxy.conf est correctement renseigné. Ce fichier envoie le trafic NTP sur le sftunnel.

   Un exemple du fichier /etc/sf/sfipproxy.conf sur un périphérique géré est montré ici :

   <#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;
            }
        }
    }
}
```

Un exemple du fichier /etc/sf/sfipproxy.conf sur un FireSIGHT Management Center est montré ici :

<#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. Assurez-vous que l'identificateur unique universel (UUID) sous la section homologues correspond au fichier ims.conf de l'homologue. Par exemple, l'UUID trouvé sous la section

pairs du fichier /etc/sf/sfipproxy.conf sur un FireSIGHT Management Center doit correspondre à l'UUID trouvé sur le fichier /etc/ims.conf de son périphérique géré. De même, l'UUID trouvé sous la section pairs du fichier /etc/sf/sfipproxy.conf sur un périphérique géré doit correspondre à l'UUID trouvé sur le fichier /etc/ims.conf de son appliance de gestion.

Vous pouvez récupérer l'UUID des périphériques avec cette commande :

```
<#root>

admin@FireSIGHT:~$

sudo grep UUID /etc/sf/ims.conf


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

Celles-ci doivent normalement être automatiquement remplies par la politique du système, mais il y a eu des cas où ces strophes ont été perdues. S'ils doivent être modifiés ou modifiés, vous devez redémarrer sfipproxy et sftunnel comme le montre cet exemple :

```
<#root>

admin@FireSIGHT:~$

sudo pmtool restartbyid sfipproxy

admin@FireSIGHT:~$

sudo pmtool restartbyid sftunnel
```

3. Vérifiez si un fichier ntp.conf est disponible dans le répertoire /etc.

```
<#root>

admin@FireSIGHT:~$

ls /etc/ntp.conf*
```

Si un fichier de configuration NTP n'est pas disponible, vous pouvez en faire une copie à partir du fichier de configuration de sauvegarde. Exemple :

```
<#root>

admin@FireSIGHT:~$

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

4. Vérifiez si le fichier /etc/ntp.conf est correctement renseigné. Lorsque vous appliquez une stratégie système, le fichier ntp.conf est réécrit.

> Remarque : Le résultat d'un fichier ntp.conf montre les paramètres du serveur de temps configurés sur une stratégie système. L'entrée d'horodatage doit indiquer l'heure à laquelle la dernière stratégie système a été appliquée à un périphérique. L'entrée du serveur doit afficher l'adresse du serveur de temps spécifiée.

<#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
```

Vérifiez les versions NTP sur deux périphériques et assurez-vous qu'elles sont identiques.

Pour plus d'informations sur les bases du protocole NTP, référez-vous à Meilleures pratiques d'utilisation du protocole NTP.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.