Dépannez les questions avec le Protocole NTP (Network Time Protocol) sur des systèmes de FirePOWER

Contenu

Introduction

Ce document décrit des problèmes courants avec la synchronisation horaire sur des systèmes de FireSIGHT et comment les dépanner. Vous pouvez choisir de synchroniser le temps entre vos systèmes de FireSIGHT de trois manières différentes, telles que manuellement avec les serveurs externes de Protocole NTP (Network Time Protocol), ou avec le centre de Gestion de FireSIGHT qui sert de serveur de NTP. Vous pouvez configurer un centre de Gestion de FireSIGHT comme un Serveur de synchronisation avec le NTP et puis l'employez pour synchroniser le temps entre le centre de Gestion de FireSIGHT et les périphériques gérés.

Conditions préalables

Conditions requises

Afin de configurer la configuration de synchronisation horaire, vous avez besoin du niveau d'accès d'`admin à` votre centre de Gestion de FireSIGHT.

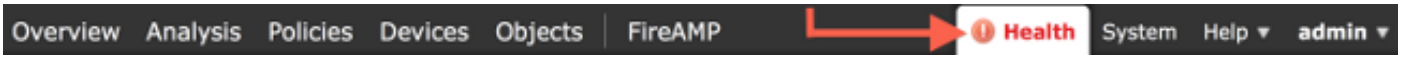
Composants utilisés

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

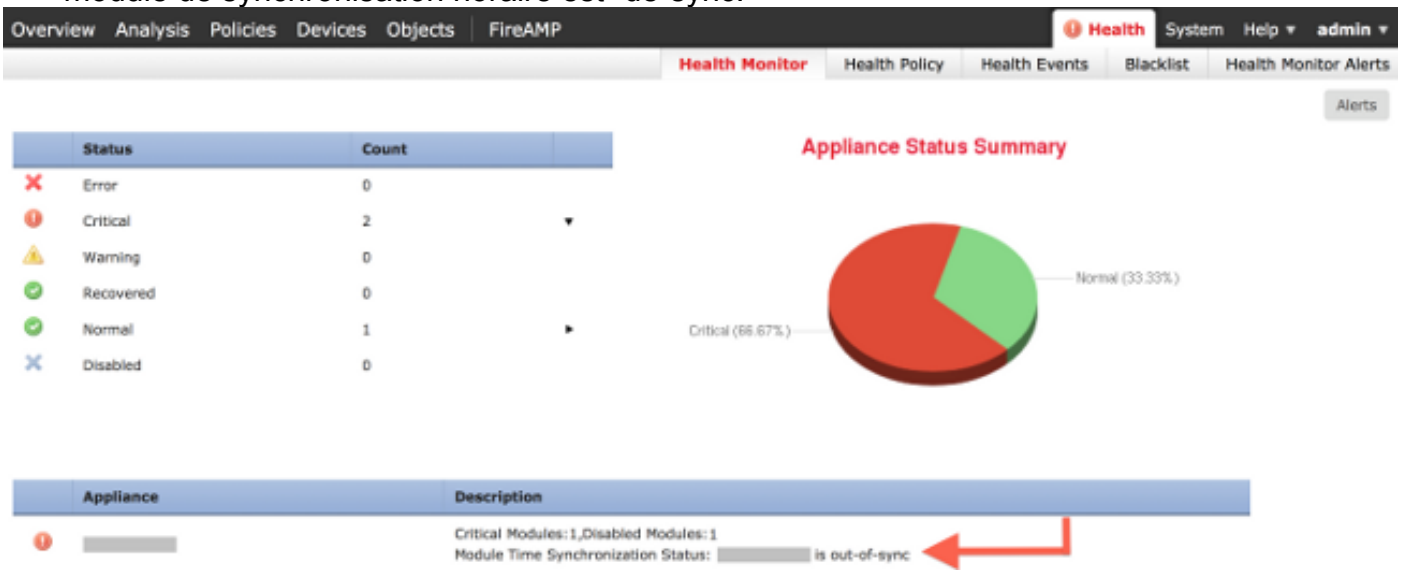
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Symptômes

- Le centre de Gestion de FireSIGHT affiche des alertes de santés sur l'interface web.



- La page de **moniteur de santés** affiche une appliance comme critial, parce que le statut de module de synchronisation horaire est -de-sync.



- Vous pourriez voir des alertes intermittentes de santés si les appliances ne restent pas synchronisées.
- Après qu'une stratégie de système soit appliquée vous pourriez voir des alertes de santés, parce qu'un centre de Gestion de FireSIGHT et ses périphériques gérés pourraient prendre à 20 minutes pour se terminer la synchronisation. C'est parce qu'un centre de Gestion de FireSIGHT doit d'abord synchroniser avec son serveur configuré de NTP avant qu'il puisse servir le temps à un périphérique géré.
- Le temps entre un centre de Gestion de FireSIGHT et un périphérique géré ne s'assortit pas.
- Les événements générés au capteur pourraient prendre des minutes ou des heures pour devenir visibles à un centre de Gestion de FireSIGHT.
- Si vous exécutez les appliances virtuelles et la page de **moniteur de santés** indique que l'installation d'horloge pour votre appliance virtuelle n'est pas synchronisée, vérifiez vos configurations de synchronisation horaire de stratégie de système. Cisco recommande que vous synchronisiez vos appliances virtuelles à un serveur physique de NTP. Ne synchronisez pas vos périphériques gérés (virtuels ou physiques) à un centre virtuel de la défense.

Dépannez

Étape 1 : Vérifiez la configuration de NTP

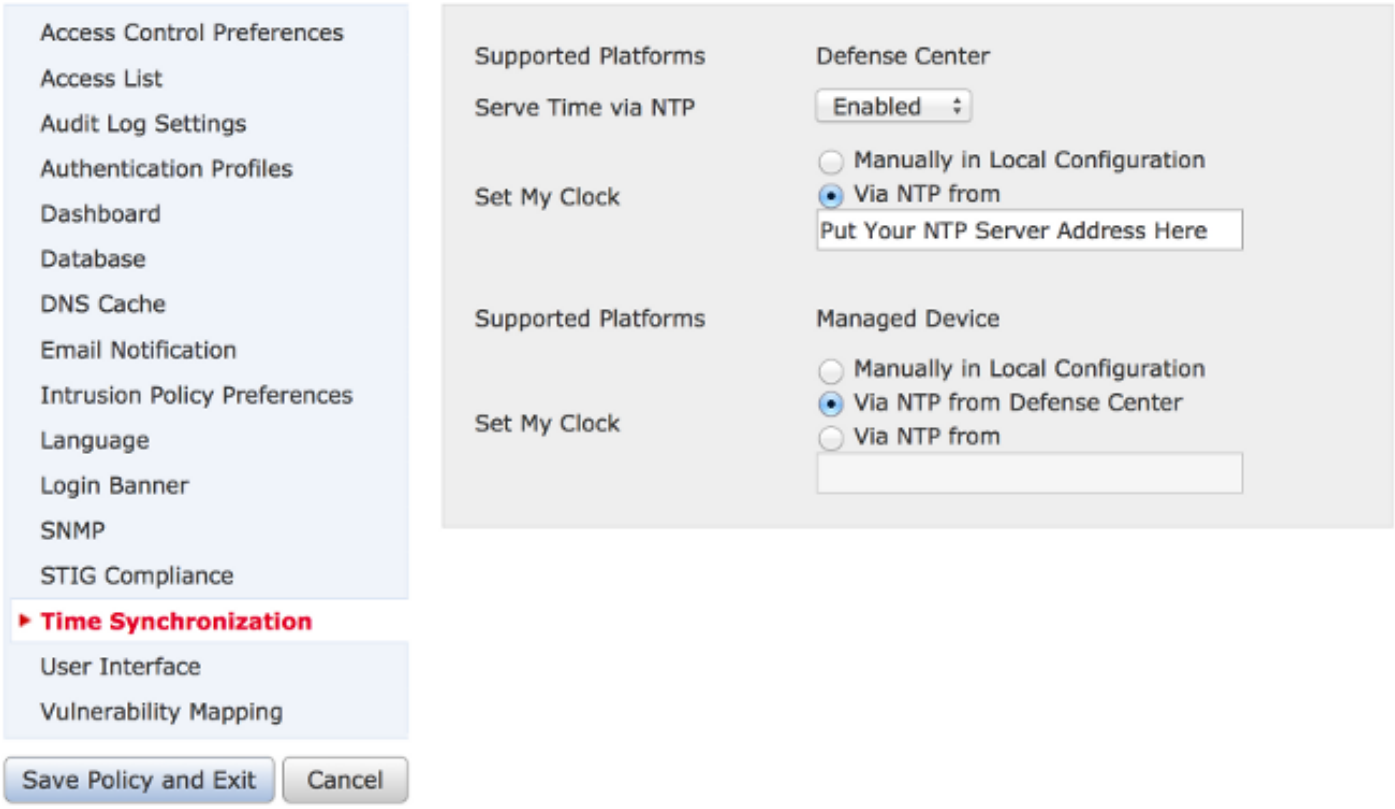
Comment vérifier dans les versions 5.4 et antérieures

Vérifiez que le NTP est activé sur la stratégie de système qui est appliquée sur les systèmes de FireSIGHT. Afin de vérifier cela, terminez-vous ces étapes :

1. Choisissez le **système > la stratégie de gens du pays > de système**.
2. Éditez la stratégie de système appliquée sur vos systèmes de FireSIGHT.
3. Choisissez la **synchronisation horaire**.

Vérifiez si le centre de Gestion de FireSIGHT (également connu sous le nom de centre de la défense ou C.C) a le clock set à **par l'intermédiaire du NTP de**, et une adresse d'un serveur de NTP est fournie. Confirmez également que le périphérique géré est placé à **par l'intermédiaire du NTP du centre de la défense**.

Si vous spécifiez un serveur externe distant de NTP, votre appliance doit avoir l'accès au réseau à elle. Ne spécifiez pas un serveur non approuvé de NTP. Ne synchronisez pas vos périphériques gérés (virtuels ou physiques) à un centre virtuel de Gestion de FireSIGHT. Cisco recommande que vous synchronisiez vos appliances virtuelles à un serveur physique de NTP.



Comment vérifier dans les versions 6.0 et ultérieures

Dans les versions 6.0.0 et ultérieures, les configurations de synchronisation horaire sont configurées dans les endroits distincts sur le centre de Gestion de FirePOWER, bien qu'elles suivent la même logique que les étapes pour 5.4.

Les configurations de synchronisation horaire pour le centre de Gestion de FirePOWER elle-même sont trouvées sous le **système > la configuration > la synchronisation horaire**.

Les configurations de synchronisation horaire pour les périphériques gérés sont trouvées sous des **périphériques > des configurations de plate-forme.** Cliquez sur **éditent** à côté des configurations de plate-forme la stratégie appliquée au périphérique et puis choisissent la **synchronisation horaire.**

Après que vous appliquiez la configuration pour la synchronisation horaire (indépendamment de la version), assurez-vous que le temps à votre centre de Gestion et correspondances de

périphériques gérés. Autrement, les conséquences involontaires pourraient se produire quand les périphériques gérés communiquent avec le centre de Gestion.

Étape 2 : Identifiez un serveur temporel et c'est état

- Afin de recueillir des informations au sujet de la connexion à un Serveur de synchronisation, sélectionnez cette commande à votre centre de Gestion de 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
  ```
  Un astérisque « * » sous le `distant` indique le serveur que vous êtes actuellement synchronisé à. Si une entrée avec un astérisque est indisponible, l'horloge n'est pas actuellement synchronisée avec elle est timesource.Sur un périphérique géré, vous pouvez sélectionner cette commande sur le shell afin de déterminer l'adresse de votre serveur de NTP :
  ```
  > show ntp

  NTP Server : 127.0.0.2 (Cannot Resolve)
  Status : Being Used
  Offset : -8.344 (milliseconds)
  Last Update : 188 (seconds)
  ```
  Note: Si un périphérique géré est configuré pour recevoir le temps d'un centre de Gestion de FireSIGHT, le périphérique affiche un timesource avec l'adresse de bouclage, telle que `127.0.0.2`. Cette adresse IP est une entrée de sfipproxy et indique que le réseau virtuel de Gestion est utilisé pour synchroniser le temps.
- Si affichages des appareils qu'ils des syncs avec `127.127.1.1`, il indiquent que les syncs d'appareils avec sa propre horloge. Il se produit quand un serveur temporel configuré sur une stratégie de système n'est pas synchronizable. Exemple :
  ```
  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
  ```
- Sur la sortie de commande de `ntpq`, si vous notez la valeur de `St` (strate) est 16, il indique que le serveur temporel est inaccessible et l'appliance ne peut pas sychronize avec ce serveur temporel.
- Sur la sortie de commande de `ntpq`, la `portée` affiche un nombre octal qui indique le succès ou échec pour atteindre la source pour les huit tentatives de vote les plus récentes. Si vous voyez la valeur est 377, il signifie que les 8 dernières tentatives étaient réussies. Toutes les autres valeurs pourraient indiquer qu'un ou plusieurs des huit dernières tentatives étaient infructueuses.

Étape 3 : Vérifiez la Connectivité

1. Vérifiez la Connectivité de base au Serveur de synchronisation.
   ```
   admin@FireSIGHT:~$ ping <IP_addres_of_NTP_server>
   ```
2. Assurez-vous que le port 123 est ouvert sur votre système de FireSIGHT.
   ```
   admin@FireSIGHT:~$ netstat -an | grep 123
   ```
3. Confirmez que le port 123 est ouvert sur le Pare-feu.

4. Vérifiez l'horloge de matériel :
```
admin@FireSIGHT:~$ sudo hwclock
```

   Si l'horloge de matériel est périmée trop lointain, ils pourraient jamais avec succès sync. Afin de forcer manuellement l'horloge à placer avec un Serveur de synchronisation, sélectionnez cette commande :

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

   Puis `ntpd de` reprise :

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

Étape 4 : Vérifiez les fichiers de configuration

1. Vérifiez si le `fichier sfipproxy.conf` est rempli correctement. Ce fichier envoie le trafic de NTP au-dessus du sftunnel.
   Un exemple du fichier de `/etc/sf/sfipproxy.conf` sur un périphérique géré est affiché ici :

```
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 de `/etc/sf/sfipproxy.conf à un` centre de Gestion de FireSIGHT est affiché ici :

```
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 qu'universellement l'identifiant unique (UUID) sous les correspondances de section de `pairs` avec le `fichier ims.conf le` pair. Par exemple, l'UUID trouvé sous le peerssection du `fichier de` /etc/sf/sfipproxy.conf à un centre de Gestion de FireSIGHT devrait s'assortir avec l'UUID trouvé sur le `fichier de` /etc/ims.conf de son périphérique géré. De même, l'UUID trouvé sous le peerssection du `fichier de` /etc/sf/sfipproxy.conf sur un périphérique géré devrait s'assortir avec l'UUID trouvé sur le `fichier de` /etc/ims.conf de son appliance de Gestion. Vous pouvez récupérer l'UUID des périphériques avec cette commande :

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

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

   Ceux-ci devraient normalement être automatiquement remplis par la stratégie de système, mais il y a eu des cas où ces strophes manquaient. S'ils doivent être modifiés ou changés vous devrez redémarrer le sfipproxy et le sftunnel comme suit :

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

3. Vérifiez si un `fichier ntp.conf` est disponible sur le `répertoire de` /etc.

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

   Si un fichier de configuration de NTP est indisponible, vous pouvez tirer une copie à partir du fichier de configuration de sauvegarde. Exemple :

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

4. Vérifiez si le fichier de `/etc/ntp.conf` est rempli correctement. Quand vous appliquez une stratégie de système, le `fichier ntp.conf` est réécrit. **Note**: La sortie d'un `fichier ntp.conf` affiche les configurations de serveur temporel configurées sur une stratégie de système. L'entrée de groupe date/heure devrait afficher le moment où la dernière stratégie de système a appliqué à un périphérique. L'entrée de serveur affichez l'adresse spécifiée de serveur temporel.

```
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
```