Risoluzione dei problemi con Network Time Protocol (NTP) sui sistemi FireSIGHT

Sommario

Introduzione

Questo documento descrive i problemi comuni relativi alla sincronizzazione dell'ora sui sistemi FireSIGHT e come risolverli.

Prerequisiti

Requisiti

Per configurare l'impostazione di sincronizzazione dell'ora, è necessario il livello di accesso amministrativo sul centro di gestione FireSIGHT.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

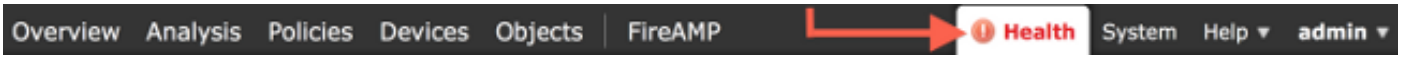
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

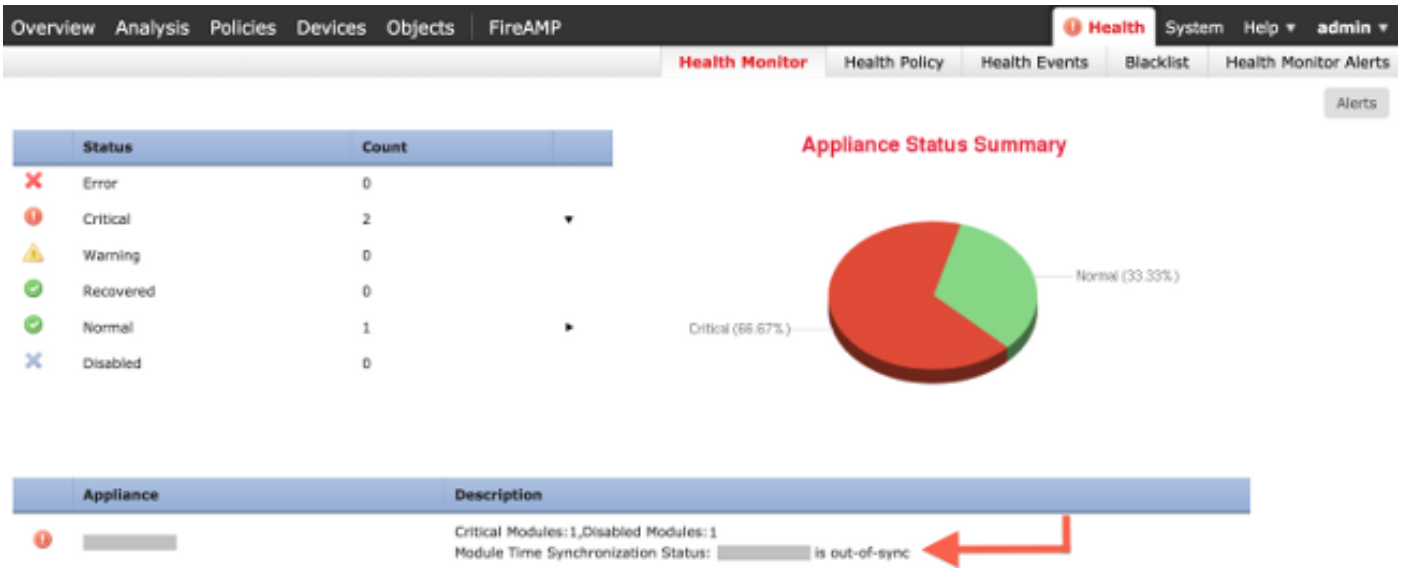
È possibile scegliere di sincronizzare l'ora tra i sistemi FireSIGHT in tre modi diversi, ad esempio manualmente con i server NTP (Network Time Protocol) esterni o con FireSIGHT Management Center che funge da server NTP. È possibile configurare un centro di gestione FireSIGHT come server di riferimento orario con NTP e quindi utilizzarlo per sincronizzare l'ora tra il centro di gestione FireSIGHT e i dispositivi gestiti.

Sintomi

- FireSIGHT Management Center visualizza avvisi di stato sull'interfaccia del browser.



- Nella pagina Health Monitor un accessorio viene visualizzato come critico, in quanto lo stato del modulo di sincronizzazione dell'ora non è sincronizzato.



- Gli avvisi intermittenti sullo stato di salute possono essere visualizzati se gli accessori non sono sincronizzati.
- Dopo l'applicazione di un criterio di sistema è possibile visualizzare gli avvisi di integrità, in quanto la sincronizzazione di un centro di gestione FireSIGHT e dei relativi dispositivi gestiti potrebbe richiedere fino a 20 minuti. Infatti un centro di gestione FireSIGHT deve prima sincronizzarsi con il proprio server NTP configurato prima di poter passare del tempo a un dispositivo gestito.
- Il tempo tra un centro di gestione FireSIGHT e un dispositivo gestito non corrisponde.
- Gli eventi generati al sensore possono impiegare minuti o ore per essere visibili su un centro di gestione FireSIGHT.
- Se si eseguono appliance virtuali e la pagina Health Monitor indica che la configurazione dell'orologio per l'appliance virtuale non è sincronizzata, verificare le impostazioni di sincronizzazione dell'ora dei criteri di sistema. Cisco consiglia di sincronizzare le appliance virtuali con un server NTP fisico. Non sincronizzare i dispositivi gestiti (virtuali o fisici) con un centro di difesa virtuale.

Risoluzione dei problemi

Passaggio 1: Verificare la configurazione NTP

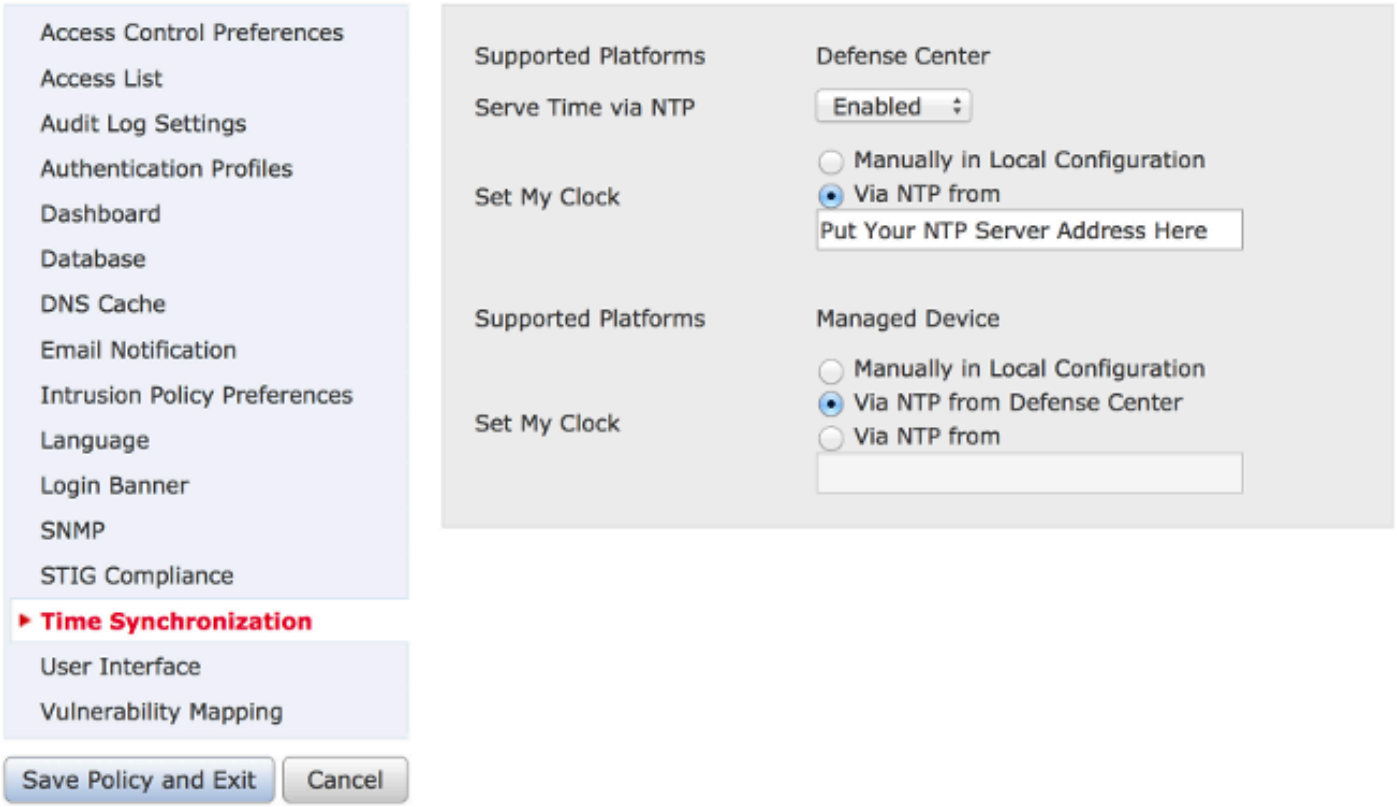
Verifica nelle versioni 5.4 e precedenti

Verificare che NTP sia abilitato sui criteri di sistema applicati ai sistemi FireSIGHT. Per verificarlo, attenersi alla seguente procedura:

1. Scegliete Sistema > Locale > Criteri di sistema.
2. Modificare i criteri di sistema applicati ai sistemi FireSIGHT.
3. Scegliere Sincronizzazione ora.

Verificare che nel centro di gestione FireSIGHT (noto anche come centro di difesa o DC) l'orologio sia impostato su Via NTP da e che sia fornito l'indirizzo di un server NTP. Verificare inoltre che il dispositivo gestito sia impostato su tramite NTP da Defense Center.

Se si specifica un server NTP esterno remoto, è necessario che l'accessorio disponga dell'accesso di rete. Non specificare un server NTP non attendibile. Non sincronizzare i dispositivi gestiti (virtuali o fisici) con un Virtual FireSIGHT Management Center. Cisco consiglia di sincronizzare le appliance virtuali con un server NTP fisico.



Verifica nelle versioni 6.0 e successive

Nelle versioni 6.0.0 e successive, le impostazioni di sincronizzazione dell'ora vengono configurate

in posizioni separate in Firepower Management Center, sebbene riescano a tracciare la stessa logica dei passaggi per 5.4.

Le impostazioni di sincronizzazione dell'ora per Firepower Management Center sono disponibili in Sistema > Configurazione > Sincronizzazione dell'ora.

Le impostazioni di sincronizzazione dell'ora per i dispositivi gestiti si trovano in Dispositivi > Impostazioni piattaforma. Fare clic su edit (Modifica) accanto al criterio Platform Settings (Impostazioni piattaforma) applicato al dispositivo, quindi selezionare Time Synchronization (Sincronizzazione ora).

Dopo aver applicato la configurazione per la sincronizzazione dell'ora (indipendentemente dalla versione), verificare che l'ora nel centro di gestione e nei dispositivi gestiti corrisponda. In caso contrario, potrebbero verificarsi conseguenze non intenzionali quando i dispositivi gestiti comunicano con il Centro di gestione.

Passaggio 2: Identificare un server di controllo tempi e il relativo stato

- Per raccogliere informazioni sulla connessione a un time server, immettere questo comando sul centro di gestione FireSIGHT:
  <#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 asterisco '*' sotto il telecomando indica il server a cui si è attualmente sincronizzati. Se non è disponibile una voce con un asterisco, l'orologio non è sincronizzato con la relativa origine tempo.

  Su un dispositivo gestito, è possibile immettere questo comando sulla shell per determinare l'indirizzo del server NTP:

  <#root>

  ```
  >
  ```

  show ntp

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

Nota: se un dispositivo gestito è configurato per la ricezione di tempo da un centro di gestione FireSIGHT, il dispositivo mostra una risorsa tempo con indirizzo di loopback, ad esempio 127.0.0.2. Questo indirizzo IP è una voce sfipproxy e indica che la rete virtuale di gestione viene utilizzata per sincronizzare l'ora.

- Se un accessorio visualizza la sincronizzazione con 127.127.1.1, significa che l'accessorio esegue la sincronizzazione con il proprio orologio. Si verifica quando un server di controllo tempi configurato in un criterio di sistema non è sincronizzabile. Ad esempio:
  <#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
```

- Nell'output del comando ntpq, se il valore di st (stratum) è 16, il server di riferimento orario non è raggiungibile e l'accessorio non è in grado di eseguire la sincronizzazione con il server di riferimento orario.
- Nell'output del comando ntpq, il comando reach mostra un numero ottale che indica se è riuscito o meno a raggiungere l'origine per gli ultimi otto tentativi di polling. Se viene visualizzato il valore 377, significa che gli ultimi 8 tentativi hanno avuto esito positivo. Qualsiasi altro valore può indicare che uno o più degli ultimi otto tentativi non sono riusciti.

Passaggio 3: Verifica della connettività

1. Verificare la connettività di base al server di riferimento ora.
   <#root>

   admin@FireSIGHT:~$

   ping

2. Verificare che la porta 123 sia aperta sul sistema FireSIGHT.
   <#root>

   admin@FireSIGHT:~$

   netstat -an | grep 123

3. Verificare che la porta 123 sia aperta sul firewall.
4. Controllare l'orologio dell'hardware:
   <#root>

   admin@FireSIGHT:~$

   sudo hwclock

   Se l'orologio dell'hardware è troppo obsoleto, la sincronizzazione non verrà mai eseguita correttamente. Per imporre manualmente l'impostazione dell'orologio con un server di riferimento orario, immettere questo comando:

   <#root>

   admin@FireSIGHT:~$

   sudo ntpdate -u

   Quindi riavvia ntpd:

   <#root>

   admin@FireSIGHT:~$

   sudo pmtool restartbyid ntpd

Passaggio 4: Verifica dei file di configurazione

1. Verificare che il file sfipproxy.conf sia compilato correttamente. Questo file invia traffico NTP sul tunnel sfaccettatura.

   Di seguito è riportato un esempio del file /etc/sf/sfipproxy.conf su un dispositivo gestito:

   <#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;
            }
        }
    }
}
```

Di seguito è riportato un esempio del file /etc/sf/sfipproxy.conf su un centro di gestione FireSIGHT:

<#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. Verificare che l'UUID (Universally Unique Identifier) nella sezione peer corrisponda al file ims.conf del peer. Ad esempio, l'UUID trovato nella sezione peer del file /etc/sf/sfipproxy.conf su un centro di gestione FireSIGHT deve corrispondere all'UUID trovato nel file /etc/ims.conf del dispositivo gestito. Analogamente, l'UUID individuato nella sezione peer del file /etc/sf/sfipproxy.conf su un dispositivo gestito deve corrispondere all'UUID individuato nel file /etc/ims.conf dell'accessorio di gestione.

   Per recuperare l'UUID dei dispositivi, usare questo comando:

   <#root>

   admin@FireSIGHT:~$

   sudo grep UUID /etc/sf/ims.conf

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

   Di solito queste stanze devono essere automaticamente popolate dalla politica del sistema, ma ci sono stati casi in cui queste stanze sono state perse. Se è necessario modificare o cambiare le porte, riavviare sfipproxy e sftunnel come mostrato nell'esempio:

   <#root>

   admin@FireSIGHT:~$

   sudo pmtool restartbyid sfipproxy

   admin@FireSIGHT:~$

   sudo pmtool restartbyid sftunnel

3. Verificare se un file ntp.conf è disponibile nella directory /etc.
   <#root>

   admin@FireSIGHT:~$

   ls /etc/ntp.conf*

   Se un file di configurazione NTP non è disponibile, è possibile crearne una copia dal file di configurazione di backup. Ad esempio:

   <#root>

   admin@FireSIGHT:~$

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

4. Verificare che il file /etc/ntp.conf sia compilato correttamente. Quando si applica un criterio di sistema, il file ntp.conf viene riscritto.

> Nota: l'output di un file ntp.conf mostra le impostazioni del server di riferimento orario configurate in un criterio di sistema. La voce relativa al timestamp deve indicare l'ora in cui l'ultimo criterio di sistema è stato applicato a un dispositivo. La voce server deve contenere l'indirizzo del server di riferimento orario specificato.

<#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
```

Verificare le versioni NTP su due dispositivi e assicurarsi che corrispondano.

Per ulteriori informazioni sulle nozioni di base dell'NTP, fare riferimento a Utilizzare le best practice per il protocollo NTP.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).