Cyber Vision CenterでのNTP同期&更新設定のトラブルシューティング

内容

はじめに

このドキュメントでは、NTP設定の検証、NTPサービスの変更とトラブルシューティングの方法について説明します。これは、Cyber Vision Center 2.x、3.x、4.xソフトウェアトレインに適用されます。

NTPサーバピアリングを検証する手順

ntpq -c peer <ピアデバイスIP>

ピアリングを使用すると、センターはネットワーク内のルータやゲートウェイなどのピアデバイスから時刻を取得します。

NTPクライアントのアソシエーション

NTPアソシエーションは、各NTPサーバへのクライアントアソシエーションのステータスを示します。

ntpq -c associations <時刻が同期されているデバイス>

出力例：

```
root@center:~# ntpq -c associations 169.254.0.10
ind assid status  conf reach auth condition  last_event cnt
===========================================================
  1 48380  961a   yes   yes  none  sys.peer    sys_peer  1
root@center:~#
```

例：名前解決の失敗を示す問題

```
***Can't find host peer

server (local      remote           refid      st t when poll reach   delay   offset  jitter

==============================================================================
localhost.lo *LOCAL(0)        .LOCL.          10 l    -   64  377    0.000    0.000   0.000
```

現在の日付を確認する

```
cv-admin@Center:~$ date

Tue Jul 11 18:01:05 UTC 2023
```

NTPデーモンのステータスを確認します。

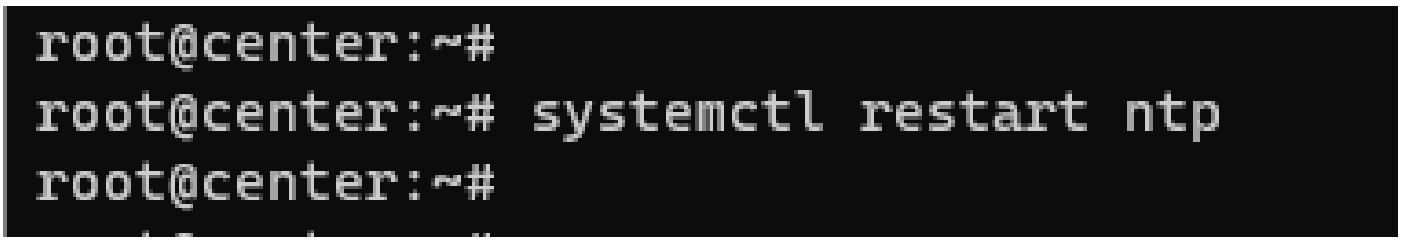
systemctlステータスntp

```
● ntp.service - Network time service
     Loaded: loaded (/lib/systemd/system/ntp.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2023-07-11 16:51:49 UTC; 1h 9min ago
   Main PID: 1120 (lxc-start)
      Tasks: 3 (limit: 77132)
     Memory: 4.0M
     CGroup: /system.slice/ntp.service
             ├─lxc.monitor.ntpd
             │ └─1120 /usr/bin/lxc-start -F -n ntpd
             └─lxc.payload.ntpd
               └─1171 /usr/sbin/ntpd -c /data/etc/ntp.conf -p /run/ntpd.pid -g -n -u ntp -I ntpd-nic
```

NTP設定の変更

```
sbs-timeconf -h to learn about the commands to tune NTP on the center.
sbs-timeconf -s with IP or hostname.
```

変更が完了したら、次のコマンドを使用してntpサービスを再起動します。



NTP設定の検証

cat /data/etc/ntp.conf

NTPモード6の脆弱性

この問題を解決するには、2つの方法があります。

オプション#1：アクセスリストの使用

1. このルールを使用して、/data/etcの下にrc.localファイルを作成します (導入に1つのインターフェイス実装がある場合はeth0のみ、またはデュアルインターフェイスの場合はeth1でのみ) 。次にルールの例を示します。

```
iptables -I FORWARD -i eth0 -o brntpd -p udp -m udp --dport 123 -j DROP

iptables -I FORWARD -i eth0 -o brntpd -p udp -m udp -s X.X.X.X -d 169.254.0.10 --dport 123 -j ACCEPT
```

上記のコマンドで、X.X.X.Xは認可されたNTPサーバのIPアドレスです。複数のNTPサーバがある場合は、ソリューションで使用される各承認済みNTPサーバのAcceptルールを追加できます。

2. センターを再起動する

オプション#2:ntp.confファイルから

1. /data/etc/ntp.confファイルで、次の2行を既存の設定に追加します

```
restrict default kod nomodify notrap nopeer noquery

restrict -6 default kod nomodify notrap nopeer noquery
```

2-「systemctl restart ntp」コマンドを使用してntpサービスを再起動します。

両方のオプションを組み合わせて、NTPセキュリティを向上させることもできます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。