Cyber Vision Center에서 NTP 동기화 & 업데이트 컨피그레이션 문제 해결

목차

소개

이 문서에서는 NTP 컨피그레이션의 유효성을 검사하고 NTP 서비스를 변경 및 트러블슈팅하는 방법에 대해 설명합니다. Cyber Vision Center 2.x, 3.x, 4.x 소프트웨어 트레인에도 적용됩니다.

NTP 서버 피어링 확인 단계

ntpq -c peer <peer device IP>

피어링(peering)을 통해, 센터는 네트워크의 라우터 또는 게이트웨이와 같은 피어 디바이스에서 시간을 빼앗습니다.

NTP 클라이언트 연결

NTP 연결은 각 NTP 서버에 대한 클라이언트 연결의 상태를 표시합니다.

ntpq -c 연결 <시간이 동기화되는 디바이스>

샘플 출력:

```
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:~#
```

예: 이름 확인에 실패했음을 나타내는 문제

```
***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
```

현재 날짜 확인

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

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

NTP 데몬 상태 확인

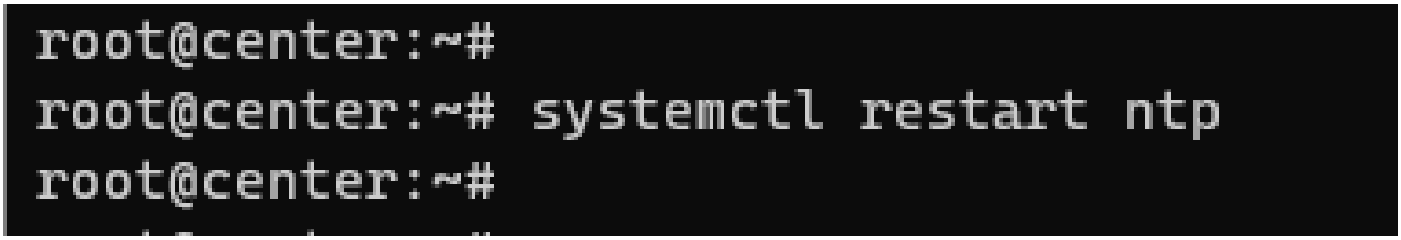
시스템tl 상태 ntp

```
● 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 컨피그레이션 변경

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

변경 후 다음 명령을 사용하여 ntp 서비스를 다시 시작합니다.



NTP 컨피그레이션 확인

고양이 /data/etc/ntp.conf

NTP 모드 6 취약성

이를 해결하기 위한 두 가지 옵션이 있습니다.

옵션 #1: 액세스 목록 사용

1. /data/etc 아래에 이 규칙을 사용하여 rc.local 파일을 만듭니다(구축에 단일 인터페이스 구현이 있는 경우 eth0에, 또는 이중 인터페이스의 경우 eth1에). 아래의 샘플 규칙:

```
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
```

위의 명령에서 X.X.X.X는 인증된 NTP 서버의 IP 주소입니다. 여러 NTP 서버가 있는 경우 솔루션에 사용된 각 인증된 NTP 서버에 대해 Accept 규칙을 추가할 수 있습니다.

2. 센터 재부팅

옵션 #2: ntp.conf 파일에서

1. /data/etc/ntp.conf 파일에서 이 두 행을 기존 컨피그레이션에 추가합니다

```
restrict default kod nomodify notrap nopeer noquery

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

2 - "systemctl restart ntp" 명령을 사용하여 ntp 서비스를 재시작합니다.

두 옵션 모두 더 우수한 NTP 보안을 위해 결합할 수 있습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.