Troubleshoot NTP synchronization & update configuration on Cyber Vision Center

Contents

Introduction

This document describes how to validate NTP configuration, change & troubleshoot the NTP service. Its applicable for Cyber Vision Center 2.x, 3.x, 4.x software trains.

Steps to Validate NTP server peering

ntpq -c peer <peer device IP>

With peering, the center gets its time off a peer device like a router or a Gateway in the network.

NTP client association

The NTP association shows the status of the client associations to each NTP server.

ntpq -c associations <device where the time is synchronized>

Sample output:

```
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:~#
```

Example: Issue showing failure with name resolution

```
***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
```

Check the current date

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

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

Check NTP daemon status

systemctl status 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
```

Change NTP configuration

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

After the changes, restart the ntp service with the following command:

```
root@center:~#
root@center:~# systemctl restart ntp
root@center:~#
```

Validate NTP configuration

cat /data/etc/ntp.conf

NTP mode 6 Vulnerability

There are two options to resolve this.

Option #1: Use of Access Lists

1. Create rc.local file under /data/etc with this rule (only on eth0 if the deployment has a single interface implementation or in eth1 for dual interface). Sample rules below:

```
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
```

On the command above, X.X.X.X is the IP address of your authorized NTP server. If you have multiple NTP servers, you can add Accept rules for each authorized NTP server used in the solution.

2. Reboot your center

Option #2: From the ntp.conf file

1. On the /data/etc/ntp.conf file add these two lines to the existing config

```
restrict default kod nomodify notrap nopeer noquery

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

2- Restart the ntp service using the command â€œsystemctl restart ntpâ€�

Both options can be combined for better NTP security as well.