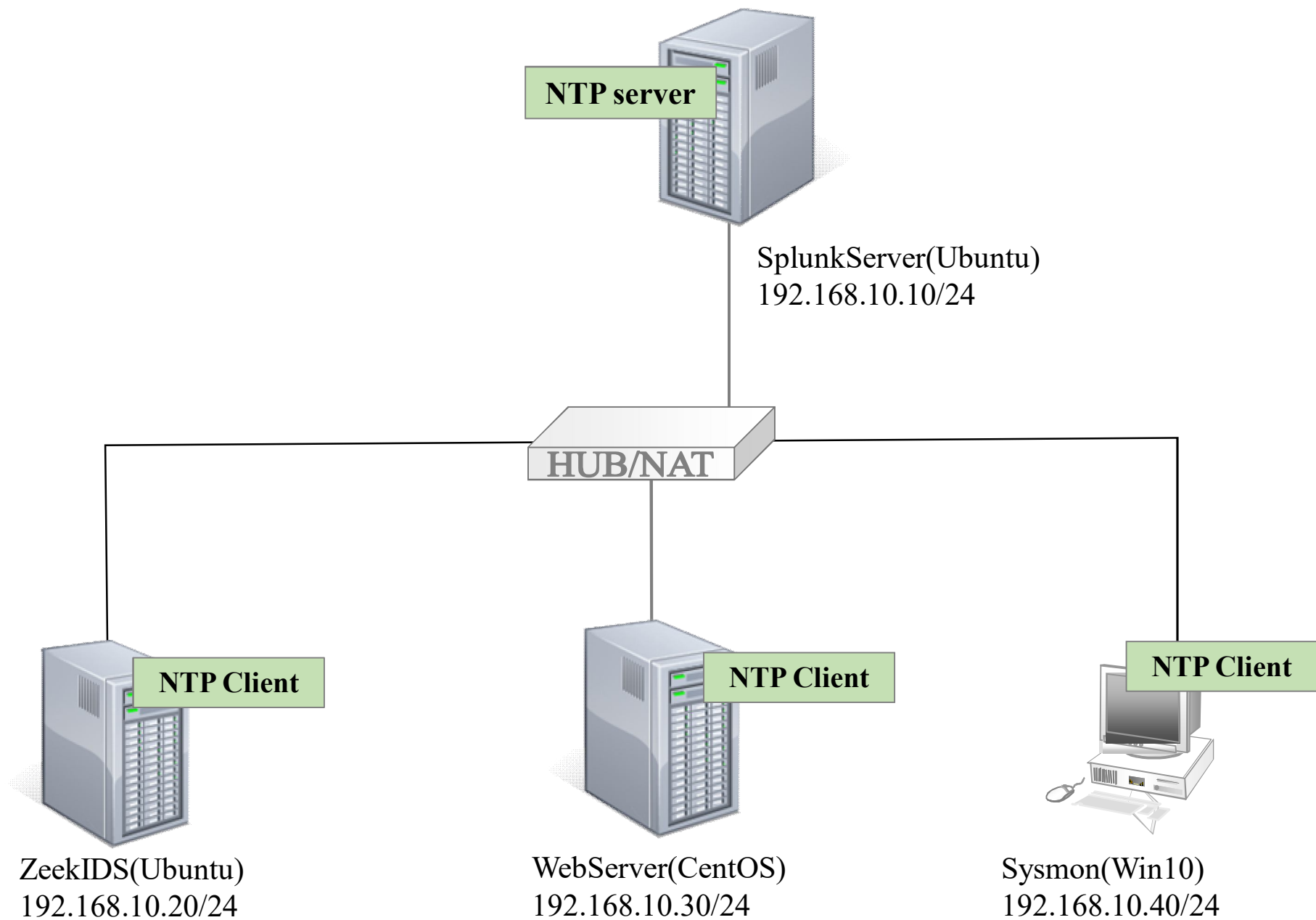


# **NTP Installation**

- 1) [Ubuntu-SplunkServer] NTP Server Installation
- 2) [Ubuntu-ZeepIDS] NTP Client Installation
- 3) [CentOS] NTP Client Installation
- 4) [Win10 ] NTP Client Installation



# NTP(Network Time Protocol)

- 시간 동기화 서비스를 제공하는 프로토콜
- UDP 123 번호
- NTP 서버들에 대한 정보를 제공(<https://www.ntppool.org>)

## << 시간 동기화 목적 >>

- ❶ 백업이나 패치등 예약한 작업들이 실행되지 않는 것을 방지
- ❷ 로그에 대한 신뢰도
  - 언제 어떤 작업을 했는지 보여주는 로그의 시간은 정확해야 함
- ❸ 보안. 암호화 인증 프로토콜 과정 시 timestamp 및 lifetime이 추가
  - 이때 서버와 클라이언트의 시간과 일치하지 않으면, 서비스에 접근을 차단

## 1) [Ubuntu-SplunkServer] NTP Server Installation

### ❶ 리포지토리 인덱스 업데이트와 NTP 서버 설치

```
#apt update
```

```
#apt-get install -y ntp
```

```
#sntp --version
```

```
root@splunk-server:~# sntp --version  
sntp 4.2.8p12@1.3728-o (1)  
root@splunk-server:~#
```

## ② 가장 가까운 NTP server pool로 전환

<http://pool.ntp.org/zone/kr>

← → ↻ pool.ntp.org/zone/kr

👤+ JOIN THE POOL 👤 USE THE POOL ⚙️ MANAGE SERVERS

# Korea — kr.pool.ntp.org

We need more servers in this country. If you have a server with a static IP, please consider joining the pool.

To use this specific pool zone, add the following to your ntp.conf file:

```
server 1.kr.pool.ntp.org
server 2.asia.pool.ntp.org
server 3.asia.pool.ntp.org
```

In most cases it's best to use **pool.ntp.org** to find an NTP server (or 0.pool.ntp.org, 1.pool.ntp.org, or 2.pool.ntp.org for specific server names). The system will try finding the closest available servers for you. If you do not use NTP, please see our [information for vendors](#).

pool.ntp.org 이름들은 매 시간마다 변하면서 임의의 서버들을 지정

#nano /etc/ntp.conf

각 서버마다 network이나 기타 이유로 poll은 달라짐

```
GNU nano 4.8 /etc/ntp.conf
# Enable this if you want statistics to be logged.
#statsdir /var/log/ntpstats/

statistics loopstats peerstats clockstats
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable

# Specify one or more NTP servers.

# Use servers from the NTP Pool Project. Approved by Ubuntu Technical Board
# on 2011-02-08 (LP: #104525). See http://www.pool.ntp.org/join.html for
# more information.
pool 0.ubuntu.pool.ntp.org iburst
pool 1.ubuntu.pool.ntp.org iburst
pool 2.ubuntu.pool.ntp.org iburst
pool 3.ubuntu.pool.ntp.org iburst

# Use Ubuntu's ntp server as a fallback.
pool ntp.ubuntu.com
```

server 1.kr.pool.ntp.org iburst  
server 2.asia.pool.ntp.org iburst  
server 3.asia.pool.ntp.org iburst

<<ntp 서버 주소 지정>>

```
GNU nano 4.8
# Specify one or more NTP servers.

# Use servers from the NTP Pool Project. App
# on 2011-02-08 (LP: #104525). See http://w
# more information.
#pool 0.ubuntu.pool.ntp.org iburst
#pool 1.ubuntu.pool.ntp.org iburst
#pool 2.ubuntu.pool.ntp.org iburst
#pool 3.ubuntu.pool.ntp.org iburst

server 1.kr.pool.ntp.org iburst
server 2.asia.pool.ntp.org iburst
server 3.asia.pool.ntp.org iburst
```



### ③ NTP 서버 재시작과 실행상태 확인

#service ntp restart

#service ntp status

```
root@splunk-server:/# nano /etc/ntp.conf
root@splunk-server:/# service ntp restart
root@splunk-server:/# service ntp status
● ntp.service - Network Time Service
   Loaded: loaded (/lib/systemd/system/ntp.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2022-08-06 22:45:26 KST; 10s ago
     Docs: man:ntpd(8)
  Process: 4025 ExecStart=/usr/lib/ntp/ntp-systemd-wrapper (code=exited, status=0/SUCCESS)
 Main PID: 4033 (ntpd)
    Tasks: 2 (limit: 9420)
   Memory: 852.0K
    CGroup: /system.slice/ntp.service
            └─4033 /usr/sbin/ntpd -p /var/run/ntpd.pid -g -u 126:133

8월 06 22:45:26 splunk-server ntpd[4033]: Listen normally on 5 ens33 [fe80::486c:cdfe:ff65:8b80%2]:123
8월 06 22:45:26 splunk-server ntpd[4033]: Listening on routing socket on fd #22 for interface updates
8월 06 22:45:26 splunk-server ntpd[4033]: kernel reports TIME_ERROR: 0x2041: Clock Unsynchronized
8월 06 22:45:26 splunk-server ntpd[4033]: kernel reports TIME_ERROR: 0x2041: Clock Unsynchronized
8월 06 22:45:28 splunk-server ntpd[4033]: Soliciting pool server 185.125.190.56
8월 06 22:45:29 splunk-server ntpd[4033]: Soliciting pool server 185.125.190.58
8월 06 22:45:30 splunk-server ntpd[4033]: Soliciting pool server 185.125.190.57
8월 06 22:45:31 splunk-server ntpd[4033]: Soliciting pool server 91.189.94.4
8월 06 22:45:32 splunk-server ntpd[4033]: Soliciting pool server 91.189.91.157
8월 06 22:45:33 splunk-server ntpd[4033]: Soliciting pool server 2620:2d:4000:1::41
```

#### ④ 클라이언트가 NTP 서버에 액세스할 수 있도록 방화벽 구성

```
#ufw allow from any to any port 123 proto udp
```

```
#ufw status
```

```
root@splunk-server:/#  
root@splunk-server:/# ufw allow from any to any port 123 proto udp  
규칙이 추가되었습니다  
규칙이 추가되었습니다 (v6)  
root@splunk-server:/# ufw status  
상태: 활성
```

목적	동작	출발
--	--	--
123/udp	ALLOW	Anywhere
123/udp (v6)	ALLOW	Anywhere (v6)

```
root@splunk-server:/#
```



#ntpq -p // 현재 동기화중인 NTP 서버정보를 출력

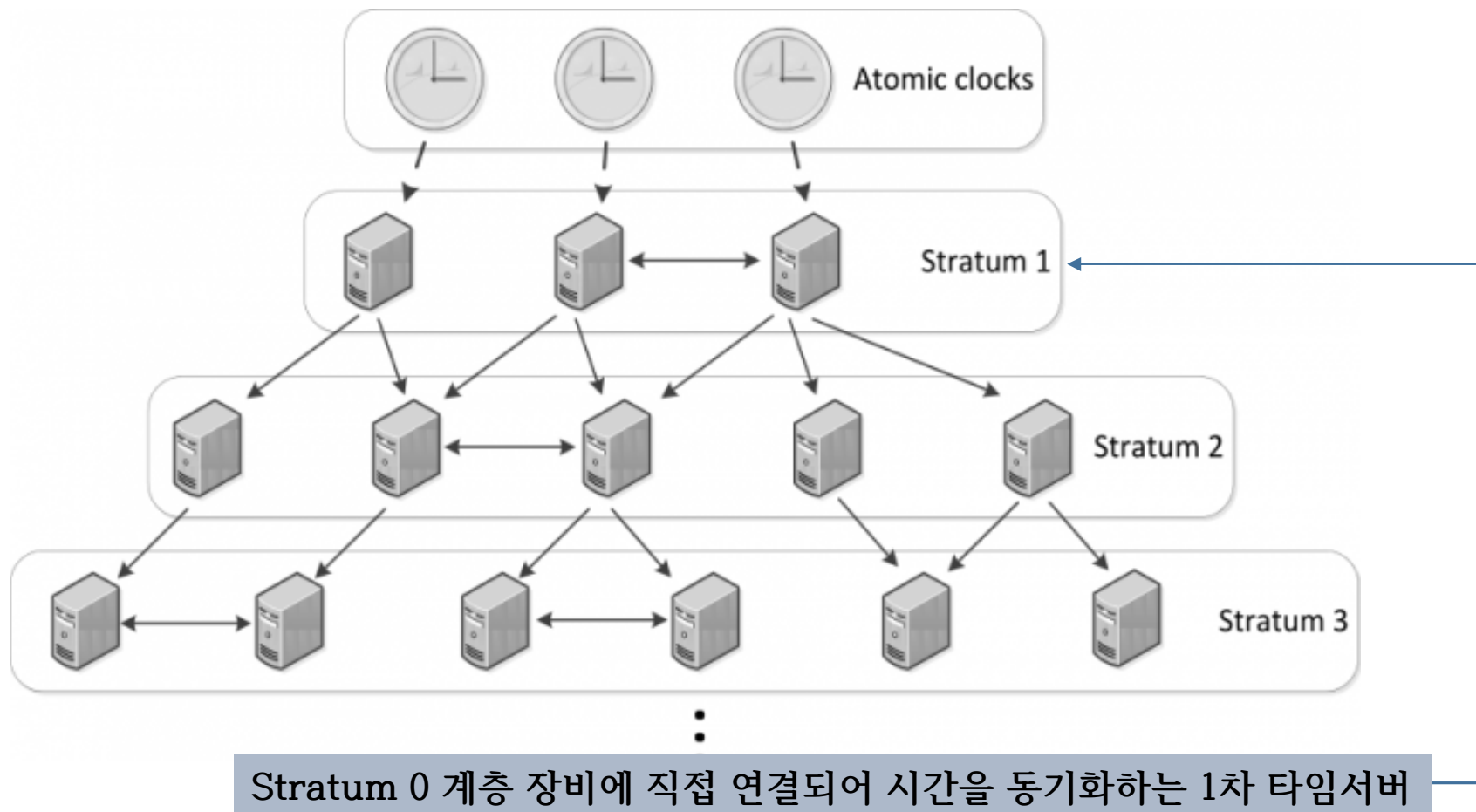
#date -R

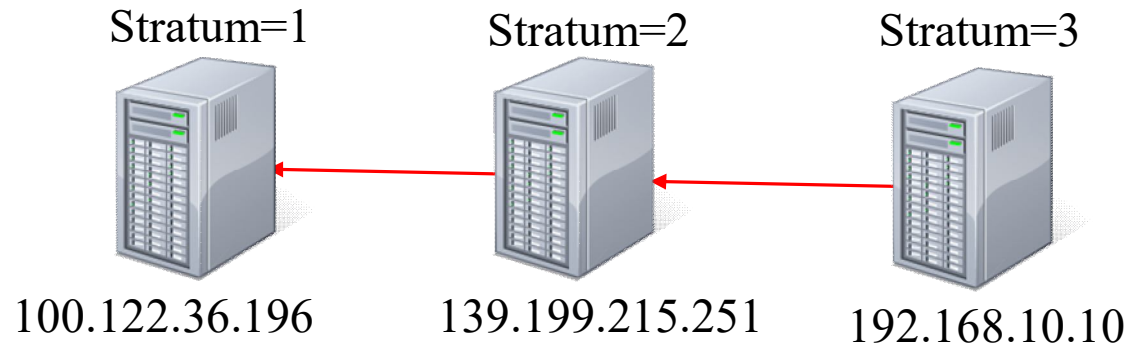
#timedatectl //현재 날짜, 시간, 타임존, 타임서버와의 동기화 여부를 모두 확인 가능

```
root@splunk-server:/# ntpq -p
      remote               refid              st t when poll reach  delay  offset  jitter
=====
ntp.ubuntu.com .POOL.          16 p   -   64    0    0.000   0.000   0.000
+121.174.142.81 220.73.142.66    3 u    2   64   77   16.161   0.791   2.403
+103.153.176.123 17.253.116.253   2 u    3   64   77  170.959 -48.258   4.743
*185.78.166.99  10.123.123.43    2 u    3   64   77  111.588 -11.251   3.514
-185.125.190.56 17.253.34.125    2 u   12   64   77  249.047  -6.848   4.824
-185.125.190.58 17.253.34.125    2 u    7   64   77  258.225 -13.660   6.572
-185.125.190.57 17.253.34.123    2 u   13   64   77  249.197  -6.520   6.030
-pugot.canonical 94.198.159.10    2 u    7   64   77  246.059   7.984   2.042
-alphyn.canonica 194.58.200.20    2 u   13   64   77  226.992   5.446   2.301
root@splunk-server:/#
root@splunk-server:/# date -R
Sat, 06 Aug 2022 22:51:33 +0900
root@splunk-server:/#
root@splunk-server:/# timedatectl
          Local time: 토 2022-08-06 22:51:45 KST
          Universal time: 토 2022-08-06 13:51:45 UTC
            RTC time: 토 2022-08-06 13:51:45
          Time zone: Asia/Seoul (KST, +0900)
System clock synchronized: no
              NTP service: n/a
          RTC in local TZ: no
```

# Stratum

- 시간을 전송하는 장비





```

root@splunk-server:~# ntpq -p
      remote               refid              st t when poll reach  delay  offset  jitter
=====
ntp.ubuntu.com   .POOL.              16 p   -   64    0    0.000   0.000   0.000
+121.174.142.81  220.73.142.66       3 u   37   64    1   13.245   3.263   2.069
*139.199.215.251 100.122.36.196       2 u   38   64    1  101.012   8.095   1.608
+time1.isu.net.s 209.51.161.238       2 u   40   64    1  354.928   6.616   3.082
185.125.190.57   17.253.34.123       2 u   46   64    1  232.358   6.206   0.000
185.125.190.56   17.253.34.125       2 u   49   64    1  266.257   8.657   0.000
pugot.canonical 193.204.114.232     2 u   48   64    1  265.277   3.744   0.000
alphyn.canonica 142.3.100.2          2 u   50   64    1  224.596  11.022   0.000
185.125.190.58   17.253.34.125       2 u   49   64    1  241.513   0.117   0.000
  
```

①

②

③

④

\* : 지금 동기화하고 있는 NTP sever IP  
 + : 동기화가 가능한 second NTP server IP  
 공백 : 접속이 불가능한 IP

Stratum

시간을 받아들이는 방식

Unicast/Broadcast/Multicast



## 2) [Ubuntu-Zeep] NTP Client Installation

### ① ntpdate 설치

#apt-get install ntpdate

\* ntpdate : 리눅스 시간을 timeserver와 동기화하는 명령어

```
root@zeek-IDS:~# apt-get install ntpdate
패키지 목록을 읽는 중입니다... 완료
의존성 트리를 만드는 중입니다
상태 정보를 읽는 중입니다... 완료
다음 새 패키지를 설치할 것입니다:
  ntpdate
0개 업그레이드, 1개 새로 설치, 0개 제거 및 0개 업그레이드 안 함.
49.0 k바이트 아카이브를 받아야 합니다.
이 작업 후 178 k바이트의 디스크 공간을 더 사용하게 됩니다.
받기:1 http://mirror.kakao.com/ubuntu focal/universe amd64 ntpdate amd64 1:4.2.8p12+dfsg-3ubuntu4 [49.0 kB]
내려받기 49.0 k바이트, 소요시간 0초 (402 k바이트/초)
Selecting previously unselected package ntpdate.
(데이터베이스 읽는중 ...현재 181840개의 파일과 디렉터리가 설치되어 있습니다.)
Preparing to unpack .../ntpdate_1%3a4.2.8p12+dfsg-3ubuntu4_amd64.deb ...
Unpacking ntpdate (1:4.2.8p12+dfsg-3ubuntu4) ...
ntpdate (1:4.2.8p12+dfsg-3ubuntu4) 설정하는 중입니다 ...
Processing triggers for man-db (2.9.1-1) ...
root@zeek-IDS:~#
```

## ②호스트 파일에서 NTP 서버의 IP 및 호스트 이름 지정

#nano /etc/hosts

192.168.10.10 splunkserver

```
root@zeek-IDS:~# cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      zeek-IDS
192.168.10.10  splunk-server

# The following lines are desirable for IPv6 capable hosts
::1           ip6-localhost ip6-loopback
fe00::0       ip6-localnet
ff00::0       ip6-mcastprefix
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters
root@zeek-IDS:~#
```

### ③ NTP 서버와 동기화되었는지 확인

#ntpdate splunkserver

```
root@zeek-IDS:~# ntpdate splunk-server
6 Aug 23:06:52 ntpdate[2162]: adjust time server 192.168.10.10 offset -0.018658 sec
root@zeek-IDS:~#
```

### ④ systemd timesyncd 서비스 비활성화

#timedatectl set-ntp off

```
root@zeek-IDS:~# timedatectl set-ntp off
root@zeek-IDS:~#
```

\* 시스템 시간(리눅스 커널시간 또는 소프트웨어시간) 동기화를 비활성화



## ⑤ 동기화된 시간 확인

#date

#date -R

#timedatectl

```
root@zeek-IDS:~# date
2022. 08. 06. (토) 23:10:38 KST
root@zeek-IDS:~#
root@zeek-IDS:~# date -R
Sat, 06 Aug 2022 23:10:55 +0900
root@zeek-IDS:~#
root@zeek-IDS:~# timedatectl
          Local time: 토 2022-08-06 23:11:09 KST
        Universal time: 토 2022-08-06 14:11:09 UTC
              RTC time: 토 2022-08-06 14:11:09
            Time zone: Asia/Seoul (KST, +0900)
System clock synchronized: yes
              NTP service: inactive
          RTC in local TZ: no
root@zeek-IDS:~#
```

### 3) [CentOS] NTP Client Installation

#### **chrony**

- Redhat 계열 리눅스 기본 시간 동기화 프로그램
- Redhat Enterprise Linux 8 부터 기본 시간 동기화 프로그램으로 채택
- CentOS 8 chrony를 기본 시간 동기화 프로그램으로 사용
- Chrony 는 기본 설치가 되어 있어 CentOS 8 에서 별도 설치를 하지 않고 사용

```
[root@localhost ~]# rpm -qa | grep chrony
chrony-3.3-3.el8.x86_64
[root@localhost ~]#
```

#### **<< chrony 사용법>>**

- 설정 파일에 해당 지역의 NTP 서버 등록
- chrony 서비스 재시작
- 시간 동기화 적용 확인, NTP 서버 동작 확인

## ❶ NTP 호스트명 등록

#gedit /etc/hosts

192.168.10.10 splunkserver

```
[root@localhost ~]# gedit /etc/hosts
[root@localhost ~]# cat /etc/hosts
192.168.10.10    splunk-server
127.0.0.1       localhost localhost.localdomain localhost4 localhost4.localdomain4
::1            localhost localhost.localdomain localhost6 localhost6.localdomain6
[root@localhost ~]#
```

## ② NTP 서버 등록

#gedit /etc/chrony.conf

server splunkserver iburst

```
[root@localhost ~]# gedit /etc/chrony.conf
[root@localhost ~]# head /etc/chrony.conf
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
#pool 2.centos.pool.ntp.org iburst

server splunk-server iburst

# Record the rate at which the system clock gains/losses time.
driftfile /var/lib/chrony/drift

# Allow the system clock to be stepped in the first three updates
[root@localhost ~]#
```

### ③ chronyd 서비스 활성화와 상태 확인

#systemctl restart chronyd

#systemctl status chronyd

```
[root@localhost ~]# systemctl restart chronyd
[root@localhost ~]# systemctl status chronyd
● chronyd.service - NTP client/server
   Loaded: loaded (/usr/lib/systemd/system/chronyd.service; disabled; vendor preset: enabled)
   Active: active (running) since Sat 2022-08-06 23:33:35 KST; 32s ago
     Docs: man:chronyd(8)
           man:chrony.conf(5)
  Process: 3121 ExecStartPost=/usr/libexec/chrony-helper update-daemon (code=exited, status=0/SUCCESS)
  Process: 3117 ExecStart=/usr/sbin/chronyd $OPTIONS (code=exited, status=0/SUCCESS)
 Main PID: 3119 (chronyd)
    Tasks: 1 (limit: 24877)
   Memory: 1.3M
    CGroup: /system.slice/chronyd.service
            └─3119 /usr/sbin/chronyd

8월 06 23:33:35 localhost.localdomain systemd[1]: Starting NTP client/server...
8월 06 23:33:35 localhost.localdomain chronyd[3119]: chronyd version 3.3 starting (+CMDMON +NTP +REFCLO
8월 06 23:33:35 localhost.localdomain chronyd[3119]: Using right/UTC timezone to obtain leap second data
8월 06 23:33:35 localhost.localdomain systemd[1]: Started NTP client/server.
8월 06 23:33:39 localhost.localdomain chronyd[3119]: Selected source 192.168.10.10
8월 06 23:33:39 localhost.localdomain chronyd[3119]: System clock TAI offset set to 37 seconds
```

## ④ NTP 설정 환경과 시간 확인

```
#chrony sources -v
```

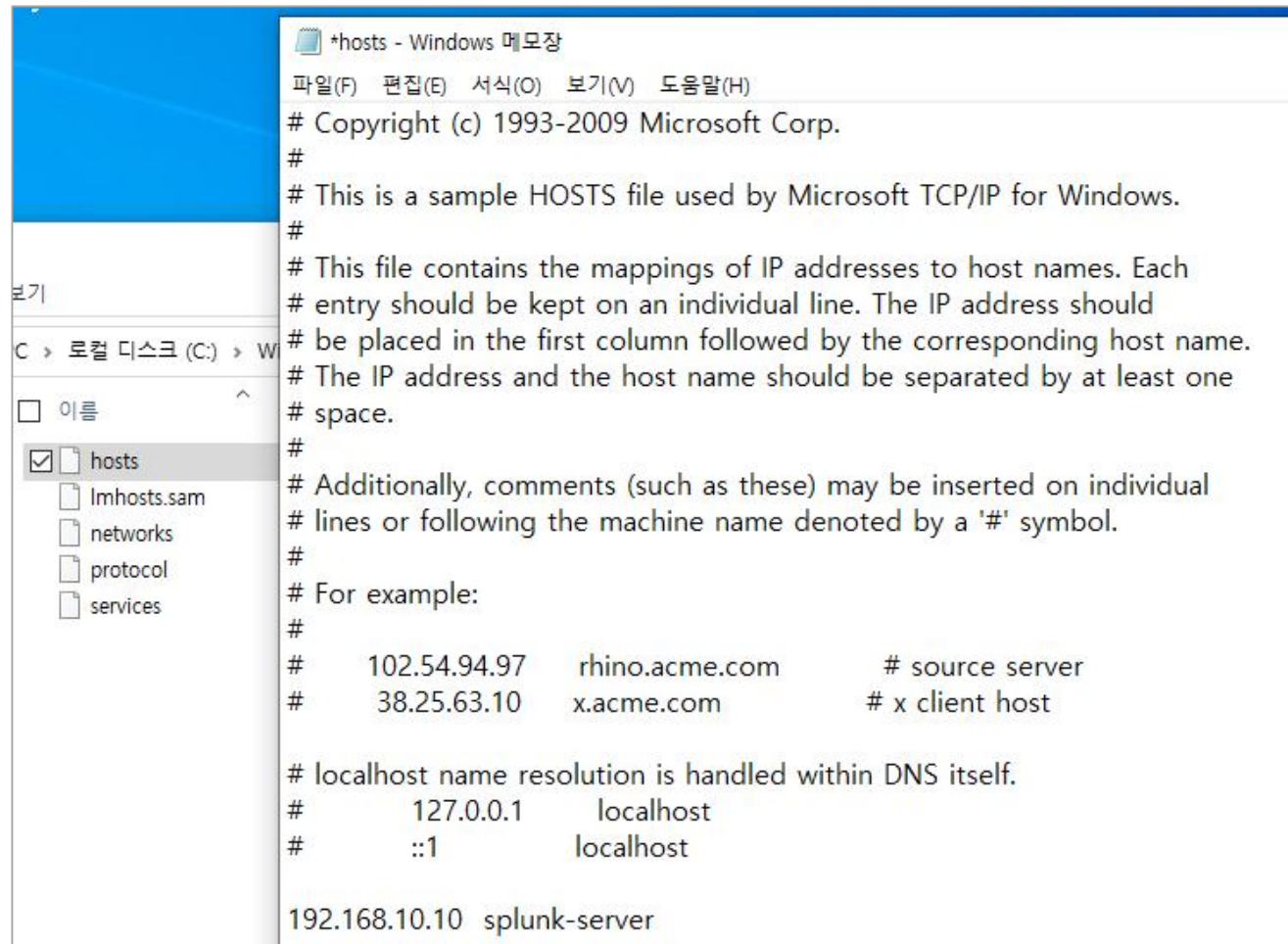
# #timedatectl

```
[root@localhost ~]# chronyc sources -v
210 Number of sources = 1

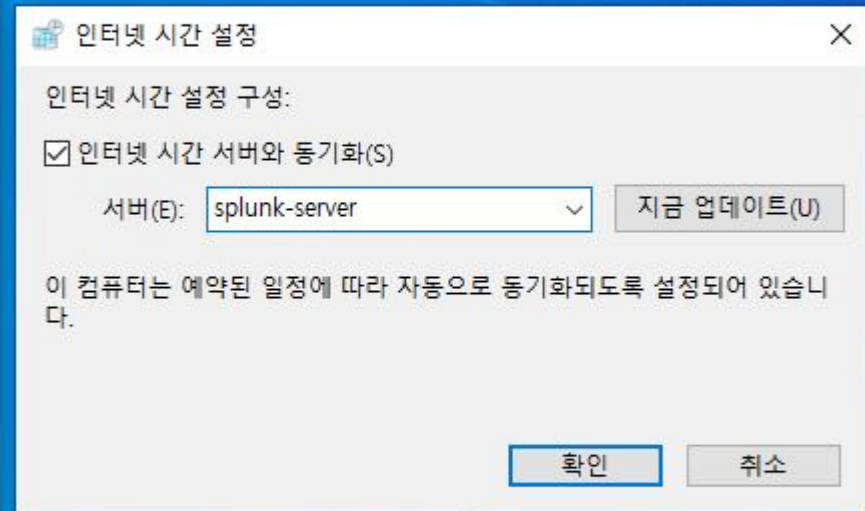
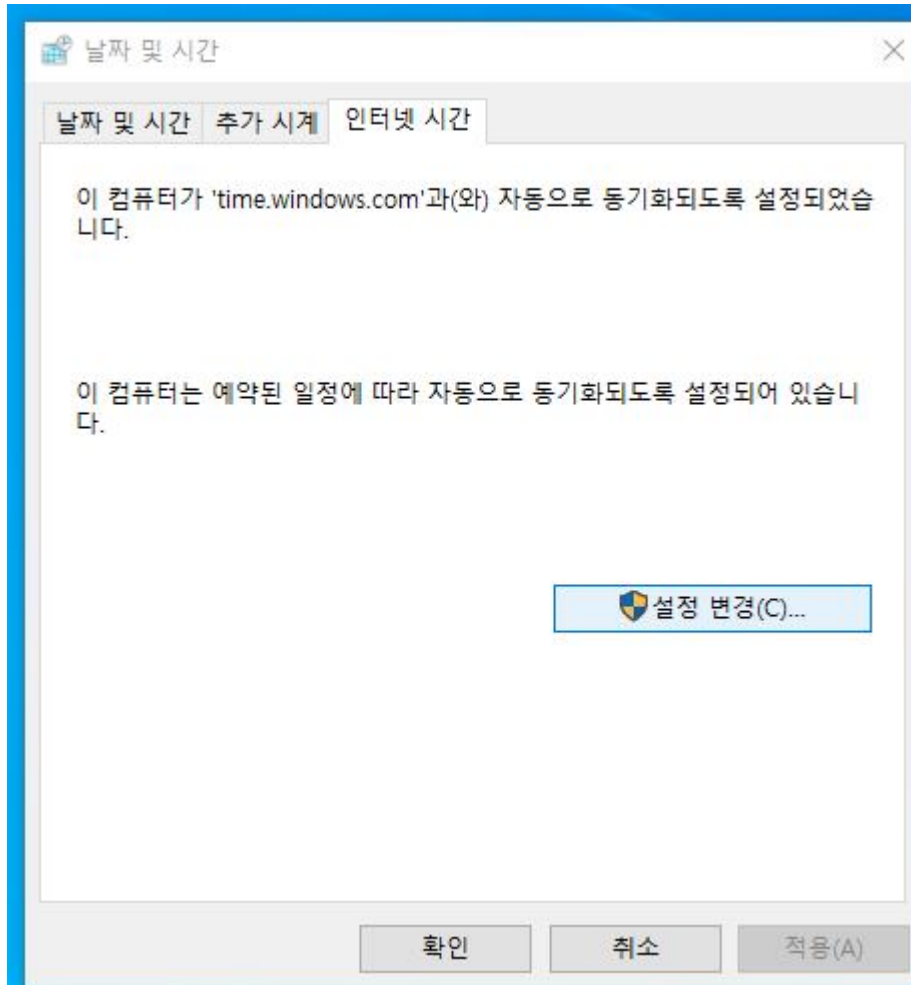
.-- Source mode   '^' = server, '=' = peer, '#' = local clock.
/.- Source state '*' = current synced, '+' = combined , '-' = not combined,
/  '?' = unreachable, 'x' = time may be in error, '~' = time too variable.
|                                     .- xxxx [ yyyy ] +/- zzzz
|                                     |xxxx = adjusted offset,
|      Reachability register (octal) -.    |yyyy = measured offset,
|      Log2(Polling interval) --.         |zzzz = estimated error.
|                                     \
|                                     |
MS Name/IP address             Stratum Poll Reach LastRx Last sample
=====
^* splunk-server                3     6     77    43    +11us[ +498us] +/- 164ms
[root@localhost ~]#
[root@localhost ~]# timedatectl
          Local time: 토 2022-08-06 23:36:39 KST
        Universal time: 토 2022-08-06 14:36:39 UTC
           RTC time: 토 2022-08-06 14:36:39
          Time zone: Asia/Seoul (KST, +0900)
System clock synchronized: yes
            NTP service: active
          RTC in local TZ: no
[root@localhost ~]#
[root@localhost ~]# date -R
Sat, 06 Aug 2022 23:37:18 +0900
[root@localhost ~]#
```



## 4) [Win10 ] NTP Client Installation



```
*hosts - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97    rhino.acme.com    # source server
#      38.25.63.10    x.acme.com        # x client host
#
# localhost name resolution is handled within DNS itself.
#      127.0.0.1      localhost
#      ::1            localhost
192.168.10.10 splunk-server
```



## \* 동기화 상태 확인

c:\>w32tm /query /status

```
C:\Users\sysmon>w32tm /query /status
윤초 조정: 0(경고 없음)
계층: 4(보조 참조 - (S)NTP로 동기화됨)
정밀도: -23(틱당 119.209ns)
루트 지연: 0.2347758s
루트 분산: 8.6461542s
참조 ID: 0xC0A80A0A(원본 IP: 192.168.10.10)
마지막으로 동기화한 시간: 2022-08-06 오후 11:50:37
원본: splunk-server, 0x9
폴링 간격: 10(1024s)
```

c:\>w32tm /dumpreg /subkey:parameters

```
C:\Users\sysmon>
C:\Users\sysmon>w32tm /dumpreg /subkey:parameters
```

값 이름	값 종류	값 데이터
NtpServer	REG_SZ	splunk-server, 0x9
ServiceDll	REG_EXPAND_SZ	%systemroot%\system32\w32time.dll
ServiceDllUnloadOnStop	REG_DWORD	1
ServiceMain	REG_SZ	SvchostEntry_W32Time
Type	REG_SZ	NTP