BaroPAM 가이드(Database)

목차

1. BaroPAM 설치

데이터베이스에 접속해 데이터베이스에서 제공하는 대화형 SQL 명령어 처리 유틸리티, 데이터베이스 내에 존재하는 데이터를 테이블 단위로 다운로드 하거나 업로드 할 수 있도록 데이터베이스에서 제공하는 유틸리티에 BaroPAM의 일회용 인증키를 적용한다.

1.1 BaroPAM 설치 전 준비사항

데이터베이스에 접속하는 경우 BaroPAM 모듈을 사용하기 위해서는 신뢰성 있고 안전한 서비스를 제공하기 위하여 OpenSSL(Open Secure Socket Layer) 패키지가 반드시 설치되어 있는지 확인한 후 설치되어 있지 않으면 설치하면 된다.

```
[root]# openssl version
OpenSSL 0.9.8e-fips-rhel5 01 Jul 2008
```

BaroPAM 인증 모듈을 다운로드 및 설치하기 위해서 root 계정으로 접속한 후 모듈을 다운로드 및 설치하기 위한 디렉토리(/usr/baropam)를 다음과 같이 생성한다.

```
[root]# mkdir /usr/baropam
```

BaroPAM 모듈을 다운로드 및 설치하기 위한 디렉토리의 권한(읽기, 쓰기, 실행)을 다음과 같이 부여한다.

```
[root]# chmod -R 777 /usr/baropam
```

1.2 BaroPAM 설치 모듈 다운로드

BaroPAM 인증 모듈은 root 계정으로 접속한 후 모듈을 다운로드 및 설치하기 위한 디렉토리(/usr/baropam)로 이동하여 모듈을 다운로드 하는 방법은 다음과 같다.

```
[root] /usr/baropam > wget http://nuriapp.com/download/libpam_baro_auth_cmd-x.x.tar
```

BaroPAM 인증 모듈의 다운로드가 완료되면 tar 파일의 압축을 해제하는 방법은 다음과 같다.

```
[root] /usr/baropam > tar -xvf libpam_baro_auth_cmd-x.x.tar
```

BaroPAM 인증 모듈의 압축을 해제하면 baropam 디렉토리에 다음과 같은 BaroPAM 관련 모듈이 생성된다.

```
[root] /usr/baropam > ls -al
합계 180
drwxrwxrwx  7 root root   4096  8월 23 09:59 .
drwxr-xr-x 17 root root   4096  2월 10  2017 ..
-r--r--r--  1 root root    270  2월 18 14:12 .baro_auths
-rwxr-xr-x  1 root root  46933  2월 18 14:10 baro_auths
-rwxr-xr-x  1 root root  97681  2월 18 14:08 barodb
-rw-r--r--  1 root root    199  2월 18 14:57 setauths.sh
```

BaroPAM 인증 모듈은 Database 설치 계정으로 접속한 후 실행 파일이 존재하는 디렉토리(~/bin)로 실행파

일을 다음과 같이 복사한다.

Oracle인 경우)

```
[oracle] $ cd $ORACLE_HOME/bin
[oracle] ~/bin $
[oracle] ~/bin $ cp /usr/baropam/barodb sqlplus
[oracle] ~/bin $ cp /usr/baropam/barodb imp
[oracle] ~/bin $ cp /usr/baropam/barodb exp
```

Tibero인 경우)

```
[tibero] $ cd $TB_HOME/bin
[tibero] ~/bin $
[tibero] ~/bin $ cp /usr/baropam/barodb tbsql
```

Altibase인 경우)

```
[altibase] $ cd $ALTIBASE_HOME/bin
[altibase] ~/bin $
[altibase] ~/bin $ cp /usr/baropam/barodb isql
```

1.3 BaroPAM 환경 설정 파일 설정

BaroPAM 환경 설정 파일은 baro_auths 프로그램을 실행하여 반드시 생성하는데, BaroPAM 인증 모듈의 디렉토리인 /usr/baropam 밑에 위치 하도록 한다.

형식)

```
baro_auths -r rate_limit -R rate_time -t cycle_time -c corr_time -k key_method -H hostname -a apply_yn -S secure_key -s filename
```

BaroPAM 환경 설정 파일의 설정 항목에 대한 내용은 다음과 같다.

옵션	설명	설정값	비고
-r	일회용 인증키의 제한횟수(1~10) 설정	3	
-R	일회용 인증키의 제한시간(초, 15~600초) 설정.	30	
-t	일회용 인증키의 인증주기(초, 3~60초)	30	
-c	일회용 인증키의 보증오차시간(초)	0	
-k	일회용 인증키의 인증방식(app1, app256, app384, app512: 앱, card1, card256, card384, card512: 인증카드)	app512	
-H	서버의 호스트명(uname -n)	nurit.co.kr	
-a	2차 인증의 적용여부(yes or no)	yes	
-S	Secure key(라이선스 키)	Ri5+xgVdtEBJGlrSD2hvituZxAq0vttx	
-s	BaroPAM 환경설정 파일을 생성할 디렉토리를 포함한 파일명	/usr/baropam/.baro_auths	

주의) -s 옵션의 filename는 PAM 환경 설정 파일명(**파일 접근권한은 444**)이며, 설정한 서버의 호스트명(hostname)이 맞지 않는 경우 BaroPAM이 정상적으로 작동되지 않을 수 있으니, 호스트명(hostname)이 변경되는 경우 반드시 환경 설정의 해당 항목에 반영해야 한다.

사용 예)

```
[root] /usr/baropam > /usr/baropam/baro_auths -r 3 -R 30 -t 30 -c 0 -k app512 -H nurit.co.kr -a yes
-S WSa1MUyG+aaiJ1JS/uqtXuBSoRBIIZOL -s /usr/baropam/.baro_auths
```

1) Your emergency one-time authentication keys are :
응급 일회용 인증키는 **일회용 인증키** 생성기인 BaroPAM 어플을 사용할 수 없을 때 분실한 경우를 대비하여 데이터베이스에 다시 액세스하는데 사용할 수 있는 접속이 가능한 Super 인증키 이므로 어딘가에 적어 두는 것이 좋다.

2) 다음에 나오는 물음에 대해서는 모두 "**y**"를 입력한다.
중간자(man-in-the-middle) 공격을 예방할 것인가? y
같은 **일회용 인증키**는 하나의 계정 외에 다른 계정에도 로그인이 가능하게 할 것인가? y
일회용 인증키의 제한 시간을 30초로 지정할 것인가? y

BaroPAM 환경 설정 파일인 .baro_auths에 설정한 내용은 다음과 같다.

```
[root] /usr/baropam > cat .baro_auths
" AUTH_KEY
" RATE_LIMIT 3 30
" KEY_METHOD app512
" CORR_TIME 0
" CYCLE_TIME 30
" SECURE_KEY WSa1MUyG+aaiJ1JS/uqtXuBSoRBIIZOL
" APPLY_YN yes
" HOSTNAME nurit.co.kr
" WINDOW_SIZE 17
" DISALLOW_REUSE
67399918
84550299
43914873
60281106
10699129
```

BaroPAM 환경설정 파일인 .baro_auths의 설정 항목에 대한 내용은 다음과 같다.

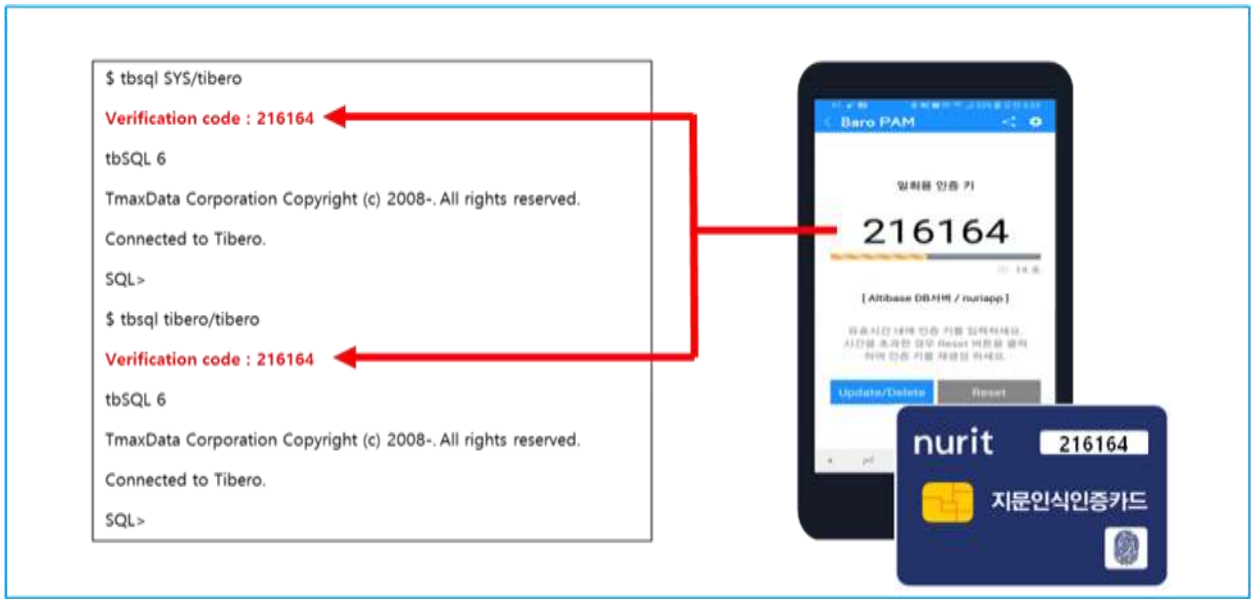
항목	설명	설정값	비고
AUTH_KEY	인증 구분자(고정)		
APPLY_YN	**2차 인증** 적용여부(yes or no)	yes	
RATE_LIMIT	**일회용 인증키**의 제한횟수(1~10), 제한시간(초, 15~600초) 설정.	3 30	
KEY_METHOD	**일회용 인증키**의 인증방식(app1, app256, app384, app512: 앱, card1, card256, card384, card512: 인증카드)	app512	
CORR_TIME	**일회용 인증키**의 보증오차시간(초)	0	
CYCLE_TIME	**일회용 인증키**의 인증주기(초, 3~60초)	30	
SECURE_KEY	Secure key(라이선스 키)	WSa1MUyG+aaiJ1JS/uqtXuBSoRBIIZOL	
HOSTNAME	서버의 호스트명(uname -n)	nurit.co.kr	
APPLY_YN	**2차 인증**의 적용여부(yes or no)	yes	
WINDOW_SIZE	현재 시간을 기준으로 **일회용 인증키**의 보정시간(-7~7초)	17	

1.4 Database Utility로 접속 방법

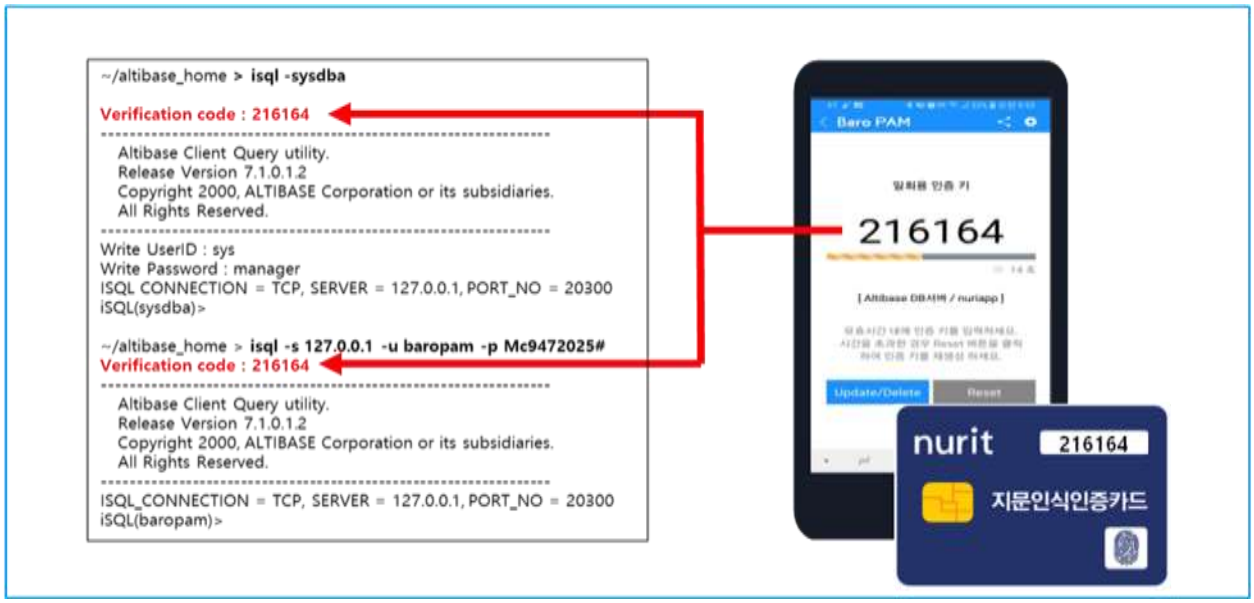
Database의 대화형 SQL 명령어 처리 유틸리티로 접속하여 **2차 인증**하는 방법은 다음과 같다.

Oracle에서 제공하는 대화형 SQL 명령어 처리 유틸리티인 sqlplus와 Oracle 내에 존재하는 데이터를 테이블 단위로 다운로드 / 업로드 유틸리티인 sqlloader에 **일회용 인증키**를 적용한 모습이다.

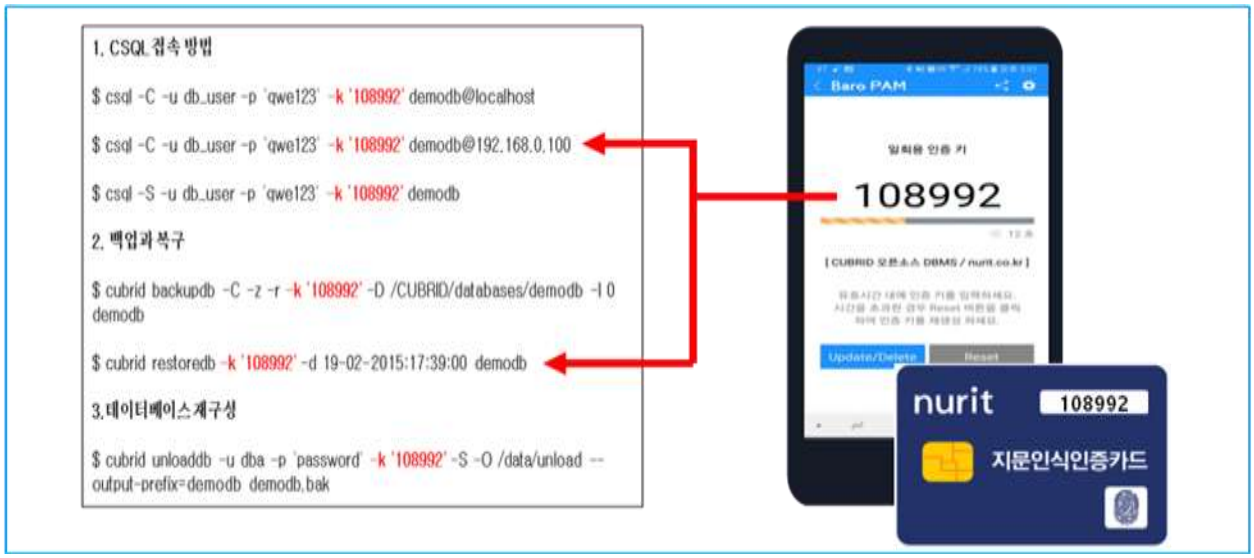
Tibro에서 제공하는 대화형 SQL 명령어 처리 유틸리티인 tbsql 과 Tibero 내에 존재하는 데이터를 테이블 단위로 다운로드 / 업로드 유틸리티인 iloader에 **일회용 인증키**를 적용한 모습이다.



Altibase 데이타베이스 정보와 서버의 정보를 조회하고 제어할 수 있는 도구인 iSQL과 Altibase 내에 존재하는 데이터를 테이블 단위로 다운로드 / 업로드 유틸리티인 iloader에 **일회용 인증키**를 적용한 모습이다.

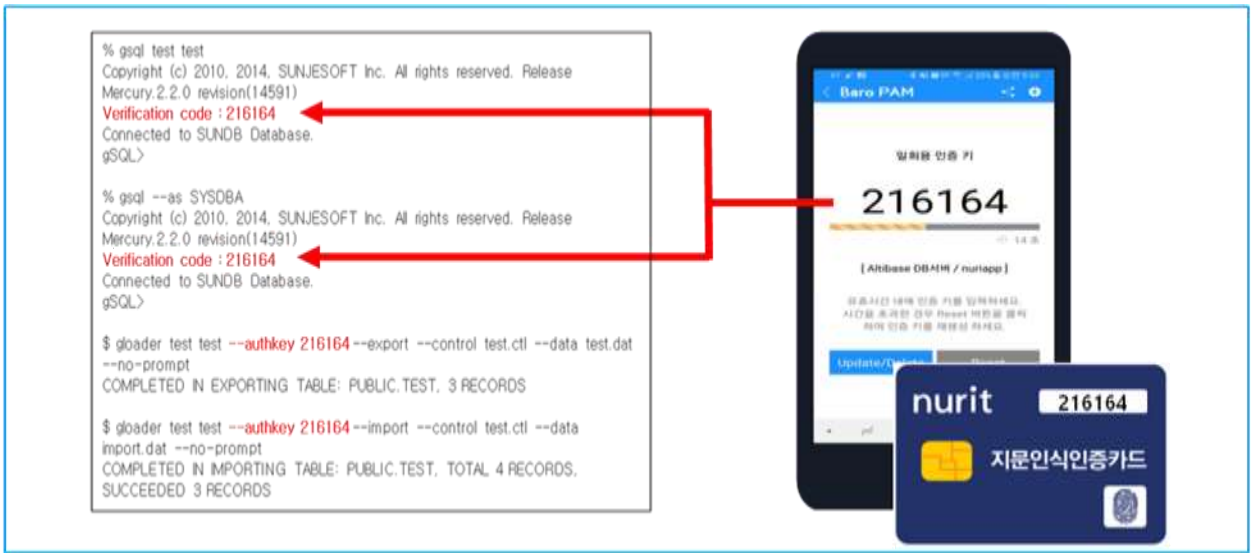


CUBRID 오픈소스 DBMS에 CSQL 인터프리터, 백업 및 복구, 데이터베이스 재구성 등에 **일회용 인증키**를 적용한 모습이다.



CUBRID GUI 도구인 CUBRID Manager에 "**CM 사용자**", "**CM 비밀번호**" 이외에 **일회용 인증키**를 입력할 수 있는 "**Verification code**" 항목을 추가하여 보안 강화시킬 수 있다.

sunje Mercury DBMS에 접속해 데이터베이스 정보와 서버의 정보를 조회하고 제어할 수 있는 도구인 gsql/gsqlnet과 DBMS 내에 존재하는 데이터를 다운로드 / 업로드 유틸리티인 gloader/gloadernet에 **일회용 인증키**를 적용한 모습이다.



1.5 Shell script로 접속 방법

Shell script를 통하여 Database에 접속하여 일괄작업을 하는 경우는 "**-skey**" 파라미터를 사용하여 부여된 Secure key를 다음과 같이 지정하여 실행하면 된다.

```
$ vi analyze_all.sh
#! /usr/bin/ksh
export ORACLE_SID=ORCL
export ORACLE_HOME=/home/oracle/app/oracle/product/11.2.0/db_1
export PATH=$ORACLE_HOME/bin:$PATH

sqlplus -skey WSa1MUyG+aaiJ1JS/uqtXuBSoRBIIZOL rims/rims <<!
    show recyclebin;
    purge recyclebin;
    set pages 0
    SPOOL   ANALYZE_RIMS
    SELECT 'ANALYZE  TABLE ' || TABLE_NAME   || ' ESTIMATE  STATISTICS; ' FROM  USER_TABLES;
    SELECT 'ANALYZE   INDEX ' || B.INDEX_NAME || ' ESTIMATE  STATISTICS; ' FROM  USER_TABLES A,
(SELECT TABLE_NAME, INDEX_NAME, COUNT(*) FROM USER_IND_COLUMNS GROUP BY TABLE_NAME, INDEX_NAME) B
WHERE B.TABLE_NAME = A.TABLE_NAME;
    SPOOL   OFF
    START   ANALYZE_RIMS.lst
    exit
!
```

2. NTP(Network Time Protocol) 설정

최근에는 정보자산에 대한 시간 동기화(타임서버 시간 동기화)하는 방법으로 NTP(Network Time Protocol)을 이용하여 관리자 계정에서 시스템의 시각을 현재 시각으로 설정할 수 있다.

2.1 Linux 환경

최근에는 Windows/서버/데이터베이스/네트워크 장비/저장장치에 대한 시간 동기화(타임서버 시간 동기화)하는 방법으로 NTP(Network Time Protocol)을 이용하여 루트 계정에서 시스템의 시각을 현재 시각으로 설정할 수 있다.

NTP를 사용하기 위해서는 기본적으로 NTP 패키지가 반드시 설치되어 있어야 한다. 설치 확인은 다음의 명령어를 실행하여 확인한다. 만약, 설치되어 있지 않으면 "**yum install ntp**" 명령어로 설치하면 된다.

```
[root]# rpm -qa | grep ntp
ntp-4.2.2p1-18.el5.centos
chkfontpath-1.10.1-1.1
```

ntpd 서비스를 서버 부팅 시 시작프로그램에 등록 및 ntp 활성화 여부 확인은 다음과 같은 명령어로 확인할 수 있다.

```
[root]# chkconfig ntpd on
[root]# chkconfig —list | grep ntp
ntpd            0:해제  1:해제  2:활성  3:활성  4:활성  5:활성  6:해제
```

chkconfig 이용하여 서버 부팅시 ntpd 데몬 활성화 여부 확인 3, 5 level 에 off(해제) 가 되어 있으면 자동 활성화 되지 않는다. 자동 활성화 하기 위해서는 3, 5 에 on(활성)으로 다음과 같은 명령어로 변경해야 한다.

```
[root]# chkconfig —level 3 ntpd on
[root]# chkconfig —level 5 ntpd on
```

우리나라에서 운영되고 있는 NTP 서버는 다음과 같다.

```
server kr.pool.ntp.org
server time.bora.net
server time.kornet.net
```

우리나라에서 운영되고 있는 NTP 서버를 ntpd 데몬 설정을 위한 설정 파일인 "**/etc/ntp.conf**"에 다음과 같이 설정한다.

```
[root]# vi /etc/ntp.conf
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
#server 0.centos.pool.ntp.org
#server 1.centos.pool.ntp.org
#server 2.centos.pool.ntp.org
#server 3.centos.pool.ntp.org
server kr.pool.ntp.org
```

```
server time.bora.net
server time.kornet.net
```

ntpd 데몬 설정을 위한 설정이 끝나면 반드시 NTP 설정이 제대로 추가되었는지 확인한 후 NTP 데몬의 Restart 작업이 반드시 필요하다.

```
[root]# /etc/init.d/ntpd restart
ntpd를 종료 중: [  OK  ]
ntpd (을)를 시작 중: [  OK  ]
```

ntpd 시간 확인은 다음과 같은 명령어로 확인할 수 있다.

```
[root]# ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 static.betaidc. 106.247.248.106  3 u    7   64    1    2.884  287.718   0.001
 time.bora.net   .INIT.          16 u    -   64    0    0.000    0.000   0.000
 183.110.225.61  .INIT.          16 u    -   64    0    0.000    0.000   0.000
 LOCAL(0)        .LOCL.          10 l    4   64    1    0.000    0.000   0.001
```

* 표시된 ip 가 현재 시간을 가져오고 있는 ntp 서버임

NTP를 사용하기 위해서는 기본적으로 NTP 패키지가 반드시 설치되어 있어야 한다. 설치 확인은 다음의 명령어를 실행하여 확인한다. 만약, 설치되어 있지 않으면 Redhat, CentOS 8 이상 버젼은 "**yum install chrony**" 명령어로 설치하면 된다.

```
[root@baropam ~]# rpm -qa | grep chrony
chrony-3.5-1.el8.x86_64
```

우리나라에서 운영되고 있는 NTP 서버는 다음과 같다.

```
server kr.pool.ntp.org
server time.bora.net
server time.kornet.net
```

우리나라에서 운영되고 있는 NTP 서버를 ntpd 데몬 설정을 위한 설정 파일인 "**/etc/chrony.conf**"에 다음과 같이 설정한다.

```
[root@baropam ~]# vi /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 kr.pool.ntp.org iburst
server time.bora.net   iburst
server time.kornet.net 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
# if its offset is larger than 1 second.
makestep 1.0 3
```

```
# Enable kernel synchronization of the real-time clock (RTC).
rtcsync

# Enable hardware timestamping on all interfaces that support it.
#hwtimestamp *

# Increase the minimum number of selectable sources required to adjust
# the system clock.
#minsources 2

# Allow NTP client access from local network.
allow 192.168.0.0/16

# Serve time even if not synchronized to a time source.
#local stratum 10

# Specify file containing keys for NTP authentication.
keyfile /etc/chrony.keys

# Get TAI-UTC offset and leap seconds from the system tz database.
leapsectz right/UTC

# Specify directory for log files.
logdir /var/log/chrony

# Select which information is logged.
#log measurements statistics tracking
```

ntpd 데몬 설정을 위한 설정이 끝나면 반드시 NTP 설정이 제대로 추가되었는지 확인한 후 NTP 데몬의 Restart 작업이 반드시 필요하다. (chrony 서비스 시작 및 부팅시 구동 등록)

```
[root@baropam ~]# sudo systemctl enable chronyd
[root@baropam ~]# sudo systemctl restart chronyd
```

ntpd 시간 확인은 다음과 같은 명령어로 확인할 수 있다.

시간을 받아오는 서버 리스트 / chrony.conf 파일에 등록한 server 리스트)

```
[root@baropam ~]# chronyc sources
210 Number of sources = 2
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^* ec2-54-180-134-81.ap-nor>     2   6   377    43   -349us[-1059us] +/-   24ms
^- time.bora.net                 2   6   377    42  +1398us[+1398us] +/-   90ms
```

시간을 받아 오는 서버 정보)

```
[root@baropam ~]# chronyc tracking
Reference ID    : 36B48651 (ec2-54-180-134-81.ap-northeast-2.compute.amazonaw)
Stratum         : 3
Ref time (UTC)  : Sun Mar 22 07:07:43 2020
System time     : 0.000130027 seconds slow of NTP time
Last offset     : -0.000710122 seconds
```

```
RMS offset      : 0.000583203 seconds
Frequency       : 19.980 ppm fast
Residual freq   : +0.142 ppm
Skew            : 3.235 ppm
Root delay      : 0.013462566 seconds
Root dispersion : 0.017946836 seconds
Update interval : 65.0 seconds
Leap status     : Normal
```

시간 상태 및 동기화 등 정보 확인)

```
[root@baropam ~]# timedatectl status
               Local time: Sun 2020-03-22 16:08:45 KST
           Universal time: Sun 2020-03-22 07:08:45 UTC
                 RTC time: Sun 2020-03-22 07:08:44
                Time zone: Asia/Seoul (KST, +0900)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
```

2.2 Solaris 환경

NTP(Network Time Protocol)는 컴퓨터 클라이언트나 서버의 시간을 다른 서버나 라디오 또는 위성 수신기와 같은 참조할 수 있는 타임 소스 또는 모뎀에 동기화하는데 사용된다.

1) 세 가지 유형의 시간 서버(Time Server)

① peer host_address [key #] [version #] [prefer]
- 로컬 서버가 호스트 주소로서 지정된 원격 서버와 함께 symmetric active 모드로 운영.
- 로컬 서버는 원격 서버에 맞추어 동기화 할수 있음.

② server host_address [kery #] [version #] [prefer] [mode #] server
- 로컬 서버가 command에서 이름이 지정된 원격 서버와 함께 client 모드로 운영.
- 이 모드에서 로컬 서버는 원격 서버에 맞추어 동기화될 수 있지만 원격 서버는 로컬 서버에 동기화 할 수 없음.

③ broadcast host_address [key#] [version #] [ttl #]
로컬 서버가 broadcast 모드로 운영된다는 것을 지정한다. 이 모드에서 로컬 서버는 명령어에서 지정된 broadcast/multicast 주소의 클라이언트 무리에게 정기 적인 broadcast 메시지를 전송한다.
- key 주소에 전송된 모든 패킷이 지정된 키 번호를 사용하여 암호화된 인증 필드를 포함
- version outgoing NTP 패킷에 사용되는 버전 번호를 지정 Version ①, ②, ③ 선택 기본 버전 ③번.
- prefer 호스트를 선택된 호스트로 표시,동기화를 위해 다른 비교 가능한 호스트보다 이 호스트가 선택.

2) NTP SERVER 설정. (server 모드) 방법

```
(sun>root)/etc/inet# cp ntp.server ntp.conf
(sun>root)/etc/inet# vi ntp.conf
# Either a peer or server.  Replace "XType" with a value from the
```

```
# table above.
#server 127.127.XType.0 prefer
#fudge 127.127.XType.0 stratum 0
server 127.127.1.0 ---> 언제나 로컬로 돌아갈수 있음.
server time.kriss.re.kr prefer
server 127.127.1.0
server gps.bora.net
server ntp.ewha.net
server time.bora.net
server time.nuri.net
server ntp2.gngidc.net
server time.kriss.re.kr

#broadcast 224.0.1.1 ttl 4 -->기본 설정 ( 네트웍내 여러개의 ntp 서버가 존재할 경우 변경)
broadcast 192.168.0.222 ttl 4
wq!
```

3) NTP SERVER 설정. (피어(peer) 모드) 방법

peer gps.bora.net key 0 version 3 prefer --> server 모드와 동일 server 설정대신 peer 설정.

```
(sun>root)/etc/inet# /etc/init.d/xntpd start
(sun>root)/etc/inet# ps -ef | grep ntp
    root  479  400  0 08:40:55 pts/2    0:00 grep ntp
    root  456    1  0 08:23:07 ?       0:01 /usr/lib/inet/xntpd
(sun>root)/etc/inet# ntpq -p (NTP 서버에게 피어 리스트에 관해 질의)
     remote           refid      st t when poll reach   delay   offset    disp
==============================================================================
 sun            0.0.0.0         16 -    -  64    0    0.00    0.000 16000.0
 gps.bora.net    0.0.0.0         16 u  48  64    0    0.00    0.000 16000.0
(e220>root)/# snoop -d hme0 port 123
Using device /dev/hme (promiscuous mode)
192.168.0.222 -> gps.bora.net NTP  symmetric active (Fri Feb 24 08:35:26 2006)
gps.bora.net -> 192.168.0.222 NTP  server (Sat Jan 19 03:58:31 2002)
       e220 -> 192.168.0.222 NTP  client (Fri Feb 24 08:35:46 2006)
192.168.0.222 -> e220        NTP  server (Fri Feb 24 08:35:47 2006)
```

4) NTP Client 설정

```
(sun>root)/etc/inet# cp ntp.client ntp.conf
```

기본 ntp.client 파일은 multicast를 사용하여 ntp 업데이트를 수신한다. NTP 클라이언트가 이러한 업데이트를 수신할 수 있는 장소를 제한하려는 경우 이것을 broadcast로 변경한다.(broadcast 패킷은 다른 서브넥에 전달되지 않는 반면 multicast 패킷은 전달 된다.)

```
(sun>root)/etc/inet# /etc/init.d/xntpd start
#multicastclient 224.0.1.1 --> 기본설정
server 192.168.0.222
wq!

(sun>root)/etc/inet# ps -ef | grep ntp
    root  479  400  0 08:40:55 pts/2    0:00 grep ntp
    root  456    1  0 08:23:07 ?       0:01 /usr/lib/inet/xntpd
```

```
(sun>root)/etc/inet#
(sun>root)/etc/inet# ntpq -p
     remote           refid      st t when poll reach   delay   offset    disp
==============================================================================
 sun             0.0.0.0         16 -    -  64    0    0.00    0.000 16000.0
 gps.bora.net     0.0.0.0         16 u  48  64    0    0.00    0.000 16000.0
```

remote-원격 피어, refid-피어가 동기화되는 호스트, st-stratum 번호, t-유형 즉 unicast, multcst, local(- = 알수 없음), poll-초 단위 폴링 간격, reach-도달 가능성 레지스터
* 원격에서 현재 선택된 피어를 나타낸다.
+ 호스트가 동기화에 대한 수락 가능한 피어이지만 수락되지 않았음을 나타냄.
_ 수락 불가능

2.3 HP-UX 환경

최근에는 정보자산에 대한 시간 동기화(타임서버 시간 동기화)하는 방법으로 NTP(Network Time Protocol)을 이용하여 루트 계정에서 시스템의 시각을 현재 시각으로 설정할 수 있다.

1) SERVER 설정 (Time Server)

① /etc/ntp.conf 구성

```
$ vi /etc/ntp.conf
server 0.0.0.0(맨 마지막 줄 서버IP)
```

② Start xntpdDeamon

```
$ vi /etc/rc.config.d/netdaemons
export NTPDATE_SERVER=0.0.0.0    (ntp server IP Address or hostname)
export XNTPD=1 <-------- 0을 1로 변경
```

③ XNTP Deamon시작

```
$ /sbin/init.d/xntpd start      <-------- Deamon시작
```

④ XNTP 확인

```
$ ntpq -crv
status=c011 sync_alarm, sync_unspec, 1 event, event_restart
system="UNIX/HPUX", leap=11, stratum=16, rootdelay=0.00, rootdispersion=0.00, peer=0,
refid=0.0.0.0, reftime=00000000.00000000  Thu, Feb  7 2036 15:28:16.000, poll=4,
clock=c7bba289.c8740000  Fri, Mar 10 2006 16:00:25.783, phase=0.000, freq=0.00, error=0.00
```

* 여기서 'reftime=' 부분이 00이면 아직 server에서 sync 받지 못한 것임. 이 부분이 16진수로 표시되면 time information을 client에게 줄 준비완료.

```
$ ntpq -crv
status=0544 leap_none, sync_local_proto, 4 events, event_peer/strat_chg
system="UNIX/HPUX", leap=00, stratum=4, rootdelay=0.00, rootdispersion=885.01, peer=2116,
```

```
refid=LOCAL(1),  reftime=c7bba37a.1c2c2000  Fri,  Mar  10  2006  16:04:26.110,  poll=6,
clock=c7bba3b1.8ecdb000  Fri, Mar 10 2006 16:05:21.557, phase=0.000, freq=0.00, error=885.01
```

```
$ ntpq -p
   remote           refidst t when poll reach   delay   offset  disp
==============================================================
*LOCAL(1)        LOCAL(1)         3 l   21   64  377    0.00    0.000   10.01
```

* 5분 정도 기다려 이 명령어로 remote부분에 * 표시가 생기면 정상적으로 동작하는 것임.

2) CLIENT 설정

① /etc/ntp.conf에 time server의 IP 설정

```
$ vi /etc/ntp.conf
server 0.0.0.0   {Time Server IP Address 또는 Hostname(/etc/hosts 등록되어 있어야 함)}
```

② 여기에서 주의를 요하는데, clock syncronization 초기화 하는데 있어 ntpdate를 사용하는데 반드시 xntpd daemon이 떠 있으면 않된다.

```
$ ps -ef | grep xntpd
$ /sbin/init.d/xntpd stop
```

* Daemon 떠 있으면 종료한다. 또한 종료되지 않을 경우 Kill 죽인다.(kill -9 사용)

```
$ ntpdate <ip address>
```

③ xntpd시작

```
$ vi /etc/rc.config.d/netdaemons
---------- 생략 ----------
export NTPDATE_SERVER=0.0.0.0   (ntp server IP or hostname)
export XNTPD=1 (0을 1로변경)
$ /sbin/init.d/xntpd start (Deamon 시작)
```

④ xntpd 확인

```
$ ntpq -p
```

* 5분 정도 기다려 이 command로 remote부분에 * 표시가 생기면 정상적으로 동작하는 것임.

```
$ ntpq -crv
status=0644 leap_none, sync_ntp, 4 events, event_peer/strat_chg
system="UNIX/HPUX",  leap=00,  stratum=5,  rootdelay=0.18,  rootdispersion=10.70,  peer=46996,
refid=192.168.1.177,  reftime=c7bbba2d.7bee7000  Fri,  Mar  10  2006  17:41:17.484,  poll=6,
clock=c7bbba3b.9a39b000  Fri, Mar 10 2006 17:41:31.602, phase=-0.234, freq=-28.50, error=0.26
```

**server 가 database server 인 경우 시간을 되돌리기는 큰문제를 일으킬 수 있습니다. 따라서 ntp 사용시 time backward 를 disable 하는 기능이 있다. -x option을 사용하여 이 기능을 사용할 수 있다.

```
$ vi /etc/rc.config.d/netdaemons
export NTPDATE_SERVER=ntp server IP or hostname
export XNTPD=1
export XNTPD_ARGS=-x  =>-x option 추가

$ /sbin/init.d/xntpd stop
```

```
$ /sbin/init.d/xntpd start
```

* -x option 기능을 사용하면 시간이 되돌려지지는 않고 서서히 clinet쪽 시간을 느리게 하여 시간을 fix 하게 한다.

3) 장애유형

sbin/init.d/xntpd start 명령을 실행하면 xntpd 데몬이 시작되지 않고 다음과 같은 오류가 발생된다.
"socket(AF_INET, SOCK_DGRAM, 0) failed: Too many open files

[해결]
xntpd에 필요한 파일 설명자수는 시스템의 인터페이스 수와 열려 있는 몇 개의 일반 파일에 따라 결정
maxfiles:
==========
xntpd -d -d -d를 실행하면 열려있는 인터페이스 수가 표시된다.
일반 작업의 경우 fd를 10을 더 추가 해야 한다.

기본규칙
maxfiles 60 -> 120 (double it)
나중에 lan 인터페이스를 추가 하는 경우 maxfiles를 늘려야 한다.
nfiles:
========
sar -o temp -v 1 120을 실행하여 nfile이 최대 값에 도달 했는지 확인한다. 그럴 경우 커널 nfile의 크기를 늘린다.
16:54:03 text-szovproc-szovinod-szov file-szov
16:54:04 N/A N/A 103/276 0 0/476 0 355/920 0
^^^^^^^

추가 maxfiles 또는 nfile을 사용하여 새 커널을 만드는 경우 /sbin/init.d/xntpd start를 실행하여 xntpd 데몬을 시작해야 한다.

2.4 AIX 환경

최근에는 정보자산에 대한 시간 동기화(타임서버 시간 동기화)하는 방법으로 NTP(Network Time Protocol)을 이용하여 루트 계정에서 시스템의 시각을 현재 시각으로 설정할 수 있다.

1) NTP 설명

① NTP(Network Time Protocol)는 UDP 포트 123번을 사용
② 이 포트가 Open되어 잇지 않으면 NTP 서버와 동기화할 수 없음.
③ 8~10분 정도가 지난 후 서버와 클라이언트 간에 시간이 동기화 됨.

2) NTP 서버 구성

① 현재 Timezone / 시간 확인

▶ 현재 Timezone이 어떻게 설정 되었는지 확인한다. 하기 결과창에는 CDT 측, 북아메리카 Timezone으로 설정되어 있다.

```
$ date
```

```
Sat Mar 14 01:01:43 CDT 2015
```

▶ 한국에서 일반적으로 "KORST-9" Timezone을 사용하기 때문에 AIX 설치 시 기본적으로 설정되는 "CDT" Timezone을 "KORST-9"로 변경해준 후에 서버 재기동을 해야 한다.

▶ Timezone을 변경하고, 다시 로그인을 하게 되면 Timezone이 KORST로 변경된 것을 확인할 수 있으나, 이는 실제 AIX에 적용된 값이 아닌 변경된 값을 보여 주는 것일 뿐이다. Timezone 변경 후, 반드시 재기동이 필요하다.

```
$ chtz "KORST-9"
```

② NTP Server 설정

▶ /etc/ntp.conf 파일을 하기와 같이 수정한다.
-첫번째로 참조한 Timeserver는 뒤에 prefer를 붙여줌.
-아래 ntp.conf 파일 상에서는 참조한 NTP_Server_IP 뒤에 prefer를 붙여 줬음.
-아래 설정파일을 해석해 보면, NTP_Server_IP를 첫번째로 참조하고, 두번째로 자기 자신의 Local clock을 참조하겠다고 설정한 것이다.

```
$ vi /etc/ntp.conf
#broadcast client
server NTP_server_IP prefer   #NTP Server IP as reference
server 127.127.1.0            #local clock as reference
fudge 127.127.1.0 stratum 0   #values for local clock
driftfile /etc/ntp.drift      #where to keep drift data
tracefile /etc/ntp.trace
```

▶ xntpd daemon 확인

```
$ lssrc -a | grep -i xntpd
Xntpd      tcpip      inoperative
```

▶ ntp 활성화 정보 확인

```
$ ntpq -nq
remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 10.0.0.1         0.0.0.0      3 u    7   64    1    2.884  287.718   0.001
 127.127.1.0   127.127.0.1     16 u    -   64    0    0.000    0.000   0.000
```

③ NTP daemon 시작

동기화 과정에서 NTP Client 측에서 시간이 뒤로 돌아가는 것을 방지하기 위해서, Daemon 시작시, -X option을 준다. (Time backward 방지, 클라이언트 시간 흐름을 조절하여 동기화)

```
$ startsrc -s xntpd -a "-x"
0513-059 The xntpd Subsystem has been started. Subsystem PID is 6946978.
```

④ NTP daemon 확인

▶ xntpd daemon 확인

```
$ lssrc -a | grep -i xntpd
Xntpd        tcpip          inoperative
```

▶ ntp 활성화 정보 확인

```
$ ntpq -nq
remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 10.0.0.1        0.0.0.0      3 u    7   64    1    2.884  287.718   0.001
 127.127.1.0   127.127.0.1    16 u    -   64    0    0.000    0.000   0.000
```

3) NTP 클라이언트 구성

① 현재 Timezone / 시간 확인

▶ Timezone은 NTP Server와 동일하게 맞춰 줌.
▶ xntpd는 Server / Client간 1000초(16분) 이상 차이가 나면 더 이상 동기화 하지 않는다.
▶ NTP Server / Client간 시간을 맞추기 위해, Client단에서 #smitty date 명령어를 통해 16분 이상 차이가 나지 않게 설정해 준다. (권장사항은 NTP Server와 가장 근소한 시간으로 맞추는 것)

② NTP Client 설정

```
$ vi /etc/ntp.conf
#broadcast client
server NTP_server_IP prefer   #NTP Server IP as reference

driftfile /etc/ntp.drift            #where to keep drift data
tracefile /etc/ntp.trace
```

참조하고자 하는 NTP Server IP를 Server 항목에 입력

③ NTP daemon 시작

동기화 과정에서 NTP Client 측에서 시간이 뒤로 돌아가는 것을 방지하기 위해서, Daemon 시작시, -X option을 준다. (Time backward 방지, 클라이언트 시간 흐름을 조절하여 동기화)

```
$ startsrc -s xntpd -a "-x"
0513-059 The xntpd Subsystem has been started. Subsystem PID is 6946978.
```

④ NTP daemon 확인

▶ 대부분의 경우 Reach 값이 377에 다다르면 동기화가 완료된다.
▶ 보통 6~10분 사이에 동기화되며, 바로 시간을 맞추려면 NTP 서버가 active인 상태에서 클라이언트 단에서 "$ ntpdate <ip_of_NTP_Server>" 또는 "setclock <NTP_Server_Hostname>" 명령어를 수행해 주면 된다.
▶ ntpupdate 명령어 수행 후 xntpd daemon을 재기동해 준다.

4) 재기동시에도 NTP 자동실행 설정

① /etc/rc.tcpip 파일 수정

```
start /usr/sbin/xntpd "$src_running" "-x"
```

▶ AIX default 설정 상에는 xntpd이 자동 실행으로 설정이 되어 있지 않음.
▶ /etc/rc.tcpip 파일에서 xntpd와 관련된 라인의 주석을 해제하고 위의 명령어 형태로 수정.

5) 참고사항

xntpd를 이용하여 시간을 동기화 한 후 Time 서버의 시간을 바꾸면 전체 클라이언트의 시간이 바뀐다. Time 서버의 시간을 임시로 바꾸려면 Time 서버 단에서 xntpd를 정지 시킨 후($ stopsrc -s xntpd) 작업한다.

2.5 FreeBSD 환경

최근에는 정보자산에 대한 시간 동기화(타임서버 시간 동기화)하는 방법으로 NTP(Network Time Protocol)을 이용하여 루트 계정에서 시스템의 시각을 현재 시각으로 설정할 수 있다.

NTP를 사용하기 위해서는 기본적으로 NTP 패키지가 반드시 설치되어 있어야 한다. 설치 확인은 다음의 명령어를 실행하여 확인한다. 만약, 설치되어 있지 않으면 "**pkg install ntp**" 명령어로 설치하면 된다.

```
[root]# pkg install ntp
```

ntpd 서비스를 활성화 하기 위해서는 다음 같은 명령어를 사용하여 "/etc/rc.conf"에 등록 해야 한다.

```
[root]# /etc/rc.d/ntpd enabled
```

우리나라에서 운영되고 있는 NTP 서버는 다음과 같다.

```
server kr.pool.ntp.org
server time.bora.net
server time.kornet.net
```

우리나라에서 운영되고 있는 NTP 서버를 ntpd 데몬 설정을 위한 설정 파일인 "**/etc/ntp.conf**"에 다음과 같이 설정한다.

```
[root]# vi /etc/ntp.conf
#
# NTP
#
server kr.pool.ntp.org
server time.bora.net
server time.kornet.net
```

ntpd 데몬 설정을 위한 설정이 끝나면 반드시 NTP 설정이 제대로 추가되었는지 확인한 후 NTP 데몬의 Restart 작업이 반드시 필요하다.

```
[root]# /etc/rc.d/ntpd restart
ntpd not running? (check /var/run/ntpd.pid).
```

```
Starting ntpd.
```

ntpd 시간 확인은 다음과 같은 명령어로 확인할 수 있다.

```
[root]# ntpq -p
remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 0.freebsd.pool. .POOL.          16 p    -   64    0    0.000    0.000   0.000
 106.247.248.106 141.223.182.106  2 u    7   64    1    4.412    0.544   0.000
 time.bora.net   204.123.2.5      2 u    7   64    1    5.206    7.741   0.000
*send.mx.cdnetwo 204.123.2.5      2 u    1   64    1    3.968    3.807   0.446
 211.52.209.148  216.239.35.12    2 u    1   64    1   11.862    2.838   0.259
 dadns.cdnetwork 204.123.2.5      2 u    2   64    1    4.833    0.005   0.408
 92.223.73.5 (st 106.247.248.106  3 u    -   64    1    5.015    1.397   0.482
```

* 표시된 ip 가 현재 시간을 가져오고 있는 ntp 서버임

3. About BaroPAM

Version 1.0 - Official Release - 2016.12.1
Copyright ⓒ Nurit corp. All rights reserved.
http://www.nurit.co.kr

제 조 사 : 주식회사 누리아이티
등록번호 : 258-87-00901
대표이사 : 이종일
이 메 일 : mc529@nurit.co.kr
주 소 : 서울시 강서구 마곡중앙2로 15, 913호(마곡동, 마곡테크노타워2)

조달총판 : 주식회사 루시드네트웍스
등록번호 : 848-86-00615
대표이사 : 박병호
대표전화 : 031-8018-4770(영업문의) / 031-8018-4771(기술지원)
이 메 일 : sales@lucidnet.co.kr
주 소 : 경기도 하남시 미사대로520, CA동 904,905호(덕풍동, 현대지식산업센터 한강미사2차)

공 급 사 : 주식회사 트루인테크놀로지스
등록번호 : 314-86-56237
대표이사 : 손원찬
대표전화 : 010-3404-1156(영업문의) / 080-488-8803(기술지원)
이 메 일 : wcson@truin.kr
주 소 : 대전시 서구 문예로 137, 4층(둔산동, 케이티엔지대전빌딩)

공 급 사 : 주식회사 디에이치솔루션
등록번호 : 606-86-54064
대표이사 : 조동환
대표전화 : 051-323-0705(영업문의) / 070-4632-0869(기술지원)
이 메 일 : sales@dhsolution.kr
주 소 : 부산시 해운대구 센텀동로 71, 벽산e센텀클래스원2차 1105호

공 급 사 : 주식회사 반디데이타
등록번호 : 264-81-49402
대표이사 : 백욱인
대표전화 : 02-864-5653(영업문의, 기술지원)
이 메 일 : bandidata@bandidata.com
주 소 : 서울시 금천구 벚꽃로 278, 1503호(가산동, SJ테크노빌)