

# BaroPAM 가이드(CDP)

## 목차

목차.....	0
1. CDP(Cloudera Data Platform)란?.....	1
2. Linux 사용자로 PAM 인증 구성.....	2
3. BaroPAM 설치 및 설정.....	4
3.1 BaroPAM 설치 전 준비사항.....	4
3.2 BaroPAM 설치 모듈 다운로드.....	5
3.3 BaroPAM 환경 설정 파일 생성.....	6
3.4 NTP(Network Time Protocol) 설정.....	8
4. BaroPAM 구성.....	12
4.1 BaroPAM 구성.....	12
5. Cloudera Manager 접속 테스트.....	13
5.1 신규 사용자 생성.....	13
5.2 BaroPAM 환경 설정 파일 생성.....	13
5.3 Cloudera Manager 접속 테스트.....	15
6. BaroPAM 적용.....	16
6.1 BaroPAM 적용 프로세스.....	16
6.2 BaroPAM 적용 화면.....	16
6.3 본인확인 적용 프로세스.....	17
6.4 본인확인 적용 화면.....	18
6.5 Cloudera Manager 로그인.....	19
7. About BaroPAM.....	21



## 2. Linux 사용자로 PAM 인증 구성

기본적으로 제공되는 Linux 사용자가 Cloudera Manager에 로그인할 수 있도록 PAM 인증을 구성할 수 있다.

### 1. Cloudera Manager Server 호스트를 구성

Cloudera Manager(예: cloudera-scm)를 실행하는 Linux 사용자에게는 시스템 새도우 파일에 대한 읽기 액세스 권한이 있어야 한다.

Cloudera Manager Server 호스트에서 다음 명령을 실행하여 새도우 파일 그룹 권한을 확인한다.

```
$ ls -l /etc/shadow
-r----- 1 root root 1738 Jul 16 17:09 /etc/shadow
```

위의 예에서는 새도우 파일의 루트 그룹이 새도우 그룹이 아닌 소유자 그룹임을 보여준다.

'-r'은 루트 그룹의 사용자가 새도우 파일에 대한 읽기 액세스 권한을 가질 수 있음을 나타낸다.

----- 1 root root 1611 Jul 16 17:09 /etc/shadow와 같은 내용이 표시되면 그룹 읽기 권한이 할당되지 않은 것이다.

다음 명령을 실행하여 파일에 해당 권한을 추가한다.

```
$ chmod g+r /etc/shadow
```

### 2. 소유자 그룹에 사용자를 추가

```
$ usermod -a -G root cloudera-scm
```

소유자 그룹이 새도우 그룹인 경우)

```
$ usermod -a -G shadow cloudera-scm
```

### 3. Cloudera Manager에서 "Administration > Settings > External Authentication"을 클릭

#### 4. 인증 백엔드 순서 속성이 "Database Only."으로 설정되어 있지 않은지 확인

#### 5. 인증 백엔드 순서 속성이 "Database Only."으로 설정되어 있지 않은지 확인 데이터베이스 전용으로 설정하면 외부 그룹 매핑이 작동하지 않는다.

#### 6. 외부 인증 유형(external authentication type)으로 "PAM"을 선택

#### 7. Cloudera Manager에 사용하려는 특정 PAM 구성이 있는 경우 해당 구성 이름으로 PAM 서비스 이름 속성을 수정(/etc/pam.d/에 있는 파일과 일치해야 함).

그렇지 않으면 기본값인 로그인을 사용한다.

#### 8. 변경 사항을 저장.

## 9. 완료되면 Cloudera Manager Server를 다시 시작

```
$ sudo systemctl restart cloudera-scm-server
```

## 10. 테스트

테스트하려면 Linux 사용자로 Cloudera Manager에 로그인하고 호스트 서버 콘솔에서 다음 명령을 실행하여 사용자를 생성하고 사용자에게 그룹을 할당한다.

### 1) 사용자를 생성

```
$ useradd testUser  
$ passwd testUser
```

### 2) 사용자에게 그룹을 할당

```
$ groupadd testGroup  
$ usermod -a -G testGroup testUser
```

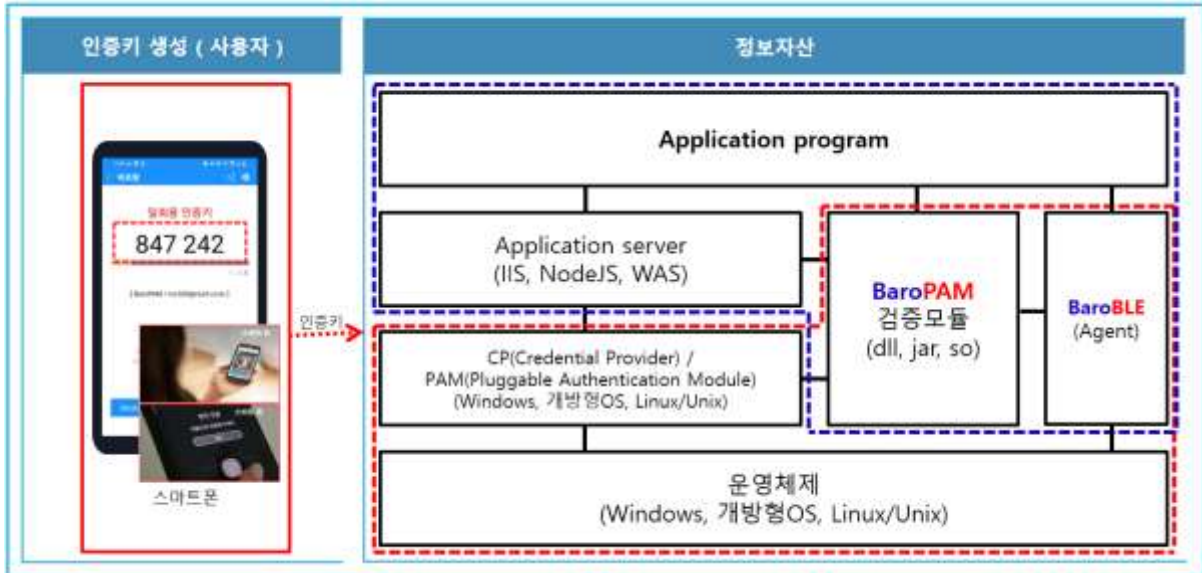
## 11. Cloudera Manager에서 사용자가 속한 그룹에 역할을 매핑

"Administration > Users & Roles > LDAP/PAM Groups"을 클릭한 다음 LDAP/PAM 그룹 매핑 추가를 클릭한다.

이제 방금 생성한 Linux 사용자를 사용하여 Cloudera Manager에 로그인할 수 있다.

### 3. BaroPAM 설치 및 설정

BaroPAM 솔루션은 **제로 트러스트(Zero Trust) 보안 모델**로 정보자산의 보안 강화를 위하여 **2차 인증(추가 인증)**이 필요한 다양한 운영체제와 애플리케이션에 누구나 손쉽게 곧바로 적용할 수 있는 **플러그인 가능한 인증 모듈(PAM, Pluggable Authentication Module) 방식**을 기반으로 하는 보안에 최적화된 **생체인식이 적용된 3단계 인증 솔루션**이다.



#### 3.1 BaroPAM 설치 전 준비사항

PAM 모듈을 사용하기 위해서는 기본적으로 PAM 패키지가 반드시 설치되어 있어야 한다. 설치 확인은 다음의 명령어를 실행하여 확인한다. 만약, 설치되어 있지 않으면 Redhat, CentOS는 "`dnf -y install *pam*`" 그외는 "`sudo apt-get install pam`" 명령어로 설치하면 된다.

```
[root]# rpm -qa | grep pam
pam_smb-1.1.7-7.2.1
pam_passwdqc-1.0.2-1.2.2
pam-0.99.6.2-14.el5_11
pam_krb5-2.2.14-22.el5
pam-devel-0.99.6.2-14.el5_11
pam_ccreds-3-5
pam_smb-1.1.7-7.2.1
pam_pkcs11-0.5.3-26.el5
pam-devel-0.99.6.2-14.el5_11
pam_passwdqc-1.0.2-1.2.2
pam-0.99.6.2-14.el5_11
pam_ccreds-3-5
pam_krb5-2.2.14-22.el5
pam_pkcs11-0.5.3-26.el5
```

Redhat, CentOS인 경우 "Selinux"는 "Security Enhanced Linux"의 약자로 기본의 리눅스보다 더욱 뛰어난 보안정책을 제공하는데, 너무 뛰어난 나머지 활성화 되어 있을 경우 보안문제로 막혀서 BaroPAM이 안되는 부분이 발생(Failed to open tmp secret file "/usr/baropam/.baro\_auth~" [Permission denied])한다. 그

래서 웬만하면 대부분이 비활성화(SELinux=enforcing → disabled)한다.

```
[root] /etc > vi /etc/sysconfig/selinux
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - SELinux is fully disabled.
SELINUX=disabled
# SELINUXTYPE= type of policy in use. Possible values are:
#     targeted - Only targeted network daemons are protected.
#     strict - Full SELinux protection.
SELINUXTYPE=targeted

# SETLOCALDEFS= Check local definition changes
SETLOCALDEFS=0
```

바로 적용은 되지 않으며 재부팅을 해야 적용이 된다.

재부팅을 하지 않고 현재 접속된 터미널에 한해 변경된 내용을 적용하고 싶을 경우 다음의 명령어를 실행하면 된다.

```
[root] /etc > /usr/sbin/setenforce 0
```

CentOS 7/8 인스턴스에 IPv4 전달이 활성화하기 위하여 다음과 같이 설정한다.

```
[root] /etc > vi /etc/sysctl.conf
net.ipv4.ip_forward=1
```

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 777 /usr/baropam
```

## 3.2 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-x.x.tar
```

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

```
[root] /usr/baropam > tar -xvf libpam_baro_auth-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 8 3월 24 2021 .baro_acl
-r--r--r-- 1 root root 305 7월 2 14:41 .baro_auth
-r--r--r-- 1 root root 290 6월 30 12:55 .baro_curl
-rwxr-xr-x 1 root root 69149 4월 6 19:12 baro_auth
-rwxr-xr-x 1 root root 65072 6월 29 16:36 baro_curl
drwxr-xr-x 2 root root 4096 7월 20 2021 jilee
-rwxr-xr-x 1 root root 152649 6월 9 08:19 pam_baro_auth.so
-rwxr-xr-x 1 root root 116158 6월 30 12:54 pam_baro_curl.so
-rw-r--r-- 1 root root 150 6월 29 16:29 setcurl.sh
-rw-r--r-- 1 root root 221 6월 27 15:59 setenv.sh
```

### 3.3 BaroPAM 환경 설정 파일 생성

BaroPAM 환경 설정 파일은 **baro\_auth** 프로그램을 실행하여 반드시 생성하는데, BaroPAM 인증 모듈의 디렉토리인 **/usr/baropam** 밑에 위치하도록 한다.

형식)

```
baro_auth -r rate_limit -R rate_time -t cycle_time -k key_method -e encrypt_flag -H hostname -A
acl_type -a acl_filename -S secure_key -s filename
```

BaroPAM 환경설정 파일의 설정 옵션에 대한 내용은 다음과 같다.

옵션	설명	설정값	비고
-r	일회용 인증키의 제한횟수(1~10)	3	
-R	일회용 인증키의 제한시간(초, 15~600초)	30	
-t	일회용 인증키의 인증주기(초, 3~60초)	30	
-k	일회용 인증키의 인증방식(app1, app256, app384, app512).	app512	
-e	환경설정 파일의 암호화 여부(yes or no)	no	
-H	서버의 호스트명(uname -n)	nur it.co.kr	
-A	2차 인증에서 허용(allow) 또는 제외(deny)할지 선택	deny	
-a	2차 인증에서 허용(allow) 또는 제외(deny)할 계정에 대한 ACL 파일명(파일 접근권한은 444)	/usr/baropam/.baro_acl	
-S	벤더에서 제공하는 Secure key(라이선스 키)를 사용해야 하는데, Cloudera Data Platform 특성상 사용자별 폰번호로 대체.	01012341234	
-s	BaroPAM 환경설정 파일을 생성할 디렉토리를 포함한 파일명	/usr/baropam/.baro_auth	

주의) -s 옵션의 filename은 BaroPAM 환경설정 파일을 생성할 디렉토리를 포함한 파일명(파일 접근권한은 444)이며, 설정한 서버의 호스트명(hostname)이 맞지 않는 경우 BaroPAM이 정상적으로 작동되지 않을 수 있으니, 호스트명(hostname)가 변경되는 경우 반드시 환경 설정의 해당 항목에 반영해야 한다.

```
[root] /usr/baropam > ./baro_auth -r 3 -R 30 -t 30 -k app512 -e no -H nur it.co.kr -A deny -a
~/baro_acl -S 01012341234 -s /usr/baropam/.baro_auth
```

1) Your emergency one-time authentication keys are :

**응급 일회용 인증키**는 **일회용 인증키** 생성기인 **BaroPAM** 앱을 사용할 수 없을 때 분실한 경우를 대비하여 SSH 서버에 다시 액세스하는데 사용할 수 있는 접속이 가능한 Super 인증키 이므로 어딘가에 적어 두는 것이 좋다.

2) 다음에 나오는 물음에 대해서는 모두 "y"를 입력한다.

"/usr/baropam/.baro\_auth" 파일을 업데이트하시겠습니까 (y/n) **y**  
 중간자(man-in-the-middle) 공격을 예방할 것인가 (y/n) **y**

**BaroPAM** 환경 설정 파일인 **.baro\_auth**에 설정한 내용은 다음과 같다.

```
[root] /usr/baropam > cat .baro_auth
" AUTH_KEY
" RATE_LIMIT 3 30
" KEY_METHOD app512
" CYCLE_TIME 30
" SECURE_KEY 01012341234
" ACL_NAME /usr/baropam/.baro_acl
" ACL_TYPE deny
" HOSTNAME nurit.co.kr
" DISALLOW_REUSE
33458936
19035576
15364353
54649370
84342192
```

**BaroPAM** 환경설정 파일인 **.baro\_auth**의 설정 항목에 대한 내용은 다음과 같다.

항목	설명	설정값	비고
AUTH_KEY	인증 구분자(고정)		
RATE_LIMIT	<b>일회용 인증키</b> 의 제한횟수(1~10), 제한시간(초, 15~600초)	3 30	
KEY_METHOD	<b>일회용 인증키</b> 의 인증방식(app1, app256, app384, app512)	app512	
CYCLE_TIME	<b>일회용 인증키</b> 의 인증주기(초, 3~60초)	30	
SECURE_KEY	벤더에서 제공하는 Secure key(라이선스 키)를 사용해야 하는데, Cloudera Data Platform 특성상 사용자별 폰번호로 대체.	01012341234	
HOSTNAME	서버의 호스트명(uname -n)	nurit.co.kr	
ACL_TYPE	<b>2차 인증</b> 에서 허용(allow) 또는 제외(deny) 구분	deny	
ACL_NAME	<b>2차 인증</b> 에서 허용 또는 제외할 계정에 대한 ACL Filename( <b>파일 접근권한은 444</b> )	/usr/baropam/.baro_acl	
DISALLOW_REUSE or ALLOW_REUSE	중간자(man-in-the-middle) 공격을 예방할 경우는 "DISALLOW_REUSE"을 설정한 경우 <b>일회용 인증키</b> 의 인증주기 동안은 다른 사용자가 로그인 할 수 없으며, 만약 허용할 경우는 "ALLOW_REUSE"을 설정한다.	DISALLOW_REUSE	

**BaroPAM** 모듈 사용 시 **2차 인증**에서 제외할 계정에 대한 ACL에 제외해야 하는 경우 **BaroPAM** 환경 설정 시 설정한 디렉토리에 ACL(Access Control List) 파일을 생성한 후 제외할 계정을 다음과 같이 입력한다. (.baro\_acl에 대한 파일 접근권한을 444로 설정해야 한다.)

```
[root] /usr/baropam > vi .baro_acl
barokey
baropam
```

### 3.4 NTP(Network Time Protocol) 설정

BaroPAM은 시간 동기화 방식이므로 서버의 시간이 현재 시간과 다를 경우 **일회용 인증키**가 서로 일치하지 않아서 서버에 로그인을 못하는 경우가 발생할 수 있다.

최근에는 정보자산에 대한 시간 동기화(타임서버 시간 동기화)하는 방법으로 NTP(Network Time Protocol)을 이용하여 **root** 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 Redhat, CentOS 8 이하 버전은 "yum install ntp" 그외는 "sudo apt-get 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 level에 off(해제) 가 되어 있으면 자동 활성화되지 않는다. 자동 활성화하기 위해서는 3, 5에 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
```

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 iburst
```

```
server time.bora.net iburst
```

**iburst** 옵션은 일종의 옵션 설정으로써 동기화 하는데 걸리는 시간을 짧게 줄여주는 옵션임.

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 버전은 "yum install chrony" 명령어로 설치하면 된다.

```
[root]# 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]# 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

# 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]# sudo systemctl enable chronyd
[root]# sudo systemctl restart chronyd
```

ntpd 시간 확인은 다음과 같은 명령어로 확인할 수 있다.

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

```
[root]# 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 받아오는 서버 정보)

```
[root]# chronyc tracking
Reference ID      : 36B48651 (ec2-54-180-134-81.ap-northeast-2.compute.amazonaws)
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]# 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
```

## 4. BaroPAM 구성

### 4.1 BaroPAM 구성

Cloudera Data Platform 특성상 사용자별 계정마다 BaroPAM 환경 설정파일을 각각 설정하기 위하여 BaroPAM 환경 설정파일전용 디렉토리(/usr/baropam/cloudera)를 다음과 같이 생성한다.

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

BaroPAM 환경 설정파일전용 디렉토리(/usr/baropam/cloudera)의 권한(읽기, 쓰기)을 다음과 같이 부여한다.

```
[root]# chmod -R 755 /usr/baropam/cloudera
```

Cloudera Data Platform 특성상 사용자별 계정마다 BaroPAM 환경 설정파일을 각각 설정하는 경우 BaroPAM 모듈을 설정하기 위해서 /etc/pam.d/login 파일에 설정하는 방법은 다음과 같이 최 상단에 입력해 준다.

```
[root] /usr/baropam > vi /etc/pam.d/login
#%PAM-1.0
auth    required /usr/baropam/pam_baro_auth.so forward_pass
secret=/usr/baropam/cloudera/.$USER_auth encrypt=no
```

참고로 secret 파라미터는 BaroPAM 환경설정 파일명, encrypt 파라미터는 BaroPAM 환경설정 파일의 암호화 플래그(yes or no)를 설정한다.

forward\_pass를 이용하여 암호 입력창(Password:)에 암호와 같이 일회용 인증키를 입력할 경우, 암호를 먼저 입력하고 공백 없이 이어서 일회용 인증키를 입력하면 된다. 예를 들어 암호가 "baropam" 이고 일회용 인증키가 "123456" 이라면 "baropam123456"으로 입력하면 된다.

forward\_pass를 이용하면 인증을 필요로 하는 대부분의 서비스에 2-factor 인증을 가능하게 할 수 있다.

## 5. Cloudera Manager 접속 테스트

### 5.1 신규 사용자 생성

Linux 사용자로 Cloudera Manager에 로그인하고 호스트 서버 콘솔에서 다음 명령을 실행하여 사용자를 생성하고 사용자에게 그룹을 할당한다.

#### 1. 사용자를 생성

```
$ useradd baropam
$ passwd baropam
```

#### 2. 사용자에게 그룹을 할당

```
$ groupadd cloudera
$ usermod -a -G cloudera baropam
```

### 5.2 BaroPAM 환경 설정 파일 생성

사용자의 로그인 정보(로그인-ID, 폰번호) 관련 쉘 스크립트를 실행하기 위하여 BaroPAM 등록 디렉토리 (/usr/baropam/cloudera)로 이동하여 실행한다.

참고) 쉘 스크립트 실행 시 인수나 인수값의 구분은 공백(space)으로 해야 한다.

#### 1) 신규 사용자의 BaroPAM 환경설정 파일을 생성하는 쉘 스크립트 - setuser.sh

```
#!/bin/sh

export LANG=C
ENV_HOME=/usr/baropam/radius;
ACC_HOME=/home/$1

userdel -rf $1
Wrm ${ENV_HOME}/.$1_auth

useradd -d ${ACC_HOME} -m -s /bin/bash $1
echo $2 | passwd -stdin $1

groupadd cloudera
usermod -a -G cloudera $1

Wcp ${ENV_HOME}/.baro_auth ${ENV_HOME}/.$1_auth

sed -i "s/01012341234/$3/g" ${ENV_HOME}/.$1_auth
```

신규 사용자(로그인-ID)의 BaroPAM의 환경 설정 파일을 생성하는 쉘 스크립트(setuser.sh) 실행 시 파라미

터는 다음과 같다.

사용자(로그인-ID)를 생성하는 쉘 스크립트(setuser.sh) 실행 시 파라미터.

\$1 : 생성할 로그인-ID

\$2 : 로그인-ID의 비밀번호

\$3 : 로그인-ID의 폰번호

```
[root]# sh setuser.sh baropam !@nurit# 01027714076
```

## 2) 사용자(로그인-ID)의 비밀번호를 변경하는 쉘 스크립트 - setpasswd.sh

```
#!/bin/sh
```

```
export LANG=C
```

```
echo $2 | passwd -stdin $1
```

사용자(로그인-ID)의 비밀번호를 변경하는 쉘 스크립트(setpasswd.sh) 실행 시 파라미터는 다음과 같다.

\$1 : 로그인-ID

\$2 : 변경할 비밀번호

```
[root]# sh setpasswd.sh baropam !@Baropam#
```

## 3) 사용자(로그인-ID)의 폰번호를 변경하는 쉘 스크립트 - setphone.sh

```
#!/bin/sh
```

```
export LANG=C
```

```
ENV_HOME=/usr/baropam/cloudera;
```

```
sed -i "s/$2/$3/g" ${ENV_HOME}/.$1_auth
```

사용자(로그인-ID)의 폰번호를 BaroPAM의 환경 설정 파일에서 변경하는 쉘 스크립트(setphone.sh) 실행 시 파라미터는 다음과 같다.

\$1 : 로그인-ID

\$2 : 변경전 폰번호

\$3 : 변경후 폰번호

```
[root]# sh setphone.sh baropam 01012341234 01027714076
```

## 4) 사용자(로그인-ID)의 비밀번호와 폰번호를 변경하는 쉘 스크립트 - chgpaswd.sh

```
#!/bin/sh
```

```
export LANG=C
```

```
echo $2 | passwd -stdin $1
```

```
sed -i "s/$3/$4/g" ${ENV_HOME}/.$1_auth
```

사용자(로그인-ID)의 비밀번호와 BaroPAM의 환경 설정 파일에서 폰번호를 변경하는 쉘 스크립트(setpasswd.sh) 실행 시 파라미터는 다음과 같다.

\$1 : 로그인-ID

\$2 : 변경할 비밀번호

\$3 : 변경전 폰번호  
 \$4 : 변경후 폰번호

```
[root]# sh chpasswd.sh baropam !@Baropam# 01012341234 01027714076
```

5) 사용자(로그인-ID)를 삭제하는 쉘 스크립트 - deluser.sh

```
#!/bin/sh

export LANG=C
ENV_HOME=/usr/baropam/cloudera;
ACC_HOME=/home/$1

userdel -rf $1
Wrm ${ENV_HOME}/.$1_auth
```

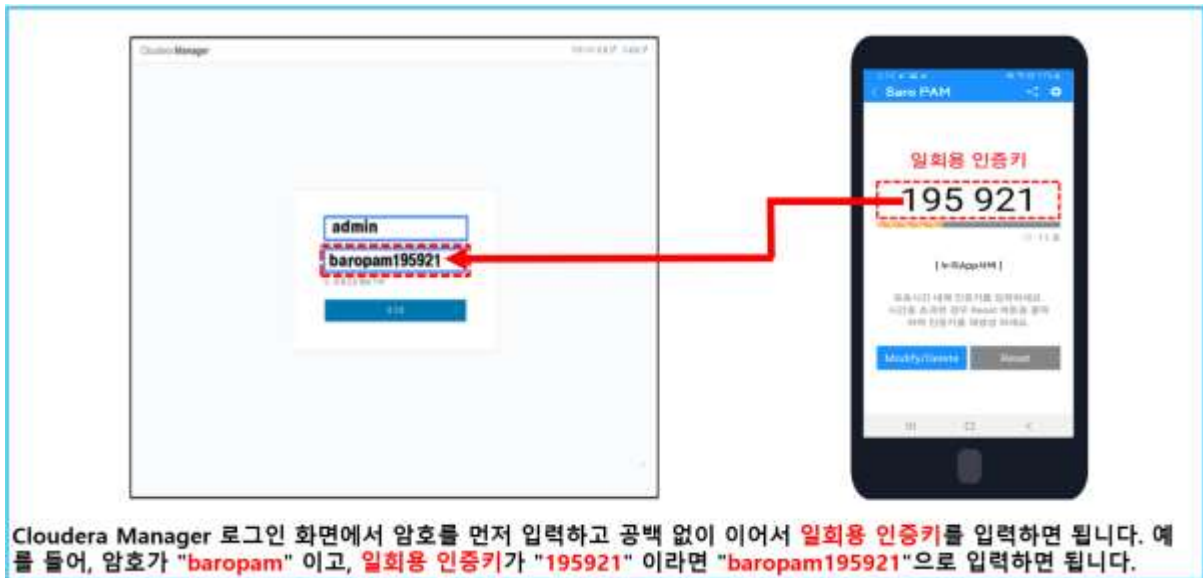
사용자(로그인-ID)를 삭제하는 쉘 스크립트(deluser.sh) 실행 시 파라미터는 다음과 같다.  
 \$1 : 삭제할 로그인-ID

```
[root]# sh deluser.sh baropam
```

5.3 Cloudera Manager 접속 테스트

Cloudera Data Platform의 Cloudera Manager에서 사용자, 암호, 검증 코드를 묻는다. 사용자는 "admin"이고 비밀번호는 위에서 임의로 생성되어 사용자에게 전송된 비밀번호와 검증코드에 BaroPAM 인증 코드를 추가하여 생성할 수 있는 인증 토큰이다. 따라서 암호가 "baropam"이고, BaroPAM 앱에서 생성한 인증 코드인 "195921"이라면 비밀번호 프롬프트에 "baropam195921"을 입력하면 된다.

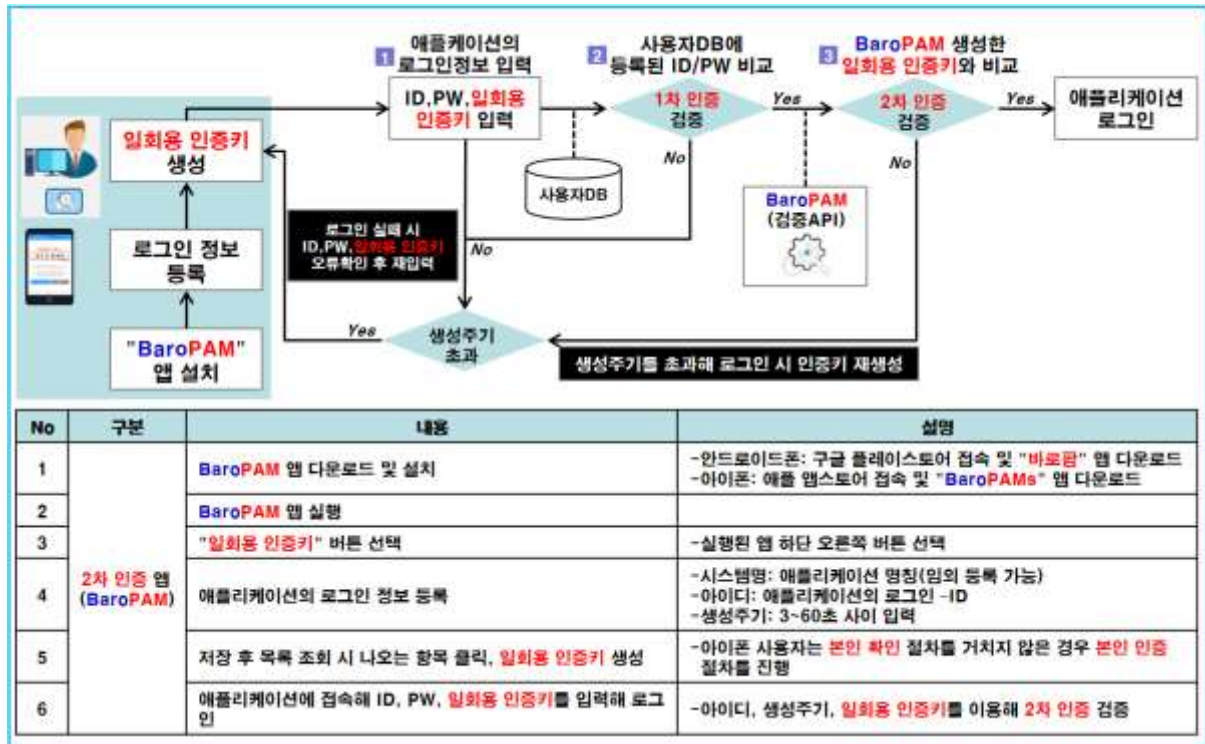
모든 것이 올바르게 작동하면 다음과 같이 표시된다.



## 6. BaroPAM 적용

### 6.1 BaroPAM 적용 프로세스

Cloudera Manager의 로그인 화면에서 Verification code의 "요청값"란에 "BaroPAM" 앱에서 생성한 일회용 인증키를 입력하기 위한 적용 절차는 다음과 같다.



### 6.2 BaroPAM 적용 화면

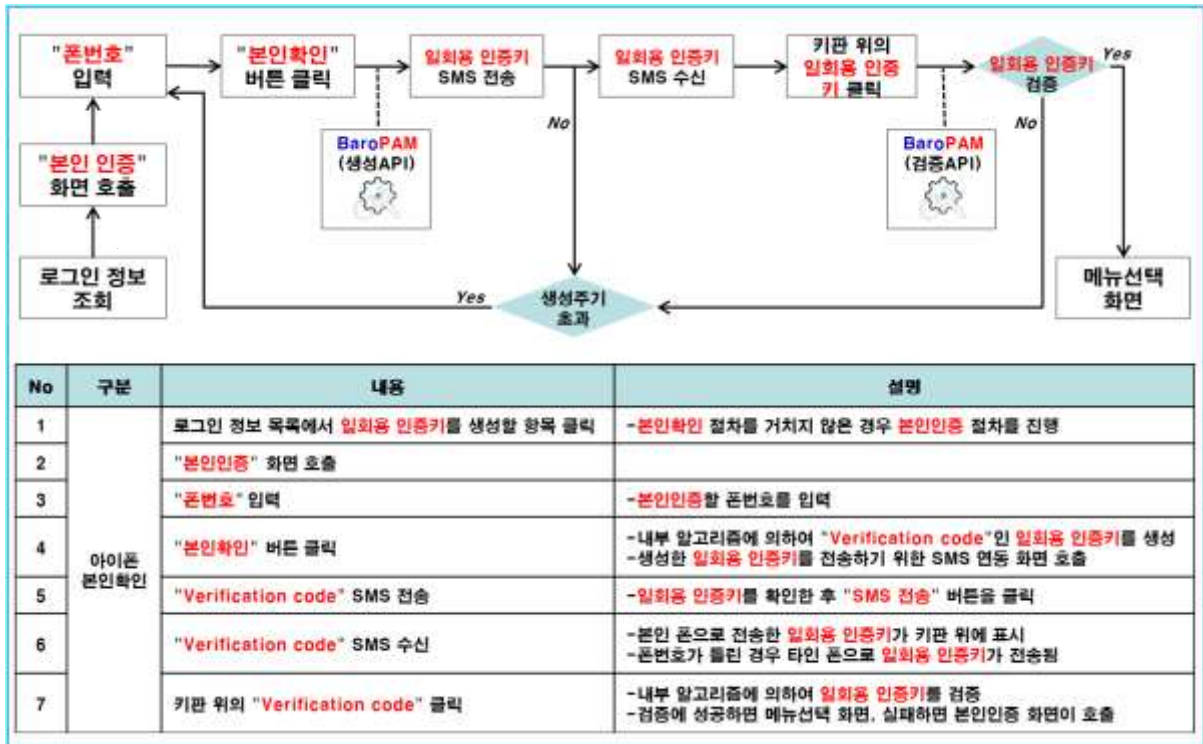
Cloudera Manager의 로그인 화면에서 Verification code의 "요청값"란에 "BaroPAM" 앱에서 생성한 일회용 인증키를 입력하기 위한 적용 절차는 다음과 같다.



### 6.3 본인확인 적용 프로세스

아이폰(iPhone)의 기기정보를 얻지 못해서 **2차 인증키(일회용 인증키)**를 생성하기 위해서 로그인 정보 항목을 선택했을 때 "**일회용 인증키**" 생성 화면으로 이동하지 않은 경우가 발생할 수 있다.

또한, 타인의 전화번호를 부정으로 사용하지 못하도록 하기 위해서 별도의 본인확인 기능을 적용할 필요가 있는데, "**BaroPAM**" 앱에서는 자체 알고리즘을 적용하여 자체적으로 본인확인 절차를 실행하고 있다.



### 6.4 본인확인 적용 화면

아이폰(iPhone)의 기기정보를 얻지 못해서 2차 인증키(일회용 인증키)를 생성하기 위해서 로그인 정보 항목을 선택했을 때 "일회용 인증키" 생성 화면으로 이동하지 않은 경우가 발생할 수 있다.

또한, 타인의 폰번호를 부정으로 사용하지 못하도록 하기 위해서 별도의 본인확인 기능을 적용할 필요가 있는데, "BaroPAM" 앱에서는 자체 알고리즘을 적용하여 자체적으로 본인확인 절차를 실행하고 있다.



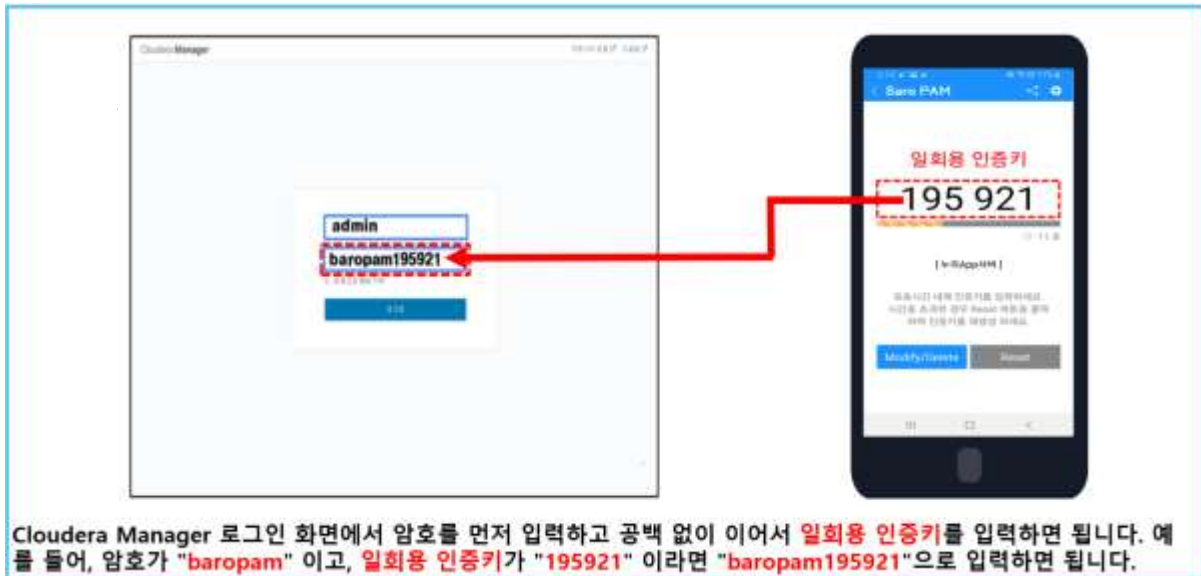
참고) SMS로 전송한 OTA key가 수신은 되었는데 키판 위에 표시되지 않거나 SMS로 전송한 OTA key가 수신되지 않은 경우



아이폰의 "암호 자동 완성 기능"이 설정되지 않아서 발생한다. "BaroPAM" 앱을 설치한 후 iOS12 부터는 더욱 편리한 암호 자동 완성 기능을 반드시 설정해야 한다. (아이폰의 "설정" -> "암호" -> "암호 자동 완성" -> "허용")

### 6.5 Cloudera Manager 로그인

Cloudera Data Platform의 보안 강화를 위하여 Cloudera Manager 로그인 화면에서 "사용자"를 입력하고, 암호가 "baropam"이고, BaroPAM 앱에서 생성한 인증 코드인 "613045"이라면 비밀번호 프롬프트에 "baropam613045"을 입력한 후 하단의 "로그인" 버튼을 클릭한다.



## 7. 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  
대표전화 : 02-2665-0119(영업문의/기술지원)  
이 메 일 : mc529@nurit.co.kr  
주 소 : 서울시 강서구 마곡중앙2로 15, 913호(마곡동, 마곡테크노타워2)