

BaroPAM 가이드(AIX)

목차

목차.....	0
1. BaroPAM 설치.....	1
1.1 BaroPAM 설치 전 준비사항.....	1
1.2 BaroPAM 설치 모듈 다운로드.....	2
1.3 BaroPAM 환경 설정 파일 생성.....	3
1.4 BaroPAM 환경 설정.....	4
1.5 NTP(Network Time Protocol) 설정.....	7
2. BaroPAM 적용.....	11
2.1 BaroPAM 적용 프로세스.....	11
2.2 BaroPAM 적용 화면.....	11
2.3 AIX 로그인 방법.....	12
2.4 ssh/sftp 접속 틀.....	13
3. BaroPAM 제거.....	19
3.1 BaroPAM 환경 제거.....	19
4. BaroPAM FAQ.....	20
5. About BaroPAM.....	24

1. BaroPAM 설치

1.1 BaroPAM 설치 전 준비사항

PAM 모듈을 사용하기 위해서는 기본적으로 PAM 패키지가 반드시 설치되어 있어야 한다. 설치 확인은 다음의 명령어를 실행하여 확인한다.

```
[root] /root > ls /usr/lib/security
32          pam_authok_check.so      pam_krb5_keytab.so.1    pam_tty_tickets.so
64          pam_authok_check.so.1  pam_krb5_migrate.so    pam_tty_tickets.so.1
amd64      pam_authok_common      pam_krb5_migrate.so.1  pam_unix_account.so
audit_binfile.so      pam_authok_get.so      pam_krb5_only          pam_unix_account.so.1
audit_binfile.so.1   pam_authok_get.so.1   pam_krb5_optional     pam_unix_auth.so
audit_remote.so      pam_authok_store.so   pam_ldap.so           pam_unix_auth.so.1
audit_remote.so.1    pam_authok_store.so.1 pam_ldap.so.1         pam_unix_cred.so
audit_syslog.so      pam_deny.so           pam_list.so           pam_unix_cred.so.1
audit_syslog.so.1    pam_deny.so.1        pam_list.so.1         pam_unix_session.so
crypt_bsdbf.so       pam_dhkeys.so        pam_passwd_auth.so    pam_unix_session.so.1
crypt_bsdbf.so.1     pam_dhkeys.so.1      pam_passwd_auth.so.1  pam_user_policy.so
crypt_bsmd5.so       pam_dial_auth.so     pam_rhosts_auth.so    pam_user_policy.so.1
crypt_bsmd5.so.1     pam_dial_auth.so.1   pam_rhosts_auth.so.1  pam_zfs_key.so
crypt_sha256.so      pam_gss_s4u          pam_roles.so          pam_zfs_key.so.1
crypt_sha256.so.1    pam_gss_s4u.so       pam_roles.so.1        pkcs11_kernel.so
crypt_sha512.so      pam_gss_s4u.so.1     pam_sample.so         pkcs11_kernel.so.1
crypt_sha512.so.1    pam_krb5.so          pam_sample.so.1       pkcs11_softtoken.so
crypt_sunmd5.so      pam_krb5.so.1        pam_smbfs_login.so    pkcs11_softtoken.so.1
crypt_sunmd5.so.1    pam_krb5_first       pam_smbfs_login.so.1  pkcs11_tpm.so
pam_allow.so        pam_krb5_keytab      pam_tsol_account.so   pkcs11_tpm.so.1
pam_allow.so.1      pam_krb5_keytab.so   pam_tsol_account.so.1
```

정보자산에 접속하여 PAM 모듈을 사용하기 위해서는 신뢰성 있고 안전한 ssh, sftp 서비스를 제공하기 위하여 OpenSSH(Open Secure Shell) 패키지가 반드시 설치되어 있어야 한다. 설치 확인은 다음의 명령어를 실행하여 확인한다. 만약, 설치되어 있지 않으면 "installp -ac -Y -d .openssh.base openssl.base openssl.man.en_US openssh.man.en_US" 명령어로 설치하면 된다.

```
[root] /root > ssh -V or ls|pp -i openssh.base.server
Sun_SSH_2.2, SSH protocols 1.5/2.0, OpenSSL 0x1000110f
```

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
```

1.2 BaroPAM 설치 모듈 다운로드

설치하고 하는 AIX 시스템의 운영체제에 대한 이름 또는 시스템 정보, 커널 정보를 확인하기 위하여 root 계정으로 접속한 후 다음과 같은 명령어를 실행한다.

```
[root] /usr/baropam > uname -a
AIX aix 1 7 000CE03CD600
```

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
-rwxr-xr-x 1 root root 69149 4월 6 19:12 baro_auth
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
-rw-r--r-- 1 root root 221 6월 27 15:59 setauth.sh
```

PAM에 사용되는 Library는 /usr/lib/security에 위치하는지, 아니면 Symbolic link(링크를 연결하여 원본 파일을 직접 사용하는 것과 같은 효과를 내는 링크)로 다음과 같이 지정해야 적용할 수 있다.

```
[root] /usr/baropam > cp pam_baro_auth.so /usr/lib/security
[root] /usr/baropam > chown root:security /usr/lib/security/pam_baro_auth.so
또는
[root] /usr/baropam > ln -s /usr/baropam/pam_baro_auth.so /usr/lib/security/pam_baro_auth.so
[root] /usr/baropam > chown root:security /usr/lib/security/pam_baro_auth.so
```

Permission denied (publickey,keyboard-interactive).

생성한 BaroPAM 인증 모듈이 시스템에 맞는 모듈인지 다음과 같은 명령어를 실행하여 확인한다.

```
[root] /usr/baropam > file pam_baro_auth.so
pam_baro_auth.so: executable (RISC System/6000) or object module not stripped

[root] /usr/baropam > ldd pam_baro_auth.so
pam_baro_auth.so needs:
/opt/freeware/lib/libgcc_s.a(shr.o)
/usr/lib/libc.a(shr.o)
/usr/lib/libpam.a(shr.o)
/usr/lib/libcrypto.a(libcrypto.so)
```

```

/unix
/usr/lib/libcrypt.a(shr.o)
/usr/lib/libm.a(shr.o)
/usr/lib/libpthread.a(shr_xpg5.o)
/usr/lib/libm.a(shr.o)
/usr/lib/libodm.a(shr.o)
/usr/lib/libpthread.a(shr_comm.o)
    
```

1.3 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 -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) 설정	3	
-R	일회용 인증키의 제한시간(초, 15~600초) 설정.	30	
-t	일회용 인증키의 인증주기(초, 3~60초)	30	
-k	일회용 인증키의 인증방식(app1, app256, app384, app512: 앱)	app512	
-e	환경설정 파일의 암호화 여부(yes or no)	no	
-A	2차 인증에서 허용(allow) 또는 제외(deny) 구분	deny	
-a	2차 인증에서 허용 또는 제외할 계정에 대한 ACL 파일명(파일 접근권한은 444)	/usr/baropam/.baro_acl	
-S	Secure key(라이선스 키)	j l q l c h b V q d p j 7 b 4 P z B p M 2 D i l e B v m H F V /	
-s	BaroPAM 환경설정 파일을 생성할 디렉토리를 포함한 파일명	/usr/baropam/.baro_auth	

주의) -s 옵션의 filename는 BaroPAM 환경설정 파일을 생성할 디렉토리를 포함한 파일명(파일 접근권한은 444)이다.

사용 예)

```

[root] /usr/baropam > ./baro_auth -r 3 -R 30 -t 30 -k app512 -e no -A deny -a
/usr/baropam/.baro_acl -S j l q l c h b V q d p j 7 b 4 P z B p M 2 D i l e B v m H F V / -s /usr/baropam/.baro_auth
    
```

만약, 계정마다 BaroPAM 환경 설정파일을 각각 설정하는 경우 해당 계정으로 접속하여 작업을 진행한다. (Not root)

```

[root] /usr/baropam > ./baro_auth -r 3 -R 30 -t 30 -k app512 -e no -A deny -a ~/.baro_acl -S
j l q l c h b V q d p j 7 b 4 P z B p M 2 D i l e B v m H F V / -s ~/.baro_auth
    
```

1) Your emergency one-time authentication keys are :

응급 일회용 인증키는 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 것

이 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_auth에 설정한 내용은 다음과 같다.

```
[root] /usr/baropam > cat .baro_auth
" AUTH_KEY
" RATE_LIMIT 3 30
" KEY_METHOD app512
" CYCLE_TIME 30
" SECURE_KEY j|q|c|HbVqdpj7b4PzBpM2DilEbvMHFV/
" ACL_NAME /usr/baropam/.baro_acl
" ACL_TYPE deny
" DISALLOW_REUSE
33458936
19035576
15364353
54649370
84342192
```

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

항목	설명	설정값	비고
AUTH_KEY	인증 구분자(고정)		
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)	app512	
CYCLE_TIME	일회용 인증키 의 인증주기(초, 3~60초)	30	
SECURE_KEY	Secure key(라이선스 키)	j q c HbVqdpj7b4PzBpM2DilEbvMHFV/	
ACL_TYPE	2차 인증 에서 허용(allow) 또는 제외(deny) 구분	deny	
ACL_NAME	2차 인증 에서 허용 또는 제외할 계정에 대한 ACL Filename(파일 접근권한은 444)	/usr/baropam/.baro_acl	
DISALLOW_REUSE or ALLOW_REUSE	중간자(man-in-the-middle) 공격을 예방할 경우는 "DISALLOW_REUSE"을 설정한 경우 인증키 인증주기 동안은 다른 사용자가 로그인할 수 없으며, 만약 허용할 경우는 "ALLOW_REUSE"을 설정한다.	DISALLOW_REUSE	

1.4 BaroPAM 환경 설정

BaroPAM 모듈을 설정하기 위해서 sshd 파일에 설정하는 방법은 다음과 같이 최 상단에 입력해 준다.

```
[root] /usr/baropam > vi /etc/pam.conf
#
# Authentication
```

```
#
sshd auth required /usr/lib/security/pam_aix
sshd auth required /usr/lib/security/pam_baro_auth.so nullok secret=/usr/baropam/.baro_auth
encrypt=no
#
# Account Management
#
sshd account required /usr/lib/security/pam_aix
#
# Password Management
#
sshd password required /usr/lib/security/pam_aix
#
# Session Management
#
sshd session required /usr/lib/security/pam_aix
```

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

만약, 계정마다 BaroPAM 환경 설정파일을 각각 설정하는 경우 BaroPAM 모듈을 설정하기 위해서 sshd 파일에 설정하는 방법은 다음과 같이 최 상단에 입력해 준다.

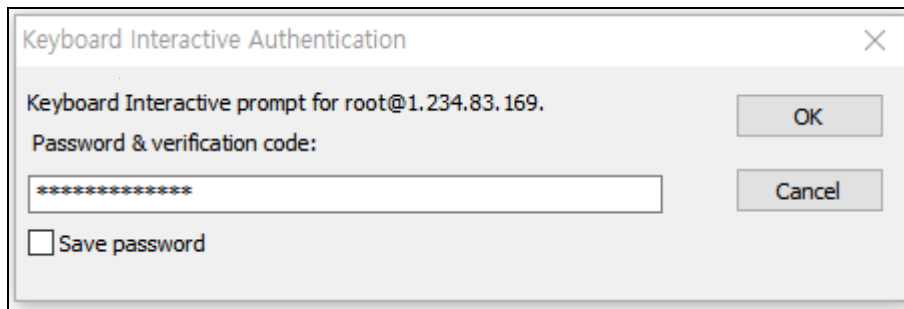
```
[root] /usr/baropam > vi /etc/pam.conf
#
# Authentication
#
sshd auth required /usr/lib/security/pam_aix
sshd auth required /usr/lib/security/pam_baro_auth.so nullok secret=${HOME}/.baro_auth encrypt=no
#
# Account Management
#
sshd account required /usr/lib/security/pam_aix
#
# Password Management
#
sshd password required /usr/lib/security/pam_aix
#
# Session Management
#
sshd session required /usr/lib/security/pam_aix
```

* "nullok"는 호출된 PAM 모듈이 null 값의 암호를 입력하는 것을 허용한다는 의미다.

filezilla처럼 "Interactive process"가 불가능한 프로그램들을 위해서는 PAM에서 **forward_pass** 옵션을 사용하여 암호 입력 시에 암호와 일회용 인증키를 같이 입력하도록 하는 수밖에 없다. 이 경우, openssh client나 Windows의 RDP(Remote Desktop Protocol), VMware Horizon, filezilla 등 모두 이렇게 입력을 하는 수밖에 없다.

```
[root] /usr/baropam > vi /etc/pam.conf
#%PAM-1.0
sshd auth required /usr/lib/security/pam_baro_auth.so forward_pass secret=/usr/baropam/.baro_auth
encrypt=no
```

forward_pass를 이용하여 암호 입력창(Password & verification code:)에 암호와 같이 **일회용 인증키**를 입력할 경우, 암호를 먼저 입력하고 공백 없이 이어서 **일회용 인증키**를 입력하면 된다. 예를 들어 암호가 "baropam" 이고 **일회용 인증키**가 "123456" 이라면 "baropam123456"으로 입력하면 됩니다.



forward_pass를 이용하면 인증을 필요로 하는 대부분의 서비스에 **2-factor 인증**을 가능하게 할 수 있다.

```
[root] /usr/baropam > vi /etc/pam.conf
#%PAM-1.0
su auth required /usr/lib/security/pam_baro_auth.so nullok secret=/usr/baropam/.baro_auth
encrypt=no
```

/etc/pam.conf 파일에 BaroPAM 모듈을 최 상단에 추가하면 "su" 명령어로 일반계정이 "root"로 권한 상승을 시도하는 경우에도 **2차 인증(추가 인증)**을 적용할 수 있어서 보안이 한층 더 향상된다.

```
$ su - root
Verification code:
```

인증 유형을 PAM으로 설정하기 위하여 다음과 같은 명령어를 수행한다.

```
[root] /usr/baropam > chsec -f /etc/security/login.cfg -s usw -a auth_type=PAM_AUTH
```

또는

```
[root] /usr/baropam > vi /etc/security/login.cfg
usw:
shells = /bin/sh,/bin/bsh,/bin/csh,/bin/ksh,/bin/tsh,/bin/ksh93
maxlogins = 32767
logintimeout = 60
maxroles = 8
auth_type = PAM_AUTH
pwd_algorithm = md5
```

sshd 데몬 설정을 위한 설정 파일인 "/etc/ssh/sshd_config" 파일의 내용 중 다음과 같은 인자는 변경이 필요하다.

인자	기존	변경	비고
PasswordAuthentication	yes	no	
ChallengeResponseAuthentication or KbdInteractiveAuthentication	no	yes	
UsePAM	no	yes	

sshd 설정이 끝나면 반드시 PAM 모듈이 제대로 추가되었는지 확인한 후 SSH Server의 Restart 작업이 반드시 필요하다.

```
[root] /usr/baropam > stopsrc -g ssh or stopsrc -s sshd
[root] /usr/baropam > startsrc -g ssh or startsrc -s sshd
```

sshd 설정이 끝나면 반드시 PAM 모듈이 제대로 추가되었는지 확인한 후 ssh 데몬을 재부팅해야 한다.

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

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

1.5 NTP(Network Time Protocol) 설정

정보자산의 시간이 현재 시간과 다를 경우 **일회용 인증키**와 매칭이 되지 않아 **일회용 인증키**가 맞질 않으므로 시간을 같게 시간 동기화 해야 한다.

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 있지 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 설정되었는지 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
logfile /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.

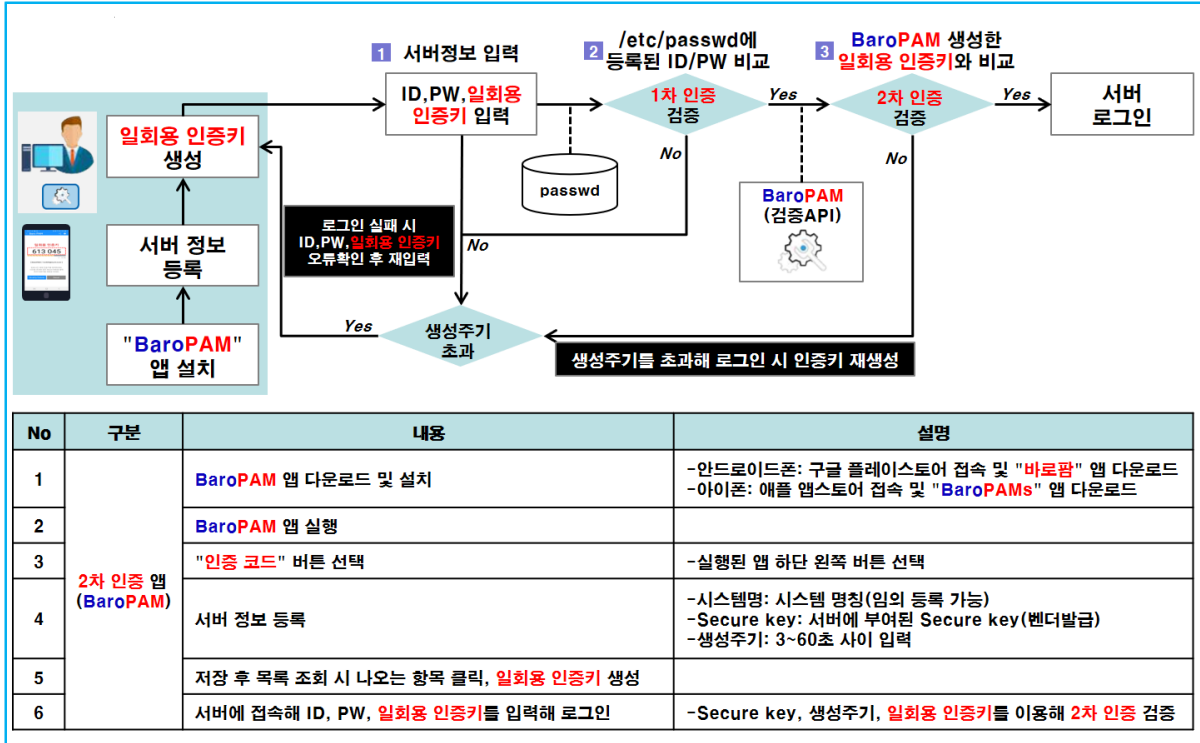
5) 참고사항

xntpd를 이용하여 시간을 동기화 한 후 Time 서버의 시간을 바꾸면 전체 클라이언트의 시간이 바뀐다.

Time 서버의 시간을 임시로 바꾸려면 Time 서버 단에서 xntpd를 정지시킨 후(\$ stopsrc -s xntpd) 작업한다.

2. BaroPAM 적용

2.1 BaroPAM 적용 프로세스

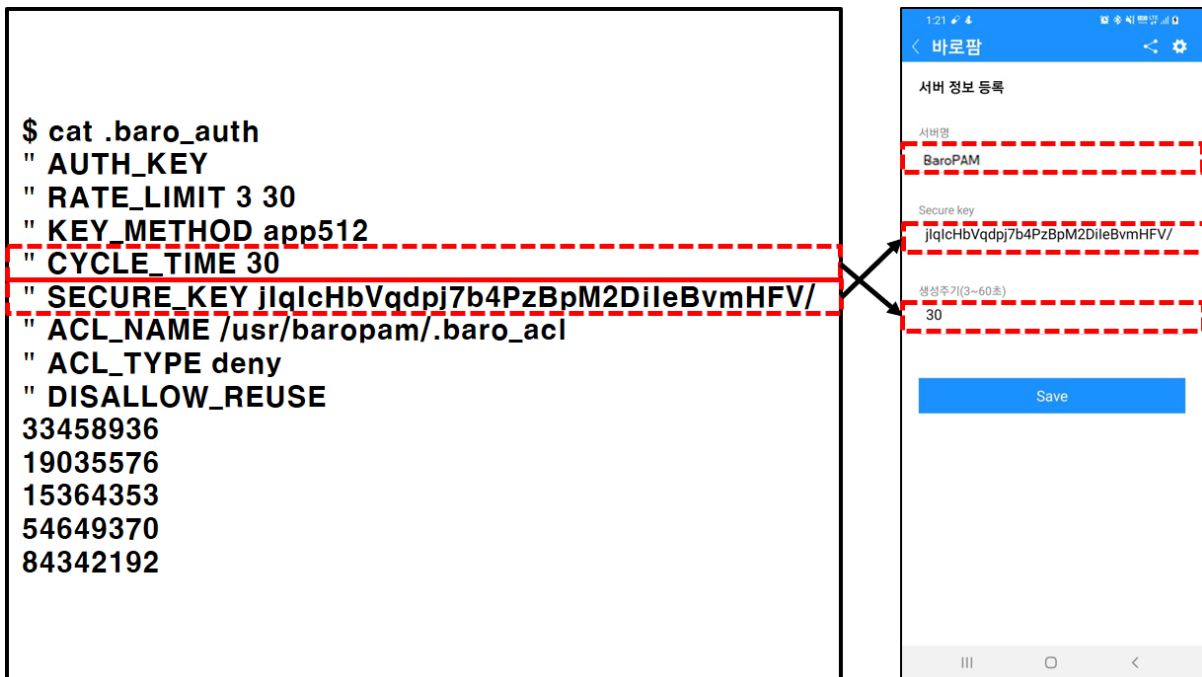


2.2 BaroPAM 적용 화면



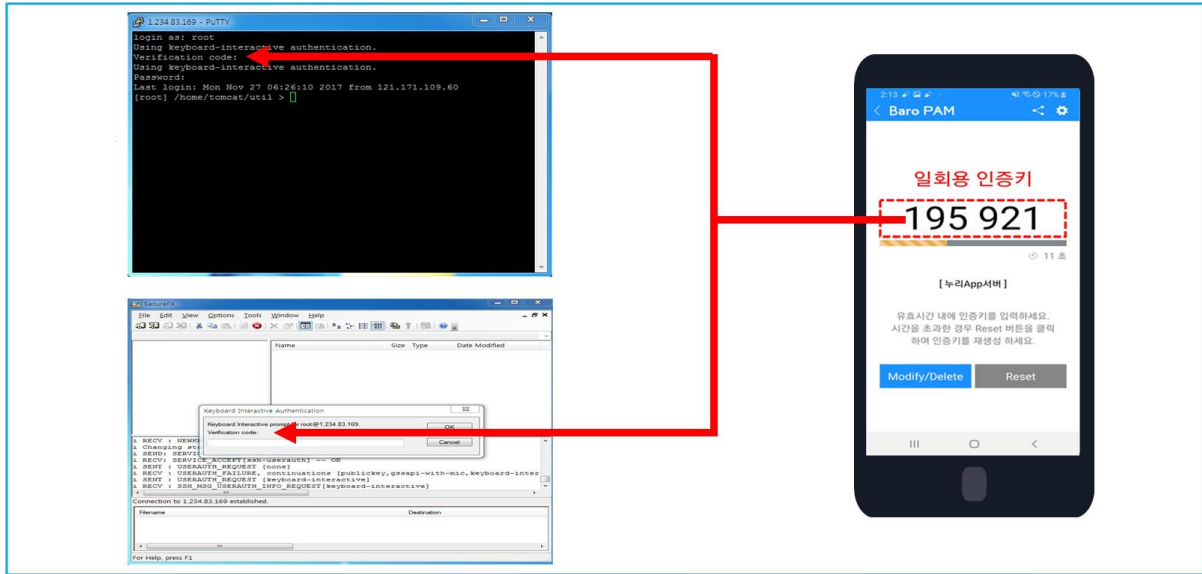
2.3 AIX 로그인 방법

먼저, "BaroPAM Setup" 화면에서 입력한 "인증주기, Secure key, 서버명"을 "BaroPAM" 앱의 "서버 정보 등록" 화면에서 동일하게 입력해야 한다.



AIX 환경에 로그인 시 사용자 계정(Username)을 입력하고, 스마트 폰의 "BaroPAM" 앱에서 일회용 인증키를

생성한 후 "Verification code"에 생성한 **일회용 인증키**와 "Password"를 입력한 후 "Enter" 버튼을 클릭하면 BaroPAM 모듈에 인증을 요청하여 검증이 성공하면 AIX의 로그인 인증 정책이 적용된다.



AIX의 로그인 화면에서 입력한 **일회용 인증키**를 BaroPAM 검증모듈에서 인증에 실패하면 "Access denied." 메시지가 로그인 화면에 나타난다. BaroPAM의 인증과 관련한 각종 메시지는 syslog(/var/log/messages)에 남긴다.

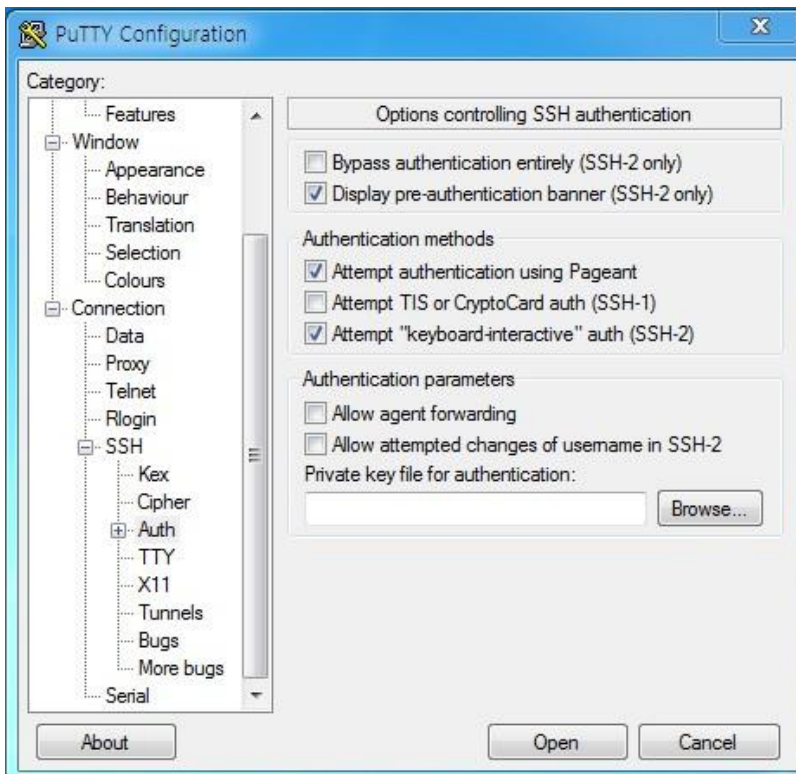
```

Mar 25 11:10:42 qsh-0415 sshd[27482]: pam_unix(sshd:session): session closed for user root
Mar 25 13:52:25 qsh-0415 sshd(pam_baro_auth)[2052]: Try to update RATE_LIMIT line.[3 30 1648183945]
Mar 25 13:52:45 qsh-0415 sshd[2050]: Accepted keyboard-interactive/pam for root from 222.108.117.41 port 49835 ssh2
Mar 25 13:52:45 qsh-0415 sshd[2050]: pam_unix(sshd:session): session opened for user root by (uid=0)
Mar 25 15:25:47 qsh-0415 sshd(pam_baro_auth)[14119]: Try to update RATE_LIMIT line.[3 30 1648189547]
Mar 25 15:25:49 qsh-0415 sshd(pam_baro_auth)[14119]: Verification code generation failed.[Success]
Mar 25 15:25:49 qsh-0415 sshd(pam_baro_auth)[14119]: Invalid verification code
Mar 25 15:25:51 qsh-0415 sshd[14118]: Received disconnect from 222.108.117.41: 13: The user canceled au
    
```

2.4 ssh/sftp 접속 틀

putty인 경우)

Putty로 접속할 때 보통 접속 과정과 동일하게 해주시면 되는데, 하나 설정해 주어야 할 것이 있다. 환경 설정에서 "connection -> SSH -> auth"에서 attempt "Keyboard-Interactive" auth(SSH-2)를 선택한 후 SSH 접속을 하면 된다.

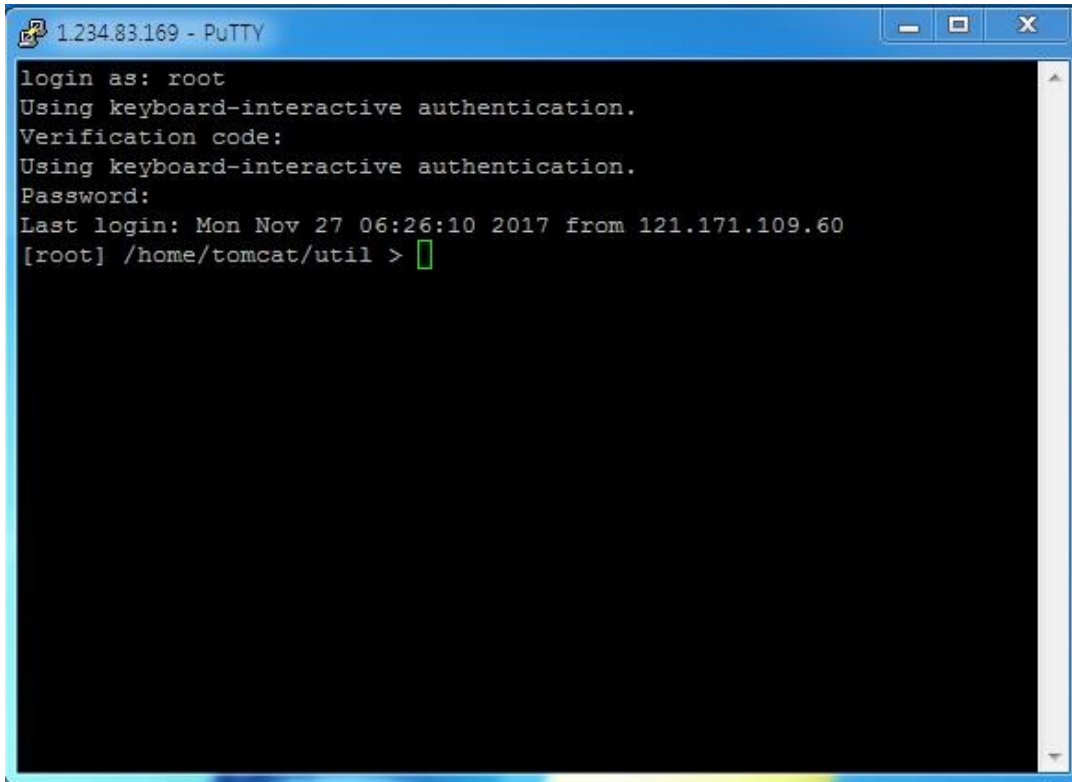


Putty Download 및 Documentation 관련 자료는 다음 URL에서 찾을 수 있다.

<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>

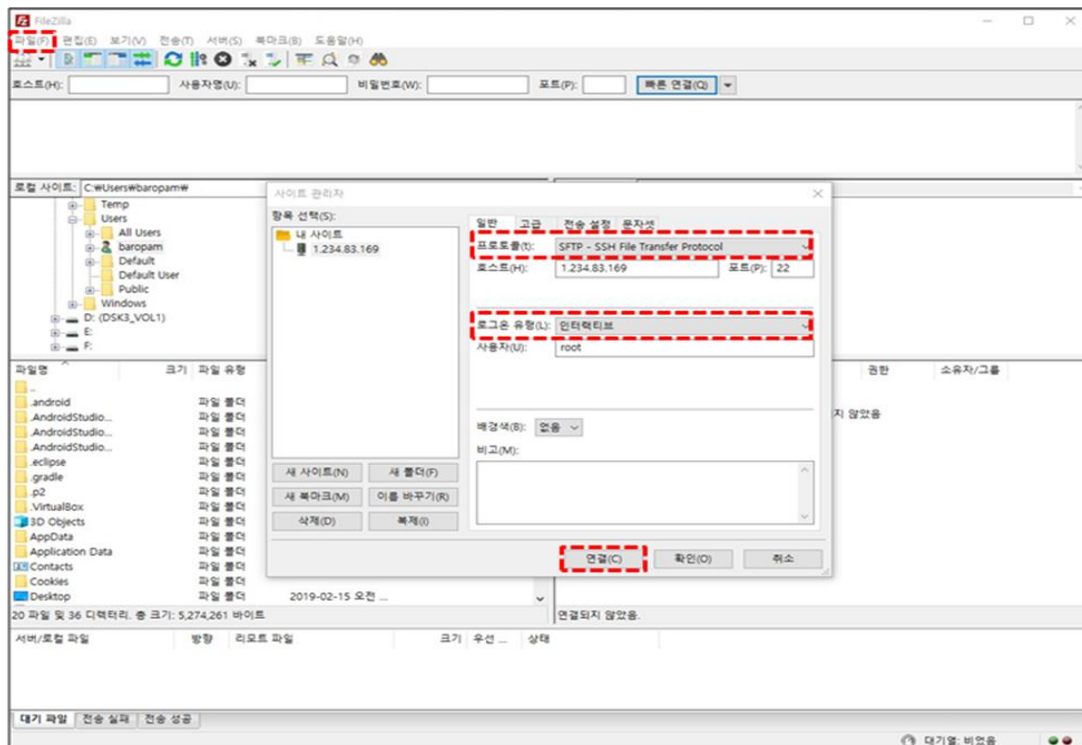
"Verification code"를 입력하라는 메시지가 표시되면 BaroPAM 앱에서 생성한 **일회용 인증키**를 입력한다.

인증에 성공하면 다음과 같이 SSH 로그인 비밀번호를 입력할 수 있다.

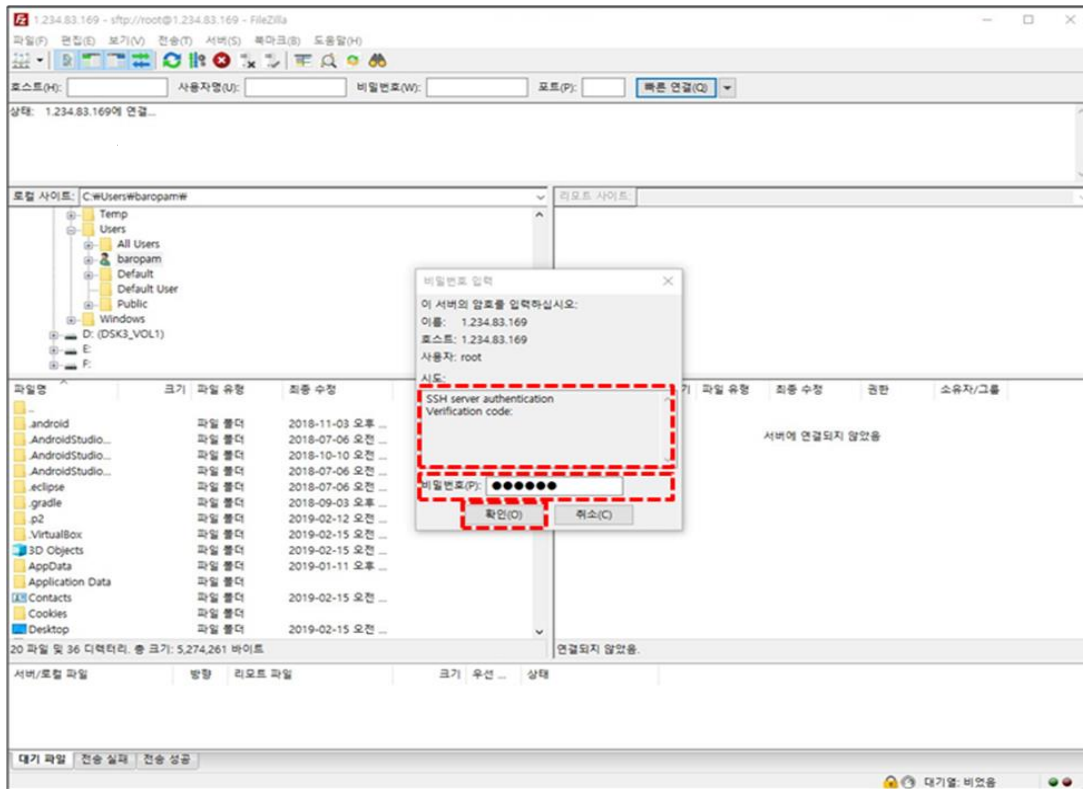


FileZilla인 경우)

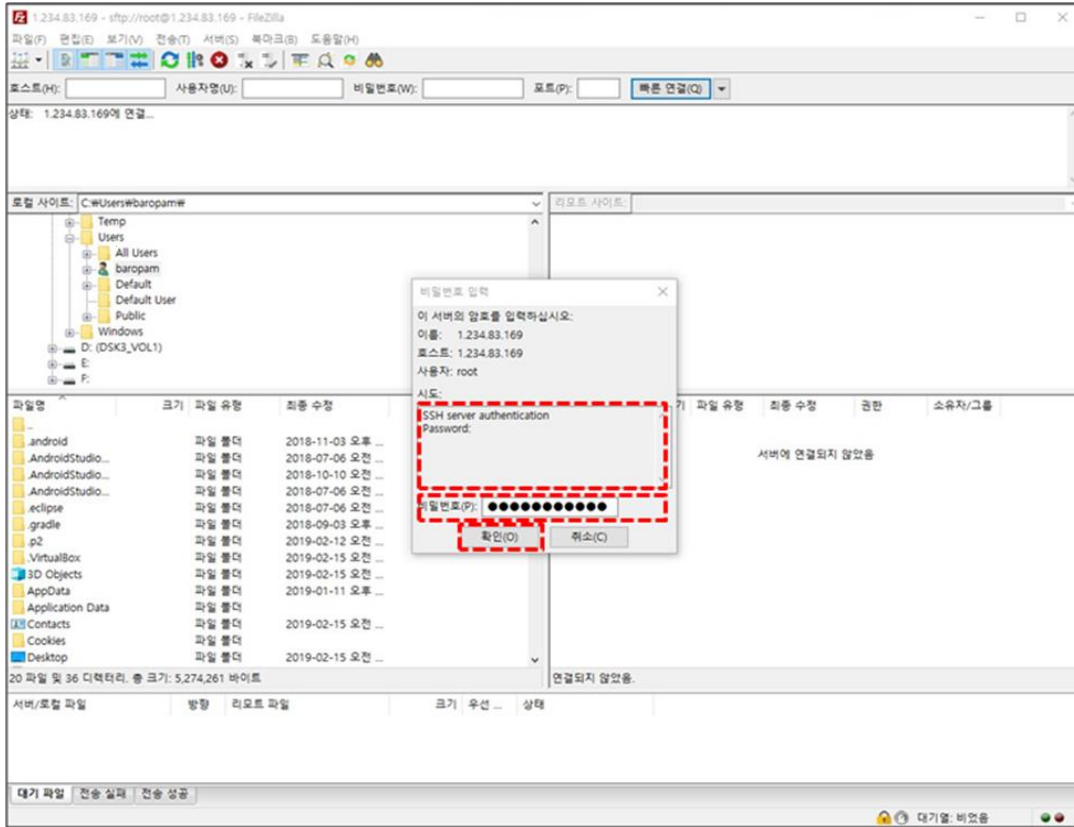
FileZilla로 접속할 때 보통 접속 과정과 다른데, 상단 왼쪽 메뉴에서 "파일(F) -> 사이트 관리자(S)"를 선택하여 일반 탭 화면에서 "프로토콜(t):" 항목에서 "SFTP - SSH File Transfer Protocol"과 "로그온 유형(L):" 항목에서 "인터랙티브"를 선택한 후 다음과 같이 "연결(C)" 버튼을 클릭한다.



그러면 다음과 같이 비밀번호 입력 화면이 나타난다. 비밀번호 입력 화면에서 "시도:" 내용을 확인하고, 스마트 폰에서 생성한 **일회용 인증키**를 "비밀번호(P):" 입력 항목에 입력한 후 "확인(O)" 버튼을 클릭한다.



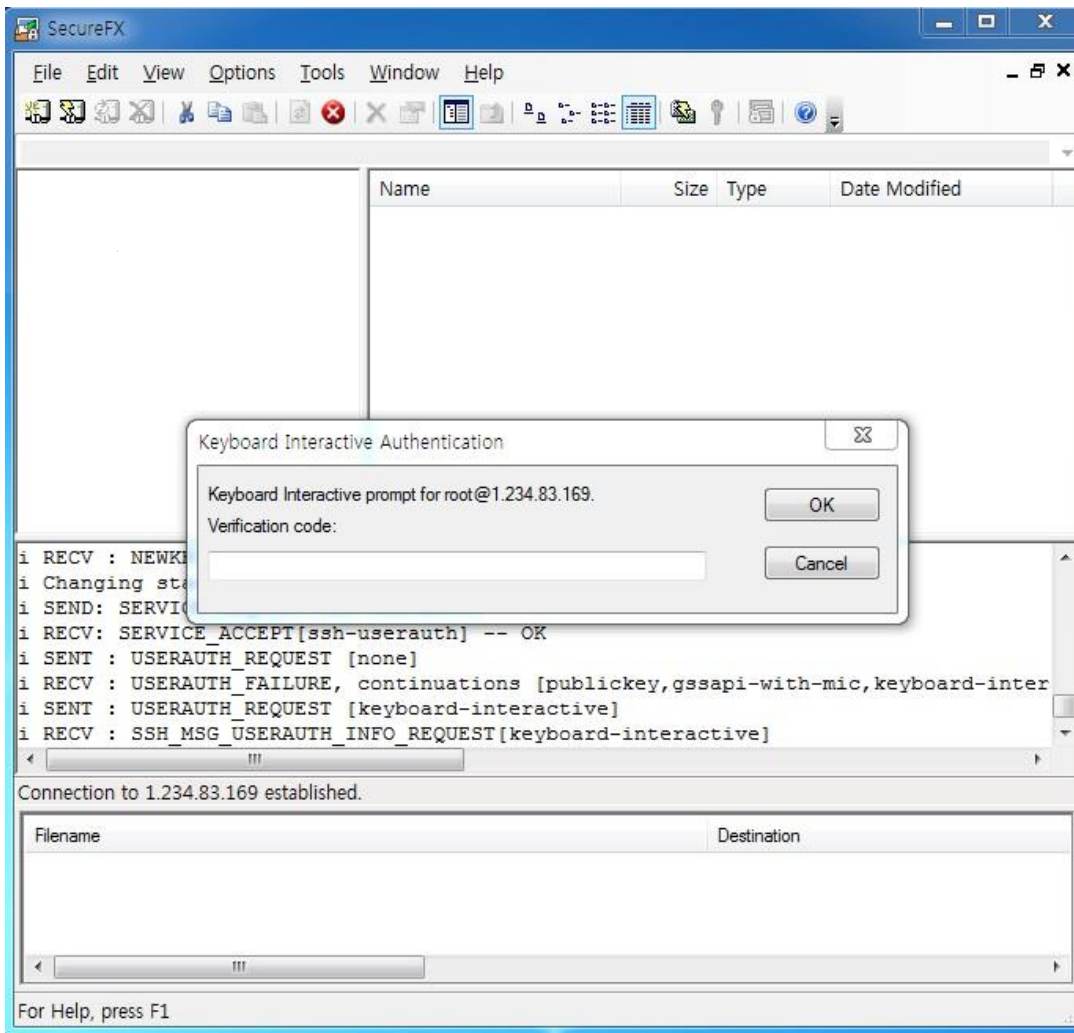
그러면 다음과 같이 비밀번호 입력 화면이 나타난다. 비밀번호 입력 화면에서 "시도:" 내용을 확인하고, 로그인 계정에 대한 비밀번호를 "비밀번호(P):" 입력 항목에 입력한 후 "확인(O)" 버튼을 클릭하여 서버에 접속한다.



SFTP인 경우)

"Verification code"를 입력하라는 메시지가 표시되면 BaroPAM 앱에서 생성한 일회용 인증기를 입력한다.

인증에 성공하면 다음과 같이 SFTP 로그인 비밀번호를 입력할 수 있다.



SecureFX Download 및 Documentation 관련 자료는 다음 URL에서 찾을 수 있다.

<https://www.vandyke.com/>

결론적으로, **2차 인증**은 추가 보호 계층을 추가하여 암호 인증을 보호하는 효과적인 수단이 될 수 있으며, 사용 여부와 상관없이 사용자의 선택에 달려 있지만 **2차 인증**의 채택은 산업의 동향이다.

3. BaroPAM 제거

3.1 BaroPAM 환경 제거

BaroPAM이 설치된 상태에서 BaroPAM 모듈을 사용하지 않을 경우 sshd 파일에 설정한 내용을 제거하는 방법은 다음과 같이 주석(#) 처리나 삭제하면 된다.

```
[root] /usr/baropam > vi /etc/pam.conf
#
# Authentication
#
#sshd auth required /usr/lib/security/pam_baro_auth.so nullok secret=/usr/baropam/.baro_auth
```

sshd 데몬에 설정한 "/etc/ssh/sshd_config" 파일의 내용 중 다음과 같은 인자를 변경해야 한다.

인자	기존	변경	비고
PasswordAuthentication	no	yes	
ChallengeResponseAuthentication	yes	no	
UsePAM	yes	no	

sshd 설정이 끝나면 반드시 PAM 모듈이 제대로 제거되었는지 확인한 후 SSH Server의 Restart 작업이 반드시 필요하다.

```
[root] /usr/baropam > startsrc -g ssh or startsrc -s sshd
```

sshd 설정이 끝나면 반드시 PAM 모듈이 제대로 제거되었는지 확인한 후 ssh 데몬을 재부팅해야 한다.

4. BaroPAM FAQ

현상 : 일회용 인증키가 맞지 않아서 로그인을 하지 못하는 경우

원인 : BaroPAM은 시간 동기화 방식으로 폰과 Windows나 Server의 시간이 동일해야 함,

조치 : 폰과 Windows나 Server의 시간이 맞는지 확인.

현상 : Feb 7 07:59:09 eactive sshd(pam_baro_auth)[29657]: ACL file ".baro_acl" must only be accessible by user id root

원인 : .baro_acl 파일의 Permission이 다름.

조치 : .baro_acl 파일의 Permission를 444로 설정.

현상 : Feb 7 08:02:15 eactive sshd(pam_baro_auth)[29739]: Failed to acl file read ".baro_acl"

원인 : .baro_acl 파일이 존재하지 않는 경우에 발생.

조치 : baropam 홈 디렉토리에 .baro_acl 파일을 생성. (Permission를 444로 설정)

현상 : Cannot look up user id xxxxx

원인 : 사용자 ID xxxxx를 조회 할 수 없는 경우 발생.

조치 : /etc/passwd 파일에 user id xxxxx를 등록.

현상 : Failed to secret file read .baro_auth

원인 : 사용자 ID xxxxx를 조회 할 수 없는 경우 발생.

조치 : /etc/passwd 파일에 user id xxxxx를 등록.

현상 : Failed to secret file read

원인 : Secret file이 존재하지 않은 경우에 발생.

조치 : Secret file의 존재여부를 확인.

현상 : Secret file .baro_auth must only be accessible by root

원인 : .baro_auth 파일의 Permission이 다른 경우에 발생.

조치 : .baro_auth 파일의 Permission를 444로 설정.

현상 : Invalid file size for .baro_auth

원인 : .baro_auth 파일의 크기가 $1 < \text{size} < 64\text{K}$ 가 아닌 경우 발생.

조치 : .baro_auth 파일의 크기를 확인.

현상 : Could not read .baro_auth

원인 : .baro_auth 파일이 존재하지 않거나 파일의 Permission이 444가 아닌 경우 발생.

조치 : .baro_auth 파일의 존재여부 및 파일의 Permission를 확인.

현상 : Invalid file contents in .baro_auth

원인 : .baro_auth 파일의 내용(규칙)이 잘못된 경우에 발생.

조치 : .baro_auth 파일의 내용을 확인.

현상 : Failed to create tmp secret file[error message]

원인 : 임시 secret file을 생성하지 못한 경우에 발생.

조치 : 임시 secret file을 생성하지 못한 이유는 error message를 확인.

현상 : Failed to open tmp secret file .baro_auth-[error message]

원인 : 임시 secret file인 .baro_auth-을 오픈하지 못한 경우에 발생.

조치 : 임시 secret file인 .baro_auth-을 오픈하지 못한 이유는 error message를 확인.

현상 : Secret file .baro_auth changed while trying to use one-time authentication key

원인 : 일회용 인증키를 사용하는 동안 비밀 파일 .baro_auth가 변경된 경우 발생.

조치 : 다시 로그인을 시도.

현상 : Failed to update secret file .baro_auth[error message]

원인 : secret file을 변경하지 못한 경우에 발생.

조치 : secret file을 변경하지 못한 이유는 error message를 확인.

현상 : Invalid RATE_LIMIT option. Check .baro_auth

원인 : Secret file인 .baro_auth 파일의 내용 중 RATE_LIMIT 설정값이 잘못 설정되어 있는 경우 발생.

조치 : 제한 횟수($1 < \text{RATE_LIMIT} < 100$), 제한 시간($1 < \text{interval} < 3600$)의 설정 값을 확인.

현상 : Invalid list of timestamps in RATE_LIMIT. Check .baro_auth

원인 : Secret file인 .baro_auth 파일의 내용 중 RATE_LIMIT 옵션에 Update된 timestamps가 잘못된 경우 발생.

조치 : Secret file인 .baro_auth 파일의 RATE_LIMIT 옵션에 Update된 timestamps를 확인.

현상 : Try to update RATE_LIMIT line.

원인 : 정상적으로 로그인 한 경우 출력되는 메시지.

조치 : No action

현상 : Too many concurrent login attempts. Please try again.

원인 : Secret file인 .baro_auth 파일의 DISALLOW_REUSE 옵션(일회용 인증키 생성 주기 내에는 하나의 로그인만 가능)이 설정된 경우

로그인 성공 후 일회용 인증키 생성 주기 내에 로그인을 재 시도한 경우 발생.

조치 : 일회용 인증키 생성 주기 후에 로그인 재 시도.

현상 : Invalid WINDOW_SIZE option in .baro_auth

원인 : Secret file인 .baro_auth 파일의 내용 중 WINDOW_SIZE 설정값(현재 시간을 기준으로 보정시간)이 잘못 설정되어 있는 경우 발생.

조치 : 현재 시간을 기준으로 일회용 인증키 보정시간($1 < \text{WINDOW_SIZE} < 100$)의 설정 값을 확인.

현상 : Trying to reuse a previously used time-based code.

Retry again in 30 seconds.

Warning! This might mean, you are currently subject to a man-in-the-middle attack.

원인 : Secret file인 .baro_auth 파일의 DISALLOW_REUSE 옵션은 중간자 공격(man-in-the-middle)을 대비한 옵션.

중간자 공격(man-in-the-middle)은 권한이 없는 개체가 두 통신 시스템 사이에서 스스로를 배치하고 현재 진행 중인 정보의 전달을 가로채면서 발생.

간단히 말해서, 현대판 도청 시스템이라고 할 수 있는 것

조치 : No action

현상 : Failed to allocate memory when updating .baro_auth

원인 : Secret file인 .baro_auth를 업데이트 할 때 메모리 할당에 실패한 경우 발생.

조치 : Technical support

현상 : Can't find SECURE_KEY[error message]

원인 : Secret file인 .baro_auth 파일의 SECURE_KEY 옵션이나 설정값이 없는 경우에 발생.

조치 : Secret file인 .baro_auth 파일의 SECURE_KEY 옵션이나 설정값 확인.

현상 : Verification code generation failed.[error message]

원인 : 일회용 인증키 검증에 실패한 경우 발생.

조치 : 로그인 재 시도.

현상 : Invalid verification code

원인 : 일회용 인증키 검증에 실패한 경우 발생.
조치 : 로그인 재 시도.

**현상 : Invalid verification code
Can not make/remove entry for session.**

원인 : 서버의 시스템 시간이 맞지 않아서 발생.
조치 : date 명령어로 서버의 시스템 시간이 맞는지 확인하여 틀리면 시간을 맞춰줘야 함.
1. date 명령어 서버의 시스템 시간을 변경(임시 방편)
2. ntp가 설정되어 있는지 확인하여 설정되어 있으면 ntp 시간을 설정하는 주기를 줄여 주어야 하며, 설정되어 있지 않으면 ntp를 설정해야 함.

현상 : Mar 12 15:37:01 baropam gdm(pam_baro_auth)[1215]: [ID 128276 auth.error] No user name available when checking verification code

원인 : 인증 코드를 검증할 때 사용 가능한 사용자가 아닌 경우(등록된 사용자가 아닌 경우 발생).
조치 : 시스템 관리자에게 로그인-ID가 등록되어 있는지 확인.

**현상 : Apr 3 13:06:13 kdn sshd[3577]: PAM unable to dlopen(/usr/baropam/pam_baro_auth.so):
/usr/baropam/pam_baro_auth.so: cannot open shared object file: No such file or directory
Apr 3 13:06:13 kdn sshd[3577]: PAM adding faulty module: /usr/baropam/pam_baro_auth.so**

원인 : /usr/baropam/pam_baro_auth.so 파일이 존재하지 않아서 발생.
조치 : BaroPAM 모듈 파일(pam_baro_auth.so)의 존재하는지 확인하여 없으면 BaroPAM의 설치 파일에서 복사한다.

현상 : May 19 12:37:37 baropam sshd(pam_baro_auth)[1416]: Failed to acl file read "(null)"

원인 : acl file 존재여부 및 파일 permission 문제로 발생
조치 :

현상 : Failed to compute location of secret file

원인 : pam에 설정된 secret file이 해당 디렉토리에 존재하지 않은 경우 발생.
조치 : pam에 설정된 secret file이 해당 디렉토리에 존재하지 않으면 secret file을 해당 디렉토리에 생성해 줘야 함.
ex) auth required /usr/baropam/pam_baro_auth.so nullok secret=/usr/baropam/.baro_auth encrypt=no

현상 : Failed to compute location of encrypt flag

원인 : pam에 암호화 플래그가 존재하지 않은 경우 발생.
조치 : pam에 암호화 플래그(yes, no)을 설정해 줘야 함.
ex) auth required /usr/baropam/pam_baro_auth.so nullok secret=/usr/baropam/.baro_auth encrypt=no

**현상 : Did not receive verification code from user
error: ssh_msg_send: write: Broken pipe**

원인 : Secure key가 잘못 설정된 경우에 발생
조치 : 설정된 Secure key를 확인.
벤더에서 제공된 Secure key인지 확인.

현상 : PAM: authentication thread exited unexpectedly.

***** glibc detected *** su: free(): invalid pointer: 0x00002aede020c9e2 *****
원인 : BaroPAM 환경 설정 파일(.baro_nurit)이 존재하지 않는 경우에 발생.
조치 : BaroPAM 환경 설정 파일(.baro_nurit)의 존재하는지 확인하여 없으면 BaroPAM의 설치 파일에서 복사한다.

현상 : 서버에 BaroPAM 적용 후 일회용 인증키를 입력하는 항목(Verification code: 또는 Password &

Verification code:)을 스킵(Skip)하여 로그인이 안되는 현상 발생

서버 접근제어 솔루션이 적용되어 있는 경우 BaroPAM을 적용 했는데, 로그인 되지 않는 현상

원인 : 서버 접근제어 솔루션에서 /etc/pam.d/sshd 설정한 것 보다 BaroPAM 설정이 앞에 설정하여 발생함

조치 : 다음과 같이 /etc/pam.d/sshd 설정의 순서를 변경하면 됨.

변경 전)

```
auth      required      /usr/baropam/pam_baro_auth.so nullok secret=/usr/baropam/.baro_auth
encrypt=no
auth      required      pam_sepermit.so
auth      include       password-auth
account   required      pam_nologin.so
account   include       password-auth
password  include       password-auth
```

변경 후)

```
auth      required      pam_sepermit.so
auth      substack     password-auth
account   required      pam_nologin.so
account   include       password-auth
password  include       password-auth
auth      required      /usr/baropam/pam_baro_auth.so nullok secret=/usr/baropam/.baro_auth
encrypt=no
```

PAM 설정 시 특정 모듈의 성공과 실패를 어떻게 처리할 것인지를 나타내는 것을 Control이라 한다.

Control 중 include과 substack은 다른 PAM 관련 모듈을 불러오는 것은 동일 하지만, substack은 substack의 동작 결과에 따라 나머지 모듈을 처리하지 않는다는 차이점이 있다.

5. 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)