nurit

For 3-step authentication to strengthen the security of information assets

BaroPAM Solution Installation Summary (Linux)

Mar, 2024

1. Pre-requisites

1) Check hostname and OS version

```
[root@baropam root]# uname -a
Linux baropam 4.18.0-348.7.1.el8_5.x86_64 #1 SMP Wed Dec 22 13:25:12 UTC 2021 x86_64 x86_64 x86_64
GNU/Linux
```

2) Check the versions of ssh and openssl to provide ssh and sftp services

```
[root@baropam root]# ssh -V
OpenSSH_8.0p1, OpenSSL 1.1.1k  FIPS 25 Mar 2021

[root@baropam baropam]# openssl
OpenSSL> version
OpenSSL 1.1.1k  FIPS 25 Mar 2021
OpenSSL> q
```

3) Disable "Selinux" in case of Redhat, CentOS series

```
[root] /etc > vi /etc/sysconfig/selinux
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       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
```

4) If you want to apply the changes only to the currently connected terminal without rebooting, execute the following command

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

Remember the following Linux information.

-Hostname/OS version
-ssh/openssl version
-For Redhat, CentOS series Disable "Selinux"

2. Install BaroPAM

1) Create a directory to install the BaroPAM module and set permissions (with the root account)

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

2) Authorize the directory to install the BaroPAM module

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

3) Download BaroPAM installation module (Check OS version)

https://mc529.tistory.com/1407

4) Unpack the BaroPAM installation module (eg for CentOS 8.x 64bit)

```
[root] /usr/baropam > tar -xvf libpam_baro_auth-8.1.10-x64.tar
```

If you know the tar file name to install

```
[root] /usr/baropam > wget http://nuriapp.com/download/libpam_baro_auth-8.1.10-x64.tar
```

5) Check the BaroPAM module

```
[root] /usr/baropam > ls -al
Total 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        → ACL file
-r--r--r--  1 root   root    305  7월  2 14:41 .baro_auth       → Configuration file for PAM authentication
-r--r--r--  1 root   root    290  6월 30 12:55 .baro_curl       → Configuration file for cURL authentication
-rwxr-xr-x  1 root   root  69149  4월  6 19:12 baro_auth        → An executable program that creates environment files for PAM authentication
-rwxr-xr-x  1 root   root  65072  6월 29 16:36 baro_curl        → An executable program that creates environment files for cURL authentication
drwxr-xr-x  2 root   root   4096  7월 20  2021 jilee            → Directory where PAM authentication security-related files exist
-rwxr-xr-x  1 root   root 152649  6월  9 08:19 pam_baro_auth.so → A module that verifies the OTA key of PAM authentication
-rwxr-xr-x  1 root   root 116158  6월 30 12:54 pam_baro_curl.so → A module that verifies the OTA key of cURL authentication
-rw-r--r--  1 root   root    221  6월 27 15:59 setauth.sh       → Shell script to create environment file for PAM authentication
-rw-r--r--  1 root   root    150  6월 29 16:29 setcurl.sh       → Shell script to create environment file for cURL authentication
```

3. Create BaroPAM configuration file (PAM authentication)

1) Shell script to create environment file (setauth.sh)

```
[root] /usr/baropam > cat setauth.sh
#!/bin/sh

HOSTNAME=`hostname`
export BAROPAM_HOME=/usr/baropam;

$BAROPAM_HOME/baro_auth -r 3 -R 30 -t 30 -k app512 -H $HOSTNAME -e no -A deny -a $BAROPAM_HOME/.baro_acl -S
jlqlcHbVqdpj7b4PzBpM2DileBvmHFV/ -s $BAROPAM_HOME/.baro_auth
```

2) Information on configuration options in the BaroPAM configuration file

Optino	Decumentation	Set value	Etc
-r	OTA key limited number of times (1~10)	3	
-R	OTA key time limit (15~600 sec)	30	
-t	OTA key authentication cycle (3~60 sec)	30	
-k	OTA key authentication method (app1, app256, app384, app512)	app512	
-e	Encryption of configuration files (yes or no)	no	
-H	Server's hostname (uname -n)	nurit.co.kr	
-A	Choose whether to allow or deny 2nd authentication	deny	
-a	ACL file name for the account to allow or deny from 2nd authentication (file access permission is 444)	/usr/baropam/.baro_acl	
-S	Secure key (license key) provided by the vendor	jlqlcHbVqdpj7b4PzBpM2DileBvmHFV/	
-s	File name including the directory in which to create the BaroPAM configuration file	/usr/baropam/.baro_auth	

3) Run the setenv.sh shell script

```
[root] /usr/baropam > sh setauth.sh
```

```
1) Your emergency one-time authentication keys are:
The emergency OTA key is a super authentication key that can be used
to access the SSH server again in case you lose it when the OTA key
generator, the BaroPAM app, is unavailable, so it is good to write
it down somewhere.

2) Enter "y" for all the questions that follow.
   Will it prevent man-in-the-middle attacks? y
   Will the same OTA key enable login to other accounts besides one
   account? y
   Shall we set the OTA key time limit to 30 seconds? y

[root] /usr/baropam > cat .baro_auth
" AUTH_KEY
" RATE_LIMIT 3 30
" KEY_METHOD app512
" CYCLE_TIME 30
" SECURE_KEY jlqlcHbVqdpj7b4PzBpM2DileBvmHFV/
" ACL_NAME /usr/baropam/.baro_acl
" ACL_TYPE deny
" HOSTNAME nurit.co.kr
" DISALLOW_REUSE
33458936
19035576
15364353
54649370
84342192
```

3. Create BaroPAM configuration file (cURL authentication)

1) Shell script to create environment file (setcurl.sh)

```
[root] /usr/baropam > cat setcurl.sh
#!/bin/sh

HOSTNAME=`hostname`
export BAROPAM_HOME=/usr/baropam;

$BAROPAM_HOME/baro_curl -r 3 -R 30 -t 30 -k app512 -H $HOSTNAME -e no -u http://1.23.456.789/baropam/web/result_curl.jsp -s
$BAROPAM_HOME/.baro_curl
```

2) Information on configuration options in the BaroPAM configuration file

Option	Decumentation	Set value	Etc
-r	OTA key limited number of times (1~10)	3	
-R	OTA key time limit (15~600 sec)	30	
-t	OTA key authentication cycle (3~60 sec)	30	
-k	OTA key authentication method (app1, app256, app384, app512: app, card1, card256, card384, card512: authentication card)	app512	
-e	Encryption of configuration files (yes or no)	no	
-H	Server's hostname (uname -n)	nurit.co.kr	
-u	The URL to be called includes parameters such as host name (hostname), user account (username), authentication cycle (cycle_time), and OTA key (auth_key)	http://1.23.456.789/baropam/web/result_curl.jsp	
-s	File name including the directory in which to create the BaroPAM configuration file	/usr/baropam/.baro_curl	

3) Run the setenv.sh shell script

```
[root] /usr/baropam > sh setcurl.sh
```

1) Enter "y" for all the questions that follow.
   Will it prevent man-in-the-middle attacks? y
   Will the same OTA key enable login to other accounts besides one account? y
   Shall we set the OTA key time limit to 30 seconds? y

```
[root] /usr/baropam > cat .baro_curl
" AUTH_KEY
" RATE_LIMIT 3 30
" AUTH_URL http://1.23.456.789/baropam/web/result_curl.jsp
" KEY_METHOD app512
" CYCLE_TIME 30
" HOSTNAME qsh-0415.cafe24.com
" DISALLOW_REUSE
```

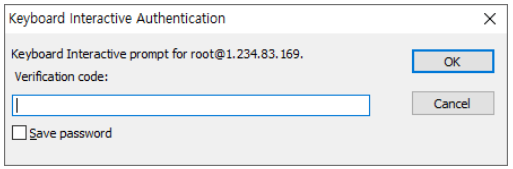
4. BaroPAM settings (PAM authentication)

1) at the top of the sshd file

[root] /usr/baropam > vi /etc/pam.d/sshd

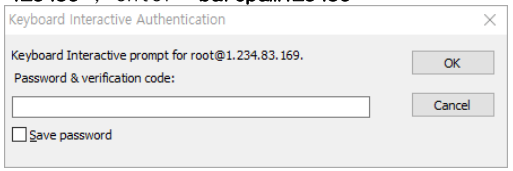
auth required /usr/baropam/pam_baro_auth.so nullok secret=/usr/baropam/.baro_auth encrypt=no

→ "nullok" means that the called PAM module allows entering a password with a null value



auth required /usr/baropam/pam_baro_auth.so forward_pass secret=/usr/baropam/.baro_auth encrypt=no

→ When entering a OTA key like a password in the password input window (Password & verification code:) using forward_pass, enter the password first and then enter the OTA key without a space. For example, if the password is "baropam" and the OTA key is "123456", enter "baropam123456"



2) Set at the top of su, lightdm, gdm-password files, etc

[root] /usr/baropam > vi /etc/pam.d/su

auth required /usr/baropam/pam_baro_auth.so nullok secret=/usr/baropam/.baro_auth encrypt=no

3) Among the contents of the "/etc/ssh/sshd_config" file, which is a configuration file for setting the sshd daemon, the following parameters need to be changed

Factor	Before	After	Etc
PasswordAuthentication	yes	no	
ChallengeResponseAuthentication or KbdInteractiveAuthentication	no	yes	
UsePAM	no	yes	

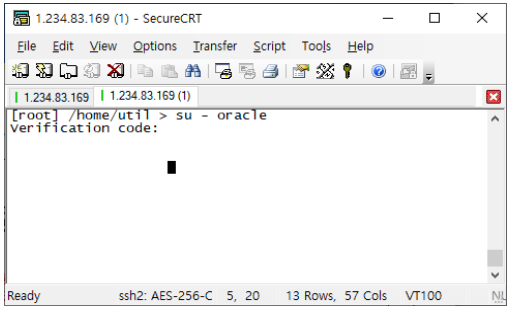
4) After sshd setup is complete, make sure that the PAM module is properly added and restart the SSH Server

[root] /usr/baropam > service sshd restart or systemctl restart sshd

sshd Stopping: [OK]

sshd Starting: [OK]

[root] /usr/baropam > service lightdm restart or systemctl restart lightdm



5) When using the BaroPAM module, the ACL for the account to be excluded from secondary authentication needs to be excluded

[root] /usr/baropam > vi .baro_acl

barokey

baropam

nurit

4. BaroPAM settings (cURL authentication)

1) at the top of the sshd file

[root] /usr/baropam > vi /etc/pam.d/sshd

auth required /usr/baropam/pam_baro_curl.so nullok secret=/usr/baropam/.baro_curl encrypt=no

→ "nullok" means that the called PAM module allows entering a password with a null value

auth required /usr/baropam/pam_baro_curl.so forward_pass secret=/usr/baropam/.baro_curl encrypt=no

→ When entering a OTA key like a password in the password input window (Password & verification code:) using forward_pass, enter the password first and then enter the OTA key without a space. For example, if the password is "baropam" and the OTA key is "123456", enter "baropam123456"

2) su, lightdm, gdm-password 파일 등의 최상단에 설정

[root] /usr/baropam > vi /etc/pam.d/su

auth required /usr/baropam/pam_baro_curl.so nullok secret=/usr/baropam/.baro_curl encrypt=no

3) Among the contents of the "/etc/ssh/sshd_config" file, which is a configuration file for setting the sshd daemon, the following parameters need to be changed

Factor	Before	After	Etc
PasswordAuthentication	yes	no	
ChallengeResponseAuthentication or KbdInteractiveAuthentication	no	yes	
UsePAM	no	yes	

4) After sshd setup is complete, make sure that the PAM module is properly added and restart the SSH Server

[root] /usr/baropam > service sshd restart or systemctl restart sshd

sshd Stopping: [OK]

sshd Starting: [OK]

[root] /usr/baropam > service lightdm restart or systemctl restart lightdm

5) When using the BaroPAM module, the ACL for the account to be excluded from secondary authentication needs to be excluded

[root] /usr/baropam > vi .baro_acl

barokey

baropam

5. How to apply BaroPAM

Password alone is never safe when logging in to all information assets, and new application methods (additional authentication, password replacement, new password) that can replace or additionally authenticate the password (secondary authentication) are required each time it is used

1) additional authentication

Apply one-time authentication key as additional authentication (secondary authentication) other than account (login-ID) and password(ID/PW/OTA)

```
auth required /usr/baropam/pam_baro_auth.so nullok secret=/usr/baropam/.baro_auth encrypt=no
auth required /usr/baropam/pam_baro_curl.so nullok secret=/usr/baropam/.baro_curl encrypt=no
```

2) password replacement

Remove password and replace with OTA key (ID/OTA) - OTA key

```
auth required /usr/baropam/pam_baro_auth.so forward_pass secret=/usr/baropam/.baro_auth encrypt=no
auth required /usr/baropam/pam_baro_curl.so forward_pass secret=/usr/baropam/.baro_curl encrypt=no
```

Note) When replacing the password with a OTA key, the password of the account (login-ID) must be set the same as the account.

3) new password

By combining the password and the OTA key, a new OTP is generated and applied for each OTA key generation cycle(ID/PW+OTA)

```
auth required /usr/baropam/pam_baro_auth.so forward_pass secret=/usr/baropam/.baro_auth encrypt=no
auth required /usr/baropam/pam_baro_curl.so forward_pass secret=/usr/baropam/.baro_curl encrypt=no
```

Note) Since Linux/Unix servers do not support autologin, a password must exist.

Added) How to apply .baro_auth

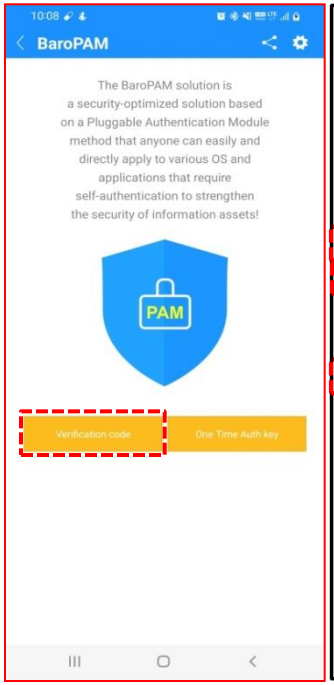
```
auth required /usr/baropam/pam_baro_auth.so nullok secret=/usr/baropam/.baro_auth encrypt=no          → Default setting
auth required /usr/baropam/pam_baro_auth.so nullok secret={HOME}/.baro_auth encrypt=no              → Set in the home directory per account
auth required /usr/baropam/pam_baro_auth.so nullok secret=/usr/baropam/auth/.{USER}_auth encrypt=no → Configuration file settings per account
```

5. Install the BaroPAM app and set up information

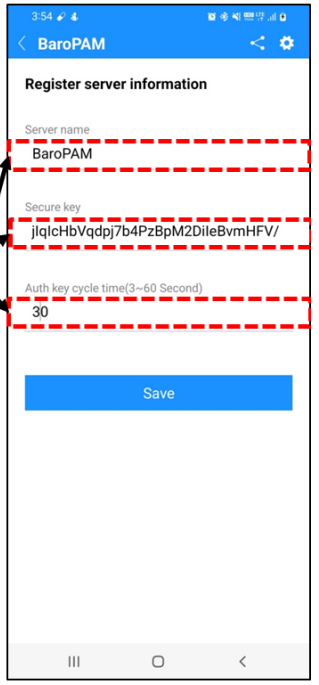
BaroPAM App Download

Google Play

App Store




```
$ cat .baro_auth
" AUTH_KEY
" RATE_LIMIT 3 30
" KEY_METHOD app512
" CYCLE_TIME 30
" SECURE_KEY jlqlcHbVqdpj7b4PzBpM2DileBvmHFV/
" ACL_NAME /usr/baropam/.baro_acl
" ACL_TYPE deny
" HOSTNAME BaroPAM
" DISALLOW_REUSE
33458936
19035576
15364353
54649370
84342192
```



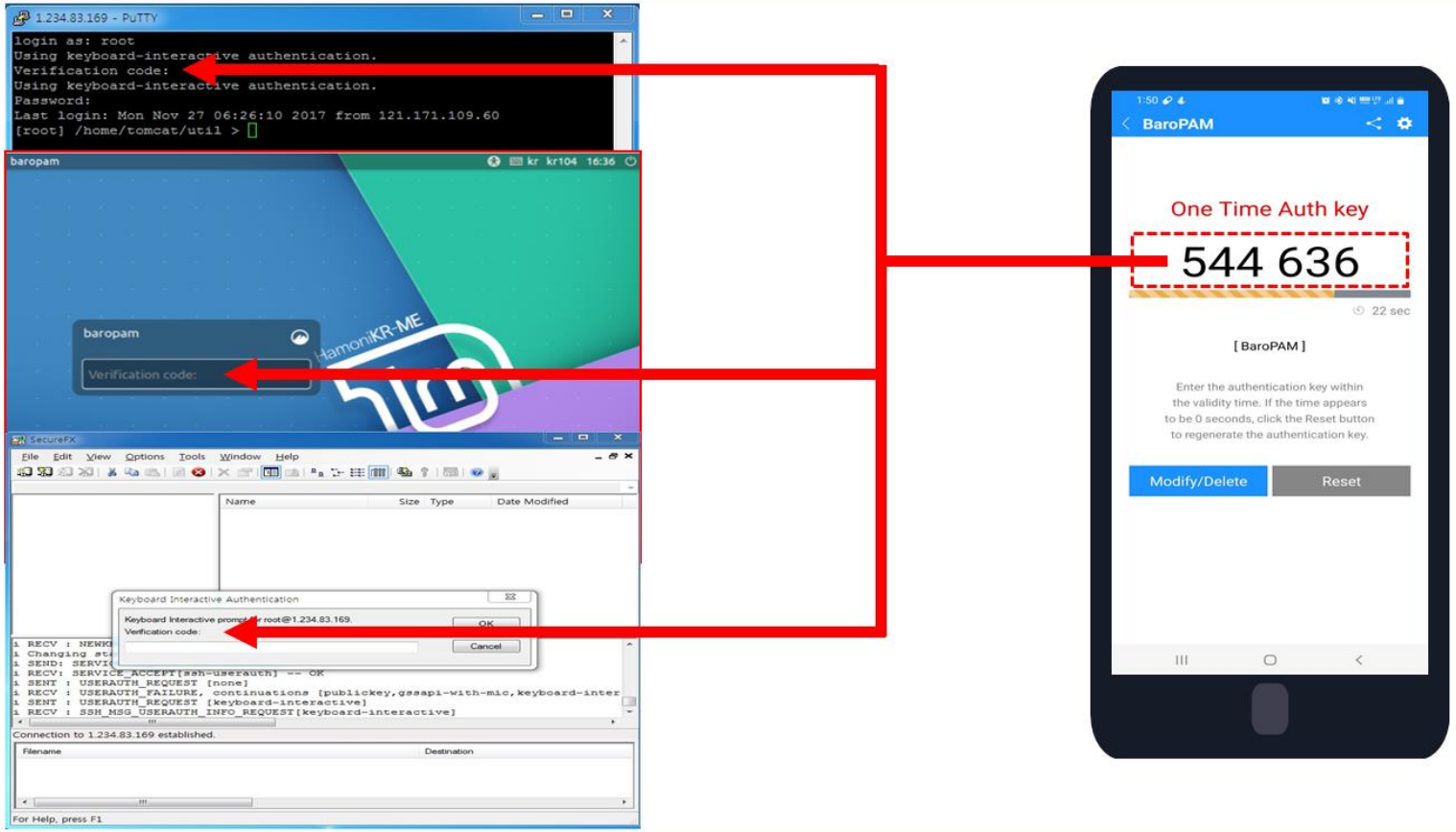
BaroPAM app can be used on Android 6.0 (Marshmalliw) API 23, iOS 13.0 or higher, and does not support landscape mode. After installing the BaroPAM app, launch the BaroPAM app and click the "Verification Code" button on the menu selection screen to enter the BaroPAM configuration file ".baro_auth".
You must enter the same "cycle time, secure key, server name" set in the "Register server information" screen of the BaroPAM app.
If you set the app code (kr: Korean, en: English, jp: Japanese, cn: Chinese) on the **BaroPAM** app settings -> change screen settings screen, the **BaroPAM** app changes accordingly.

Message: The "OTA key" is incorrect because the date and time of the Android phone or iPhone are different from the current time.
Cause: This is caused by not using the time provided by the network for the Android or iPhone's date and time.
Action: For Android phones, go to "Settings" -> "General management" -> "Date and time" -> "Automatic date and time" and "Automatic time zone" -> "Allow" For iPhone, go to "Settings" -> "Date & Time" -> "Set Automatically" -> "Allow"

Message: If you cannot log in because the OTA key does not match.
Cause: BaroPAM is a time synchronization method, so the time of the phone and Server must be the same.
Action: Check if the phone and Server time are correct.

nurit

6. Linux login



Enter your Linux user account (Username), generate a OTA key in the BaroPAM app on your smartphone, and create a OTA key in "Verification code" and Linux "Password", click "Enter" or "OK" button to request authentication to the BaroPAM module, and if verification is successful, Linux is logged in.

7. What to check when a problem occurs

1) Check system login Syslog
Redhat series: /var/log/secure, others: Check the message that "pam_baro_auth" exists among the contents of the /var/log/auth.log file

2) Check Linux system information
$ uname -a

3) Check Openssl information
$ openssl version

4) Check the BaroPAM installation directory and file permissions
$ ls -al /usr/baropam

5) Check the BaroPAM installed module
$ file pam_baro_auth.so
$ ldd pam_baro_auth.so

6) Check BaroPAM configuration information
$ cat /usr/baropam/.baro_auth

7) Check your PAM settings
$cat /etc/pam.d/sshd or su or sudo or lightdm etc

8) Check sshd_config settings
$ cat /etc/ssh/sshd_config

9) Check NTP settings and status (Redhat 8 and later versions use chrony)
$ cat /etc/ntp.conf or /etc/chrony.conf
$ ntpq -p or timedatectl status

nurit

Password you don't need to remember!
BaroPAM will be with you.

Thank You!

www.nurit.co.kr
mc529@nurit.co.kr