BaroPAM Guide(Linux)

Index

1. Install BaroPAM

1.1 Preparation before installing BaroPAM

To use the PAM module, the PAM package must be installed by default. To check the installation, run the following command. If it is not installed, use the command "**dnf install pam**" for Redhat series and "**sudo apt-get install pam**" for others.

```
[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
```

In order to access information assets and use the PAM module, the OpenSSH (Open Secure Shell) package must be installed to provide reliable and safe ssh and sftp services. To check the installation, run the following command. If it is not installed, use "**dnf install openssh**" and "**dnf install openssl**" for Redhat series, and "**sudo apt-get install openssl**" for others.

```
[root]# rpm -qa | grep openssh
openssh-clients-4.3p2-82.el5
openssh-server-4.3p2-82.el5
openssh-4.3p2-82.el5

[root]# rpm -qa | grep openssl
openssl-0.9.8e-40.el5_11
openssl101e-1.0.1e-11.el5
openssl097a-0.9.7a-12.el5_10.1
openssl-devel-0.9.8e-40.el5_11
openssl-perl-0.9.8e-40.el5_11
openssl-devel-0.9.8e-40.el5_11
openssl101e-devel-1.0.1e-11.el5
openssl101e-static-1.0.1e-11.el5
openssl-0.9.8e-40.el5_11
openssl101e-devel-1.0.1e-11.el5
openssl101e-static-1.0.1e-11.el5
openssl101e-perl-1.0.1e-11.el5
openssl097a-0.9.7a-12.el5_10.1
openssl101e-1.0.1e-11.el5
```

```
[root]# ssh -V
OpenSSH_4.3p2, OpenSSL 0.9.8e-fips-rhel5 01 Jul 2008
```

In the case of Redhat series, "**Selinux**" is an abbreviation of "**Security Enhanced Linux**" and provides a more excellent security policy than the basic Linux. If it is so outstanding that it is activated, a part where BaroPAM cannot be blocked due to security problems occurs (**Failed to open tmp secret file "/usr/baropam/.baro_auth~" [Permission denied]**). So, if possible, most of them are disabled (**SELINUX=enforcing → disabled**).

```
[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
```

It doesn't take effect right away and requires a reboot to take effect.

If you want to apply the changes only to the currently connected terminal without rebooting, run the following command.

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

When setting environment setting information to MariaDB during PAM authentication, MariaDB Client must be installed.

```
[root] /etc > dnf -y install mariadb-client      ➔ Redhat level
[root] /etc > sudo apt -y install mariadb-client ➔ Other than that
```

To download and install the BaroPAM authentication module, connect with the **root** account and create a directory (/usr/baropam) to download and install the module as follows.

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

Grant permissions (read, write, execute) of the directory to download and install the BaroPAM module as follows.

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

1.2 Download BaroPAM installation module

In order to check the operating system name, system information, and kernel information of the

Linux system to be installed, connect to the **root** account and execute the following command.

```
[root] /usr/baropam > uname -a
Linux baropam 3.10.0-862.el7.x86_64 #1 SMP Fri Apr 20 16:44:24 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
```

After accessing the BaroPAM authentication module with the **root** account, move to the directory (/usr/baropam) to download and install the module, and download the module as follows.

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

When the download of the BaroPAM authentication module is complete, the **tar** file is decompressed as follows.

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

When the BaroPAM authentication module is unzipped, the following BaroPAM related modules are created in the baropam directory.

```
[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
-r--r--r--  1 root    root    287  2월 28 12:19 .baro_sql
-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
-rwxr-xr-x  1 root    root  57074  2월 28 12:18 baro_sql
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
-rwxr-xr-x  1 root    root 170863  2월 28 12:18 pam_baro_sql.so
-rw-r--r--  1 root   root    221  6월 27 15:59 setauth.sh
-rw-r--r--  1 root   root    150  6월 29 16:29 setcurl.sh
-rw-r--r--  1 root    root    180  2월 28 12:19 setsql.sh
```

Execute the following command to check whether the created BaroPAM authentication module is suitable for the system.

```
[root] /usr/baropam > file pam_baro_auth.so
pam_baro_auth.so: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, BuildID[sha1]=d2d7b4ffe8b1a25f6a11685cb7ad4ec9787163b5, not stripped

[root] /usr/baropam > ldd pam_baro_auth.so
        linux-vdso.so.1 =>  (0x00007ffe7f503000)
        libpam.so.0 => /usr/lib64/libpam.so.0 (0x00007f23a3318000)
        libssl.so.10 => /usr/lib64/libssl.so.10 (0x00007f23a30a6000)
        libcrypto.so.10 => /usr/lib64/libcrypto.so.10 (0x00007f23a2c45000)
        libdl.so.2 => /usr/lib64/libdl.so.2 (0x00007f23a2a41000)
        libz.so.1 => /usr/lib64/libz.so.1 (0x00007f23a282b000)
        libc.so.6 => /usr/lib64/libc.so.6 (0x00007f23a245e000)
```

```
        libaudit.so.1 => /usr/lib64/libaudit.so.1 (0x00007f23a2235000)
        libgssapi_krb5.so.2 => /usr/lib64/libgssapi_krb5.so.2 (0x00007f23a1fe8000)
        libkrb5.so.3 => /usr/lib64/libkrb5.so.3 (0x00007f23a1d00000)
        libcom_err.so.2 => /usr/lib64/libcom_err.so.2 (0x00007f23a1afc000)
        libk5crypto.so.3 => /usr/lib64/libk5crypto.so.3 (0x00007f23a18c9000)
        /lib64/ld-linux-x86-64.so.2 (0x00007f23a372f000)
        libcap-ng.so.0 => /usr/lib64/libcap-ng.so.0 (0x00007f23a16c3000)
        libkrb5support.so.0 => /usr/lib64/libkrb5support.so.0 (0x00007f23a14b5000)
        libkeyutils.so.1 => /usr/lib64/libkeyutils.so.1 (0x00007f23a12b1000)
        libresolv.so.2 => /usr/lib64/libresolv.so.2 (0x00007f23a1098000)
        libpthread.so.0 => /usr/lib64/libpthread.so.0 (0x00007f23a0e7c000)
        libselinux.so.1 => /usr/lib64/libselinux.so.1 (0x00007f23a0c55000)
        libpcre.so.1 => /usr/lib64/libpcre.so.1 (0x00007f23a09f3000)
```

1.3 Create BaroPAM configuration file

1) PAM authentication (.baro_auth): Set environment setting information in File

The BaroPAM environment setting file must be created by executing the **baro_auth** program, and it must be located under **/usr/baropam**, the directory of the BaroPAM authentication module.

Format)

```
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
```

The configuration options of the BaroPAM configuration file are as follows.

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	
-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	

Note) The filename of the -s option is the name of the file including the directory where the BaroPAM configuration file will be created (**file access permission is 444**).

Ex of use)

```
[root] /usr/baropam > ./baro_auth -r 3 -R 30 -t 30 -k app512 -e no -A deny -a /usr/baropam/.baro_acl -S jlqlcHbVqdpj7b4PzBpM2DileBvmHFV/ -s /usr/baropam/.baro_auth
```

If the BaroPAM environment setting file is set for each account, connect to the account and

proceed with the work. (Not root)

```
[root] /usr/baropam > ./baro_auth -r 3 -R 30 -t 30 -k app512 -e no -A deny -a ~/.baro_acl -S
jlqlcHbVqdpj7b4PzBpM2DileBvmHFV/ -s ~/.baro_auth
```

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.
   Do you want me to update your "/usr/baropam/.baro_auth" file (y/n) y
   Preventing man-in-the-middle attacks (y/n) y

The contents set in .baro_auth, the BaroPAM environment setting file, are as follows.

```
[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
" DISALLOW_REUSE
33458936
19035576
15364353
54649370
84342192
```

The setting items of .baro_auth, a BaroPAM configuration file, are as follows.

Item	Documentation	Set value	Etc
AUTH_KEY	Authentication delimiter (fixed)		
RATE_LIMIT	OTA key limit count (1~10), time limit (15~600 sec)	3 30	
KEY_METHOD	OTA key authentication method (app1, app256, app384, app512: app)	app512	
CYCLE_TIME	OTA key authentication cycle (3~60 sec)	30	
SECURE_KEY	Secure key (license key) provided by the vendor	jlqlcHbVqdpj7b4PzBpM2DileBvmHFV/	
ACL_TYPE	Differentiate between allow and deny in 2nd authentication	deny	
ACL_NAME	ACL Filename for the account to be allowed or excluded from 2nd authentication (file access permission is 444)	/usr/baropam/.baro_acl	
DISALLOW_REUSE or ALLOW_REUSE	To prevent a man-in-the-middle attack, if "DISALLOW_REUSE" is set, other users cannot log in during the authentication cycle of the OTA key. If allowed, set "ALLOW_REUSE".	DISALLOW_REUSE	

2) PAM authentication (.baro_sql): Set environment configuration information in MariaDB

Connection information for linking with Mariadb, where BaroPAM configuration information exists, must be created by running the **baro_sql** program, and must be located under **/usr/baropam**, the directory of the BaroPAM authentication module.

Format)

```
baro_sql -H hostname -u username -p password -d dbname -P portno -e encrypt_flag -s filename
```

The configuration options of the BaroPAM configuration file are as follows.

Optino	Decumentation	Set value	Etc
-H	Hostname or IP address of the MariaDB server	nurit.co.kr	
-u	MariaDB username	nurit	
-p	Password for the MariaDB user	baropam	
-d	MariaDB name to connect to	baropamdb	
-p	Port number of the MariaDB server	3308	
-e	Encryption of configuration files (yes or no)	no	
-s	File name including the directory in which to create the BaroPAM configuration file	/usr/baropam/.baro_sql	

Note) The filename of the -s option is the file name containing the directory where the BaroPAM configuration file will be created (**file access permission is 444**).

Ex of use)

```
[root] /usr/baropam > ./baro_sql -H nurit.co.kr -e no -u nurit -p baropams -d baropamdb -P 3306 -s /usr/baropam/.baro_sql
```

1) Enter "**y**" for all the questions that follow.
   Do you want me to update your "/usr/baropam/.baro_sql" file (y/n) **y**

The contents set in **.baro_sql**, the BaroPAM environment setting file, are as follows.

```
[root] /usr/baropam > cat .baro_sql
" AUTH_KEY
" HOSTNAME nurit.co.kr
" USERNAME nurit
" PASSWORD baropams
" DBNAME baropamdb
" PORTNO 3306
" RATE_LIMIT 3 30
" KEY_METHOD app512
" CYCLE_TIME 30
" SECURE_KEY jlqlcHbVqdpj7b4PzBpM2DileBvmHFV/
" ACL_TYPE deny
" MIDDLE_TYPE DISALLOW_REUSE
" MIDDLE_TIME 58014762
" ENV_TYPE share
```

The setting items of **.baro_sql**, a BaroPAM configuration file, are as follows.

Item	Documentation	Set value	Etc
AUTH_KEY	Authentication delimiter (fixed)		
HOSTNAME	Hostname or IP address of the MariaDB server	nurit.co.kr	
USERNAME	MariaDB username	nurit	
PASSWORD	Password for the MariaDB user	baropam	
DBNAME	MariaDB name to connect to	baropamdb	
PORTNO	Port number of the MariaDB server	3308	
Other than that	The rest is used for internal use.		

3) cURL authentication (.baro_curl)

The name curl stands for "**client URL**" and was first released in 1997. That is, the client requests data from the server as a script. BaroPAM requests authentication by calling the http/https authentication site with curl.

The BaroPAM environment setting file must be created by executing the **baro_curl** program, and it must be located under **/usr/baropam**, the directory of the BaroPAM authentication module.

Format)

```
baro_curl -r rate_limit -R rate_time -t cycle_time -k key_method -e encrypt_flag -H hostname -u auth_url -s filename
```

The configuration options of the BaroPAM configuration file are as follows.

Option	Documentation	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)	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	

Note) The filename of the -s option is the name of the file including the directory where the BaroPAM configuration file will be created (**file access permission is 444**). If the hostname of the set server does not match, BaroPAM may not operate normally. If the hostname is changed, it must be reflected in the relevant item of the environment setting.

Ex of use)

```
[root] /usr/baropam > ./baro_curl -r 3 -R 30 -t 30 -k app512 -e no -H nurit.co.kr -u http://1.23.456.789/baropam/web/result_curl.jsp -s /usr/baropam/.baro_curl
```

1) Enter "**y**" for all the questions that follow.
   Do you want me to update your "/usr/baropam/.baro_auth" file (y/n) **y**
   Preventing man-in-the-middle attacks (y/n) **y**

The contents set in .baro_curl, a BaroPAM environment setting file, are as follows.

```
[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 baropam
" DISALLOW_REUSE
```

The setting items of .baro_curl, a BaroPAM configuration file, are as follows.

Item	Documentation	Set value	Etc
AUTH_KEY	Authentication delimiter (fixed)		
RATE_LIMIT	OTA key limit count (1~10), time limit (15~600 sec)	3 30	
AUTH_URL	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	
KEY_METHOD	OTA key authentication method (app1, app256, app384, app512)	app512	
CYCLE_TIME	OTA key authentication cycle (3~60 sec)	30	
HOSTNAME	Server's hostname (uname -n)	nurit.co.kr	
DISALLOW_REUSE or ALLOW_REUSE	To prevent a man-in-the-middle attack, if "DISALLOW_REUSE" is set, other users cannot log in during the authentication cycle of the OTA key. If allowed, set "ALLOW_REUSE".	DISALLOW_REUSE	

1.4 BaroPAM environment settings

1) PAM authentication: Set environment setting information in File

① Additional authentication (apply OTA key as additional authentication other than login-ID and password)

To configure the BaroPAM module, enter it at the top as follows to configure sshd, su, and sudo files.

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

For reference, the **secret** parameter sets the BaroPAM configuration file name, and the **encrypt** parameter sets the encryption flag (**yes** or **no**) of the BaroPAM configuration file.

If the BaroPAM environment setting file is set for each account, the way to set the sshd file to set the BaroPAM module is entered at the top as follows.

```
[root] /usr/baropam > vi /etc/pam.d/sshd
#%PAM-1.0
auth       required     /usr/baropam/pam_baro_auth.so nullok secret=${HOME}/.baro_auth encrypt=no
```

If you want to set different BaroPAM environment configuration files for each account in a specific directory instead of setting BaroPAM environment configuration files for each account, enter the following at the top to configure the BaroPAM module in the sshd file.

```
[root] /usr/baropam > vi /etc/pam.d/sshd
#%PAM-1.0
auth       required     /usr/baropam/pam_baro_auth.so nullok secret=/usr/baropam/auth/.${USER}_auth
encrypt=no
```

* "**nullok**" means that the called PAM module allows entering a password with a null value. However, Redhat 9.x and higher do not support the "**nullok**" option in **/etc/pam.d/sshd** settings.

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

If you add the BaroPAM module to the top of the **/etc/pam.d/su** file, you can apply the 2nd authentication (additional authentication) input even when a general account tries to ascend to "**root**" with the "**su**" command for security. this is further improved.

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

In the case of Desktop Linux, if you want to use BaroPAM on the GUI login screen, enter the setting as follows.

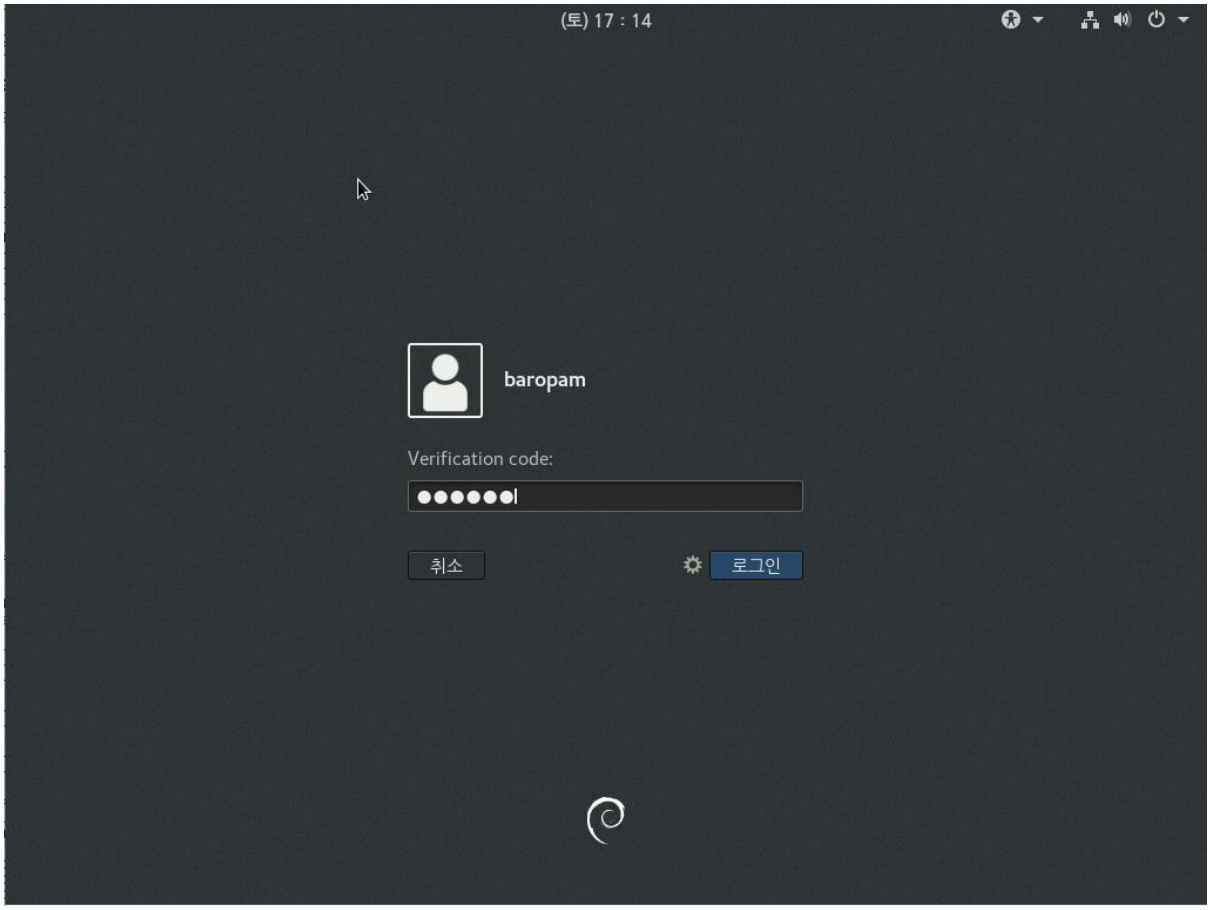
Ex) For Debian, Ubuntu, SUSE, Fedora Linux

```
[root] /usr/baropam > vi /etc/pam.d/gdm-password or gdm-autologin
#%PAM-1.0
auth          required       /usr/baropam/pam_baro_auth.so  nullok  secret=/usr/baropam/.baro_auth
encrypt=no
```

After **gdm-password and gdm-autologin** settings are finished, it is necessary to restart **gdm-password** after confirming that the PAM module has been properly added.

```
[root] /usr/baropam > systemctl restart gdm-password
```

Then, the screen to enter "**Verification code:**", which is the OTA key of BaroPAM, appears on the login screen as follows.



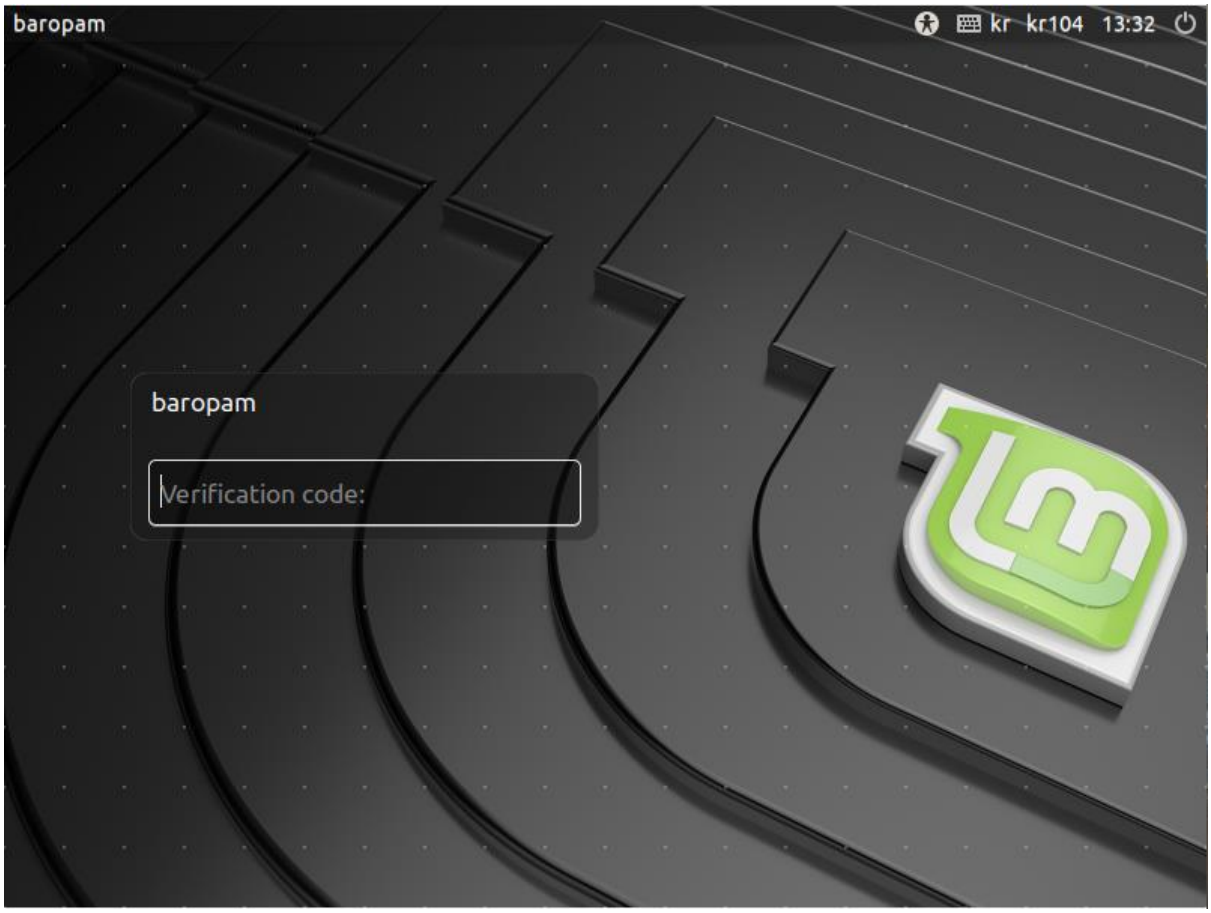
Ex) For Hamonikr OS, Gooroom OS, Mint Linux

```
[root] /usr/baropam > vi /etc/pam.d/lightdm or loghtdm-autologin
#%PAM-1.0
auth            required        /usr/baropam/pam_baro_auth.so  nullok  secret=/usr/baropam/.baro_auth
encrypt=no
```

After setting **lightdm and lightdm-autologin**, it is necessary to restart **lightdm** after confirming that the PAM module has been properly added.

```
[root] /usr/baropam > systemctl restart lightdm
```

Then, the screen to enter "**Verification code:**", which is the **OTA key** of **BaroPAM**, appears on the login screen as follows.



Note) In the case of Desktop Linux, such as an open OS, if you remove the password with the "**passwd -p *username***" command, you will not be asked for the password if you enter only the **OTA key** on the input screen of "**Verification code:**".

Ex) When connecting to a remote desktop using xrdp

```
[root] /usr/baropam > vi /etc/pam.d/xrdp-sesman
#%PAM-1.0
auth       required     /usr/baropam/pam_baro_auth.so forward_pass secret=/usr/baropam/.baro_auth
encrypt=no
```

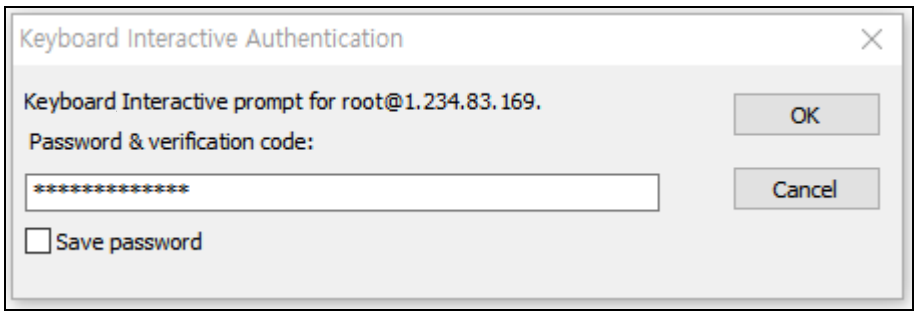
Enter the **OTA key** in the password input window (**Password**) using **forward_pass**. For example, if the **OTA key** is "**123456**", just enter "**123456**".

② Replace password (replace password with OTA key)

For programs like filezilla that cannot perform "**Interactive process**", the only way is to use the **forward_pass** option in PAM to enter the **OTA key** when entering the password. In this case, the openssh client, RDP (Remote Desktop Protocol) of Windows, Radius, filezilla, etc. all have no choice but to input like this.

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

Enter the OTA key in the password input window (**Password & verification code:**) using **forward_pass**. For example, if the OTA key is "**123456**", just enter "**123456**".



Note) When replacing the password with an OTA key, the password for the account must be set the same as the login-ID in advance with the "**passwd *username***" command.

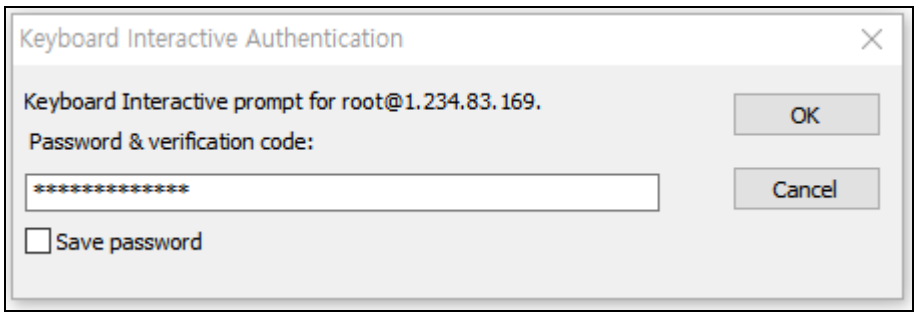
In the case of Desktop Linux, such as an open OS, remove the password with the "**passwd -p *username***" command, and enter the OTA key on the input screen of "**Password & Verification code:**" and the password will not be asked.

③ New password (by combining the password and the OTA key, a new one-time password is generated and applied for each OTA key generation cycle)

For programs like filezilla, which cannot perform "**Interactive process**", the only way is to use the **forward_pass** option in PAM to enter the password and OTA key together when entering the password. In this case, the openssh client, RDP (Remote Desktop Protocol) of Windows, Radius, filezilla, etc. all have no choice but to input like this.

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

When entering the 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 spaces. For example, if the password is "**baropam**" and the OTA key is "**123456**", enter "**baropam123456**".



Using **forward_pass**, you can enable 2nd authentication for most services that require authentication.

2) PAM authentication: Set environment configuration information in MariaDB

① Additional authentication (apply OTA key as additional authentication other than login-ID and password)

To configure the BaroPAM module, enter it at the top as follows to configure sshd, su, and sudo files.

```
[root] /usr/baropam > vi /etc/pam.d/sshd
#%PAM-1.0
auth       required     /usr/baropam/pam_baro_sql.so nullok secret=/usr/baropam/.baro_sql
encrypt=no auth=sshd
```

For reference, the **secret** parameter sets the BaroPAM configuration file name, the **encrypt** parameter sets the encryption flag (**yes** or **no**) of the BaroPAM configuration file, and the **auth** parameter sets the **sshd, su, sudo, login, radiusd, gdm-password, lightdm, xrdp-sesman**, etc. that are used for authentication using BaroPAM.

* "**nullok**" means that the called PAM module allows entering a password with a null value. However, Redhat 9.x and higher do not support the "**nullok**" option in **/etc/pam.d/sshd** settings.

```
[root] /usr/baropam > vi /etc/pam.d/su
#%PAM-1.0
auth            required        /usr/baropam/pam_baro_sql.so  nullok  secret=/usr/baropam/.baro_sql
encrypt=no auth=su
```

If you add the BaroPAM module to the top of the **/etc/pam.d/su** file, you can apply the 2nd authentication (additional authentication) input even when a general account tries to ascend to "**root**" with the "**su**" command for security. this is further improved.

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

In the case of Desktop Linux, if you want to use BaroPAM on the GUI login screen, enter the setting as follows.

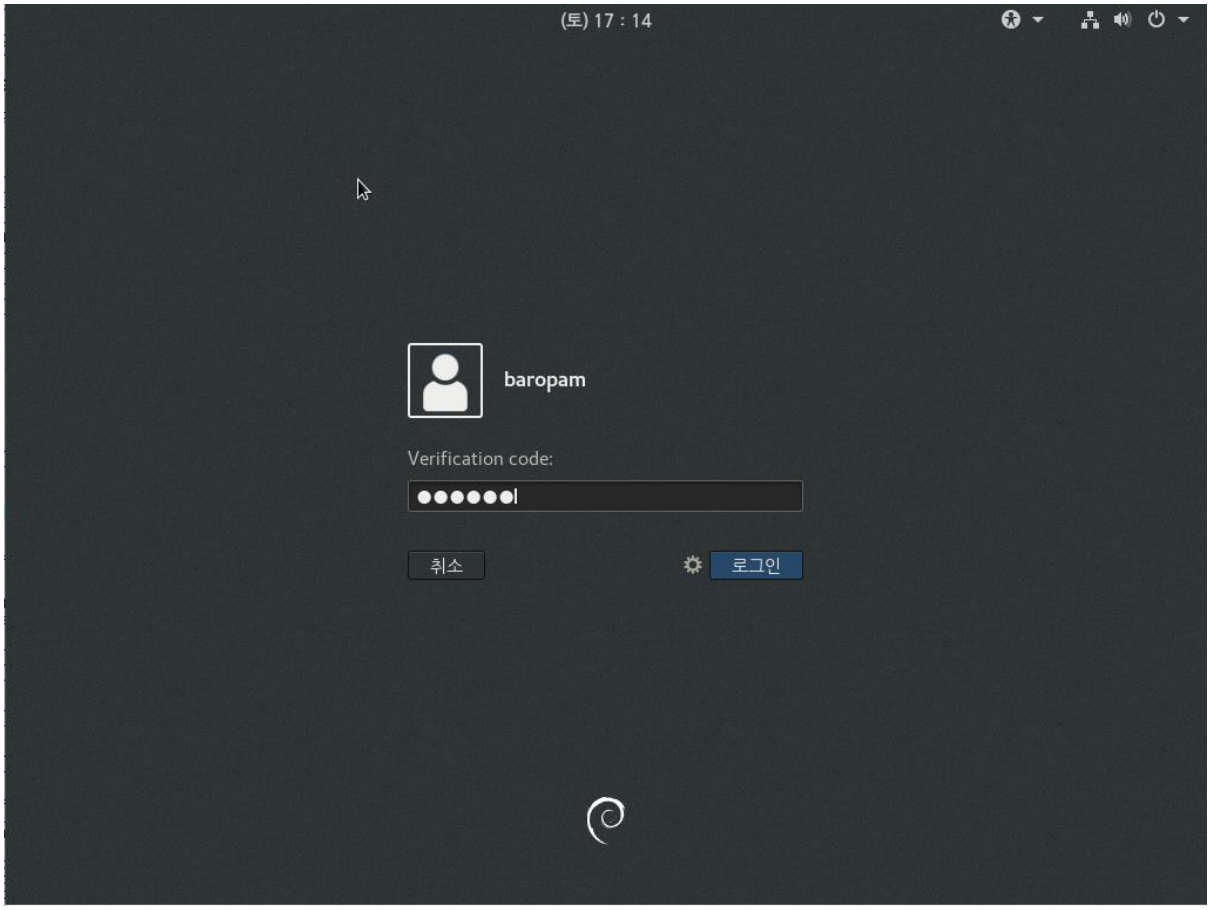
Ex) For Debian, Ubuntu, SUSE, Fedora Linux

```
[root] /usr/baropam > vi /etc/pam.d/gdm-password or gdm-autologin
#%PAM-1.0
auth            required        /usr/baropam/pam_baro_sql.so  nullok  secret=/usr/baropam/.baro_sql
encrypt=no auth=gdm-password
```

After **gdm-password and gdm-autologin** settings are finished, it is necessary to restart **gdm-password** after confirming that the PAM module has been properly added.

```
[root] /usr/baropam > systemctl restart gdm-password
```

Then, the screen to enter "**Verification code:**", which is the OTA key of BaroPAM, appears on the login screen as follows.



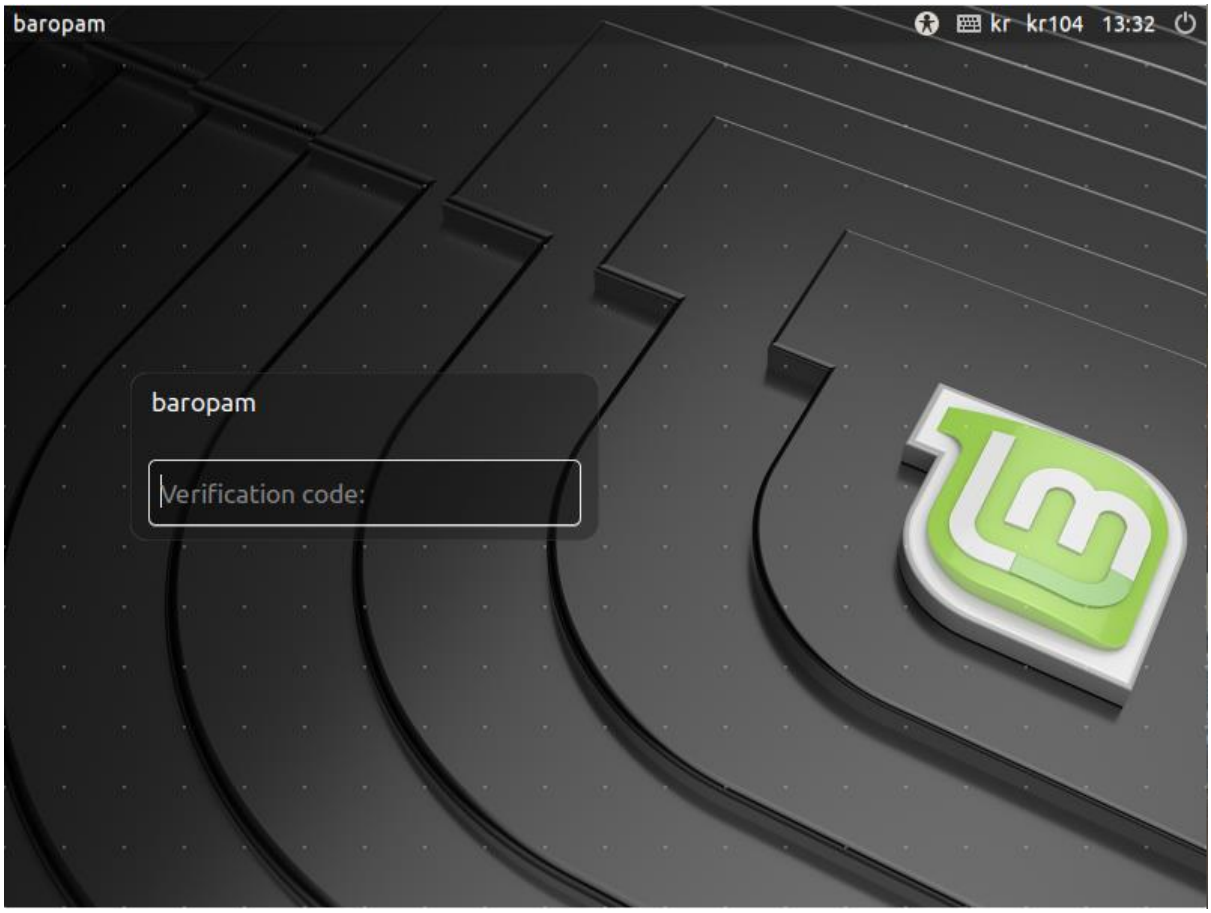
Ex) For Hamonikr OS, Gooroom OS, Mint Linux

```
[root] /usr/baropam > vi /etc/pam.d/lightdm or loghtdm-autologin
#%PAM-1.0
auth            required        /usr/baropam/pam_baro_sql.so  nullok  secret=/usr/baropam/.baro_sql
encrypt=no auth=lightdm
```

After setting **lightdm and lightdm-autologin**, it is necessary to restart **lightdm** after confirming that the PAM module has been properly added.

```
[root] /usr/baropam > systemctl restart lightdm
```

Then, the screen to enter "**Verification code:**", which is the OTA key of BaroPAM, appears on the login screen as follows.



Note) In the case of Desktop Linux, such as an open OS, if you remove the password with the "**passwd -p *username***" command, you will not be asked for the password if you enter only the **OTA key** on the input screen of "**Verification code:**".

Ex) When connecting to a remote desktop using xrdp

```
[root] /usr/baropam > vi /etc/pam.d/xrdp-sesman
#%PAM-1.0
auth       required     /usr/baropam/pam_baro_sql.so forward_pass secret=/usr/baropam/.baro_sql
encrypt=no auth=xrdp-sesman
```

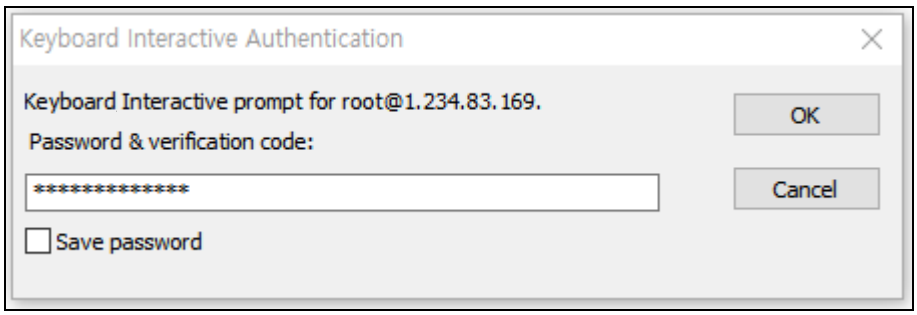
Enter the **OTA key** in the password input window (**Password**) using **forward_pass**. For example, if the **OTA key** is "**123456**", just enter "**123456**".

② Replace password (replace password with OTA key)

For programs like filezilla that cannot perform "**Interactive process**", the only way is to use the **forward_pass** option in PAM to enter the **OTA key** when entering the password. In this case, the openssh client, RDP (Remote Desktop Protocol) of Windows, Radius, filezilla, etc. all have no choice but to input like this.

```
[root] /usr/baropam > vi /etc/pam.d/sshd
#%PAM-1.0
auth       required     /usr/baropam/pam_baro_sql.so forward_pass secret=/usr/baropam/.baro_sql
encrypt=no auth=sshd
```

Enter the OTA key in the password input window (**Password & verification code:**) using **forward_pass**. For example, if the OTA key is "**123456**", just enter "**123456**".



Note) When replacing the password with an OTA key, the password for the account must be set the same as the login-ID in advance with the "**passwd *username***" command.

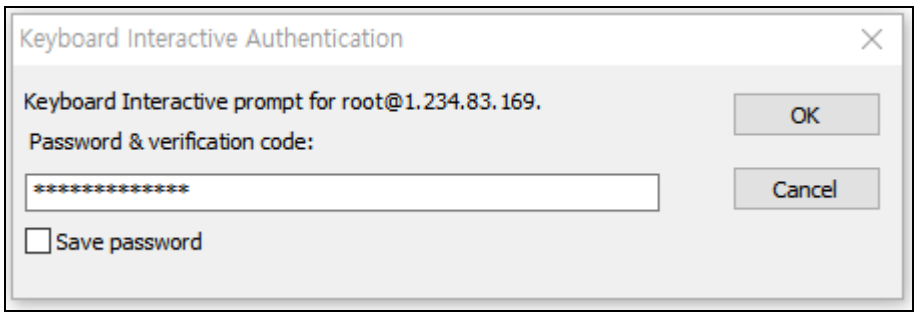
In the case of Desktop Linux, such as an open OS, remove the password with the "**passwd -p *username***" command, and enter the OTA key on the input screen of "**Password & Verification code:**" and the password will not be asked.

③ New password (by combining the password and the OTA key, a new one-time password is generated and applied for each OTA key generation cycle)

For programs like filezilla, which cannot perform "**Interactive process**", the only way is to use the **forward_pass** option in PAM to enter the password and OTA key together when entering the password. In this case, the openssh client, RDP (Remote Desktop Protocol) of Windows, Radius, filezilla, etc. all have no choice but to input like this.

```
[root] /usr/baropam > vi /etc/pam.d/sshd
#%PAM-1.0
auth       required     /usr/baropam/pam_baro_sql.so forward_pass secret=/usr/baropam/.baro_sql
encrypt=no auth=sshd
```

When entering the 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 spaces. For example, if the password is "**baropam**" and the OTA key is "**123456**", enter "**baropam123456**".



Using **forward_pass**, you can enable 2nd authentication for most services that require authentication.

3) cURL authentication

To configure the BaroPAM module, enter it at the top as follows to configure sshd, su, and sudo files.

```
[root] /usr/baropam > vi /etc/pam.d/sshd
#%PAM-1.0
auth       required     /usr/baropam/pam_baro_curl.so nullok secret=/usr/baropam/.baro_curl
encrypt=no
```

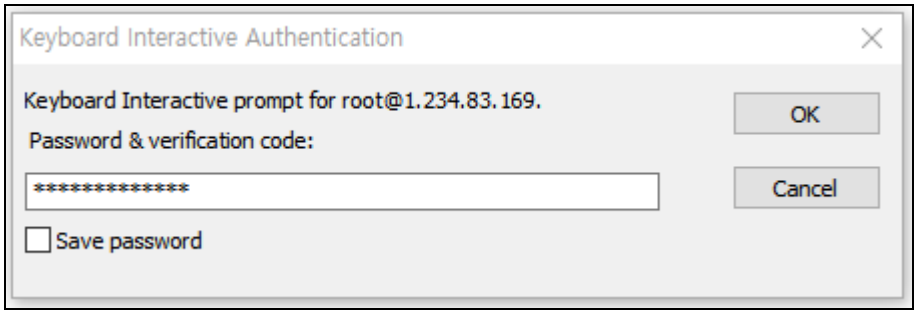
For reference, the **secret** parameter sets the BaroPAM configuration file name, and the **encrypt** parameter sets the encryption flag (**yes** or **no**) of the BaroPAM configuration file.

* "**nullok**" means that the called PAM module allows entering a password with a null value. However, Redhat 9.x and higher do not support the "**nullok**" option in **/etc/pam.d/sshd** settings.

For programs like filezilla, which cannot perform "**Interactive process**", the only way is to use the **forward_pass** option in PAM to enter the password and OTA key together when entering the password. In this case, the openssh client, RDP (Remote Desktop Protocol) of Windows, Radius, filezilla, etc. all have no choice but to input like this.

```
[root] /usr/baropam > vi /etc/pam.d/sshd
#%PAM-1.0
auth       required     /usr/baropam/pam_baro_curl.so forward_pass secret=/usr/baropam/.baro_curl
encrypt=no
```

When entering the 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 spaces. For example, if the password is "**baropam**" and the OTA key is "**123456**", enter "**baropam123456**".



Using **forward_pass**, you can enable 2nd authentication for most services that require authentication.

```
[root] /usr/baropam > vi /etc/pam.d/su
#%PAM-1.0
auth       required     /usr/baropam/pam_baro_curl.so forward_pass secret=/usr/baropam/.baro_curl
encrypt=no
```

If you add the BaroPAM module to the top of the **/etc/pam.d/su** file, you can apply the 2nd authentication (additional authentication) input even when a general account tries to ascend to "**root**" with the "**su**" command for security. this is further improved.

```
$ su - root
Password & verification code:
```

In case of Desktop Linux, if you want to use BaroPAM on the GUI login screen, the setting method is as follows.

Ex) For Debian, Ubuntu, SUSE, Fedora Linux

```
[root] /usr/baropam > vi /etc/pam.d/gdm-password or gdm-autologin
#%PAM-1.0
auth        required      /usr/baropam/pam_baro_curl.so forward_pass secret=/usr/baropam/.baro_curl
encrypt=no
```

After gdm-password and gdm-autologin settings are finished, it is necessary to restart gdm-password after confirming that the PAM module has been properly added.

```
[root] /usr/baropam > systemctl restart gdm-password
```

Ex) For Hamonikr OS, Gooroom OS, Mint Linux

```
[root] /usr/baropam > vi /etc/pam.d/lightdm or loghtdm-autologin
#%PAM-1.0
auth        required      /usr/baropam/pam_baro_curl.so forward_pass secret=/usr/baropam/.baro_curl
encrypt=no
```

After setting lightdm and lightdm-autologin, it is necessary to restart lightdm after confirming that the PAM module has been properly added.

```
[root] /usr/baropam > systemctl restart lightdm
```

Ex) When connecting to a remote desktop using xrdp

```
[root] /usr/baropam > vi /etc/pam.d/xrdp-sesman
#%PAM-1.0
auth       required     /usr/baropam/pam_baro_curl.so forward_pass secret=/usr/baropam/.baro_curl
encrypt=no
```

Enter the OTA key in the password input window (Password) using forward_pass. For example, if the OTA key is "123456", just enter "123456".

3) Configuration of the sshd daemon

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 Redhat 9.x and above	yes	No yes	
ChallengeResponseAuthentication or KbdInteractiveAuthentication	no	yes	
UsePAM	no	yes	

After completing the sshd configuration, make sure that the PAM module is properly added, and then restart the SSH Server.

```
[root] /usr/baropam > service sshd restart or systemctl restart sshd
sshd Stopping: [  OK  ]
sshd Starting: [  OK  ]
```

Ubuntu, Debian or Linux Mint, Fedora:

```
$ systemctl restart ssh
```

If, in the case of Ubuntu or Mint, you cannot connect after restarting ssh, it is a problem with the firewall settings, so you must use the following command to disable the firewall settings and restart.

```
$ sudo ufw disable
$ sudo service ufw restart
```

CentOS or RHEL:

```
$ service sshd restart or systemctl restart sshd
```

4) ACL(Access Control list) settings

1) In the case of PAM authentication (Set environment setting information in File) When using the BaroPAM module, if it is necessary to exclude from the ACL for the account to be excluded from the 2nd authentication, create an ACL file in the directory set when setting the BaroPAM environment, and enter the account to be excluded as follows. (**The file access permission for .baro_acl must be set to 444.**)

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

2) In case of PAM authentication (Set environment configuration information in MariaDB), Mariadb's ACL setting table must be used.

5) NTP(Network Time Protocol) settings

Since BaroPAM is a time synchronization method, if the server's time is different from the current time, login to the server may not be possible because the OTA keys do not match.

Recently, as a method of time synchronization (time server time synchronization) for information assets, the system time can be set to the current time in the root account using NTP (Network Time Protocol).

To use NTP, the NTP package must be installed by default. To check the installation, run the following command. If it is not installed, use the command "**yum install ntp**" for Redhat, CentOS 8 or lower, and "**sudo apt-get install ntp**" for others.

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

The following command can be used to register the ntpd service in the startup program when booting the server and to check whether ntp is activated.

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

Check whether the ntpd daemon is active when booting the server using chkconfig. If it is off in level 3 and 5, it is not activated automatically. To activate automatically, you must change 3 and 5 to on (active) with the following command.

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

NTP servers operating in Korea are as follows.

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

Set the NTP server operating in Korea in "**/etc/ntp.conf**", the configuration file for the ntpd daemon configuration, as follows.

```
[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
```

The **iburst** option is a kind of option setting that shortens the time required for synchronization.

After the setup for the ntpd daemon setup is complete, it is absolutely necessary to restart the NTP daemon after confirming that the NTP setup has been properly added.

```
[root]# /etc/init.d/ntpd restart
Stopping ntpd: [  OK  ]
Starting ntpd: [  OK  ]
```

You can check the ntpd time with the following command.

```
[root]# ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*121.174.142.82  220.73.142.66    3 u  791 1024  377    9.333   -4.250   0.428
+time.bora.net   58.224.35.2      3 u  654 1024  367    2.926  -27.295  24.481
 183.110.225.61  .INIT.          16 u    - 1024    0    0.000    0.000   0.000
 LOCAL(0)        .LOCL.          10 l   39   64  377    0.000    0.000   0.001
```

* The displayed ip is the ntp server getting the current time

To use NTP, the NTP package must be installed by default. To check the installation, run the following command. If it is not installed, use the "**dnf install chrony**" command to install Redhat, CentOS 8 or later versions.

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

NTP servers operating in Korea are as follows.

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

Set the NTP server operating in Korea in "**/etc/chrony.conf**", the configuration file for the ntpd daemon configuration, as follows.

```
[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

# 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
```

After the setup for the ntpd daemon setup is complete, it is absolutely necessary to restart the NTP daemon after confirming that the NTP setup has been properly added. (Starting chrony service and registering drive when booting)

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

You can check the ntpd time with the following command.

List of servers receiving time / list of servers registered in chrony.conf file)

```
[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
```

Server information receiving time)

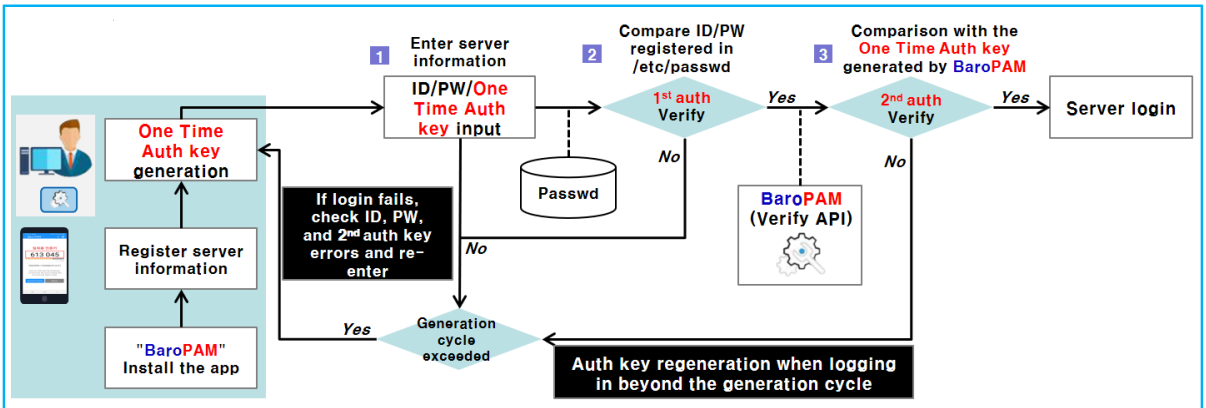
```
[root@baropam ~]# chronyc tracking
Reference ID    : 36B48651 (ec2-54-180-134-81.ap-northeast-2.compute.amazonaw)
Stratum         : 3
Ref time (UTC)  : Sun Mar 22 07:07:43 2020
System time     : 0.000130027 seconds slow of NTP time
Last offset     : -0.000710122 seconds
RMS offset      : 0.000583203 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
```

Check information such as time status and synchronization)

```
[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
```

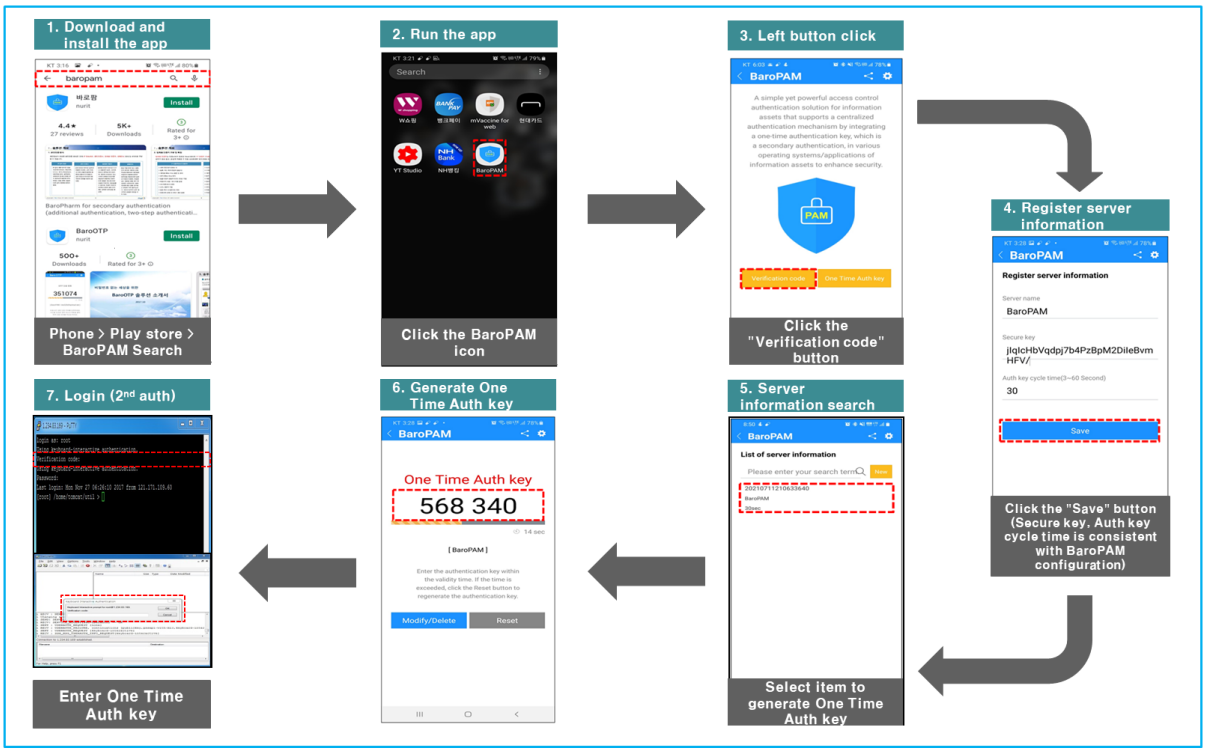
2. BaroPAM application

2.1 BaroPAM application process



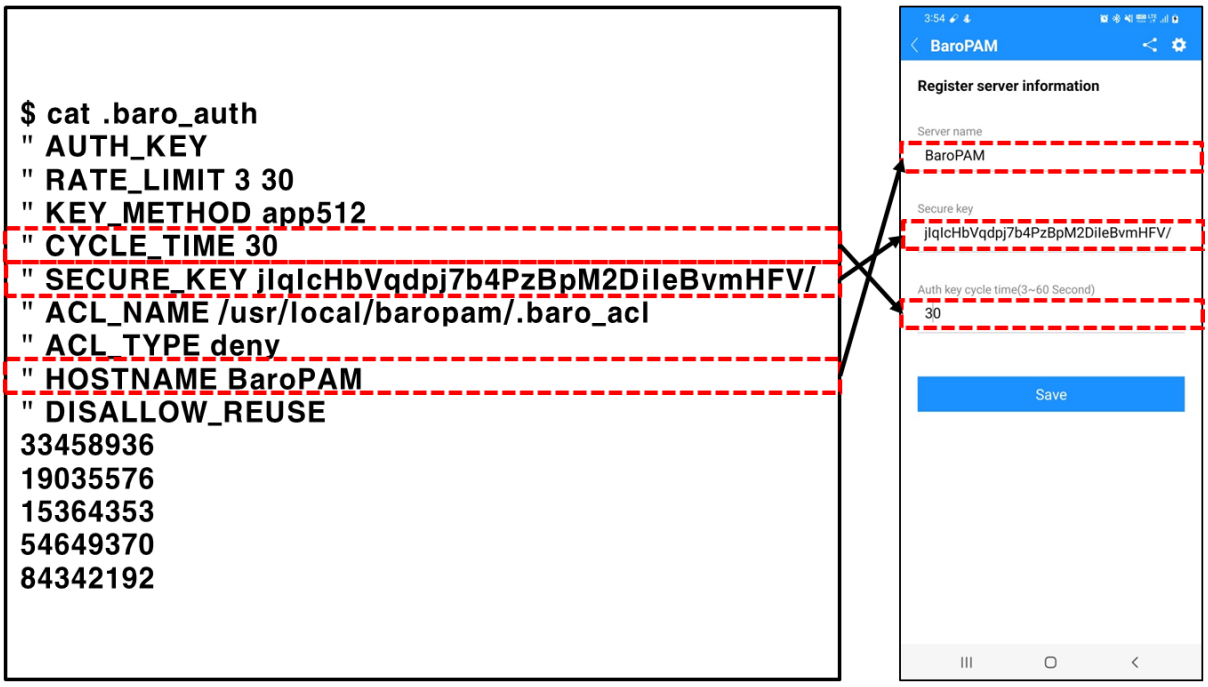
No	Division	Contents	Description
1	2nd auth App (BaroPAM)	Download and install the BaroPAM app	-Android: Play Store access and "BaroPAMs" app download -iPhone: App Store access and "BaroPAMs" app download
2		Run the BaroPAM app	
3		Select the "Verification code" button	-Select the left button at the bottom of the launched app
4		Register server information	-System name: Server name -Secure key: Secure key given to the server(vendor issued) -Auth key cycle time: input between 3 and 60 seconds
5		After saving, click the item that search when viewing the list, and create a One Time Auth key	
6		Connect to the server and log in by entering ID, PW, and One Time Auth key	-Secure key, Auth key cycle time, 2nd authentication verification using One Time Auth key

2.2 BaroPAM application screen



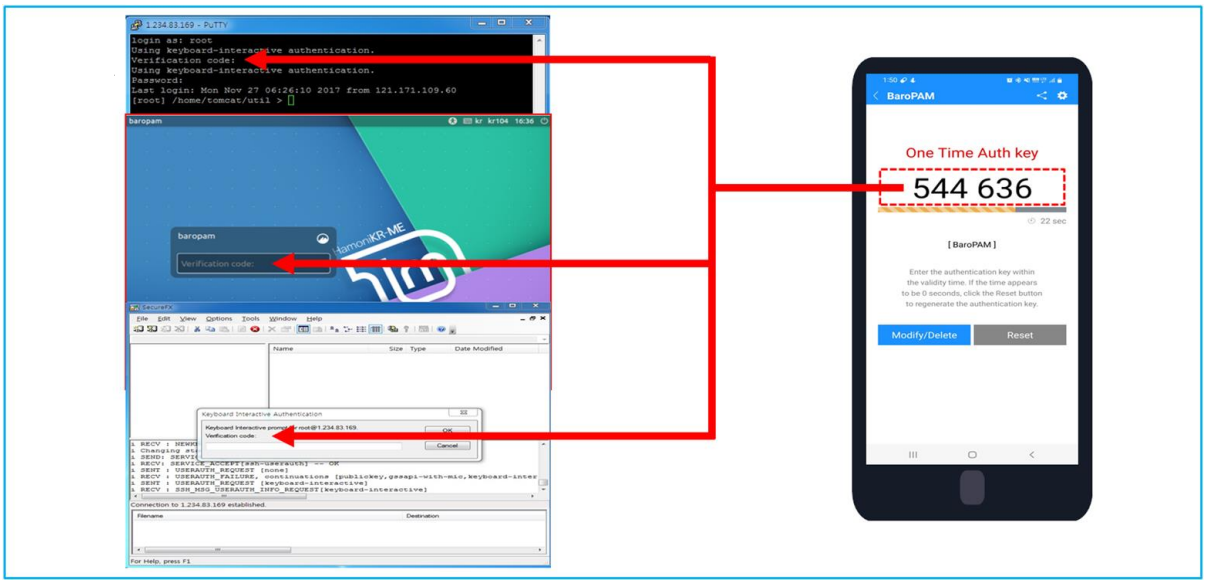
2.3 Linux login method

First, you must enter the same "**cycle time, secure key, server name**" entered on the "**BaroPAM Setup**" screen on the "**Server Information Registration**" screen of the "**BaroPAM**" app.



When logging in to the Linux/Unix environment, enter your user account (Username), create an OTA

key in the "BaroPAM" app on your smartphone, enter the OTA key and "Password" you created in "Verification code:" and press "Enter" Clicking the " button requests authentication to the BaroPAM module, and if verification is successful, the login authentication policy of Linux/Unix is applied.



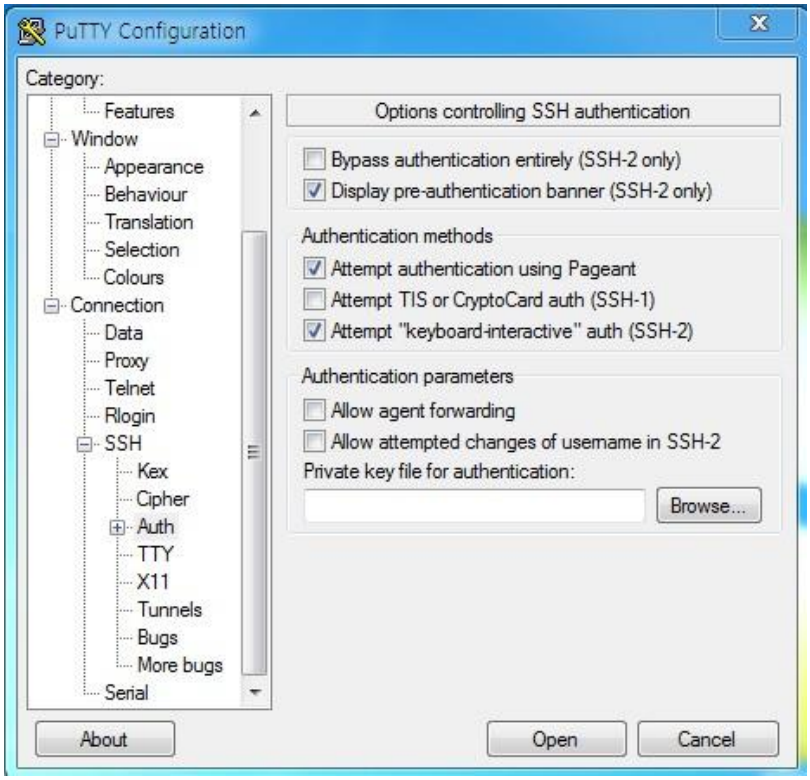
If the OTA key entered on the Linux/Unix login screen fails to be authenticated in the BaroPAM verification module, an "Access denied." message appears on the login screen. Various messages related to BaroPAM authentication are left in syslog.

```
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 connection tool

For putty)

When connecting with Putty, you can do the same as the normal connection process, but there is one thing you need to set. After selecting attempt "Keyboard-Interactive" auth (SSH-2) in "connection -> SSH -> auth" in the environment setting, connect to SSH.

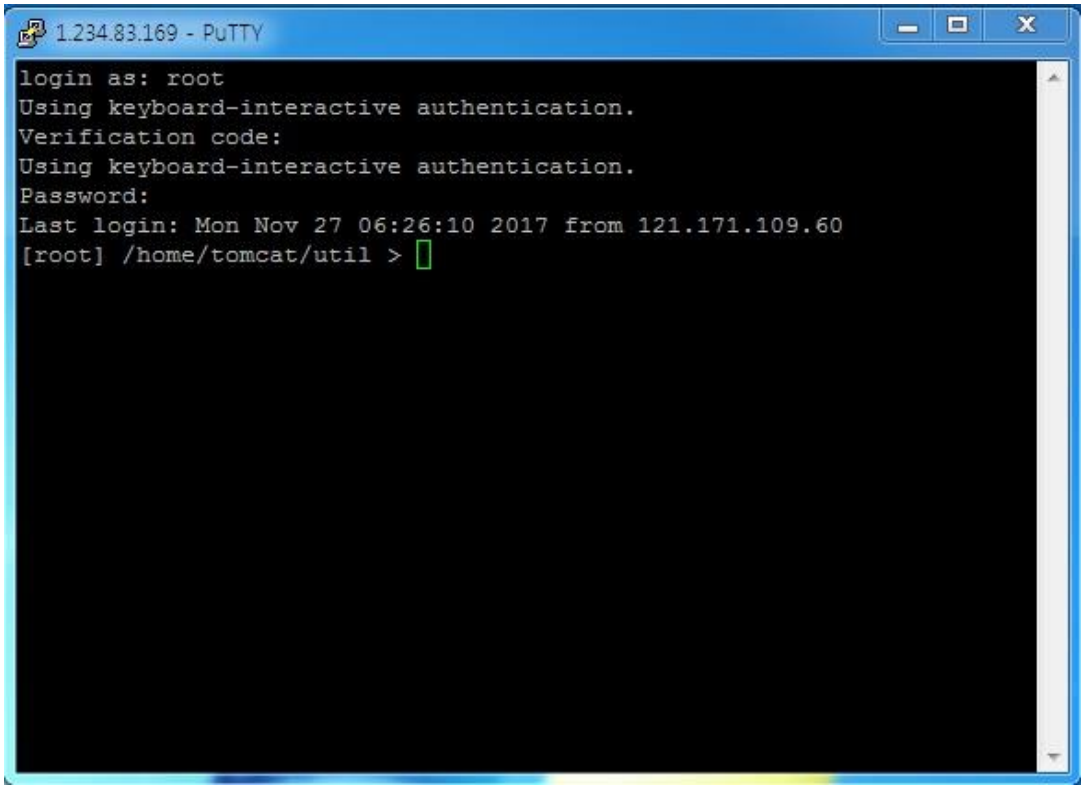


Putty Download and Documentation can be found at the following URL.

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

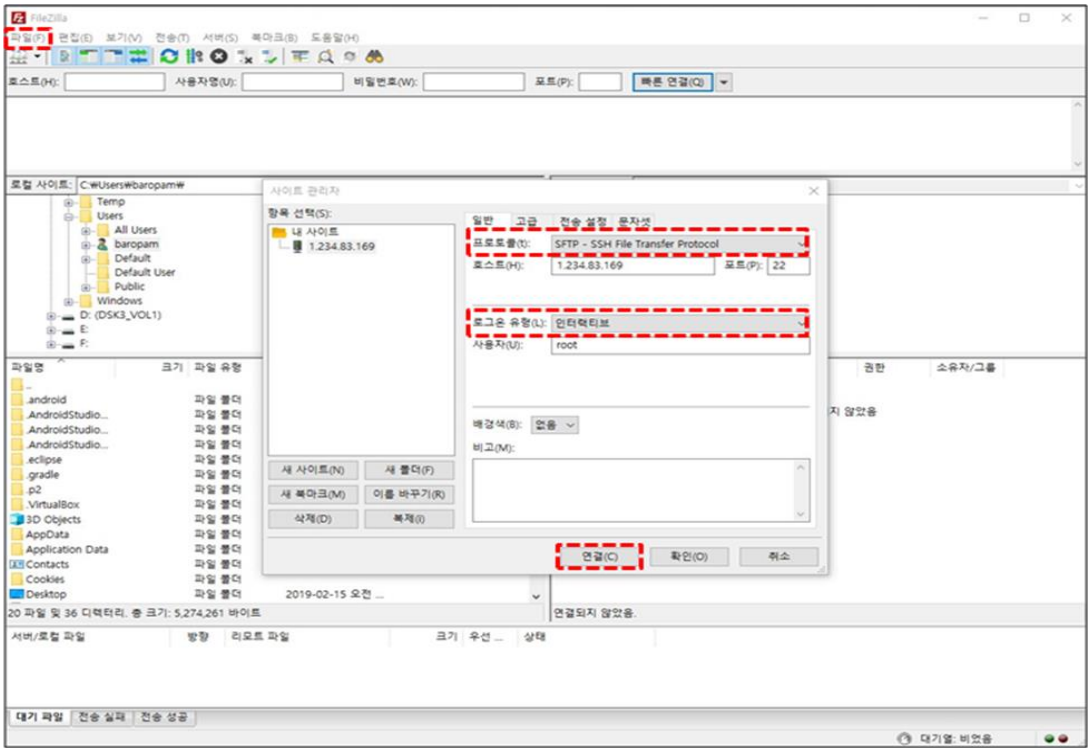
When prompted to enter "**Verification code:**", enter the OTA key generated by the BaroPAM app.

If authentication is successful, you can enter your SSH login password as follows.

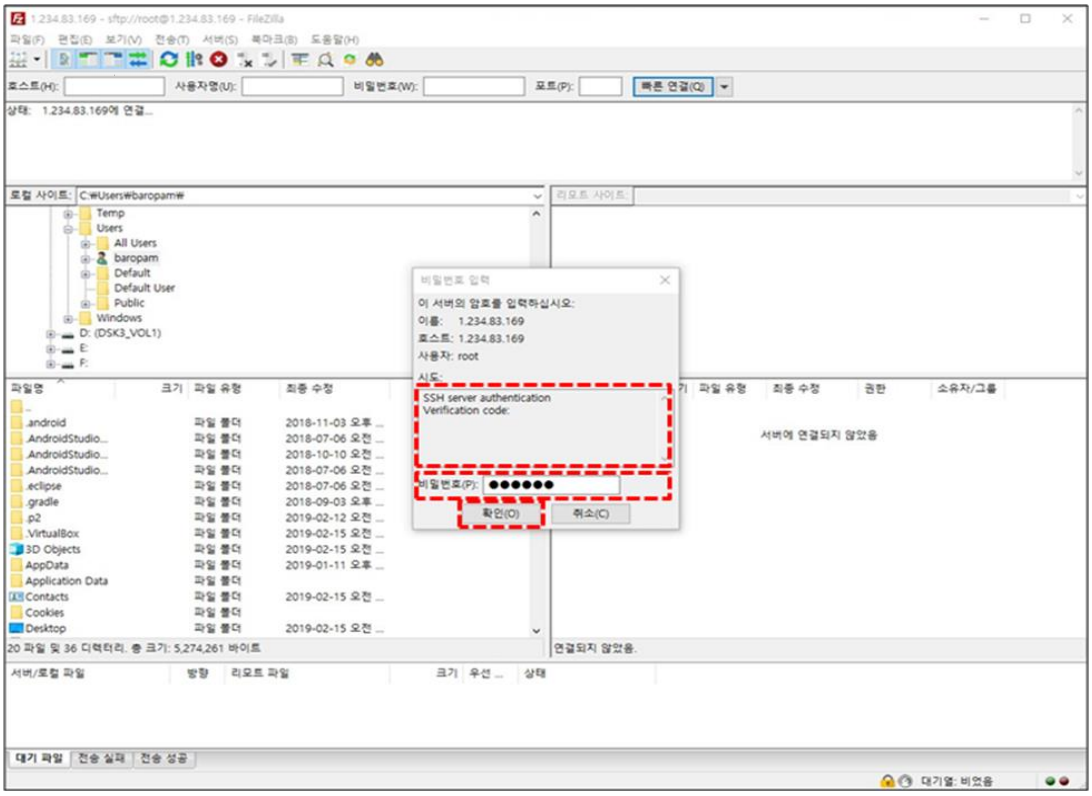


For FileZilla)

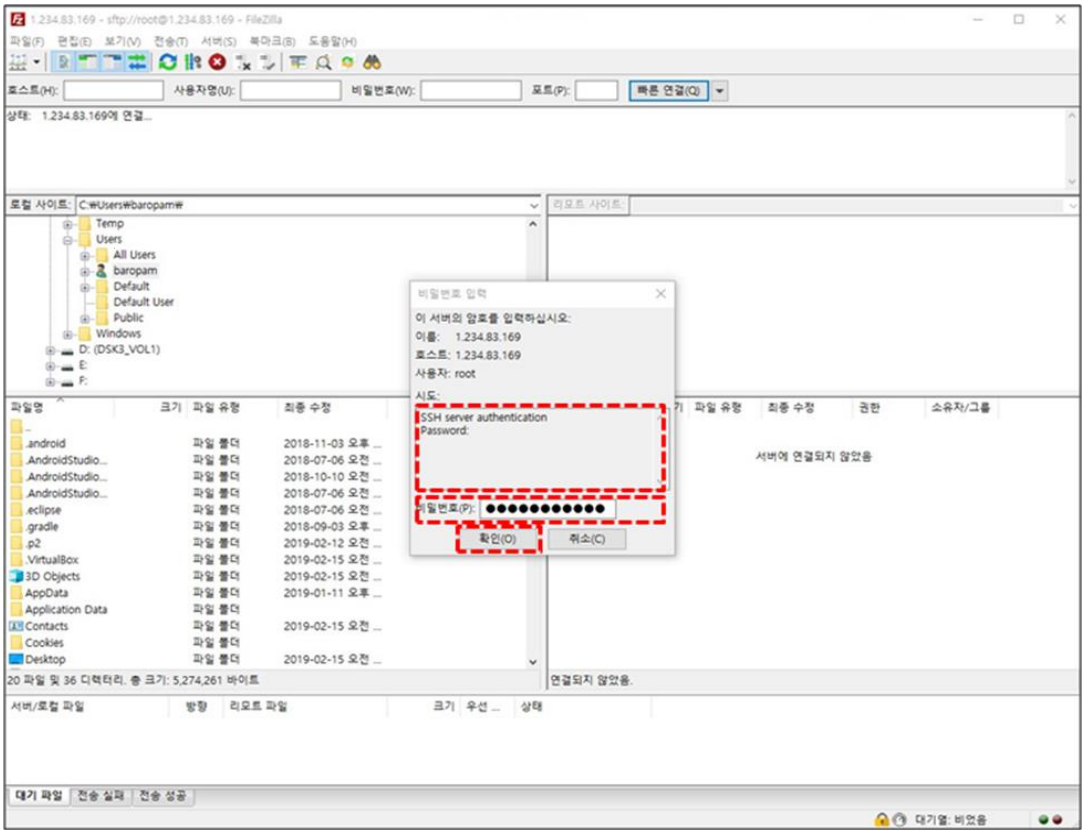
When connecting with FileZilla, it is different from the normal connection process. Select "**File(F) -> Site Manager(S)**" from the top left menu and select "**SFTP - SSH File Transfer Protocol**" from the "**Protocol(t):**" item on the general tab screen. and "**Logon type(L):**" items, select "**Interactive**" and click the "**Connect(C)**" button as follows.



Then, the password input screen appears as follows. Check the contents of "**Attempt:**" on the password input screen, enter the OTA key generated on the smartphone into the "**Password(P):**" input field, and click the "**OK(O)**" button.



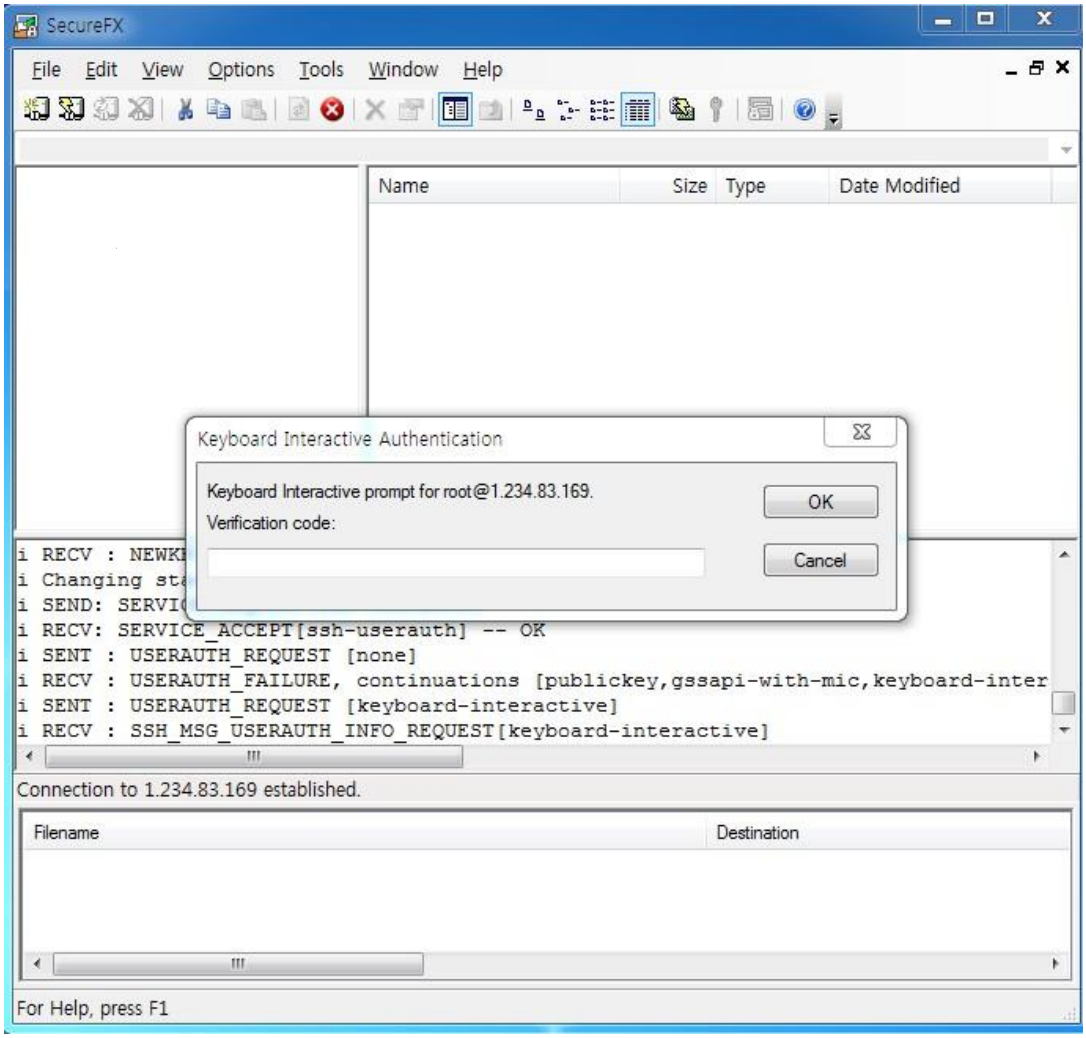
Then, the password input screen appears as follows. Check the "**Attempt:**" content on the password input screen, enter the password for the login account in the "**Password(P):**" input field, and click the "**OK(O)**" button to connect to the server.



For SFTP)

When prompted to enter "**Verification code:**", enter the OTA key generated by the BaroPAM app.

If authentication is successful, you can enter your SFTP login password as follows.



SecureFX Download and Documentation related materials can be found at the following URL.

https://www.vandyke.com/

In conclusion, 2nd authentication can be an effective means of protecting password authentication by adding an extra layer of protection. Whether or not to use it depends on the user's choice, but the adoption of 2nd authentication is an industry trend.

3. Remove BaroPAM

3.1 Remove the BaroPAM environment

If you do not use the BaroPAM module while BaroPAM is installed, comment (#) or delete the settings in the sshd, su, and sudo files as follows.

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

Among the contents of the "/etc/ssh/sshd_config" file configured for the sshd daemon, the following parameters must be changed.

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

After completing the sshd configuration, make sure that the PAM module is properly removed and restart the SSH Server.

```
[root] /usr/baropam > service sshd restart
Stopping sshd: [  OK  ]
Starting sshd: [  OK  ]
```

Ubuntu, Debian or Linux Mint:

```
$ service ssh restart
```

Fedora:

```
$ systemctl restart sshd
```

CentOS or RHEL:

```
$ service sshd restart
```

4. BaroPAM FAQ

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 Windows or Server must be the same.
Action: Check if the phone and Windows or Server time are correct.

Message: Feb 7 07:59:09 eactive sshd(pam_baro_auth)[29657]: ACL file ".baro_acl" must only be accessible by user id root
Cause: Permission of .baro_acl file is different.
Action: Set Permission of .baro_acl file to 444.

Message: Feb 7 08:02:15 eactive sshd(pam_baro_auth)[29739]: Failed to acl file read ".baro_acl"
Cause: Occurs when the .baro_acl file does not exist.
Action: Create a .baro_acl file in the baropam home directory. (Set Permission to 444)

Message: Cannot look up user id xxxxx
Cause: Occurs when user ID xxxxx cannot be retrieved.
Action: Register user id xxxxx in /etc/passwd file.

Message: Failed to secret file read .baro_auth
Cause: Occurs when the secret file does not exist.
Action: Check the existence of the secret file.

Message: Secret file .baro_auth must only be accessible by root
Cause: Occurs when the permission of the .baro_auth file is different.
Action: Set Permission of .baro_auth file to 444.

Message: Invalid file size for .baro_auth
Cause: Occurs when the size of the .baro_auth file is not 1 < size < 64K.
Action: Check the size of the .baro_auth file.

Message: Could not read .baro_auth
Cause: Occurs when the .baro_auth file does not exist or the permission of the file is not 444.
Action: Check the existence of the .baro_auth file and the permission of the file.

Message: Invalid file contents in .baro_auth
Cause: Occurs when the content (rule) of the .baro_auth file is incorrect.
Action: Check the contents of the .baro_auth file.

Message: Failed to create tmp secret file[*error message*]
Cause: Occurs when a temporary secret file cannot be created.
Action: Check the error message for the reason why the temporary secret file could not be created.

Message: Failed to open tmp secret file .baro_auth~[*error message*]
Cause: 1. In the case of Redhat and CentOS, it is blocked due to security issues because SELINUX is not disabled.
2. Occurs when the temporary secret file .baro_auth~ cannot be opened.
Action: 1. Disable SELINUX in "/etc/sysconfig/selinux" (SELINUX=enforcing → disabled)

```
[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
```

It does not take effect right away and requires a reboot for it to take effect. If you want to apply changes only to the currently connected terminal without rebooting, run the following command.

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

2. Check the error message for the reason why the temporary secret file .baro_auth~ could not be opened.

Message: Secret file .baro_auth changed while trying to use one-time authentication key
Cause: Occurs when secret file .baro_auth is changed while using OTA key.
Action: Try logging in again.

Message: Failed to update secret file .baro_auth[*error message*]
Cause: Occurs when the secret file cannot be changed.
Action: Check the error message for why the secret file could not be changed.

Message: Invalid RATE_LIMIT option. Check .baro_auth
Cause: Occurs when the RATE_LIMIT setting value of the secret file .baro_auth file is set incorrectly.
Action: Check the setting values of the limit count (1 < RATE_LIMIT < 100) and the limit time (1 < interval < 3600).

Message: Invalid list of timestamps in RATE_LIMIT. Check .baro_auth
Cause: Occurs when updated timestamps in the RATE_LIMIT option among the contents of the .baro_auth file, which is a secret file, are incorrect.
Action: Check the updated timestamps in the RATE_LIMIT option of the .baro_auth file, which is the secret file.

Message: Try to update RATE_LIMIT line.
Cause: The message displayed when you log in normally.
Action: No action

Message: Too many concurrent login attempts. Please try again.
Cause: When the DISALLOW REUSE option of the .baro_auth file, which is the secret file, (In the OTA key generation cycle, one login only) is set.
Occurs when login is retried within the OTA key creation cycle after successful login.
Action: Login retry after OTA key generation cycle.

Message: 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.
Cause: The DISALLOW_REUSE option of the .baro_auth file, which is the secret file, is an option in preparation for man-in-the-middle attacks.
A man-in-the-middle attack occurs when an unauthorized entity places itself between two communication systems and intercepts the passing of information that is currently in progress.
In a nutshell, what could be called a modern wiretapping system.
Action: No action

Message: Failed to allocate memory when updating .baro_auth
Cause: Occurs when memory allocation fails when updating the secret file, .baro_auth.
Action: Technical support

Message: Can't find SECURE_KEY[*error message*]
Cause: Occurs when there is no SECURE_KEY option or set value in the .baro_auth file, which is the secret file.
Action: Check the SECURE_KEY option or setting value of the .baro_auth file, which is the secret file.

Message: Verification code generation failed.[*error message*]
Cause: Occurs when OTA key verification fails.
Action: Login retry.

Message: Invalid verification code
Cause: Occurs when OTA key verification fails.
Action: Login retry.

Message: Invalid verification code
Can not make/remove entry for session.
Cause: The server's system time is not correct.
Action: Check if the system time of the server is correct with the date command, and if it is incorrect, adjust the time.
1. date Command Change the server's system time (temporary solution)
2. Check whether ntp is set, and if it is set, reduce the cycle for setting the ntp time. If not set, ntp must be set.

Message: Mar 12 15:37:01 baropam gdm(pam_baro_auth)[1215]: [ID 128276 auth.error] No user name available when checking verification code
Cause: If you are not a usable user when verifying the authorization code (occurs when you are not a registered user).
Action: Check with your system administrator to see if your Login-ID is registered.

Message: 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
Cause: 1. It occurs because the /usr/baropam/pam_baro_auth.so file does not exist.
2. Occurs because the installed pam_baro_auth.so module does not match the OS version.
Action: 1. Check if the BaroPAM module file (pam_baro_auth.so) exists. If not, copy it from the BaroPAM installation file.
2. After checking the OS version, you must download and reinstall the BaroPAM module that matches the OS version.

Message: mm_log_handler: write: Broken pipe
mm_request_send: write: Broken pipe
Cause: This is how often keepalive messages should be sent to the server within seconds.
The server may close connections that have been idle for too long. client
(ServerAliveInterval) or You can update the server (ClientAliveInterval).
Action: You can set ServerAliveInterval in /etc/ssh/ssh_config on the client machine or
ClientAliveInterval in /etc/ssh/sshd_config on the server machine. If the error persists,
the interval should be reduced.
ServerAliveInterval ==> If no data is received from the server, ssh sets the timeout
interval in seconds to request a response from the server by
sending a message over an encrypted channel. Defaults to 0,
indicating that this message is not sent to the server. This
option only applies to protocol version 2.
ClientAliveInterval ==> If no data is received from the client, sshd sends a message over
an encrypted channel to request a response from the client. Default
is 0. Indicates that this message is not sent to the client. This
option only applies to protocol version 2.

To update your server(and restart your sshd) ==> Update the server (to restart sshd) and
echo "ClientAliveInterval 60" | sudo tee -a /etc/ssh/sshd_config

Or client-side: ==> Or client-side:
echo "ServerAliveInterval 60" >> ~/.ssh/config

ClientAliveInterval: Interval to check if client is alive
ClientAliveCountMax: The number of times the connection is maintained even if there is no
response from the client
For example, if ClientAliveInterval=15, ClientAliveCountMax=3, disconnect after 45 seconds

Message: May 19 12:37:37 baropam sshd(pam_baro_auth)[1416]: Failed to acl file read "(null)"
Cause: Occurs due to acl file existence and file permission issues.
Action: Create empty acl file .baro_acl file with 444 permissions.

Message: Failed to compute location of secret file
Cause: Occurs when the secret file set in pam does not exist in the directory.
Action: If the secret file set in pam does not exist in the directory, the secret file must be
created in the directory.
ex) auth required /usr/baropam/pam_baro_auth.so nullok secret=/usr/baropam/.baro_auth
encrypt=no

Message: Failed to compute location of encrypt flag
Cause: Occurs when the encryption flag does not exist in pam.
Action: Encryption flags (yes, no) must be set in pam.
ex) auth required /usr/baropam/pam_baro_auth.so nullok secret=/usr/baropam/.baro_auth
encrypt=no

Message: If ssh connection is not available after installing HamoniKR OS
Cause: It occurs because the firewall of HamoniKR OS is set.
Action: After disabling the firewall of HamoniKR OS, restart ufw.
> sudo ufw disable
> sudo service ufw restart

Message: BaroPAM applied to Screen saver is released after rebooting Grooroom OS

Cause: When Grooroom OS is rebooted, lightdm, a setting file related to Screen saver, is initialized.
Action: Just set BaroPAM in the restore file "/usr/share/debian-system-adjustments/pam.d/lightdm".

Message: Oct 14 10:09:43 baropam sshd[18075]: PAM unable to dlopen(/usr/baropam/pam_baro_auth.so): /usr/baropam/pam_baro_auth.so: undefined symbol: curl_easy_setopt
Cause: It occurs because the library related to the web development tool cURL (Client for URLs) does not exist.
Action: For Redhat series, use "yum install curl" and others with "sudo apt-get install curl" command.

Message: Did not receive verification code from user
error: ssh_msg_send: write: Broken pipe
Cause: Occurs when the secure key is set incorrectly.
Action: Check the set Secure key.
Check if the secure key is provided by the vendor.

Message: PAM: authentication thread exited unexpectedly.
***** glibc detected *** su: free(): invalid pointer: 0x00002aede020c9e2 *****
Cause: Occurs when the BaroPAM environment setting file (.baro_nurit) does not exist.
Action: Check if the BaroPAM environment setting file (.baro_nurit) exists. If not, copy it from the BaroPAM installation file.

Message: 개방형OS인 구름OS에서 비밀번호를 변경한 후 로그인에 실패하여 로그인이 안되는 현상 발생.
Jul 8 09:31:51 gooroom lightdm: pam_unix(lightdm-greeter:session): session closed for user lightdm
Jul 8 09:31:51 gooroom lightdm: pam_unix(lightdm:session): session opened for user baropam(uid=1000) by (uid=0)
Jul 8 09:31:51 gooroom systemd-logind[446]: Removed session c1.
Jul 8 09:31:51 gooroom systemd-logind[446]: New session 4 of user baropam.
Jul 8 09:31:51 gooroom lightdm: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Jul 8 09:31:51 gooroom systemd-logind[446]: Removed session 4.
Jul 8 09:31:52 gooroom lightdm: pam_unix(lightdm-greeter:session): session opened for user lightdm(uid=104) by (uid=0)
Jul 8 09:31:52 gooroom systemd-logind[446]: New session c2 of user lightdm.
Cause: 약한 비밀번호로 변경한 경우 발생.
Action: 대소문자를 포함해서 8자리 이상의 강한 비밀번호로 변경.

Message: A phenomenon in which login fails after applying BaroPAM on gooroom OS, an open OS, occurs.
Cause: Occurs when setting BaroPAM in lightdm by setting one of the parameters to nullok.
Action: When setting up BaroPAM in lightdm, change nullok to forward_pass among the parameters.

Message: No supported authentication methods available (server sent publickey,gssapt-keyex,gssapt-with-mic)
Cause: Interactive mode is not supported. (When setting /etc/pam.d/sshd, do not set nullok but set it to forward_pass.)
Action: Change "PasswordAuthentication yes" in the "/etc/ssh/sshd_config" file and restart sshd.

Message: After applying BaroPAM to the Linux server, logging in is not possible due to skipping the item for entering the one-time authentication key (Verification code: or Password & Verification code:).

If a server access control solution is applied, BaroPAM is applied, but login is not possible.

Cause: This occurs because BaroPAM settings are set before those set in /etc/pam.d/sshd in the server access control solution.

Action: You can change the order of /etc/pam.d/sshd settings as follows.

Before change)

```
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
```

After change)

```
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
```

Control refers to how to handle the success or failure of a specific module when setting up PAM.

Among controls, include and substack are the same in that they load other PAM-related modules, but the difference is that substack does not process the remaining modules according to the results of the substack's operation.

5. Install and configure MySQL/MariaDB

5.1 Install MariaDB

```
[root@localhost ~]# dnf -y install mariadb-server
```

When the MaraDB installation process is completed normally, start MariaDB using the following command.

```
[root@localhost ~]# systemctl start mariadb
```

You need to take a few steps to improve MariaDB security options by running the scripts provided with MariaDB.

```
[root@localhost ~]# mysql_secure_installation
```

A series of prompts will appear, and if you don't know you set a password, press Enter when prompted.

```
Enter current password for root (enter for none): Enter
```

Next, confirm that you want to set a new **root** password and set a strong password.

```
Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.
Set root password? [Y/n] y
New password: baropam
Re-enter new password: baropam
Password updated successfully!
Reloading privilege tables..
... Success!
```

All you have to do is press Enter for the prompt that follows.

Remove anonymous users.

```
Remove anonymous users? [Y/n] y
... Success!
```

Do not allow **root** login remotely.

```
Disallow root login remotely? [Y/n] y
... Success!
```

Remove the test database.

```
Remove test database and access to it? [Y/n] y
- Dropping test database...
... Success!
```

```
- Removing privileges on test database...
... Success!
```

Reload the privilege table.

```
Reload privilege tables now? [Y/n] y
... Success!
Cleaning up...
```

5.2 MariaDB configuration

First create a database and database user for FreeRADIUS, then create a database and a user identified by a password.

Ex)

```
Database: baropamdb
User: nurit
Password: baropams
```

You can change the user and password to whatever you want, but you'll need to pay attention to the configuration you'll do later to change the values appropriately.

Start by accessing the MySQL/MariaDB console as **root**.

```
[root@baropam /]# mysql -uroot -p
Enter password: baropam
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 8.0.26 Source distribution

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

Execute command to create database and user.

```
MariaDB [(none)]> CREATE DATABASE baropamdb;
MariaDB [(none)]> CREATE USER 'nurit'@'localhost' IDENTIFIED BY 'baropams';
MariaDB [(none)]> GRANT ALL ON baropamdb.* TO 'nurit'@'localhost';
MariaDB [(none)]> FLUSH PRIVILEGES;
MariaDB [(none)]> use baropamdb
```

Next, create the RADIUS MySQL schema as the newly created database.

```
#
# Table structure for table 'TB_BARO_HOST'
```

```
#

CREATE TABLE IF NOT EXISTS TB_BARO_HOST (
  HOSTNAME       VARCHAR(30)  NOT NULL default '',
  RATE_CNT       VARCHAR(2)   NOT NULL default '5',
  RATE_SEC       VARCHAR(3)   NOT NULL default '30',
  RATE_TIME      VARCHAR(110)     NULL default '',
  KEY_METHOD     VARCHAR(6)   NOT NULL default 'app512',
  CYCLE_TIME     VARCHAR(2)   NOT NULL default '60',
  SECURE_KEY     VARCHAR(32)  NOT NULL default 'jlqlcHbVqdpj7b4PzBpM2DileBvmHFV/',
  ACL_TYPE       VARCHAR(5)   NOT NULL default 'deny',
  MIDDLE_TYPE    VARCHAR(14)  NOT NULL default 'DISALLOW_REUSE',
  MIDDLE_TIME    VARCHAR(8)       NULL default '',
  ENV_TYPE       VARCHAR(8)   NOT NULL default 'share',
  PRIMARY KEY (HOSTNAME)
) ENGINE = INNODB;

#
# Table structure for table 'TB_HOST_EOTA'
#

CREATE TABLE IF NOT EXISTS TB_HOST_EOTA (
  HOSTNAME       VARCHAR(30)  NOT NULL default '',
  EMERGENCY_KEY  VARCHAR(8)   NOT NULL default '',
  PRIMARY KEY (HOSTNAME,EMERGENCY_KEY)
) ENGINE = INNODB;

#
# Table structure for table 'TB_BARO_ACL'
#

CREATE TABLE IF NOT EXISTS TB_BARO_ACL (
  HOSTNAME       VARCHAR(30)  NOT NULL default '',
  USERNAME       VARCHAR(40)  NOT NULL default '',
  PRIMARY KEY (HOSTNAME,USERNAME)
) ENGINE = INNODB;

#
# Table structure for table 'TB_BARO_USER'
#

CREATE TABLE IF NOT EXISTS TB_BARO_USER (
  HOSTNAME       VARCHAR(30)  NOT NULL default '',
  USERNAME       VARCHAR(40)  NOT NULL default '',
  RATE_CNT       VARCHAR(2)   NOT NULL default '5',
  RATE_SEC       VARCHAR(3)   NOT NULL default '30',
  RATE_TIME      VARCHAR(110)     NULL default '',
  KEY_METHOD     VARCHAR(6)   NOT NULL default 'app512',
  CYCLE_TIME     VARCHAR(2)   NOT NULL default '60',
  SECURE_KEY     VARCHAR(32)  NOT NULL default 'jlqlcHbVqdpj7b4PzBpM2DileBvmHFV/',
  ACL_TYPE       VARCHAR(5)   NOT NULL default 'deny',
  MIDDLE_TYPE    VARCHAR(14)  NOT NULL default 'DISALLOW_REUSE',
  MIDDLE_TIME    VARCHAR(8)       NULL default '',
```

```
  PRIMARY KEY (HOSTNAME,USERNAME)
) ENGINE = INNODB;

#
# Table structure for table 'TB_USER_EOTA'
#

CREATE TABLE IF NOT EXISTS TB_USER_EOTA (
  HOSTNAME       VARCHAR(30)  NOT NULL default '',
  USERNAME       VARCHAR(40)  NOT NULL default '',
  EMERGENCY_KEY  VARCHAR(8)   NOT NULL default '',
  PRIMARY KEY (HOSTNAME,USERNAME,EMERGENCY_KEY)
) ENGINE = INNODB;

#
# Table structure for table 'TB_BARO_LOG'
#

CREATE TABLE IF NOT EXISTS TB_BARO_LOG (
  AUTH_DTTM      VARCHAR(10)  NOT NULL default '',
  HOSTNAME       VARCHAR(30)  NOT NULL default '',
  USERNAME       VARCHAR(40)  NOT NULL default '',
  REMOTE_IP      VARCHAR(30)      NULL default '',
  AUTH_MSG       VARCHAR(200) NOT NULL default '',
  PRIMARY KEY (AUTH_DTTM, HOSTNAME, USERNAME)
) ENGINE = INNODB;
```

6. About BaroPAM

Version 1.0 - Official Release - 2016.12.1

http://www.nurit.co.kr

Company: Nurit Co., Ltd.
Registration Number: 258-87-00901
CEO: Jongil Lee
Tel: +8210-2771-4076(Technical support, sales inquiry)
email: mc529@nurit.co.kr
Address: #913, 15, Magokjungang 2-ro, Gangseo-gu, Seoul (Magok-dong, Magok Techno Tower 2)