

정보자산의 보안강화를 위하여 **3단계 인증**을 위한

BaroPAM 솔루션 설치 요약서 (FreeRADIUS)

2024. 1.

II . BaroPAM FreeRADIUS 설치

1. FreeRADIUS 설치

1) 먼저, BaroPAM 설치 설치되어 있어야 함.

BaroPAM 설치 가이드(Linux) 참조

2) FreeRADIUS 설치(Redhat 계열을 기준으로 작성됨)

```
[root]# dnf -y install freeradius freeradius-utils
```

설치된 FreeRADIUS를 제거하려고 할 때 → **dnf -y erase freeradius freeradius-utils**

3) EAP에 대한 인증서 생성

```
[root]# cd /etc/raddb/certs
```

```
[root]# ./bootstrap
```

EAP에 대한 인증서를 생성하지 않으면 다음과 같은 오류가 발생.

```
Failed reading private key file /etc/raddb/certs/server.pem
:error:06065064:digital envelope routines:EVP_DecryptFinal_ex:bad decrypt
rlm_eap_tls: Failed initializing SSL context
rlm_eap (EAP): Failed to initialise rlm_eap_tls
/etc/raddb/mods-enabled/eap[17]: Instantiation failed for module "eap"
```

II . BaroPAM FreeRADIUS 설치

2. FreeRADIUS 설정

1) 사용자 및 그룹 업데이트

```
[root]# vi /etc/raddb/radiusd.conf
#user = radiusd
#group = radiusd
user = root
group = root
```

2) 문제 해결을 위한 로깅 활성화

```
[root]# [root]# vi /etc/raddb/radiusd.conf
auth = yes
auth_badpass = yes
auth_goodpass = yes
```

3) PAM 설정

```
[root]# vi /etc/raddb/sites-enabled/default

#Pluggable Authentication Modules.
pam
```

4) auth와 reply 로그 활성화

```
[root]# vi /etc/raddb/sites-enabled/default
#      auth_log
      auth_log

#      reply_log
      reply_log
```

5) PAM 모듈 활성화

```
[root]# ln -s /etc/raddb/mods-available/pam /etc/raddb/mods-enabled/
```

II. BaroPAM FreeRADIUS 설치

2. FreeRADIUS 설정

6) Client 접속 정보 설정

```
[root]# vi /etc/raddb/clients.conf
```

```
client 10.21.2.205 {  
    ipaddr = 10.21.2.205    ipv4addr = *    # any. 10.21.2.205 == localhost  
    secret = baropam  
    require_message_authenticator = no  
    nas_type = other  
}
```

기본 설정

```
client localhost {  
    ipaddr = 127.0.0.1    ipv4addr = *    # any. 127.0.0.1 == localhost  
    secret = baropam  
    require_message_authenticator = no  
    nas_type = other  
}
```

7) 인증 유형 설정

```
[root]# vi /etc/raddb/users
```

```
DEFAULT Group == "disabled", Auth-Type := Reject  
Reply-Message = "Your account has been disabled."  
DEFAULT Auth-Type := PAM
```

The screenshot shows the 'Radius Settings' window with the following configuration:

- Global RADIUS Settings**
 - RADIUS Server Timeout: 3 (seconds) (Range:1-60, Default: 3)
 - Retries: 2 (Range:0-10, Default:2)
- Radius Servers**
 - Radius Servers: 1
- Primary Server**
 - IP Address: []
 - Shared Secret: [] (Length: 1 to 64 characters)
 - Port Number: 1812 (Range:1-65535, Default:1812)
- Secondary Server** (highlighted with a red dashed box)
 - IP Address: 10.21.2.205
 - Shared Secret: [] (Length: 1 to 64 characters)
 - Port Number: 1812 (Range:1-65535, Default:1812)

Buttons: OK, Cancel

II . BaroPAM FreeRADIUS 설치

3. FreeRADIUS 기본 테스트

```
1) 디버그 모드로 실행
[root]# radiusd -X
..
[ lines of configuration details]
}
Listening on auth address * port 1812 bound to server default
Listening on acct address * port 1813 bound to server default
Listening on auth address :: port 1812 bound to server default
Listening on acct address :: port 1813 bound to server default
Listening on auth address 127.0.0.1 port 18120 bound to server inner-tunnel
Listening on proxy address * port 45094
Listening on proxy address :: port 35184
Ready to process requests

2) 테스트할 사용자 등록
[root]# $ useradd baropam
[root]# $ passwd baropam
Changing password for user baropam.
New password: nurit
Retype new password: nurit
passwd: all authentication tokens updated successfully.

3) 기본 설정으로 테스트 → radtest <username> <password> <IP Addr> 0 <secret>
[root]# radtest baropam nurit localhost 0 baropam
Sent Access-Request Id 220 from 0.0.0.0:33872 to 127.0.0.1:1812 length 77
  User-Name = "baropam"
  User-Password = "nurit"
  NAS-IP-Address = 192.168.21.1
  NAS-Port = 0
  Message-Authenticator = 0x00
  Cleartext-Password = "nurit"
Received Access-Accept Id 220 from 127.0.0.1:1812 to 0.0.0.0:0 length 20
```

II . BaroPAM FreeRADIUS 설치

4. 방화벽 설정

1) firewalld 설치

```
[root]# dnf -y install firewalld
```

2) firewalld 활성화

```
[root]# systemctl enable firewalld  
[root]# systemctl start firewalld
```

3) 포트 허용

```
[root]# firewall-cmd --permanent --zone=public --add-port=1812/udp  
success  
[root]# firewall-cmd --permanent --zone=public --add-port=1813/udp  
success
```

4) 방화벽 재로드

```
[root]# firewall-cmd --reload  
success
```

5) 작동여부 확인

```
[root]# systemctl status firewalld  
* firewalld.service - firewalld - dynamic firewall daemon  
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)  
   Active: active (running) since Tue 2024-01-09 20:35:10 KST; 14h ago  
     Docs: man:firewalld(1)  
  Main PID: 1009 (firewalld)  
    Tasks: 2 (limit: 102061)  
   Memory: 42.5M  
    CGroup: /system.slice/firewalld.service  
            └─1009 /usr/libexec/platform-python -s /usr/sbin/firewalld --nofork --nopid  
  
Jan 09 20:35:09 vpntest systemd[1]: Starting firewalld - dynamic firewall daemon...  
Jan 09 20:35:10 vpntest systemd[1]: Started firewalld - dynamic firewall daemon.
```

II . BaroPAM FreeRADIUS 설치

5. 환경 설정

1) BaroPAM 설정

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

2) BaroPAM 환경 설정 파일을 생성하기 위한 디렉토리 생성

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

3) BaroPAM 환경 설정 파일을 복사(기본)

```
[root]# cp ../.baro_auth .
```

내용 중 SECURE_KEY 값인 "j!qlcHbVqdpj7b4PzBpM2Di!eBvmHFV/"을 "01012341234" 변경해야 함.

4) 사용자(로그인-ID) 생성 쉘 스크립트(setuser.sh)

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

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

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

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

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

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

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

\$1 : 생성할 로그인-ID
\$2 : 로그인-ID의 비밀번호
\$3 : 로그인-ID의 폰번호

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

II . BaroPAM FreeRADIUS 설치

5. 환경 설정

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

```
#!/bin/sh
export LANG=C
echo $2 | passwd -stdin $1

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

사용자(로그인-ID)의 비밀번호를 변경하는 쉘 스크립트(setpasswd.sh) 실행 시 파라미터.
\$1 : 로그인-ID
\$2 : 변경할 비밀번호

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

```
#!/bin/sh
export LANG=C
ENV_HOME=/usr/baropam/radius;

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

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

사용자(로그인-ID)의 폰번호를 변경하는 쉘 스크립트(setphone.sh) 실행 시 파라미터.
\$1 : 로그인-ID
\$2 : 변경전 폰번호
\$3 : 변경후 폰번호

7) 사용자(로그인-ID)의 비밀번호와 폰번호를 변경하는 쉘 스크립트(chgpasswd.sh)

```
#!/bin/sh
export LANG=C
echo $2 | passwd -stdin $1
sed -i "s/$3/$4/g" ${ENV_HOME}/.$1_auth

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

사용자(로그인-ID)의 비밀번호/폰번호를 변경하는 쉘 스크립트(setpasswd.sh) 실행 시 파라미터.
\$1 : 로그인-ID
\$2 : 변경할 비밀번호
\$3 : 변경전 폰번호
\$4 : 변경후 폰번호

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

```
#!/bin/sh
export LANG=C
ENV_HOME=/usr/baropam/radius;
ACC_HOME=/home/$1

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

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

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

II . BaroPAM FreeRADIUS 설치

6. FreeRADIUS 실행

1) 자동 시작을 위한 RADIUS 서비스를 생성

```
[root]# systemctl enable radiusd.service  
Created symlink /etc/systemd/system/multi-user.target.wants/radiusd.service -> /usr/lib/systemd/system/radiusd.service.
```

2) FreeRADIUS 데몬 실행

```
[root]# systemctl restart radius → 데몬 재실행  
[root]# systemctl start radius → 데몬 실행  
[root]# systemctl stop radius → 데몬 종료  
[root]# systemctl status radius → 데몬 상태
```

3) FreeRADIUS 데몬인 radiusd를 백그라운드로 실행

```
[root]# radiusd -s &  
[1] 1961
```

4) FreeRADIUS 데몬인 radiusd가 사용하는 UDP 포트인 1812를 확인

```
[root]# netstat -an | grep 1812  
udp        0      0 127.0.0.1:18120      0.0.0.0:*  
udp        0      0 0.0.0.0:1812        0.0.0.0:*  
udp6       0      0 :::1812             :::*
```

5) FreeRADIUS를 연동하여 BaroPAM에서 인증한 로그 확인

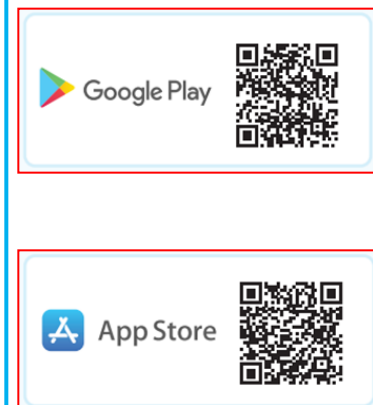
```
[root]# tail -f /var/log/secure  
Mar 26 13:54:11 localhost radiusd(pam_baro_auth)[1857]: Try to update RATE_LIMIT line.[3 30 1616734451]  
Mar 26 13:56:46 localhost radiusd(pam_baro_auth)[1857]: Try to update RATE_LIMIT line.[3 30 1616734606]  
Mar 26 14:00:48 localhost radiusd(pam_baro_auth)[1934]: Try to update RATE_LIMIT line.[3 30 1616734848]  
Mar 26 14:00:48 localhost radiusd(pam_baro_auth)[1934]: Invalid verification code  
Mar 26 14:00:48 localhost radiusd[1934]: pam_unix(radiusd:auth): authentication failure; logname=root uid=0 euid=0 tty= ruser= rhost=  
user=scjoo1  
Mar 26 14:01:13 localhost radiusd(pam_baro_auth)[1934]: Try to update RATE_LIMIT line.[3 30 1616734873]  
Mar 26 14:01:36 localhost radiusd(pam_baro_auth)[1934]: Try to update RATE_LIMIT line.[3 30 1616734873 1616734896]
```

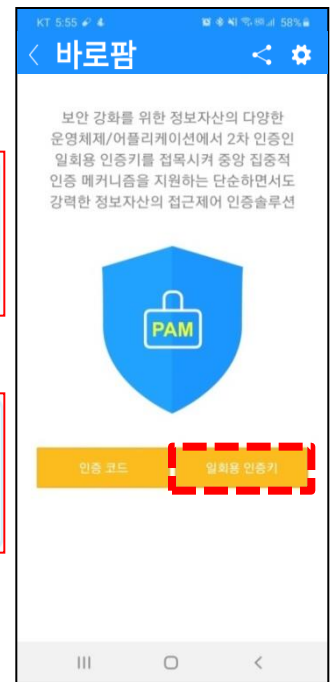
참고) FreeRADIUS 관련 로그 파일: /var/log/radius/radius.log

II. BaroPAM FreeRADIUS 설치

7. BaroPAM 앱 설치 및 정보 설정

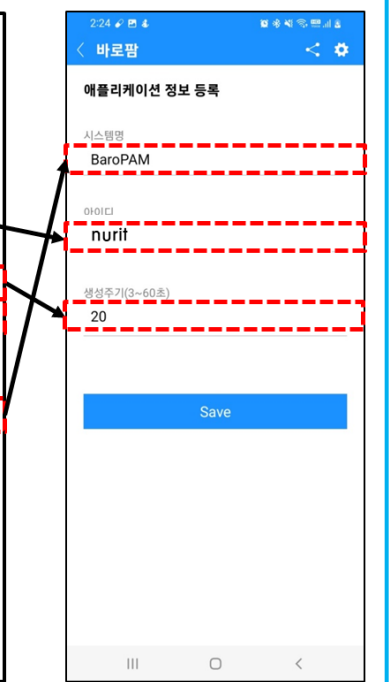
BaroPAM 앱 다운로드





로그인-ID: nurit, 폰번호: 010-2771-4076인 경우

```
$ cat .nurit_auth
" AUTH_KEY
" RATE_LIMIT 3 30
" KEY_METHOD app512
" CYCLE_TIME 20
" SECURE_KEY 01027714076
" ACL_NAME /usr/baropam/.baro_acl
" ACL_TYPE deny
" HOSTNAME BaroPAM
" DISALLOW_REUSE
33458936
19035576
15364353
54649370
84342192
```

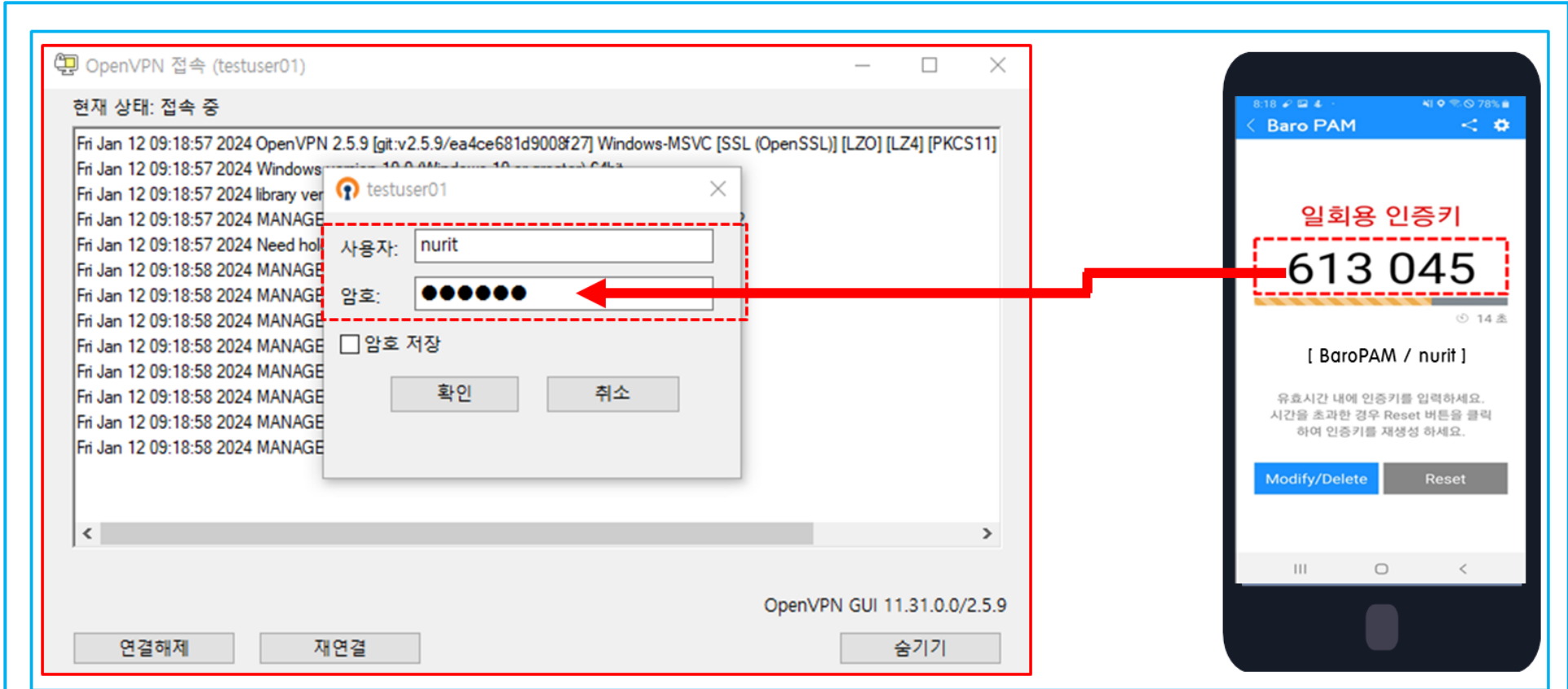


BaroPAM 앱은 Android 6.0 (Marshmallow) API 23, iOS 13.0 이상에서 사용 가능하며, 가로보기 모드를 지원하지 않는다.
BaroPAM 앱을 설치한 후 **BaroPAM** 앱을 실행하여 메뉴 선택화면에서 "일회용 인증키" 버튼을 클릭하여 RADIUS 사용자 정보에 설정한 "인증주기, 아이디, 시스템명"을 **BaroPAM** 앱의 "애플리케이션 정보 등록" 화면에서 동일하게 입력해야 한다.
BaroPAM 앱의 설정 -> 화면설정 변경 화면에서 앱코드(kr: 한국어, en: 영어, jp: 일본어, cn: 중국어)를 설정하면 **BaroPAM** 앱이 그에 맞게 변경된다.

현상 : 안드로이드폰 또는 아이폰의 날짜와 시간이 현재 시간과 차이가 발생하여 "일회용 인증키"가 맞지 않은 경우
원인 : 안드로이드폰 또는 아이폰의 날짜와 시간을 네트워크에서 제공하는 시간을 사용하지 않아서 발생.
조치 : 안드로이드폰인 경우는 폰의 "설정" -> "일반" -> "날짜 및 시간" -> "날짜 및 자동 설정"과 "시간대 자동 설정" -> "허용"
아이폰인 경우는 폰의 "설정" -> "날짜 및 시간" -> "자동으로 설정" -> "허용"

|| . BaroPAM FreeRADIUS 설치

8. 사용자 접속



RADIUS의 사용자 계정(Username)을 입력하고, 암호가 " baropam " 이고, 스마트 폰의 BaroPAM 앱에서 생성한 일회용 인증키가 " 613045 " 이라면 " 암호: " 란에 " baropam613045 " 를 입력한 후 "확인" 버튼을 클릭하면 BaroPAM 모듈에 인증을 요청하여 검증이 성공하면 접속된다.

기억할 필요가 없는 **비밀번호!**
BaroPAM이 함께 합니다.

감사합니다!

www.nurit.co.kr

서울시 강서구 마곡중앙2로 15, 913호(마곡동, 마곡테크노타워2)
주식회사 누리아이티 대표전화 : 010-2771-4076