nurit

정보자산의 보안강화를 위하여 3단계 인증을 위한

BaroPAM 솔루션 설치 요약서 (구름 OS)

2024. 3.

1. 사전 준비사항

1) Hostname 및 OS 버전을 확인

```
[root@baropam root]# uname -a
Linux baropam 5.10.0-25-amd64 #1 SMP gooroom 5.10.191-1+grm3u1 (2023-09-27) x86_64 GNU/Linux
```

2) ssh, sftp 서비스를 제공하기 위하여 ssh 및 openssl의 버전을 확인

```
[root@baropam root]# ssh -V
OpenSSH_8.4p1 Debian-5+deb11u2, OpenSSL 1.1.1w  11 Sep 2023

[root@baropam baropam]# openssl version
OpenSSL 1.1.1w  11 Sep 2023
```

다음 Gooroom 정보를 기억한다.

-Hostname/OS version
-ssh/openssl version

Copyright © Nurit Corp. All rights reserved.

2. BaroPAM 설치

1) BaroPAM 모듈을 설치하기 위한 디렉토리를 생성 및 권한 설정(root 계정으로)

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

2) BaroPAM 모듈을 설치하기 위한 디렉토리의 권한을 부여

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

3) BaroPAM 설치 모듈을 다운로드(OS version 확인)

https://mc529.tistory.com/1407

4) BaroPAM 설치 모듈의 압축을 해제(예 Gooroom 3.x 64bit인 경우)

```
[root] /usr/baropam > tar -xvf libpam_baro_auth-debian9.5.29-x64.tar
```

설치할 tar 파일명을 알 경우

```
[root] /usr/baropam > wget http://nuriapp.com/download/libpam_baro_auth-debian9.5.29-x64.tar
```

5) BaroPAM 모듈 확인

```
[root] /usr/baropam > ls -al
합계 1104
drwxrwxrwx  3 root    root      4096 11월 23 13:08 .
drwxr-xr-x 15 root    root      4096 11월 20 00:41 ..
-r--r--r--  1 root    root         6  7월 15  2020 .baro_acl        → ACL 파일
-r--r--r--  1 baropam baropam    271 11월 23 13:08 .baro_auth       → PAM 인증의 환경설정 파일
-rwxr-xr-x  1 root    root    101648  9월 24 11:21 baro_auth         → PAM 인증의 환경파일 생성하는 실행 프로그램
drwxr-xr-x  2 root    root      4096 11월  3  2020 jilee            → PAM 인증의 보안 관련 파일이 존재하는 디렉토리
-rwxr-xr-x  1 root    root    164216  9월 24 11:21 pam_baro_auth.so → PAM 인증의 일회용 인증키 검증하는 모듈
-rw-r--r--  1 root    root       236  9월 11 15:07 setauth.sh       → PAM 인증의 환경파일 생성하는 쉘 스크립트
```

Copyright © Nurit Corp. All rights reserved.

3. BaroPAM 환경설정 파일 생성

1) 환경파일 생성하는 쉘 스크립트(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) BaroPAM 환경설정 파일의 설정 옵션에 대한 내용

옵션	설명	설정값	비고
-r	일회용 인증키의 제한횟수(1~10)	3	
-R	일회용 인증키의 제한시간(초, 15~600초)	30	
-t	일회용 인증키의 인증주기(초, 3~60초)	30	
-k	일회용 인증키의 인증방식(app1, app256, app384, app512).	app512	
-e	환경설정 파일의 암호화 여부(yes or no)	no	
-H	서버의 호스트명(uname -n)	nurit.co.kr	
-A	2차 인증에서 허용(allow) 또는 제외(deny)할지 선택	deny	
-a	2차 인증에서 허용(allow) 또는 제외(deny)할 계정에 대한 ACL 파일명(**파일 접근권한은 444**)	/usr/baropam/.baro_acl	
-S	반드시 벤더에서 제공하는 Secure key(라이선스 키)	jlqlcHbVqdpj7b4PzBpM2DileBvmHFV/	
-s	BaroPAM 환경설정 파일을 생성할 디렉토리를 포함한 파일명	/usr/baropam/.baro_auth	

3) setenv.sh 쉘 스크립트 실행

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

1) Your emergency one-time authentication key are :
응급 일회용 인증키는 **일회용 인증키** 생성기인 BaroPAM 앱을 사용할 수 없을 때 분실한 경우를 대비하여 SSH 서버에 다시 액세스하는데 사용할 수 있는 접속이 가능한 Super 인증키 이므로 어딘가에 적어 두는 것이 좋다.

2) 다음에 나오는 물음에 대해서는 모두 "**y**"를 입력한다.
중간자(man-in-the-middle) 공격을 예방할 것인가? y
같은 **일회용 인증키**는 하나의 계정 외에 다른 계정에도 로그인이 가능하게 할 것인가? y
일회용 인증키의 제한 시간을 30초로 지정할 것인가? 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 baropam
" DISALLOW_REUSE
33458936
19035576
15364353
54649370
84342192
```

Copyright © Nurit Corp. All rights reserved.

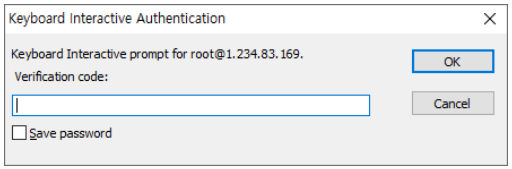
4. BaroPAM 설정

1) sshd 파일의 최상단에 설정

[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"는 호출된 PAM 모듈이 null 값의 암호를 입력하는 것을 허용한다는 의미



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

→ forward_pass를 이용하여 암호 입력창(Password & verification code:)에 암호와 같이 일회용 인증키를 입력할 경우, 암호를 먼저 입력하고 공백 없이 이어서 일회용 인증키를 입력. 예를 들어 암호가 "baropam" 이고 일회용 인증키가 "123456" 이라면 "baropam123456"으로 입력

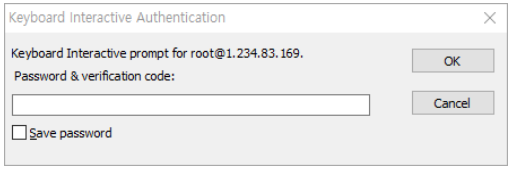
2) su, sudo, lightdm, lightdm _autologin, gnome-flashback 파일 등의 최상단에 설정(lightdm, gnome-flashback은 반드시 forward_pass로 지정해야 함)

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

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

3) sshd 데몬 설정을 위한 설정 파일인 "/etc/ssh/sshd_config" 파일의 내용 중 다음과 같은 인자는 변경이 필요

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



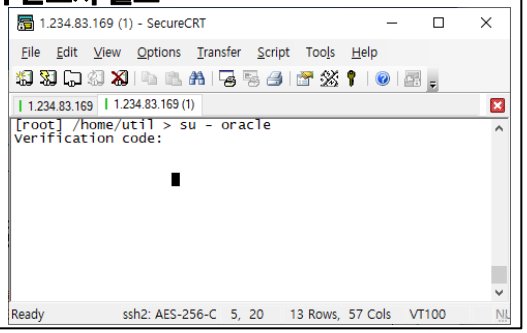
4) sshd 설정이 끝나면 반드시 PAM 모듈이 제대로 추가되었는지 확인한 후 SSH Server의 Restart 작업이 반드시 필요

[root] /usr/baropam > systemctl restart sshd

sshd 를 정지 중: [OK]

sshd (을)를 시작 중: [OK]

[root] /usr/baropam > systemctl restart lightdm



5) BaroPAM 모듈 사용 시 2차 인증에서 제외할 계정에 대한 ACL에 제외 해야 하는 경우

[root] /usr/baropam > vi .baro_acl

barokey

baropam

Copyright © Nurit Corp. All rights reserved.

5. BaroPAM 적용 방안

모든 정보자산 로그인 시 비밀번호 만으로는 결코 안전하지 않으며 매번 사용할 때마다 비밀번호를 대체 또는 추가 인증(2차 인증)할 수 있는 새로운 적용 방안(추가 인증, 비밀번호 대체, 새로운 비밀번호)이 필요

1) 추가 인증

계정(로그인-ID), 비밀번호 이외의 추가 인증(2차 인증)으로 일회용 인증키 적용(ID/PW/OTA)

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

2) 비밀번호 대체

비밀번호를 제거하고 일회용 인증키로 대체(ID/OTA)-일회용 인증키

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

참고) 비밀번호를 일회용 인증키로 대체하는 경우는 해당 계정(로그인-ID)의 비밀번호를 계정과 동일하게 설정해야 함.

3) 새로운 비밀번호

비밀번호와 일회용 인증키 결합하여 비밀번호를 일회용 인증키 생성주기별로 새로운 일회용 비밀번호를 생성하여 적용(ID/PW+OTA)

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

추가) .baro_auth 적용 방법

```
auth required /usr/baropam/pam_baro_auth.so nullok secret=/usr/baropam/.baro_auth encrypt=no          → 기본 설정
auth required /usr/baropam/pam_baro_auth.so nullok secret={HOME}/.baro_auth encrypt=no               → 계정별 홈 디렉토리에 설정
auth required /usr/baropam/pam_baro_auth.so nullok secret=/usr/baropam/auth/.{USER}_auth encrypt=no  → 계정별로 환경설정 파일 설정
```

Copyright © Nurit Corp. All rights reserved.

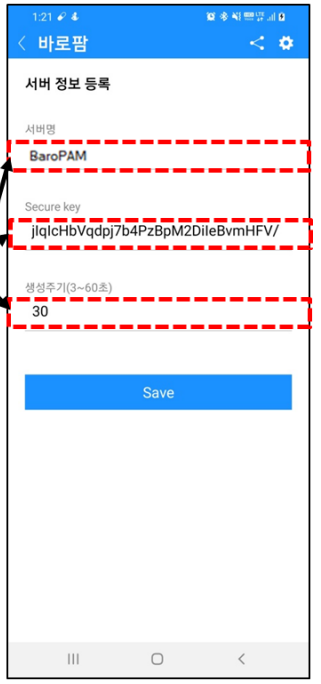
5. BaroPAM 앱 설치 및 정보 설정

BaroPAM 앱 다운로드

Google Play

App Store


```
$ cat .baro_auth
" AUTH_KEY
" RATE_LIMIT 3 30
" KEY_METHOD app512
" CYCLE_TIME 30
" SECURE_KEY jIqIcHbVqdpj7b4PzBpM2DileBvmHFV/
" ACL_NAME /usr/baropam/.baro_acl
" ACL_TYPE deny
" HOSTNAME BaroPAM
" DISALLOW_REUSE
33458936
19035576
15364353
54649370
84342192
```



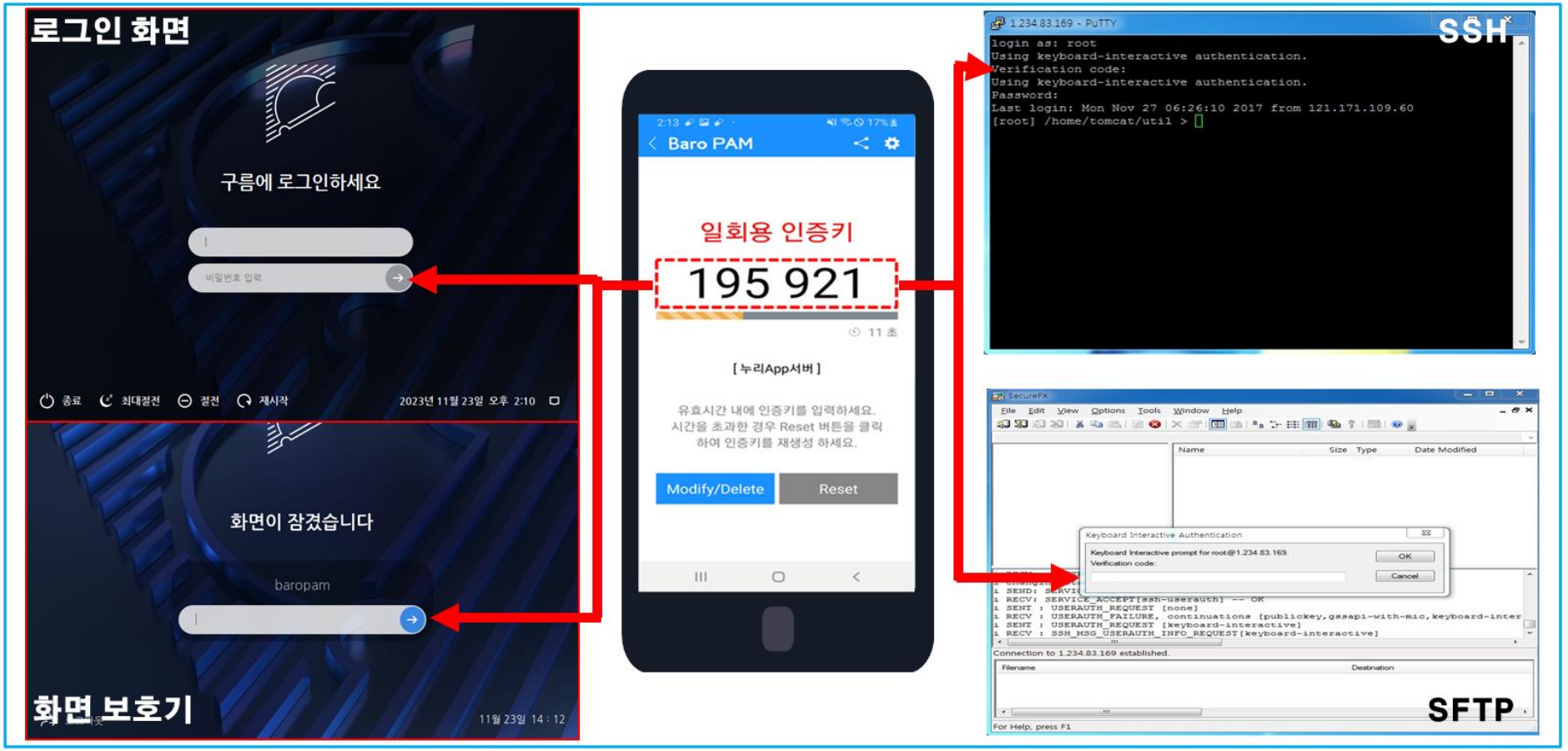
BaroPAM 앱은 Android 6.0 (Marshmalliw) API 23, iOS 13.0 이상에서 사용 가능하며, 가로보기 모드를 지원하지 않는다.
BaroPAM 앱을 설치한 후 **BaroPAM** 앱을 실행하여 메뉴 선택화면에서 "**인증 코드**" 버튼을 클릭하여 **BaroPAM**의 환경설정 파일인 "**.baro_auth**"에 설정한 "**인증주기, Secure key, 서버명**"을 **BaroPAM** 앱의 "**서버 정보 등록**" 화면에서 동일하게 입력해야 한다.
BaroPAM 앱의 설정 -> 화면설정 변경 화면에서 앱코드(kr: 한국어, en: 영어, jp: 일본어, cn: 중국어)를 설정하면 **BaroPAM** 앱이 그에 맞게 변경된다.

현상 : 안드로이폰 또는 아이폰의 날짜와 시간이 현재 시간과 차이가 발생하여 "**일회용 인증키**"가 맞지 않은 경우
원인 : 안드로이폰 또는 아이폰의 날짜와 시간을 네트워크에서 제공하는 시간을 사용하지 않아서 발생.
조치 : 안드로이폰인 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"

Copyright © Nurit Corp. All rights reserved.

nurit

6. Gooroom 로그인



Gooroom의 사용자 계정(Username)을 입력하고, 스마트 폰의 BaroPAM 앱에서 일회용 인증키를 생성한 후 로그인 화면과 화면 보호기는 비밀번호 란에 비밀번호를 먼저 입력하고 공백 없이 이어서 일회용 인증키를 입력해야 하며, ssh/sftp는 "Verification code"에 생성한 일회용 인증키와 "Password"를 입력한 후 "Enter" 또는 "OK" 버튼을 클릭하면 BaroPAM 모듈에 인증을 요청하여 검증이 성공하면 Gooroom에 로그인 된다.

Copyright © Nurit Corp. All rights reserved.

7. 문제 발생 시 확인 해야 할 사항

1) 시스템 로그인 Syslog 확인
   /var/log/auth.log 파일의 내용 중 "pam_baro_auth"가 존재하는 메시지 확인

2) Gooroom 시스템 정보 확인
   $ uname -a

3) Openssl 정보 확인
   $ openssl version

4) BaroPAM 설치 디렉토리 및 파일 권한 확인
   $ ls -al /usr/baropam

5) BaroPAM 설치 모듈 확인
   $ file pam_baro_auth.so
   $ ldd pam_baro_auth.so

6) BaroPAM 환경 설정 정보 확인
   $ cat /usr/baropam/.baro_auth

7) PAM 설정 확인
   $cat /etc/pam.d/sshd or su or sudo or lightdm or lightdm_autologin or gnome-flashback 등

8) sshd_config 설정 확인
   $ cat /etc/ssh/sshd_config

9) NTP 설정 및 상태 확인
   $ cat /etc/ntp.conf
   $ ntpq -p

Copyright © Nurit Corp. All rights reserved.

nurit

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