nurit

정보자산의 보안강화를 위하여 3단계 인증을 위한

BaroPAM 솔루션 설치 요약서 (Linux)

2024. 3.

1. 사전 준비사항

1) Hostname 및 OS 버전을 확인

```
[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) ssh, sftp 서비스를 제공하기 위하여 ssh 및 openssl의 버전을 확인

```
[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) Redhat, CentOS 계열인 경우 "Selinux"을 비활성화

```
[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) 재부팅을 하지 않고 현재 접속된 터미널에 한해 변경된 내용을 적용하고 싶을 경우 다음의 명령어를 실행

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

다음 Linux 정보를 기억한다.

-Hostname/OS version
-ssh/openssl version
-Redhat, CentOS 계열인 경우 "Selinux"을 비활성화

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 CentOS 8.x 64bit인 경우)

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

설치할 tar 파일명을 알 경우

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

5) BaroPAM 모듈 확인

```
[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          → ACL 파일
-r--r--r--  1 root   root    305  7월  2 14:41 .baro_auth         → PAM 인증의 환경설정 파일
-r--r--r--  1 root   root    290  6월 30 12:55 .baro_curl         → cURL 인증의 환경설정 파일
-rwxr-xr-x  1 root   root  69149  4월  6 19:12 baro_auth          → PAM 인증의 환경파일 생성하는 실행 프로그램
-rwxr-xr-x  1 root   root  65072  6월 29 16:36 baro_curl          → cURL 인증의 환경파일 생성하는 실행 프로그램
drwxr-xr-x  2 root   root   4096  7월 20  2021 jilee             → PAM 인증의 보안 관련 파일이 존재하는 디렉토리
-rwxr-xr-x  1 root   root 152649  6월  9 08:19 pam_baro_auth.so  → PAM 인증의 일회용 인증키 검증하는 모듈
-rwxr-xr-x  1 root   root 116158  6월 30 12:54 pam_baro_curl.so  → cURL 인증의 일회용 인증키 검증하는 모듈
-rw-r--r--  1 root   root    221  6월 27 15:59 setauth.sh         → PAM 인증의 환경파일 생성하는 쉘 스크립트
-rw-r--r--  1 root   root    150  6월 29 16:29 setcurl.sh         → cURL 인증의 환경파일 생성하는 쉘 스크립트
```

3. BaroPAM 환경설정 파일 생성(PAM 인증)

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 인증키는 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 nurit.co.kr
" DISALLOW_REUSE
33458936
19035576
15364353
54649370
84342192
```

3. BaroPAM 환경설정 파일 생성(cURL 인증)

1) 환경파일 생성하는 쉘 스크립트(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) 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	
-u	호출할 URL로 호스트명(hostname), 사용자 계정(username), 인증주기(cycle_time), 일회용 인증키(auth_key) 등의 파라미터가 포함되어 호출	http://1.23.456.789/baropam/web/result_curl.jsp	
-s	BaroPAM 환경설정 파일을 생성할 디렉토리를 포함한 파일명	/usr/baropam/.baro_curl	

3) setcurl.sh 쉘 스크립트 실행

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

1) 다음에 나오는 물음에 대해서는 모두 "y"를 입력한다.
중간자(man-in-the-middle) 공격을 예방할 것인가? y
같은 일회용 인증키는 하나의 계정 외에 다른 계정에도 로그인이 가능하게 할 것인가? y
일회용 인증키의 제한 시간을 30초로 지정할 것인가? 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
```

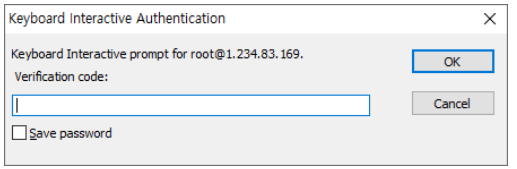
4. BaroPAM 설정(PAM 인증)

1) sshd 파일의 최상단에 설정

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

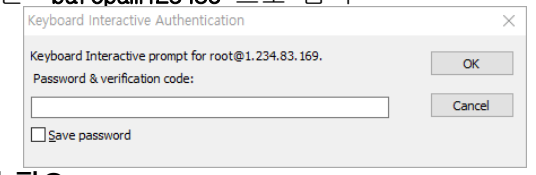
auth required /usr/baropam/pam_baro_auth.so nullok secret=/usr/baropam/.baro_auth encrypt=no

→ "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_pass"은 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, lightdm, gdm-password 파일 등의 최상단에 설정

[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) 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 or KbdInteractiveAuthentication	no	yes	
UsePAM	no	yes	

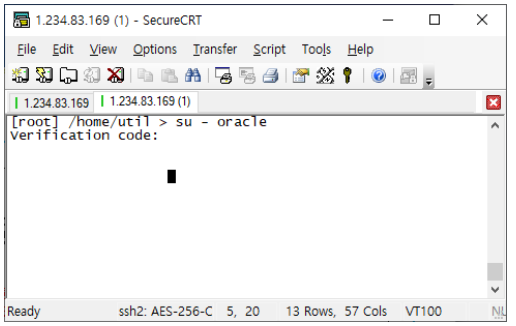
4) sshd 설정이 끝나면 반드시 PAM 모듈이 제대로 추가되었는지 확인한 후 SSH Server의 Restart 작업이 반드시 필요

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

sshd 를 정지 중: [OK]

sshd (을)를 시작 중: [OK]

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

4. BaroPAM 설정(cURL 인증)

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_pass"은 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, 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) 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 > service sshd restart or systemctl restart sshd

sshd 를 정지 중: [OK]

sshd (을)를 시작 중: [OK]

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

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

참고) Linux/Unix 서버는 자동 로그인(Autologin) 기능이 지원되지 않아서 비밀번호를 반드시 존재해야 함.

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
```

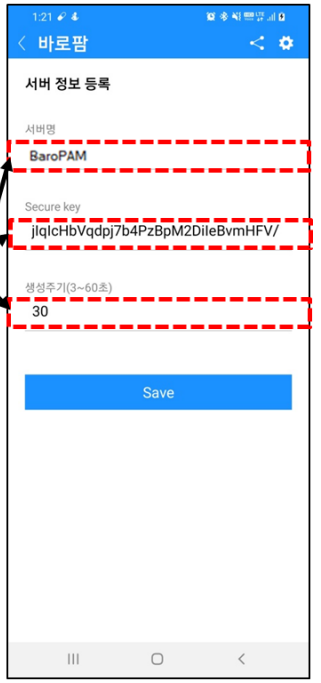
5. BaroPAM 앱 설치 및 정보 설정

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
```

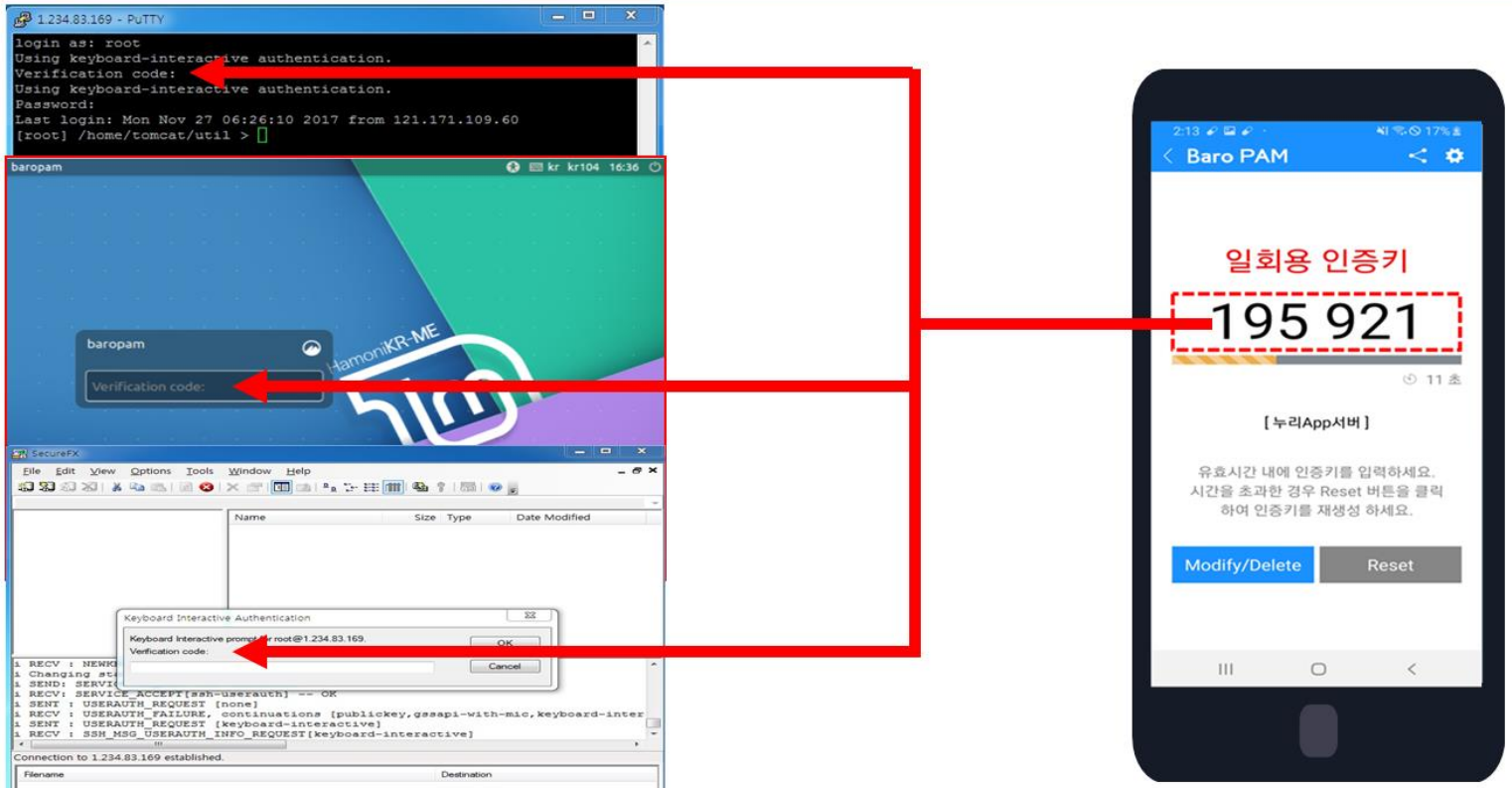


BaroPAM 앱은 Android 6.0 (Marshmalliw) API 23, iOS 13.0 이상에서 사용 가능하며, 가로보기 모드를 지원하지 않는다.
BaroPAM 앱을 설치한 후 **BaroPAM** 앱을 실행하여 메뉴 선택화면에서 "**인증 코드**" 버튼을 클릭하여 **BaroPAM**의 환경설정 파일인 "**.baro_auth**"에 설정한 "**인증주기, Secure key, 서버명**"을 **BaroPAM** 앱의 "**서버 정보 등록**" 화면에서 동일하게 입력해야 한다.
BaroPAM 앱의 설정 -> 화면설정 변경 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"

nurit

6. Linux 로그인



Linux의 사용자 계정(Username)을 입력하고, 스마트 폰의 BaroPAM 앱에서 일회용 인증키를 생성한 후 "Verification code"에 생성한 일회용 인증키와 Linux의 "Password"를 입력한 후 "Enter" 또는 "OK" 버튼을 클릭하면 BaroPAM 모듈에 인증을 요청하여 검증이 성공하면 Linux에 로그인 된다.

7. 문제 발생 시 확인 해야 할 사항

1) 시스템 로그인 Syslog 확인
Redhat 계열: /var/log/secure, 그외: /var/log/auth.log 파일의 내용 중 "pam_baro_auth"가 존재하는 메시지 확인

2) Linux 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 등

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

9) NTP 설정 및 상태 확인(Redhat 8 이상 버전은 chrony 사용)
$ cat /etc/ntp.conf or /etc/chrony.conf
$ ntpq -p or timedatectl status

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