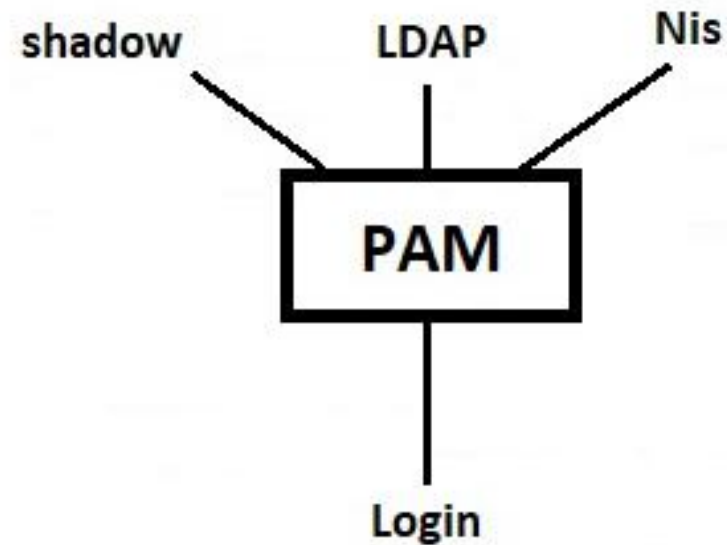


# PAM(Pluggable Authentication Module) 을 이용한 인증관리

# Linux 인증 방식

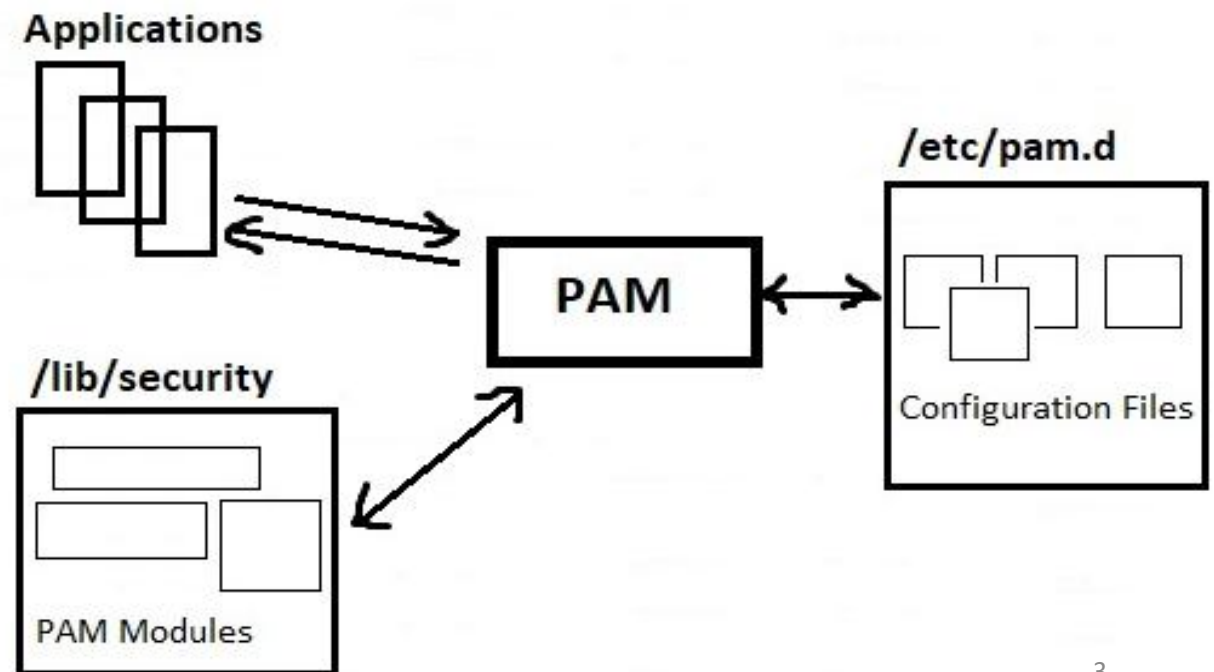
- Password 인증
- LDAP 인증
- SSH 공개키 인증

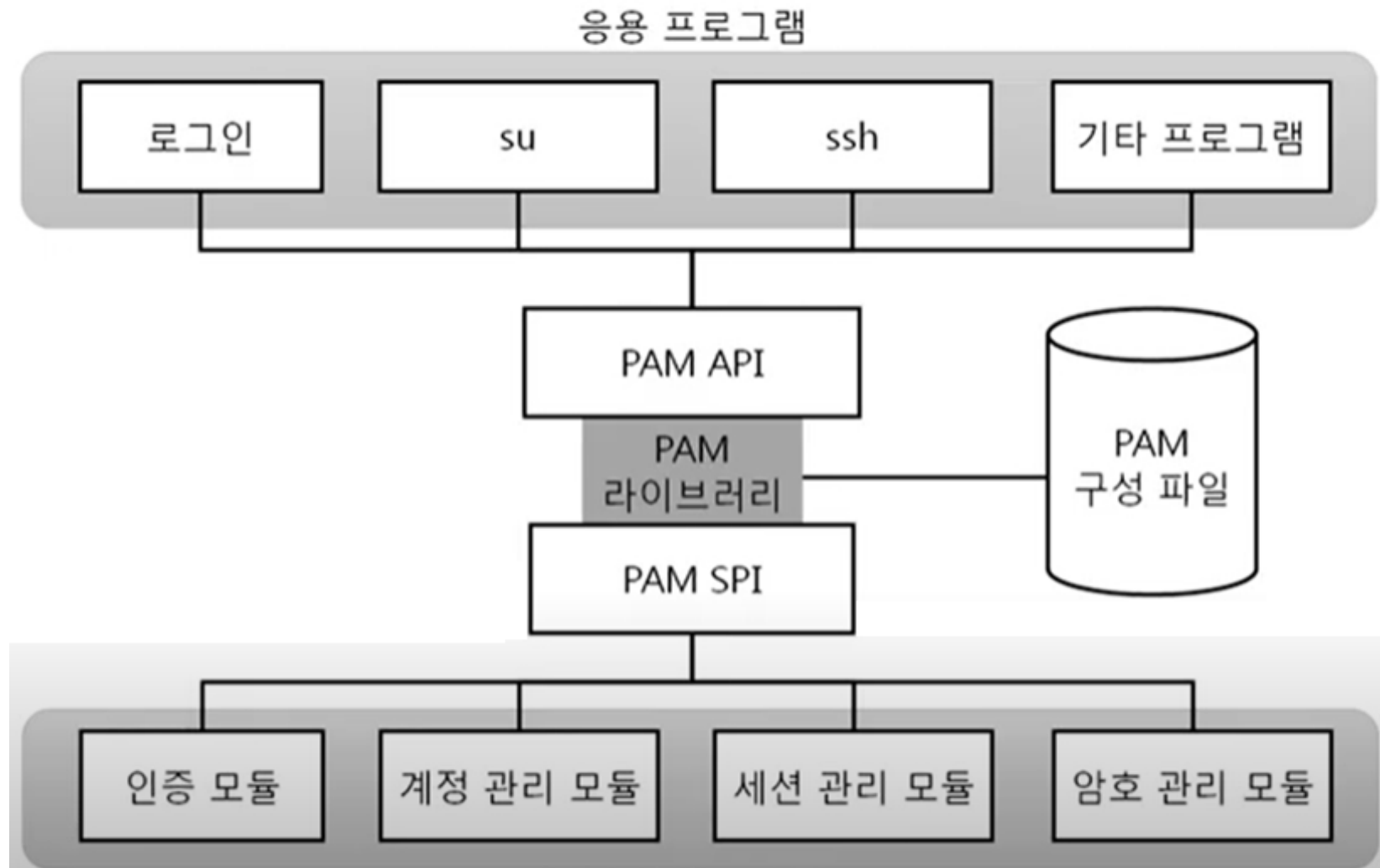
→ PAM 인증(중앙 집중형 인증 시스템)



## ◆ PAM의 구성

- 라이브러리
  - /lib64/security(또는 /lib/security)
- PAM을 이용하는 서비스 디렉터리
  - /etc/pam.d
  - /etc/pam.d/other





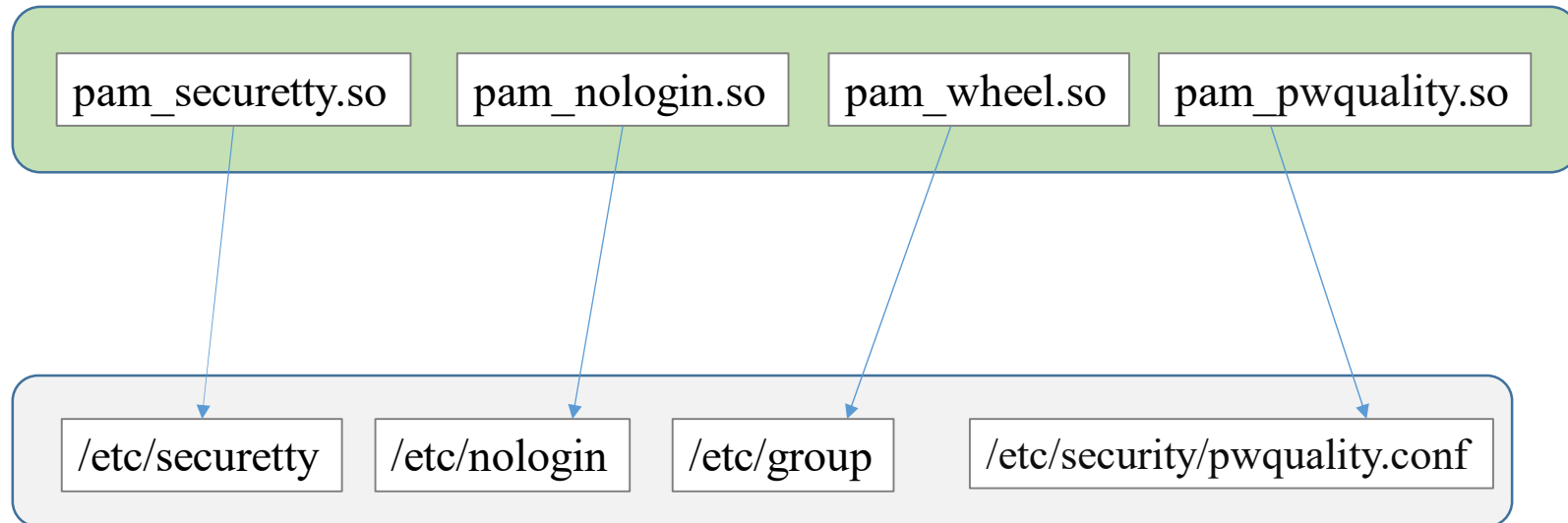
/etc/pam.d/remote

```
#auth required pam_securetty.so  
#password requisite pam_pwquality
```

/etc/pam.d/su

```
#auth required pam_securetty.so  
#password requisite pam_pwquality
```

**/lib64/security**



## PAM 지원 모듈 목록

```
[root@localhost security]# pwd
/lib64/security
[root@localhost security]# ls
pam_access.so      pam_exec.so        pam_issue.so       pam_loginuid.so
pam_cap.so         pam_faildelay.so   pam_keyinit.so     pam_mail.so
pam_chroot.so      pam_faillock.so    pam_krb5            pam_mkhome.so
pam_console.so     pam_filter         pam_krb5.so         pam_motd.so
pam_cracklib.so    pam_filter.so      pam_krb5afs.so      pam_namespace.so
pam_debug.so       pam_fprintd.so     pam_lastlog.so      pam_nologin.so
pam_deny.so        pam_ftp.so         pam_limits.so       pam_oddjob_mkhome.so
pam_echo.so        pam_gnome_keyring.so pam_listfile.so     pam_permit.so
pam_env.so         pam_group.so       pam_localuser.so    pam_postgresok.so
[root@localhost security]#
```

## PAM 설정 파일

```
[root@localhost pam.d] # pwd
/etc/pam.d
[root@localhost pam.d] # ls
atd                  gdm-password~    postlogin          su
chfn                 gdm-pin          postlogin-ac       su-l
chsh                 gdm-smartcard    ppp                sudo
config-util         ksu              remote             sudo-i
crond                liveinst         runuser            system-auth
cups                 login            runuser-l          system-auth-ac
fingerprint-auth    other            setup              systemd-user
fingerprint-auth-ac password          smartcard-auth     vlock
gdm-autologin        password-auth    smartcard-auth-ac  vmtoolsd
gdm-fingerprint      passwd           smtp               xserver
gdm-launch-environment pluto
gdm-password         polkit-1
[root@localhost pam.d] #
```

```
[root@localhost pam.d]# cat su
#%PAM-1.0
auth                sufficient      pam_rootok.so
# Uncomment the following line to implicitly trust users in the "wheel" group.
#auth               sufficient      pam_wheel.so trust use_uid
# Uncomment the following line to require a user to be in the "wheel" group.
#auth               required        pam_wheel.so use_uid
auth                substack        system-auth
auth                include         postlogin
account             sufficient      pam_succeed_if.so uid = 0 use_uid quiet
account             include         system-auth
password            include         system-auth
session             include         system-auth
session             include         postlogin
session             optional       pam_xauth.so
[root@localhost pam.d]#
```



## PAM 설정 파일 구성

```
[root@localhost pam.d] # pwd
/etc/pam.d
[root@localhost pam.d] # ls -l login
-rw-r--r--. 1 root root 796  6월 18  2014 login
[root@localhost pam.d] # cat login
#%PAM-1.0
auth [user_unknown=ignore success=ok ignore=ignore default=bad] pam_securetty.so
auth      substack      system-auth
auth      include       postlogin
account   required      pam_nologin.so
account   include       system-auth
password  include       system-auth
# pam_selinux.so close should be the first session rule
session   required      pam_selinux.so close
session   required      pam_loginuid.so
session   optional      pam_console.so
# pam_selinux.so open should only be followed by sessions to be executed in the us
er context
session   required      pam_selinux.so open
session   required      pam_namespace.so
session   optional      pam_keyinit.so force revoke
session   include       system-auth
session   include       postlogin
-session  optional      pam_ck_connector.so
[root@localhost pam.d] #
```

## 2) PAM 설정 파일 구성

<u>type</u>	<u>control</u>	<u>module_name</u>	<u>module-arguments</u>
①	②	③	④

auth	include	postlogin
account	required	pam_nologin.so
session	include	system-auth
session	required	pam_namespace.so
password	include	system-auth

/etc/pam.d/login

## 1 Type

- 어떤 타입의 인증이 사용될 것인지를 알려주는 항목

auth	include	postlogin
account	required	pam_nologin.so
session	include	system-auth
session	required	pam_namespace.so
password	include	system-auth

type	설명
account	<p>사용자 계정을 확인하는 절차 제공</p> <ul style="list-style-type: none"> <li>- 사용자가 해당 서비스에 접근이 허용되는지 여부</li> <li>- 계정 활성화/비활성화 여부 확인</li> <li>- 패스워드 기간 만료 여부를 검사</li> <li>- 특정 시간대에 접속 시도 가능여부 확인</li> </ul>
auth	<p>사용자 패스워드 유효성 검사와 같은 서비스 인증 절차에 사용</p> <ul style="list-style-type: none"> <li>- 다중 모듈(Kerberos Ticket과 같은 연동도 가능)</li> </ul> <p>사용자를 인증하고 자격증명 절차 제공</p> <ul style="list-style-type: none"> <li>- 패스워드를 통해 인증</li> </ul>
password	<p>사용자가 패스워드 등의 인증 방법을 변경하도록 할 때 제공하는 방법</p> <p>패스워드 변경 시 최소길이/복잡도 설정 등과 관련</p>
session	<p>사용자가 인증 받기 전/후에 해야 할 것을 지정</p> <p>홈 디렉터리 마운트/언마운트, 로그인/로그아웃 서비스 제한 등 포함</p>

## ② control

- PAM이 무엇을 해야 할 지를 알려줌

auth	include	postlogin
account	required	pam_nologin.so
session	include	system-auth
session	required	pam_namespace.so
password	include	system-auth

control	설명
required	지정된 모듈을 통한 인증이 실패하면 인증 거부 - 인증이 거부되기 전에 해당 서브에 등록된 다른 모듈들을 호출 한 후 거부 - 다른 인증들이 성공하더라도 해당 인증이 실행할 경우 인증 거부
requisite	이 모듈의 인증이 실패할 경우에 즉시 거부
sufficient	이전에 요청되어진 모듈이 실패하더라도 이 모듈에 의해서 인증이 성공할 경우 인증 승인
optional	서비스에 대한 응용프로그램의 성공/실패가 중요하지 않다는 것을 의미 - 성공/실패 판단 시에는 무시, 모듈에 대한 성공/실패가 없다면 이 모듈이 응용프로그램에게 주는 결과로 결정
include	이 항목 다음에는 모듈명 대신에 <b>PAM 관련 서비스</b> 가 옴 해당 서비스 인증을 통과해야 가능하도록 설정할 때 사용

## Play with PAM

 required	<b>X</b>	✓	✓	✓
 required	✓	✓	✓	✓
 requisite	✓	<b>X</b>	✓	✓
 optional	✓		<b>X</b>	<b>X</b>
 sufficient	✓		✓	<b>X</b>
 requisite				✓

## Results

<b>X</b>	<b>X</b>	✓	✓
----------	----------	---	---

Required (필수)	인증 결과와 관계 없이 다음 인증 수행	·인증결과가 성공일 경우, 다른 모듈들이 실패하지 않은 한 요청 허용 ·인증결과가 실패일 경우, 다른 인증을 수행 후 요청 거부
Requisite (필요)	인증결과가 실패일 경우 즉시 인증 종료	·인증결과가 성공일 경우, 다음 모듈 실행(최종 결과에 미반영) ·인증결과가 실패일 경우, 즉시 인증 실패를 반환(다른모듈실행안함)
Sufficient (충분)	인증결과가 성공일 경우 즉시 인증 종료	·인증결과가 성공일 경우, 즉시 인증 성공 반환 ·인증결과가 실패일 경우, 다음 인증 모듈실행(최종 인증결과에 미반영)
Optional (선택)	최종 인증결과에 반영되지 않음	

## Play with PAM

 required	<b>X</b>	✓	✓	✓
 required	✓	✓	✓	✓
 requisite	✓	<b>X</b>	✓	✓
 optional	✓		<b>X</b>	<b>X</b>
 sufficient	✓		✓	<b>X</b>
 requisite				✓
<b>Results</b>	<b>X</b>	<b>X</b>	✓	✓

\* /etc/pam.d/system-auth : 로컬 로그인 인증 설정

```
[root@localhost pam.d]# cat system-auth
auth      required      pam_env.so
auth      sufficient    pam_fprintd.so
auth      sufficient    pam_unix.so nullok try_first_pass
auth      requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth      required      pam_deny.so

account    required      pam_unix.so
account    sufficient    pam_localuser.so
account    sufficient    pam_succeed_if.so uid < 1000 quiet
account    required      pam_permit.so

password   requisite     pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=
password   sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok
password   required      pam_deny.so

session    optional      pam_keyinit.so revoke
session    required     pam_limits.so
-session   optional      pam_systemd.so
session    [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session    required     pam_unix.so
```

\* /etc/pam.d/password-auth : 원격 로그인(ssh, ftp)의 인증 설정

```
[root@localhost pam.d]# cat password-auth
auth      required      pam_env.so
auth      sufficient    pam_unix.so nullok try_first_pass
auth      requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth      required      pam_deny.so

account   required      pam_unix.so
account   sufficient    pam_localuser.so
account   sufficient    pam_succeed_if.so uid < 1000 quiet
account   required      pam_permit.so

password  requisite     pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=
password  sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok
password  required      pam_deny.so

session   optional      pam_keyinit.so revoke
session   required     pam_limits.so
-session  optional      pam_systemd.so
session   [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session   required     pam_unix.so
[root@localhost pam.d]#
```



Debug	시스템 로그 파일에 디버그 정보를 남기도록 지정
No_warn	모듈이 경고 메시지를 보내지 않도록 지정
Use_first_pass	사용자에게 패스워드 입력을 요구하지 않도록 지정 이전모듈에서 입력 받은 패스워드가 존재하지 않을 경우 인증 실패 반환
Try_first_pass	이전모듈에서 입력 받은 패스워드로 인증 시도 이전에 입력 받은 패스워드가 존재하지 않을 경우 사용자 입력 요구

### ③ module\_name

- 사용하는 모듈명을 명기하는 부분
- 절대경로를 입력하거나 /lib/security에 있는 모듈명 기입

### ④ module-arguments

- 지정한 모듈이 사용하는 인수를 기입
- 여러 인수를 사용하는 경우에는 공백으로 구분
- 인수에 공백을 포함시키려면 대괄호([])를 사용해서 묶음

```
[root@localhost pam.d]# head -4 remote
#%PAM-1.0
auth      required      pam_securetty.so
auth      required      pam_faillock.so deny=3 unlock time=60
auth      substack      password-auth
```

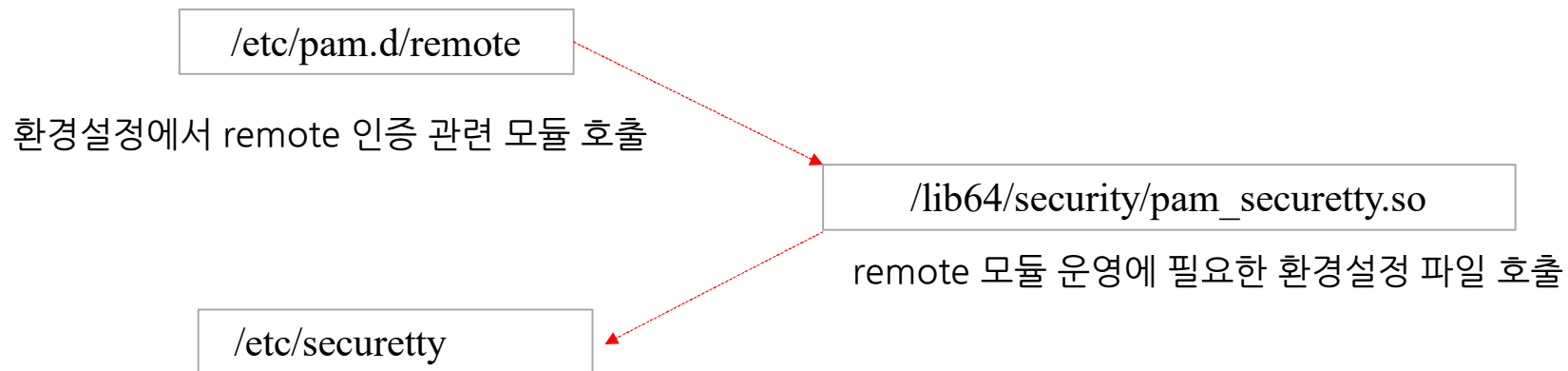
auth required pam\_faillock.so deny=3 unlock\_time=60

- 인증을 처리하는데 pam\_faillock.so 모듈 사용
- 실패 3회(deny=3)이면 30초동안 계정 잠금(unlock)


### 3) PAM 주요 모듈

#### pam\_securetty.so


- 접속하는 계정이 root인 경우 /etc/securetty 파일에 기록된 터미널을 통하는 경우에만 허가하도록 하고, 그 외 사용자는 항상 인증에 성공한 것으로 처리
- /etc/pam.d/login와 /etc/pam.d/remote 설정



```
[root@localhost pam.d]# cat remote
#%PAM- 1.0
auth      required      pam_securetty.so
auth      substack      password-auth
```



```
[root@localhost security]# ls *securetty*
pam_securetty.so
[root@localhost security]#
```



```
[root@localhost security]# cat /etc/securetty
console
tty1
tty2
tty3
tty4
tty5
```

## pam\_wheel.so

- root 권한을 얻을 수 있는 사용자를 wheel(또는 group-ID=0)이라는 그룹으로 묶어서 사용하도록 지원하는 모듈
- su 명령과 관련된 /etc/pam.d/su에 사용하면 매우 유용

argument	설명
debug	디버깅 관련 정보를 출력한다.
group=그룹명	wheel 또는 GID 0번 그룹을 검사하는 대신에 해당 그룹명으로 인증을 수행한다.
deny	모듈의 동작을 반대가 되도록 설정한다. 만약 wheel 그룹에 속한 사용자가 uid=0을 얻는 시도를 하면 접근을 거부한다.
trust	<b>wheel 그룹에 속한 사용자가 root 권한을 요구한 경우 PAM_SUCCESS를 리턴값으로 준다.</b> 즉, wheel 그룹에 속한 사용자들은 암호를 입력하지 않고도 root 권한을 획득할 수 있다.
use_uid	로그인할 때의 사용자명 대신에 현재의 UID를 사용한다. 다른 계정으로 로그인한 뒤에 su 명령을 사용한 경우가 해당된다.
root_only	단지 wheel 그룹에 속한 사용자 여부만 검사한다.

## pam\_listfile.so

- 특정 서비스에 대해 허가 목록이나 거부 목록을 만들 때 사용
- /etc/pam.d/vsftpd 파일에 설정되어 ftp 사용자 거부 목록 파일로 이용

```
[root@www ~]# cat /etc/pam.d/vsftpd
#%PAM-1.0
session    optional    pam_keyinit.so      force revoke
auth       required    pam_listfile.so     item=user sense=deny file=/etc/
vsftpd/ftpusers onerr=succeed
auth       required    pam_shells.so
auth       include     password-auth
account    include     password-auth
session    required    pam_loginuid.so
session    include     password-auth
```

## [모듈인자(module-argument)]

argument	설명
item=	목록 파일에 이용할 항목을 지정하는데, 사용자인 경우에 item=user로 설정한다. 사용자 이외에도 group, tty, shell, rhost, ruser의 설정이 가능하다.
sense=	목록 파일을 허가 또는 거부로 설정하는 항목이다. 허가이면 allow, 거부이면 deny로 설정한다.
file=	목록 파일의 경로를 지정한다. 해당 파일에 아이템 등록은 한 줄에 하나씩 적어야 한다.
onerr=	succeed 또는 fail이라고 설정하는데, 일반적으로 sense에 설정하는 값의 반대로 지정 succeed면 PAM_SUCCESS를 리턴하고, fail이면 PAM_AUTH_ERR 또는 PAM_SERVICE_ERR을 리턴
apply=	특정 사용자(user) 또는 특정 그룹(@group)으로 적용을 제한할 때 사용한다. item 항목이 tty, rhost, shell인 경우에만 의미 있는 제한이 된다.

## pam\_nologin.so

- /etc/nologin 파일이 존재하면 root만 로그인
  - 다른 사용자는 에러 메시지와 함께 거부
- 로그인과 관련된 서비스인 login, remote, sshd 등에 설정되어 있어서 대부분 영향을 받음

### [모듈인자(module-argument)]

argument	설명
file=	기본 지정 파일인 /etc/nologin 대신에 다른 파일을 이용할 경우에 사용한다. 'file=파일_절대경로' 형식으로 설정한다.
successok	기본 리턴값이 PAM_IGNORE인데, PAM_SUCCESS로 변경할 때 사용한다.



## pam\_deny.so

- 접근을 무조건 거부할 때 사용하고, 응용 프로그램에게 항상 실패를 리턴
- other, system-auth 등에 사용

```
root@www:~  
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)  
[root@www ~]# cat /etc/pam.d/system-auth  
#%PAM-1.0  
# This file is auto-generated.  
# User changes will be destroyed the next time authconfig is run.  
auth            required      pam_env.so  
auth            sufficient     pam_fprintd.so  
auth            sufficient     pam_unix.so nullok try_first_pass  
auth            requisite      pam_succeed_if.so uid >= 500 quiet  
auth            required      pam_deny.so  
  
account         required      pam_unix.so  
account         sufficient     pam_localuser.so  
account         sufficient     pam_succeed_if.so uid < 500 quiet  
account         required      pam_permit.so  
  
password        requisite      pam_cracklib.so try_first_pass retry=3 type=ss use_authok  
password        sufficient     pam_unix.so sha512 shadow nullok try_first_pass  
password        required      pam_deny.so
```

## pam\_cracklib.so

- 사전(Dictionary)에 등록된 단어를 이용한 패스워드 설정에 막기 위해 비교 및 검사할 때 사용
- password-auth, system-auth에 사용

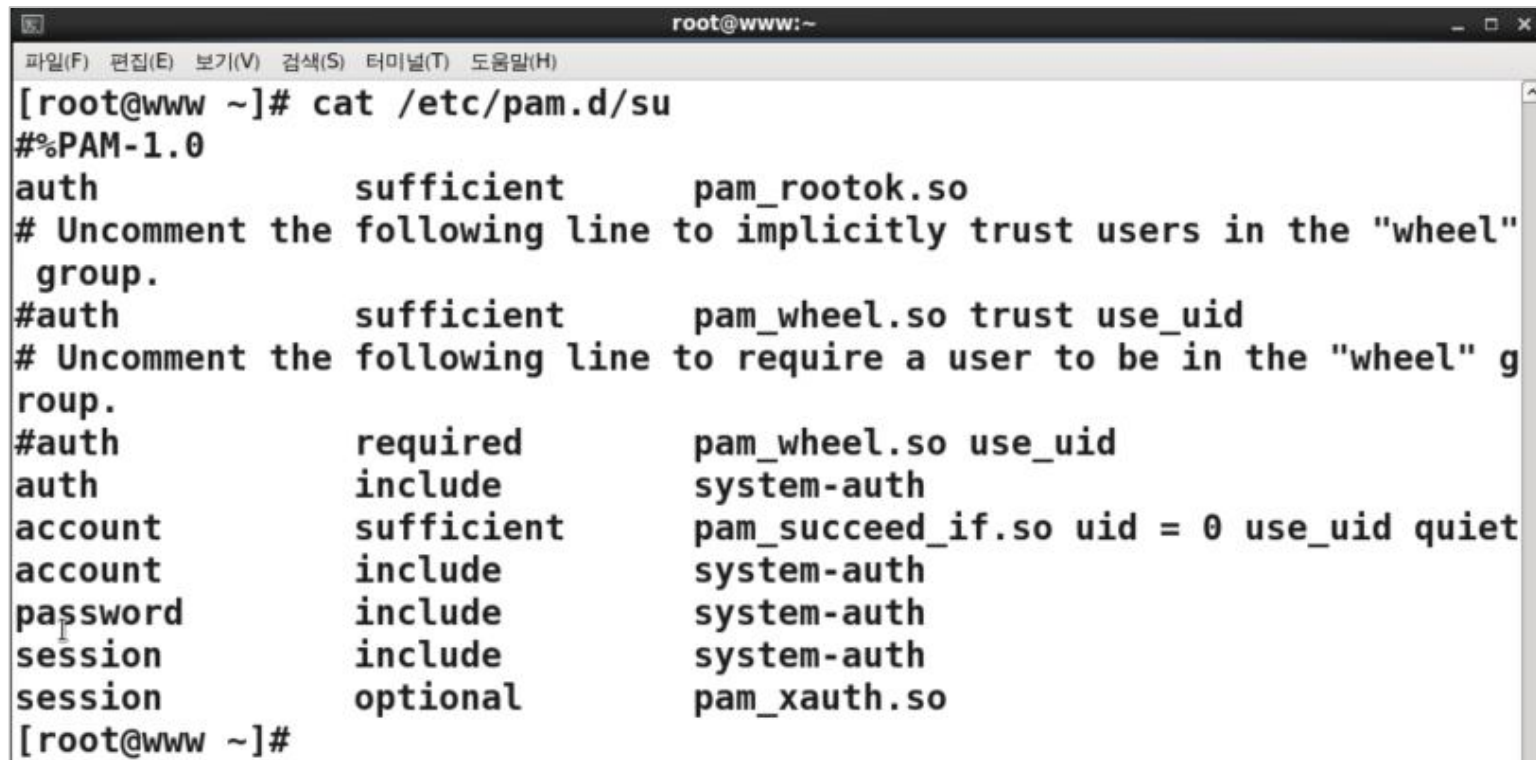
argument	설명
debug	모듈의 동작을 보여 주기 위해 syslog에 정보를 남김 이 옵션을 사용하면 패스워드 관련 정보를 로그 파일에 기록하지 않음
retry=N	새로운 패스워드 설정할 때 물어보는 횟수를 지정하는 옵션 기본값이 1인데, 이 옵션을 사용하면 지정한 값 N만큼 횟수가 늘어남
authtok_type=	새로운 패스워드 입력할 때 문구를 지정할 때 사용하면 “New UNIX password”라는 문구를 “New LINUX password”로 변경하려면 authtok_type=LINUX로 지정

## pam\_cracklib.so

argument	설명
difok=N	새 패스워드에서 예전 패스워드에 있지 않는 문자들을 몇 자나 사용해야 하는지를 지정 기본값은 5이고 새 패스워드에서 1/2이상의 글자가 이전과 다르다면 새 패스워드로 인정
minlen=N	새 패스워드로 허용될 크기를 지정하는 항목으로 글자 수에 크레딧(credit)라는 값이 더해짐 문자 종류(숫자, 대문자, 소문자, 특수문자)를 사용한 것에 대해 각각 크레딧을 부여
dcredit=N	숫자(digit)가 갖는 크레딧값을 지정( 기본값은 1)
ucredit=N	대문자(upper case)가 갖는 크레딧값을 지정( 기본값은 1)
lcredit=N	소문자(lower case)가 갖는 크레딧값을 지정( 기본값은 1)
ocredit=N	기타 특수문자(other)가 갖는 크레딧값을 지정( 기본값은 1)

## pam\_rootok.so

- UID가 0인 사용자를 인증하는 모듈로 보통 root가 암호 입력 없이 해당 서비스에 대한 접근을 허용할 때 사용
- 이 모듈을 사용하는 서비스에는 su, eject, poweroff, reboot 등이 있음



```
root@www:~  
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)  
[root@www ~]# cat /etc/pam.d/su  
#%PAM-1.0  
auth            sufficient      pam_rootok.so  
# Uncomment the following line to implicitly trust users in the "wheel"  
# group.  
#auth           sufficient      pam_wheel.so trust use_uid  
# Uncomment the following line to require a user to be in the "wheel" g  
# roup.  
#auth           required        pam_wheel.so use_uid  
auth            include         system-auth  
account         sufficient      pam_succeed_if.so uid = 0 use_uid quiet  
account         include         system-auth  
password        include         system-auth  
session         include         system-auth  
session         optional       pam_xauth.so  
[root@www ~]#
```

## pam\_tally2.so

- 로그인 시도 횟수를 세는 모듈
- 일정 횟수 이상 실패 시에는 접근을 차단 및 관리해주는 역할 수행
- pam\_tally2는 pam\_tally2.so 모듈을 이용해서 관련 파일에 설정하는 방법과 pam\_tally2라는 명령을 이용하는 방법으로 나눔
- Pam\_tally2 명령은 카운트(count) 파일에 저장된 관련 기록을 출력해주거나 관리하는 역할 수행

## pam\_tally2.so

argument	설명
deny= <i>N</i>	로그인 시도가 <i>N</i> 번 실패하면 접근을 차단
lock_time= <i>N</i>	로그인 실패 후에 <i>N</i> 초 동안 접근을 차단
unlock_time= <i>N</i>	관리자가 정한 일정 횟수 이상 로그인에 실패했을 경우 <i>N</i> 초 동안 접근을 차단해당 시간 동안은 관리자가 계정을 해제하기 전까지는 계정잠김
root_unlock_time= <i>N</i>	root 사용자가 일정 횟수 이상 로그인에 실패했을 경우 <i>N</i> 초 동안 접근 차단
file=경로	카운트 내역을 기록하는 파일 경로를 기록 기본 파일명은 /var/log/tallylog
no_log_info	syslog에 메시지를 전달하지 않음
silent	관련 정보를 출력하지 않음

## pam\_limits.so

- 시스템의 자원에 대한 사용자 제한을 설정할 때 사용하는 모듈
- 프로세스와 메모리 사용량 등을 제한
- system-auth, password-auth, sudo 등에 사용
  - 기본 환경 설정은 /etc/security/limits.conf 파일에 설정
  - /etc/security/limits.d 디렉터리 내에 \*.conf 형식으로 지정한 파일들이 존재하면 추가로 읽어들이어서 적용

## 실습 1. 계정 root로 콘솔 로그인 막기



```
[root@localhost pam.d] # ls gdm-password
gdm-password
[root@localhost pam.d] # cat gdm-password
auth      [success=done ignore=ignore default=bad] pam_selinux_permit.so
auth      substack      password-auth
auth      optional     pam_gnome_keyring.so
auth      include      postlogin

account    required     pam_nologin.so
account    include      password-auth

password    substack     password-auth
password    optional     pam_gnome_keyring.so use_authtok


session     required     pam_selinux.so close
session     required     pam_loginuid.so
session     optional     pam_console.so
-session    optional     pam_ck_connector.so
session     required     pam_selinux.so open
session     optional     pam_keyinit.so force revoke
session     required     pam_namespace.so
session     include      password-auth
session     optional     pam_gnome_keyring.so auto_start
session     include      postlogin
[root@localhost pam.d] #
```



```
auth required pam_succeed_if.so uid >= 1000
```

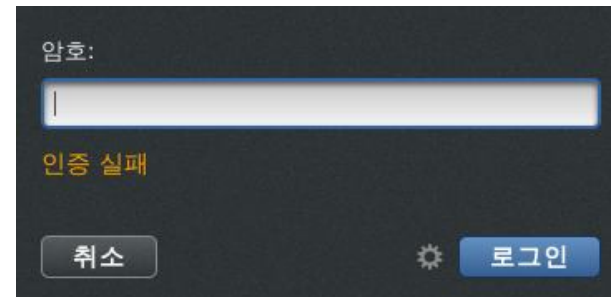
```
[root@localhost pam.d]# cat gdm-password
auth          required          pam_succeed_if.so uid >= 1000
auth          [success=done ignore=ignore default=bad] pam_selinux_permit.so
auth          substack           password-auth
auth          optional          pam_gnome_keyring.so
auth          include            postlogin
```

pam\_succeed\_if.so : UID가 1000일 경우에만 true 값을 반환하는 모듈 실패 시 아래 라인들을 수행함



사용자 이름:

취소 다음



암호:

인증 실패

취소 로그인

## 실습 2. 명령어 su 사용 시 wheel 그룹 멤버들은 패스워드 없이 로그인

```
[ root@localhost pam.d] # pwd
/etc/pam.d
[ root@localhost pam.d] # cat su
#%PAM-1.0
auth                sufficient      pam_rootok.so
# Uncomment the following line to implicitly trust users in the "wheel" group.
#auth               sufficient      pam_wheel.so trust use_uid
# Uncomment the following line to require a user to be in the "wheel" group.
#auth               required        pam_wheel.so use_uid
auth                substack        system-auth
auth                include          postlogin
account             sufficient      pam_succeed_if.so uid = 0 use_uid quiet
account             include          system-auth
password            include          system-auth
session             include          system-auth
session             include          postlogin
session             optional        pam_xauth.so
[ root@localhost pam.d] #
```

```
[gildong@localhost ~]$ whoami
gildong
[gildong@localhost ~]$ su - test01
암호:
마지막 로그인 실패: 일 10월 8 11:33:53 KST 2023 일시 pts/1
[test01@localhost ~]$
[test01@localhost ~]$ whoami
test01
[test01@localhost ~]$
```

```
[root@localhost pam.d]# cat /etc/group | grep wheel
wheel:x:10:
[root@localhost pam.d]#
```

```
auth    sufficient pam_wheel.so trust use_uid
```

```
[root@localhost pam.d]# pwd
/etc/pam.d
[root@localhost pam.d]# cat su
#%PAM- 1.0
```

```
auth            sufficient      pam_wheel.so trust use_uid
auth            sufficient      pam_rootok.so
# Uncomment the following line to implicitly trust users in the "wheel" group.
#auth           sufficient      pam_wheel.so trust use_uid
# Uncomment the following line to require a user to be in the "wheel" group.
#auth           required        pam_wheel.so use_uid
auth            substack        system-auth
auth            include         postlogin
```

```
gpasswd -a gildong wheel
```

```
cat /etc/group | grep wheel
```

```
[root@localhost /]# gpasswd -a gildong wheel
사용자 gildong을(를) wheel 그룹에 등록 중
[root@localhost /]#
[root@localhost /]# cat /etc/group | grep wheel
wheel:x:10:gildong
[root@localhost /]#
```

```
[gildong@localhost /]$ su - test01
마지막 로그인: 일 10월 15 11:09:48 KST 2023 일시 pts/1
마지막 로그인 실패: 일 10월 15 11:18:10 KST 2023
마지막 로그인 후 1 번의 로그인 시도가 실패하였습니다.
[test01@localhost ~]$
```

```
[root@localhost ~]# gpasswd -a root wheel
사용자 root을(를) wheel 그룹에 등록 중
[root@localhost ~]#
[root@localhost ~]# cat /etc/group | grep wheel
wheel:x:10:gildong, root
[root@localhost ~]# exit
logout
[gildong@localhost ~]$ su - root
마지막 로그인: 일 10월 15 11:23:47 KST 2023 일시 pts/1
[root@localhost ~]#
```

### 실습 3. wheel 그룹 멤버들만 명령어 su 사용 ( 사용시 패스워드 입력 필수)

```
auth    required pam_wheel.so use_uid
```

```
[root@localhost pam.d]# cat su
```

```
#%PAM-1.0
```

```
auth            required            pam_wheel.so use_uid
```

```
auth            sufficient          pam_rootok.so
```

```
# Uncomment the following line to implicitly trust users in the "wheel" group.
```

```
#auth           sufficient          pam_wheel.so trust use_uid
```

```
# Uncomment the following line to require a user to be in the "wheel" group.
```

```
#auth           required            pam_wheel.so use_uid
```

```
auth            substack            system-auth
```

```
auth            include             postlogin
```

```
[gildong@localhost ~]$ cat /etc/group | grep wheel
wheel:x:10:gildong,root
[gildong@localhost ~]$
[gildong@localhost ~]$ su - test01
암호:
마지막 로그인: 일 10월 15 11:44:15 KST 2023 일시 pts/2
[test01@localhost ~]$
[test01@localhost ~]$ whoami
test01
[test01@localhost ~]$ su - test02
암호:
su: 권한 부여 거부
[test01@localhost ~]$ su - root
암호:
su: 권한 부여 거부
[test01@localhost ~]$ exit
logout
[gildong@localhost ~]$ su - root
암호:
마지막 로그인: 일 10월 15 11:24:57 KST 2023 일시 pts/1
마지막 로그인 실패: 일 10월 15 11:45:26 KST 2023 일시 pts/2
마지막 로그인 후 1 번의 로그인 시도가 실패하였습니다.
[root@localhost ~]#
```

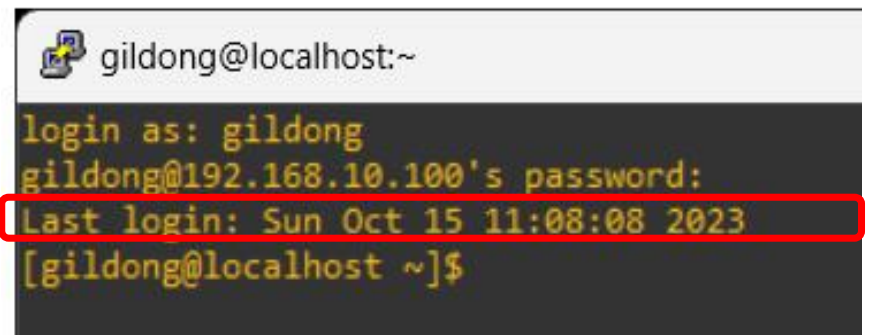
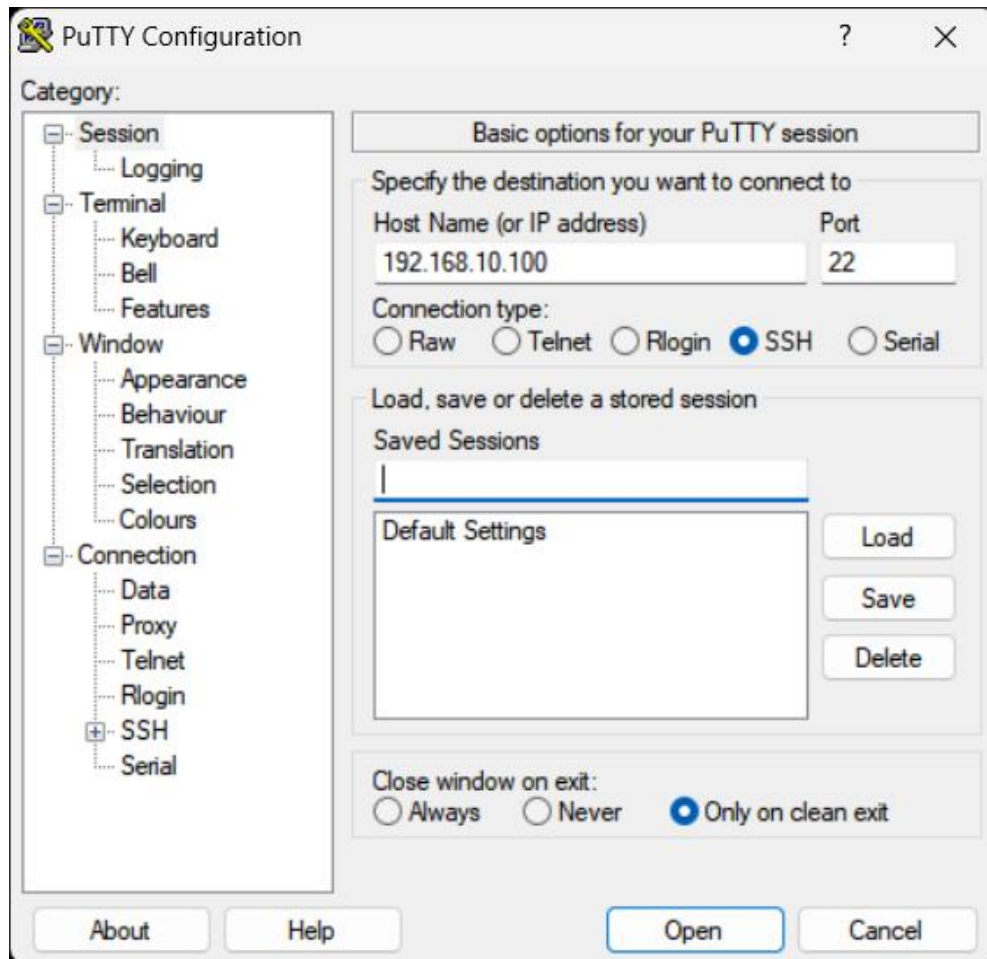
```
cat /etc/group | grep wheel
whoami
su - test01
whoami
su - test02
exit
su - root
```



## 실습 4. 원격 접속 사용 시간 제한

```
[root@localhost pam.d]# pwd
/etc/pam.d
[root@localhost pam.d]# ls sshd
sshd
[root@localhost pam.d]# cat sshd
#%PAM-1.0
auth      required      pam_sepermit.so
auth      substack      password-auth
auth      include      postlogin
account   required      pam_nologin.so
account   include      password-auth
password  include      password-auth
# pam_selinux.so close should be the first session rule
session   required      pam_selinux.so close
session   required      pam_loginuid.so
# pam_selinux.so open should only be followed by sessions to
text
session   required      pam_selinux.so open env_params
session   optional     pam_keyinit.so force revoke
session   include      password-auth
session   include      postlogin
[root@localhost pam.d]#
```

```
cd /etc/pam.d
cat sshd
```

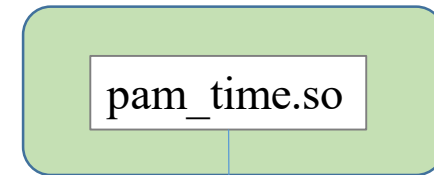


- 원격 접속 사용 시간을 평일 9시 30분부터 17시 30분으로 제한

```
[root@localhost pam.d]# cat sshd
#%PAM-1.0
account      required    pam_time.so
auth         required    pam_sepermit.so
auth         substack    password-auth
auth         include     postlogin
account      required    pam_nologin.so
account      include     password-auth
password     include     password-auth
```

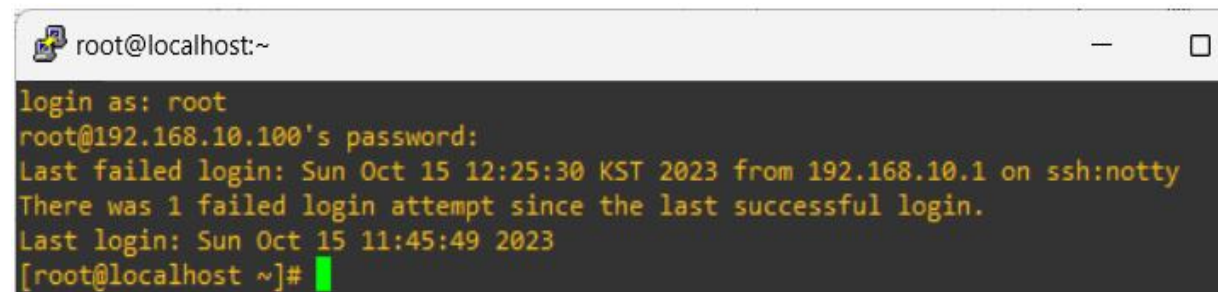
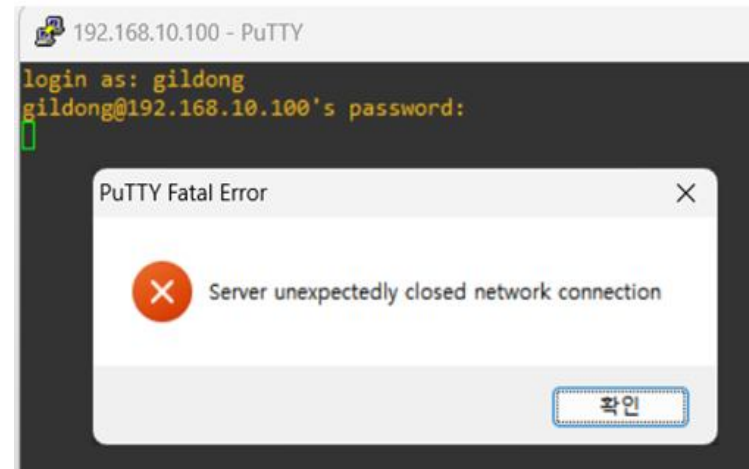
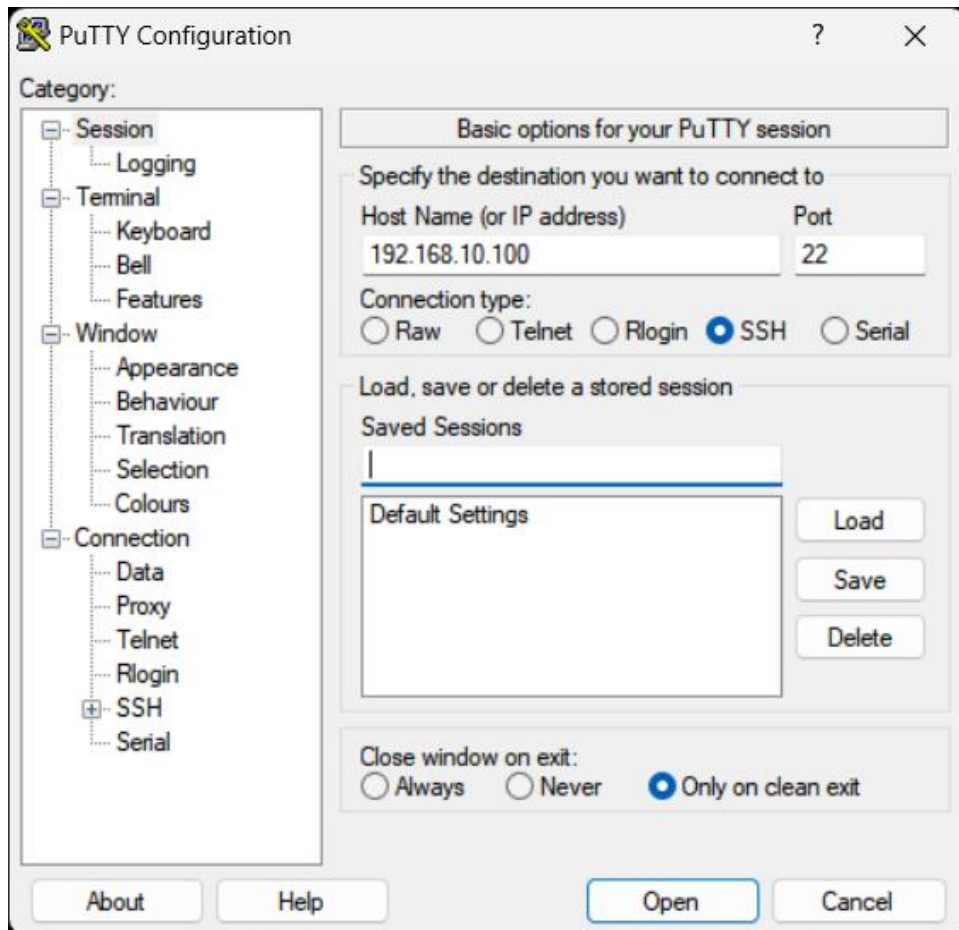
```
[root@localhost security]# pwd
/etc/security
[root@localhost security]# ls time.conf
time.conf
[root@localhost security]# tail -4 time.conf
# End of example file.
#
sshd; *; gildong; !Wd0930-1730
sshd; *; root; Wd0930-1730
[root@localhost security]#
```

**/lib64/security**



/etc/security/time.conf

sshd; \*; gildong; !wk0930-17:30  
sshd; \*; root; wk0930-17:30



## 실습 6. 콘솔로그인 시 비밀번호 정책 설정



gildong

암호:

2 로그인 실패로 인해 계정이 잠김

취소 로그인



gildong

암호:

일시적으로 계정이 잠금되었습니다 (5 초 남음)

취소 로그인

```
/etc/pam.d/password-auth
```

```
auth    required pam_tally2.so unlock_time=10
```

```
account required pam_tally2.so
```

```
pam_tally2
```

```
pam_tally2 -r -u gildong
```

```
pam_tally2 -r
```

## pam\_tally2.so

argument	설명
deny=N	로그인 시도가 N번 실패하면 접근을 차단
lock_time=N	로그인 실패 후에 N초 동안 접근을 차단
unlock_time=N	관리자가 정한 일정 횟수 이상 로그인에 실패했을 경우 N초 동안 접근을 차단 해당 시간 동안은 관리자가 계정을 해제하기 전까지는 계정잠김
root_unlock_time=N	root 사용자가 일정 횟수 이상 로그인에 실패했을 경우 N초 동안 접근 차단
file=경로	카운트 내역을 기록하는 파일 경로를 기록 기본 파일명은 /var/log/tallylog
no_log_info	syslog에 메시지를 전달하지 않음
silent	관련 정보를 출력하지 않음