

root	.....	3
Root ssh login	.....	5
	.....	5
	.....	9
	.....	12
root su	.....	12
	, , .....	13
	.....	13
	.....	13
	GID .....	13
UID	.....	13
shell	.....	13
Session Timeout	.....	13



# root

가 root

```

root      가      (      ,      ) root
          (      )      root
가

```

## RHEL 6, 7

[Telnet]

```

#cat /etc/pam.d/login
auth required /lib/security/pam_securetty.so
#cat /etc/securetty
pts/0 ~ pts/x

```

[Telnet                   ] Step 1) /etc/securetty                    pts/0 ~ pts/x                    ,  
Step 2) /etc/pam.d/login                    ,

```

(        ) #auth required /lib/security/pam_securetty.so
(        ) auth required /lib/security/pam_securetty.so

```

※ /etc/securetty : Telnet                    root                    /etc/securetty                    \*pts/x  
                  PAM                    root                    /etc/securetty  
                  pts/x

```

#echo > /etc/securetty

```

root /

```

Last login: Fri Jan 7 14:27:23 2022 from 192.168.230.1
[root@rhel7 ~]# telnet 192.168.230.143
Trying 192.168.230.143...
Connected to 192.168.230.143.

```

```
Escape character is '^]'.
Red Hat Enterprise Linux Server release 6.10 (Santiago)
Kernel 2.6.32-754.el6.x86_64 on an x86_64
rhel6 login: root
Password:
Login incorrect
```

[SSH ]

Step 1) vi /etc/ssh/sshd\_config Step 2) ,

```
( ) #PermitRootLogin Yes
( ) PermitRootLogin No
```

```
가 /etc/securetty
Red Hat Enterprise Linux /etc/securetty
가
가
```

```
echo > /etc/securetty
```

KDM, GDM XDM security 가 .

```
auth [user_unknown=ignore success=ok ignore=ignore default=bad]
pam_securetty.so
```

```
/etc/pam.d/gdm
/etc/pam.d/gdm-autologin
/etc/pam.d/gdm-fingerprint
/etc/pam.d/gdm-password
/etc/pam.d/gdm-smartcard
/etc/pam.d/kdm
/etc/pam.d/kdm-np
/etc/pam.d/xdm
```

[https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/6/html-single/security\\_guide/index#s2-wstation-privileges-noroot](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html-single/security_guide/index#s2-wstation-privileges-noroot)

RHEL 8 tty security PAM /etc/securetty RHEL . /etc/securetty 가



/etc/pam.d/passwd

가 .

```
password required pam_cracklib.so retry=3 maxsequence=3 maxrepeat=3
```

[https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/6/html-single/security\\_guide/index#sect-Security\\_Guide-Workstation\\_Security-Password\\_Security](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html-single/security_guide/index#sect-Security_Guide-Workstation_Security-Password_Security)

### RHEL 7

pam\_quality /etc/pam.d/passwd 가 .

```
password required pam_pwquality.so retry=3
```

가 /etc/security/pwquality.conf 가 8 가 .

```
minlen = 8
minclass = 4
```

/etc/security/pwquality.conf

가 .

```
maxsequence = 3
maxrepeat = 3
```

[https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/7/html-single/security\\_guide/index](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html-single/security_guide/index)

### RHEL 8

Red Hat Enterprise Linux 8 authconfig authselect .  
/etc/pam.d/ PAM system-auth password-auth

Red Hat Enterprise Linux 8  
/etc/security/pwquality.conf / authselect

1. 가

```
# authselect list
```

2.

```
# authselect current
```

3. /

```
# authselect apply-changes -b --backup=sssd.backup
```

4. sssd password-policy

```
# authselect create-profile password-policy -b sssd
```

- /etc/authselect/custom/password-policy/ .

5.

```
# authselect select custom/password-policy
# authselect current
```

6. 가 faillock

```
# authselect enable-feature with-mkhomedir
# authselect enable-feature with-faillock
```

RHEL 8.2 pam\_faillock /etc/security/faillock.conf
faillock.conf .

```
:/etc/pam.d/xxxx-auth pam_faillock.so faillock.conf
.faillock.conf
```

/etc/authselect/custom/PROFILE/xxxx-auth .

```
# Edit {system,password,fingerprint,smartcard}-auth in
/etc/authselect/custom/password-policy/
```

(Before)

```
auth required pam_env.so
auth required pam_faildelay.so
```

```

delay=2000000
auth      required                                pam_faillock.so
preauth  silent deny=4 unlock_time=1200
...snip...
auth      required                                pam_faillock.so
authfail  deny=4 unlock_time=1200
auth      required                                pam_deny.so
↓
(After)
auth      required                                pam_env.so
auth      required                                pam_faildelay.so
delay=2000000
auth      required                                pam_faillock.so
preauth
...snip...
auth      required                                pam_faillock.so
authfail
auth      required                                pam_deny.so

```

7. /etc/authselect/custom/password-policy/  
PAM system-auth password-auth /

```
# authselect apply-changes
```

8. ( )  
/etc/authselect/custom/password-policy/system-auth  
/etc/authselect/custom/password-policy/password-auth  
(pam\_pwquality.so )

```
password requisite pam_pwhistory.so remember=5 use_authok
```

9. /etc/authselect/custom/password-policy/system-auth /etc/authselect/custom/password-policy/password-auth  
pam\_pwquality.so / 가

```
enforce_for_root
```

: authselect apply-changes

10. /etc/security/pwquality.conf

```
minlen = 9 (
```





```
# faillock --user <username> --reset
```

[https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/6/html-single/security\\_guide/index#sect-Security\\_Guide-Workstation\\_Security-Account\\_Locking](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html-single/security_guide/index#sect-Security_Guide-Workstation_Security-Account_Locking)

### RHEL 7

```
3 /etc/pam.d/system-auth      가 /etc/pam.d/password-auth  10 auth 가 . .
```

```
1 auth      required      pam_env.so
2 auth      required      pam_faillock.so preauth silent audit deny=3
unlock_time=600 <- 가
3 auth      sufficient    pam_unix.so nullok try_first_pass
4 auth      [default=die] pam_faillock.so authfail audit deny=3
unlock_time=600 <- 가
5 auth      requisite     pam_succeed_if.so uid >= 1000 quiet_success
6 auth      required      pam_deny.so
```

가 .

```
account     required      pam_faillock.so
```

```
auth required pam_faillock.so /etc/pam.d/system-auth /etc/pam.d/password-auth
even_deny_root 가 .
```

```
auth      required      pam_faillock.so preauth silent audit deny=3
even_deny_root unlock_time=600
auth      sufficient    pam_unix.so nullok try_first_pass
auth      [default=die] pam_faillock.so authfail audit deny=3
even_deny_root unlock_time=600

account     required      pam_faillock.so
```

```
#faillock --user <username> --reset
```

[https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/7/html-single/security\\_guide/index#sect-Security\\_Guide-Workstation\\_Security-Account\\_Locking](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html-single/security_guide/index#sect-Security_Guide-Workstation_Security-Account_Locking)  
<https://access.redhat.com/solutions/62949>

## RHEL 8

```
/etc/pam.d/system-auth /etc/pam.d/password-auth  
    . authselect      pam_faillock      /      .
```

To enable faillock

```
# authselect enable-feature with-faillock
```

To disable faillock

```
# authselect disable-feature with-faillock
```

```
faillock      faillock      /etc/security/faillock.conf      .
```

```
deny=4  
unlock_time=1200  
silent
```

```
# faillock --user username
```

```
# faillock --user username --reset
```

```
SSHD      pam_faillock.so가      SSHD
```

```
# vi /etc/ssh/sshd_config  
ChallengeResponseAuthentication yes  
PasswordAuthentication no
```



/etc/login.defs

```

PASS_MAX_DAYS 99999          가      ( ) PASS_MIN_DAYS 0          ( )
PASS_MIN_LEN 5              PASS_WARN_AGE 7          ( )

```

/etc/passwd

/etc/group root:x:0:root

### GID

/etc/group /etc/passwd

### UID

/etc/passwd UID가

### shell

/bin/false /sbin/nologin

/etc/passwd

## Session Timeout

/etc/profile

```

HOSTNAME=`/usr/bin/hostname 2>/dev/null` HISTSIZE=5000 #
HISTTIMEFORMAT="%F %T " # TMOUT=300 #
if [ "$HISTCONTROL" = "ignorespace" ]; then

```

```

export HISTCONTROL=ignoreboth

```

else

```

export HISTCONTROL=ignoredups

```

fi

export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE HISTCONTROL HISTTIMEFORMAT TMOUT #

From:  
<https://atl.kr/dokuwiki/> - **AllThatLinux!**

Permanent link:  
<https://atl.kr/dokuwiki/doku.php/%EA%B3%84%EC%A0%95%EA%B4%80%EB%A6%AC?rev=1641883795>

Last update: **2022/01/11 06:49**

