

root	.....	3
Root ssh login	.....	4
	.....	5
	.....	6
	.....	8
root su	.....	8
	, , .....	8
	.....	8
	.....	9
	GID .....	9
UID	.....	9
shell	.....	9
Session Timeout	.....	9



# root

가 root

```

root 가 ( , ) root
가 ( ) root

```

## RHEL 6, 7

[Telnet]

```

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

```

[SSH]

```

#cat /etc/sshd_config
PermitRootLogin no

```

root /

[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

[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 securetty 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)

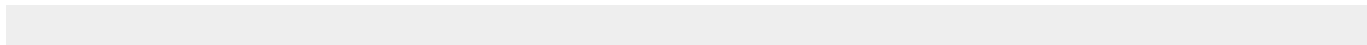
RHEL 8 tty securetty PAM  
/etc/securetty RHEL . /etc/securetty 가  
/etc/pam.d  
pam\_securetty.so 가 /etc/securetty

[https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/8/html/considerations\\_in\\_adopting\\_rhel\\_8/security\\_considerations-in-adopting-rhel-8#securetty\\_security](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/considerations_in_adopting_rhel_8/security_considerations-in-adopting-rhel-8#securetty_security)

### Root ssh login

#### RHEL 6, 7

SSH SSH /etc/ssh/sshd\_config







```
account    required    pam_faillock.so
```

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

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





```
/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=1641522030>

Last update: 2022/01/07 02:20

