

RedHat Enterprise Linux Server	가	3
가		3
		3
		3
	/	5

rhel_

Last
update:
2015/12/10
01:15

-
- https://atl.kr/dokuwiki/doku.php/rhel_%EC%84%9C%EB%B2%84_%EB%B3%B4%EC%95%88_%EC%A0%90%EA%B2%80_%EA%B0%80%EC%9D%B4%EB%93%9C

가

RedHat Enterprise Linux Server

가

가

OS

lib 가

```
[root@test ~]# cat /usr/share/doc/pam-1.1.1/txts/README*
```

```
*      : /etc/pam.d/
*      (lib      )
```

32bit	cd /lib/security/
64bit	cd /lib64/security/

system-auth

system-auth

```
[root@test ~]# 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      required      pam_tally2.so deny=3 onerr=fail
unlock_time=120 // 가
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   required      pam_tally2.so // 가
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=
password sufficient pam_unix.so sha512 shadow nullok
try_first_pass use_authok
password required pam_deny.so

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

test

```
[test1@test ~]$ su - test1
Password:
su: incorrect password // 1
[test1@test ~]$ su - test1
Password:
su: incorrect password // 2
[test1@test ~]$ su - test1
Password:
su: incorrect password // 3
[test1@test ~]$ su - test1
Account locked due to 4 failed logins // 4
Password:
su: incorrect password
[test1@test ~]$ su - test1
Account locked due to 5 failed logins // 5

Password:
su: incorrect password

[root@test ~]# pam_tally2 //
Login          Failures Latest failure    From
test1           5      01/19/15 14:17:11 pts/0

[root@test ~]# pam_tally2 --reset //          failures

Login          Failures Latest failure    From
test1           5      01/19/15 14:17:11 pts/0
[root@test ~]# pam_tally2 //
```

/

password

```
[root@test ~]# vim /etc/login.defs
#
# Please note that the parameters in this configuration file control the
# behavior of the tools from the shadow-utils component. None of these
# tools uses the PAM mechanism, and the utilities that use PAM (such as the
# passwd command) should therefore be configured elsewhere. Refer to
# /etc/pam.d/system-auth for more information.
#
# *REQUIRED*
#   Directory where mailboxes reside, _or_ name of file, relative to the
#   home directory. If you _do_ define both, MAIL_DIR takes precedence.
#   QMAIL_DIR is for Qmail
#
#QMAIL_DIR Maildir
MAIL_DIR    /var/spool/mail
#MAIL_FILE  .mail

# Password aging controls:
#
#   PASS_MAX_DAYS    Maximum number of days a password may be used.
#   PASS_MIN_DAYS    Minimum number of days allowed between password
changes.
#   PASS_MIN_LEN     Minimum acceptable password length.
#   PASS_WARN_AGE    Number of days warning given before a password expires.
#
PASS_MAX_DAYS 99999 //
PASS_MIN_DAYS 0    //
PASS_MIN_LEN  5    //
PASS_WARN_AGE 7    //                -7

#
# Min/max values for automatic uid selection in useradd
#
UID_MIN        500
UID_MAX        60000

#
# Min/max values for automatic gid selection in groupadd
#
GID_MIN        500
GID_MAX        60000

#
```

rhel_

Last update: 2015/12/10 01:15 가

```
# If defined, this command is run when removing a user.
# It should remove any at/cron/print jobs etc. owned by
# the user to be removed (passed as the first argument).
#
#USERDEL_CMD    /usr/sbin/userdel_local

#
# If useradd should create home directories for users by default
# On RH systems, we do. This option is overridden with the -m flag on
# useradd command line.
#
CREATE_HOME yes

# The permission mask is initialized to this value. If not specified,
# the permission mask will be initialized to 022.
UMASK          077

# This enables userdel to remove user groups if no members exist.
#
USERGROUPS_ENAB yes

# Use SHA512 to encrypt password.
ENCRYPT_METHOD SHA512
```

From: <https://at1.kr/dokuwiki/> - AllThatLinux!

Permanent link: https://at1.kr/dokuwiki/doku.php/rhel_%EC%84%9C%EB%B2%84_%EB%B3%B4%EC%95%88_%EC%A0%90%EA%B2%80_%EA%B0%80%EC%9D%B4%EB%93%9C

Last update: 2015/12/10 01:15

