
.....	3
root	3
.....	3
.....	4
Password complexity	4
.....	4
.....	7
.....	7
.....	7
.....	9
su	9
.....	10
/etc/login.defs	10
.....	11
.....	11
Session Timeout	12
.....	12
.....	12

— 2018/10/22 11:06

RHEL

RHEL

koovis@gmail.com

root

• :

root

root
/etc/securetty

console

root

가

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

```
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
```



root (SSH)
SSH root login

root

root SSH login

/etc/ssh/sshd_config

```
PermitRootLogin no
```

- https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/chap-Security_Guide-Securing_Your_Network.html#sect-Security_Guide-Workstation_Security-Administrative_Controls
- https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/sec-Controlling_Root_Access.html#sec-Disallowing_Root_Access

Password complexity



가

가

가

- :

RHEL6

```
##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_unix.so try_first_pass nullok
auth      required      pam_deny.so

account   required      pam_unix.so

password  requisite      pam_cracklib.so try_first_pass retry=3 type=
minlen=8 minclass=4      # <--
password  sufficient    pam_unix.so try_first_pass use_authok nullok
sha512 shadow
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

```

```

#%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_unix.so try_first_pass nullok
auth required pam_deny.so

account required pam_unix.so

password requisite pam_cracklib.so try_first_pass retry=3 type=
minlen=8 minclass=4 # <--
password sufficient pam_unix.so try_first_pass use_authtok nullok
sha512 shadow
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

```

```

/etc/pam.d/passwd . passwd
3 . pam_cracklib

```

- https://linux.die.net/man/8/pam_cracklib

RHEL7

```

RHEL7 pam_cracklib pam_pwquality .
. /etc/security/pwquality.conf
.

```

```

minlen = 8
minclass = 4

```

```

authconfig .

```

```

# authconfig --passminlen=<number> --passminclass=<number> --
passmaxrepeat=<number>

```

- -passminlen=<number>
- -passminclass=<number> (, , ,)
- -passmaxrepeat=<number>) PasssssssWord
s
- -passmaxclassrepeat=<number>) P@ssword
ssword

[pwquality.conf](#)



root pwquality

```
root pwquality /etc/pam.d/system-auth
/etc/pam.d/password-auth . local_users_only
enforce_for_root .
```

```
##%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_faildelay.so delay=2000000
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 requisite pam_pwquality.so try_first_pass enforce_for_root
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

```

- https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/chap-Security_Guide-Securing_Your_Network.html#sect-Security_Guide-Workstation_Security-Password_Security
- https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/chap-Hardening_Your_System_with_Tools_and_Services.html#sec-Password_Security

- :

RHEL 5.3

pam.tally . /etc/pam.d/system-auth
가 .

```

auth      required      pam_tally.so deny=3 onerr=fail unlock_time=1200
no_magic_root
account   required     pam_tally.so no_magic_root reset

```

RHEL 5.4

pam.tally2 . /etc/pam.d/system-auth
가 .

```

auth      required      pam_tally2.so deny=3 onerr=fail unlock_time=1200
no_magic_root

```

RHEL 6

RHEL 6 pam_faillock .

1. root 3 600 (10)
/etc/pam.d/system-auth /etc/pam.d/password-auth auth
가 .

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

2. account 가 .

```
account required pam_faillock.so
```

3. root 1 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
```

4. faillock 가 .

```
[root@localhost ~]# faillock
john:
When          Type  Source
Valid
2013-03-05 11:44:14 TTY pts/0
V
```

5. .

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

RHEL 7

/etc/pam.d/system-auth

/etc/pam.d/password-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_faillock.so preauth silent audit deny=3
unlock_time=600 # 가
auth      sufficient    pam_unix.so nullok try_first_pass
auth      [default=die] pam_faillock.so authfail audit deny=3
unlock_time=600 # 가
auth      requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth      required      pam_deny.so

account   required      pam_faillock.so # 가
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

```

- https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/chap-Security_Guide-Securing_Your_Network.html#sect-Security_Guide-Workstation_Security-Administrative_Controls
- https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/chap-Hardening_Your_System_with_Tools_and_Services.html#sect-Security_Guide-Workstation_Security-Account_Locking

SU

- :

wheel 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           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
```



trust

/etc/login.defs

login.defs shadow-utils

- /etc/default/useradd
- /etc/login.defs
- /usr/bin/chage
- /usr/bin/gpasswd
- /usr/bin/lastlog
- /usr/bin/newgrp
- /usr/bin/sg
- /usr/sbin/adduser
- /usr/sbin/chpasswd
- /usr/sbin/groupadd
- /usr/sbin/groupdel
- /usr/sbin/groupmems
- /usr/sbin/groupmod
- /usr/sbin/grpck
- /usr/sbin/grpconv

- /usr/sbin/grpunconv
- /usr/sbin/newusers
- /usr/sbin/pwck
- /usr/sbin/pwconv
- /usr/sbin/pwunconv
- /usr/sbin/useradd
- /usr/sbin/userdel
- /usr/sbin/usermod
- /usr/sbin/vigr
- /usr/sbin/vipw


/usr/bin/passwd
pam.d

login.defs

- <https://access.redhat.com/solutions/66322>

- :

/etc/login.defs



. pam.d login.defs pam.d

- <https://access.redhat.com/solutions/656833>

/etc/login.defs

```
# 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    9       # 9
PASS_WARN_AGE   7
```

Session Timeout

- :

/etc/profile TMOU

```
HOSTNAME=`/usr/bin/hostname 2>/dev/null`
HISTSZIE=5000 # 5000
HISTTIMEFORMAT="%F %T " #
TMOU=300 #
if [ "$HISTCONTROL" = "ignoreospace" ] ; then
    export HISTCONTROL=ignoreboth
else
    export HISTCONTROL=ignoredups
fi

export PATH USER LOGNAME MAIL HOSTNAME HISTSZIE HISTCONTROL HISTTIMEFORMAT
TMOU #
```

- <https://linux-audit.com/configure-the-minimum-password-length-on-linux-systems/>

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

Permanent link: https://at1.kr/dokuwiki/doku.php/%EB%B3%B4%EC%95%88%EC%B7%A8%EC%95%BD%EC%A0%90_%EC%A0%90%EA%B2%80?rev=1543904521

Last update: 2018/12/04 06:22

