Set Password Policy ***By: Imran Afzal***

- Set number of days for password Expiration.

Users must change their password within the days.
This setting impacts only when creating a user, not impacts to existing users.
If set to existing users, run the command "chage -M (days) (user)".
`vi /etc/login.defs`
line 25: set 60 for Password Expiration
PASS_MAX_DAYS 60

- Set minimum number of days available of password.

Users must use their password at least this days after changing it.
This setting impacts only when creating a user, not impacts to exisiting users.
If set to exisiting users, run the command "chage -m (days) (user)".
vi /etc/login.defs
line 26: set 2 for Minimum number of days available
PASS_MIN_DAYS 2

- Set number of days for warnings before expiration.

This setting impacts only when creating a user, not impacts to exisiting users.
If set to exisiting users, run the command "chage -W (days) (user)".
vi /etc/login.defs
line 28: set 7 for number of days for warnings
PASS_WARN_AGE 7

- Limit using a password that was used in past.

Users can not set the same password within the generation.
vi /etc/pam.d/system-auth
password sufficient pam_unix.so sha512 shadow nullok try_first_pass use_authtok remember=5

- Set minimum password length.

Users can not set their password length less than this parameter.
set 8 for minimum password length
authconfig --passminlen=8 --update
the parameter is set in a config below
grep "^minlen" /etc/security/pwquality.conf
minlen = 8

- Set minimum number of required classes of characters for the new password. (kinds ⇒ UpperCase / LowerCase / Digits / Others)

set 2 for minimum number of required classes of characters
authconfig --passminclass=2 --update
the parameter is set in a config below
grep "^minclass" /etc/security/pwquality.conf

minclass = 2

- Set maximum number of allowed consecutive same characters in the new password.

set 2 for maximum number of allowed consecutive same characters
authconfig --passmaxrepeat=2 --update
the parameter is set in a config below
grep "^maxrepeat" /etc/security/pwquality.conf
maxrepeat = 2

- Set maximum number of allowed consecutive characters of the same class in the new password.

set 4 for maximum number of allowed consecutive characters of the same class
authconfig --passmaxclassrepeat=4 --update
the parameter is set in a config below
grep "^maxclassrepeat" /etc/security/pwquality.conf
maxclassrepeat = 4

- Require at least one lowercase character in the new password.

authconfig --enablereqlower --update
the parameter is set in a config below
(if you'd like to edit the value, edit it with vi and others)
grep "^lcredit" /etc/security/pwquality.conf
lcredit = -1

- Require at least one uppercase character in the new password.

authconfig --enablerequpper --update
the parameter is set in a config below
(if you'd like to edit the value, edit it with vi and others)
grep "^ucredit" /etc/security/pwquality.conf
ucredit = -1

- Require at least one digit in the new password.

authconfig --enablereqdigit --update
the parameter is set in a config below
(if you'd like to edit the value, edit it with vi and others)
grep "^dcredit" /etc/security/pwquality.conf
dcredit = -1

- Require at least one other character in the new password.

authconfig --enablereqother --update
the parameter is set in a config below
(if you'd like to edit the value, edit it with vi and others)
grep "^ocredit" /etc/security/pwquality.conf
ocredit = -1

- Set maximum length of monotonic character sequences in the new password. (ex ⇒ '12345', 'fedcb')

vi /etc/security/pwquality.conf
add to the end
maxsequence = 3

- Set number of characters in the new password that must not be present in the old password.

vi /etc/security/pwquality.conf
add to the end
difok = 5

- Check whether the words longer than 3 characters from the GECOS field of the user's passwd entry are contained in the new password.

vi /etc/security/pwquality.conf
add to the end
gecoscheck = 1