```
[root@42ec75236ecc mydir]# man useradd > useradd-man.txt

[root@42ec75236ecc mydir]# grep -i "password" useradd-man.txt

The number of days after a password expires until the account is permanently disabled. A value of 0 disables the account as soon as the password has expired, and a value of -I disables the feature.

Example: -K PASS_MAX_DAYS=-1 can be used when creating system account to turn off password aging, even though system account has no password at all. Multiple -K options can be specified, e.g.: -K UID_MEN=100 -K UID_MAX=499

-P, --password PASSMOND

The encrypted password, as returned by crypt(3). The default is to disable the password.

Note: This option is not recommended because the password (or encrypted password) will be visible by users listing You should make sure the password respects the system's password policy.

The number of days after a password has expired before the account will be disabled.

the same name, same password, and same CID).

The maximum number of days allowed between password changes. Any password is older to the minimum number of days allowed between password changes. Any password changes are means warm shedow password svite configuration.

can't update password file

[root@42ec75236ecc mydir]# []
```

root login with password via SSH. [root@42ec75236ecc mydir]# cksum securecopy.txt 2766876939 488142 securecopy.txt [root@42ec75236ecc mydir]# []

```
Complete!

[root@42ec75236ecc mydir]# cksum securecopy.txt

2766876939 488142 securecopy.txt

[root@42ec75236ecc mydir]# nano securecopy.txt

[root@42ec75236ecc mydir]# cksum securecopy.txt

2988460550 489318 securecopy.txt

[root@42ec75236ecc mydir]# find . -name AbdullahAlharbi.txt

./mydir2/AbdullahAlharbi.txt

[root@42ec75236ecc mydir]# []
```