Important Files

 # /etc/passwd → It contains all users general information. Such as user id, gid, shell, home directory etc.

/etc/passwd- → This is backup file of /etc/passwd

/etc/shadow → It contains all users password information. such as encrypted password, password expiry, account expiry, warning period etc..

/etc/shadow- → This is backup file of /etc/shadow

/etc/group → It contains all groups general information. such as group id, group members list.

 # /etc/group- → This is backup file of /etc/group

/etc/gshadow → It contails all groups password information. such as encrypted password, group admin, group members list.

/etc/gshadow- → This is backup file of /etc/gshadow

 # /etc/default/useradd → THis is the default user administration configuration file. you can specify shell, skel, home directory, mail etc...

[root@localhost ~]# **cat /etc/default/useradd**

useradd defaults file

GROUP=100

HOME=/home

INACTIVE=-1

EXPIRE=

SHELL=/bin/bash

SKEL=/etc/skel

CREATE_MAIL_SPOOL=yes

/etc/login.defs → This is main configuration file for user administration, group adminitration, password management.

[root@localhost ~]# **cat /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

# Default initial "umask" value used by login(1) on non-PAM enabled systems.
# Default "umask" value for pam_umask(8) on PAM enabled systems.
# UMASK is also used by useradd(8) and newusers(8) to set the mode for new
# home directories if HOME_MODE is not set.
# 022 is the default value, but 027, or even 077, could be considered
# for increased privacy. There is no One True Answer here: each sysadmin
# must make up their mind.
UMASK           022

# HOME_MODE is used by useradd(8) and newusers(8) to set the mode for new
# home directories.
# If HOME_MODE is not set, the value of UMASK is used to create the mode.
HOME_MODE       0700

# 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_WARN_AGE   7

#
# Min/max values for automatic uid selection in useradd
#
UID_MIN                 1000
UID_MAX                 60000
# System accounts
SYS_UID_MIN               201
SYS_UID_MAX               999

#
# Min/max values for automatic gid selection in groupadd
#
GID_MIN                 1000
GID_MAX                 60000
# System accounts
SYS_GID_MIN               201
SYS_GID_MAX               999

#
# 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

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

#

USERGROUPS_ENAB yes

Use SHA512 to encrypt password.

ENCRYPT_METHOD SHA512

/etc/skel/ → This is skeleton directory this provides user login program, user profile program , logout program

.**bashrc** → this is local login program for user

.bash_profile → This is local profile program for user

.bash_logout → This is local logout program for user

 # /etc/bashrc → This is the global login program

 # /var/spool/mail/<username> → Local users mail box

 # /root → This is root user's home directory

/**home/<user name>** → This is local users home directory

eg: /home/jack
/home --> base directory
jack --> home directory

User Administration

Command useradd/adduser

As Linux is multiuser multitasking, multiple users can be created in machine.
using useradd command root can create multiple users.
which reflects in file /etc/passwd, the file stores the 7 fields entry.
The command will creates users home directory bydefault in /home by user name with permission mode 0700 and users ownership and group ownership

Syntax:

#useradd <username>

#adduser <username>

Eg:

[root@servera ~]# **useradd anjali**

[root@servera ~]# **adduser ankit**

[root@servera ~]# **cat /etc/passwd**

root:x:0:0:root:/root:/bin/bash

sushmita:x:1000:1000:sushmita:/home/sushmita:/bin/bash

anjali:x:1001:1001::/home/anjali:/bin/bash

ankit : x: 1002:1002: :/home/ankit:/bin/bash
1 2 3 4 5 6 8

➢ **field 1: User name.**

➢**Field 2: Redirected Password (Link to /etc/shadow file where the password details are stored)**

➢**Field 3: user uid**

➢**Field 4: Users primary group id**

➢**Field 5: Comment**

➢**Field 6: Users home directory**

➢**Field 7: Users Login shell**

[root@servera ~]# **tail -2 /etc/passwd**

anjali:x:1001:1001::/home/anjali:/bin/bash

ankit:x:1002:1002::/home/ankit:/bin/bash

[root@servera ~]# **tail -2 /etc/shadow**

anjali:!!:20276:0:99999:7:::

ankit:!!:20276:0:99999:7:::

[root@servera ~]# **tail -2 /etc/group**

anjali:x:1001:

ankit:x:1002:

[root@servera ~]# **tail -2 /etc/gshadow**

anjali:!::

ankit:!::

[root@servera ~]# **ls /home/**

anjali **ankit** sushmita

[root@servera ~]# **ls /var/spool/mail/**

anjali ankit sushmita

[root@servera ~]# **ls -ld /home/anjali/**

drwx------. 3 anjali anjali 78 Jul 7 19:30 /home/anjali/

[root@servera ~]# **id anjali**

uid=1001(anjali) gid=1001(anjali) groups=1001(anjali)

[root@servera ~]# **id ankit**

uid=1002(ankit) gid=1002(ankit) groups=1002(ankit)

[root@servera ~]# **su - anjali**

[anjali@servera ~]$ pwd

/home/anjali

[anjali@servera ~]$ touch abc

[anjali@servera ~]$ ls

abc

[anjali@servera ~]$ ll

total 0

-rw-r--r--. 1 anjali anjali 0 Jul 7 19:50 abc

[anjali@servera ~]$ **exit**

logout

[root@servera ~]# **su anjali**

[anjali@servera root]$ pwd

/root

[anjali@servera root]$ touch apple

touch: cannot touch 'apple': Permission denied

[anjali@servera root]$ **exit**

exit

PASSWORD MANAGEMENT

Cmd: passwd

The passwd command changes or assign passwords for user accounts. A normal user may only change the password for his/her own account, while the superuser may change the password for any account. passwd also changes the account or associated password validity period.

Syntax:

passwd → change password itself root user.

$ passwd → change password itself local user

passwd <username> → assign password to the other local user.

e.g.

[root@servera ~]#

[root@servera ~]# **tail -2 /etc/shadow**

anjali:!!:20276:0:99999:7:::

ankit:!!:20276:0:99999:7:::

[root@servera ~]# **passwd anjali**

Changing password for user anjali.

New password: *redhat*
BAD PASSWORD: The password is shorter than 8 characters

Retype new password: *redhat*

passwd: all authentication tokens updated successfully.

[root@servera ~]# **tail -2 /etc/shadow**

anjali:$6$2aWKtjafHWsRnkVd$8V7KOSj/cTiX6OKz4MNyqqVmL5ZdpteiGESaSsQAlhUcHPYgJk1y6SYZuDs7ywd4FEhWd31NUpTY/h5sm4Hyg/:20277:0:99999:7:::

ankit:!!:20276:0:99999:7:::

---

anjali:$6$2aWKtjafHWsRnkVd$8V7K/ : 20277 :0 : 99999 : 7 : : :
1 2 3 4 5 6 7 8 9

- **field 1: User name.**
- **field 2: Encrypted Password.**
  - 1 --> MD5
  - $2a$ --> Blowfish
  - $2y$ --> Blowfils
  - 5 --> SHA256
  - 6 --> SHA512
  - SECURE HASH ALGO 512BYTES
- **field 3: Number of days since January 1, 1970 to when the password was last changed.**
- **field 4: (Minimum password age) Minimum number of days for which password cannot be changed. (value 0 means it can be changed anytime).**
- **field 5: (Maximum Password Age) Number of days after password must be changed. (value 99999 means that the password never expires).**
- **field 6: warning Period: Number of days to warn user for expiring password.**
- **field 7: Number of days after password expires that the account is disabled.**
- **field 8: Account Expiry: The number of days from January 1, 1970 to the date when an account was disabled.**

➢ **field 9: This field is reserved for some possible future use.**

[root@servera ~]# cat /etc/default/useradd

useradd defaults file

GROUP=100

HOME=/home

INACTIVE=-1

EXPIRE=

SHELL=/bin/bash

SKEL=/etc/skel

CREATE_MAIL_SPOOL=yes

Set password using echo

[root@servera ~]# echo "redhat@123"

redhat@123

[root@servera ~]# **echo "redhat@123" | passwd ankit --stdin**

Changing password for user ankit.

passwd: all authentication tokens updated successfully.

[root@servera ~]# **tail -2 /etc/shadow**

anjali:$6$2aWKtjafHWsRnkVd$8V7KOSj/cTiX6OKz4MNyqqVmL5ZdpteiGESaSsQAlhUcHPYgJk1y6SYZuDs7ywd4FEhWd31NUpTY/h5sm4Hyg/:20277:0:99999:7:::

ankit:6Y/hWkV2pNtEpb7T9$Thqs9YDpl.RX3hob.ShN2G2ozPcthIt0sLQa0RtawMCKRCex4IVfR9MatxfgaTjeZ53m9CAthoL/Nq.94cJnE1:20277:0:99999:7:::

[root@servera ~]# **su - ankit** → ***user can change self password***

[ankit@servera ~]$ **passwd**

Changing password for user ankit.

Current password: redhat@123

New password: Linux@123!

Retype new password: Linux@123!

passwd: all authentication tokens updated successfully.

[ankit@servera ~]$ tail -1 /etc/shadow

tail: cannot open '/etc/shadow' for reading: Permission denied

[ankit@servera ~]$ **exit**

logout

[root@servera ~]# **tail -2 /etc/shadow**

anjali:$6$2aWKtjafHWsRnkVd$8V7KOSj/cTiX6OKz4MNyqqVmL5ZdpteiGESaSsQAlhUcHPYgJk1y6SYZuDs7ywd4FEhWd31NUpTY/h5sm4Hyg/:20277:0:99999:7:::

ankit:6RV/4f3OfUDziSl/Y$twQXnmFmHOFWcEzIQUUsmoo6DSsVTOHTNhfzU/VqSkOKC6CAggGSUWTkiTDjNYpLBDpgdK1mwvVm8IPLowbGK0:20277:0:99999:7:::

[root@servera ~]# **passwd** → *changing self password (root user)*

Changing password for user root.

New password:

BAD PASSWORD: The password is shorter than 8 characters

Retype new password:

passwd: all authentication tokens updated successfully.

[root@servera ~]# head -1 /etc/shadow

root:6W.rK40QgRcODu57e$EYv84FbNqc8LG4p90tBTRwNJVW.plx7JWkmvvOcW/qVSVwvShIuhgIbhlQmkWidZA4kBXr61yCzbzrt1Evs5a.:20277:0:99999:7:::

Multiple users

Command: chpasswd

Syntax:

[root@servera ~]#**chpasswd**

<username>:<password>

<username>:<password>

<username>:<password>

Assiging password to multiple users

ctrl+d → save and exit

[root@servera ~]# **useradd user1; useradd user2;useradd user3**

[root@servera ~]# **tail -3 /etc/passwd**

user1:x:1003:1003::/home/user1:/bin/bash

user2:x:1004:1004::/home/user2:/bin/bash

user3:x:1005:1005::/home/user3:/bin/bash

[root@servera ~]# **tail -3 /etc/shadow**

user1:!!:20277:0:99999:7:::

user2:!!:20277:0:99999:7:::

user3:!!:20277:0:99999:7:::

[root@servera ~]# **chpasswd**

user1:redhat

user2:redhat@123

user3:redhat@123

ctrl+d

[root@servera ~]# **tail -3 /etc/shadow**

user1:6mVwsOAkVUPprfawj$QPmfGMmWbNY6ntuNS5WrbHKcyTRmZN7E2SEiyhC9o405Pndu5f6VL/K46Ow54EHgc9GHdIksiHLmv5aisvuBz/:20277:0:99999:7:::

user2:6.q45eQTI3kH/58FI$KCkKMLro8Ry9IE.CyVbQz0k7qwsfe2/.XK5HSnp8AxolbjjdjCSLMoipiH4/uDOLQveL7zM5TCA0KULT36SwJ1:20277:0:99999:7:::

user3:6p1OxFDAH2t9dC8my$YcNer5Udy1Deqw/YnYH.aEiqgBcJguaI365rw6IMIGFa/Ifb1WaPwz0DHHz5UUmrncaLHmIBby3.HwLRdR72j1:20277:0:99999:7:::