2 User and Group Management

```
====================================================
Introduction to Linux User and Group Management
****************************************************
********
```

Linux user and group management
```
====================
```

Lab
```
`````
```
Understanding the command genet

## Listing users and service
```
====================
```

```
[root@server1 ~]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash

ntp:x:38:38::/etc/ntp:/sbin/nologin
chrony:x:997:995::/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
mivaan:x:1000:1000:mivaan:/home/mivaan:/bin/bash
gluster:x:996:994:GlusterFS daemons:/run/gluster:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd
daemon:/dev/null:/sbin/nologin
hacluster:x:189:189:cluster user:/home/hacluster:/sbin/nologin
unbound:x:995:991:Unbound DNS resolver:/etc/unbound:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
sanjeev:x:1001:1001::/home/sanjeev:/bin/bash
maximus:x:1002:1002::/home/maximus:/bin/bash
```

```
[root@server1 ~]# getent  passwd
root:x:0:0:root:/root:/bin/bash


[root@server1 ~]# grep passwd /etc/nsswitch.conf
      // password database
#passwd:   db files nisplus nis
passwd:    files sss



[root@server1 ~]# getent  group
root:x:0:

[root@server1 ~]# getent networks
default           0.0.0.0
loopback          127.0.0.0
link-local        169.254.0.0


[root@server1 ~]# getent services
```

===
=====
Managing Login Scripts
****
****

Login Scripts
====================

Objectives
`````````

Manage system-wide environment profiles
Manage templets user environment

LAB
````

Login shells and non-login shells
System login shells
Using login scripts and /etc/skel

## Login shell
``````````

/etc/profile   ~/.bash_profile

~/.bashrc   /etc/bashrc

Non - Login shell
```````````````

~/.bashrc                        /etc/bashrc

## Investigating the execution order
==================

```
[student@server1 ~]$ pwd
/home/student


[student@server1 ~]$ su -l
Password:
Last login: Sun Aug  9 10:48:33 +0545 2020 from 192.168.1.68 on pts/0
[root@server1 ~]#


[root@server1 ~]# pwd
/root


[root@server1 ~]# echo $USER
root

[root@server1 ~]# id
uid=0(root) gid=0(root) groups=0(root)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023


[root@server1 ~]# exit
logout


[student@server1 ~]$ su
                                            // root on student dir
Password:
[root@server1 student]# pwd
/home/student
[root@server1 student]#

[root@server1 student]# echo $USER
student


[root@server1 ~]# vim .bashrc
            echo "from bash"
```

```
[root@server1 ~]# vim /etc/bash_profile
echo "profile"
```

```
[root@server1 ~]# su
from bash
```

```
[root@server1 ~]# su - root
Last login: Sun Aug  9 17:06:02 +0545 2020 on pts/0
from bash
```

Note
``````

Delete both edit from .bashrc and bash_profile tooo

## System login scripts
===================

```
[root@server1 ~]# ls /etc/profile*
/etc/profile
```

**/etc/profile.d:**
```
256term.csh          colorgrep.csh  csh.local  less.sh   vim.csh
256term.sh           colorgrep.sh   lang.csh   mc.csh    vim.sh
```

abrt-console-notification.sh  colorls.csh    lang.sh    mc.sh    which2.csh
bash_completion.sh            colorls.sh    less.csh   sh.local  which2.sh

[root@server1 ~]# ls /etc/bash*
/etc/bash_profile  /etc/bashrc

**/etc/bash_completion.d:**
gluster  iprutils  redefine_filedir  scl.bash  yum-utils.bash

Lets check this example

[root@server1 ~]# echo $PS1
[\u@\h \W]\$

[root@server1 ~]# cd /tmp/
[root@server1 tmp]# ls

[root@server1 tmp]# cd /var/tmp/
[root@server1 tmp]# ls

[root@server1 ~]# vim /etc/bashrc
  [ "$PS1" = "\\s-\\v\\\$ " ] && PS1="[\u@\h \W]\\$ "
Change as

  [ "$PS1" = "\\s-\\v\\\$ " ] && PS1="[\u@\h \w]\\$ "

[root@server1 ~]# cd /var/tmp/
[root@server1 **/var/tmp**]#

**Home directory templets**
===================


[root@server1 ~]# cd /etc/skel/
[root@server1 /etc/skel]#



[root@server1 /etc/skel]# ls -la
total 24
drwxr-xr-x.  2 root root   62 Apr 11  2018 .
drwxr-xr-x. 99 root root 8192 Aug  9 17:15 ..
-rw-r--r--.  1 root root   18 Apr 11  2018 .bash_logout
-rw-r--r--.  1 root root  193 Apr 11  2018 .bash_profile
-rw-r--r--.  1 root root  231 Apr 11  2018 .bashrc



[root@server1 /etc/skel]# ls -a
.  ..  .bash_logout  .bash_profile  .bashrc

[root@server1 /etc/skel]# ls -A
.bash_logout  .bash_profile  .bashrc



[root@server1 /etc/skel]# cat .bash_logout
# ~/.bash_logout


[root@server1 /etc/skel]# cat .bash_profile

[root@server1 /etc/skel]# cat .bashrc

```
[root@server1 /etc/skel]# echo $PATH
/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin
```

```
[root@server1 /etc/skel]# cat .bashrc
if [ –f /etc/bashrc ]; then
      . /etc/bashrc
fi
```

To

```
# Source global definitions
if [ –f /etc/bashrc ]; then
      source /etc/bashrc
fi
```

```
[root@server1 /etc/skel]# cat .bash_profile
if [ –f ~/.bashrc ]; then
      . ~/.bashrc
fi
```

To

```
if [ –f ~/.bashrc ]; then
      source ~/.bashrc
fi
```

==================================================================

# Creating and Managing Local Users

*********************************************************************

**Introducing accounts and the id command**
=============================

Objectives
` ` ` ` ` ` ` ` ` `

Create, delete, and modify local user accounts

LAB
` ` ` `

Linux user identification
Create local users
Manage user passwords
Working with user defaults
Modify and delete user accounts

User identification
` ` ` ` ` ` ` ` ` ` ` ` ` `

[student@server1 ~]$ id                                    //login from
normal user:student
uid=**1003**(student) gid=**1003**(student) groups=1003(student)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023

[student@server1 ~]$ id root
uid=0(root) gid=0(root) groups=0(root)

**1 st user and group starts from 1000**

[student@server1 ~]$ id -g                          //primary group id
1003

[student@server1 ~]$ id -G                          // secondary group id

1003

[student@server1 ~]$ id –Gn
student

## Creating User Command
====================

**User account may be local or domain based accounts.**

Local account
` ` ` ` ` ` ` ` ` ` ` `

[root@server1 ~]# useradd -m user1

[root@server1 ~]# tail –n 1 /etc/passwd
user1:x:1004:1004::/home/user1:/bin/bash

[root@server1 ~]# ls /home/
maximus  mivaan  sanjeev  student  **user1**

[root@server1 ~]# ls –a /home/user1/
.  ..  .bash_logout  .bash_profile  .bashrc

[root@server1 ~]# useradd –N user2 –g users –G adm
[root@server1 ~]# !t
tail –n 1 /etc/passwd

```
user2:x:1005:100::/home/user2:/bin/bash


[root@server1 ~]# ls /home/
maximus  mivaan  sanjeev  student  user1  user2




[root@server1 ~]# useradd  user3 -G adm -s /bin/sh
[root@server1 ~]# !t
tail -n 1 /etc/passwd
user3:x:1006:1006::/home/user3:/bin/sh




[root@server1 ~]# ls -l /sbin/adduser
lrwxrwxrwx. 1 root root 7 Aug  6 17:16 /sbin/adduser -> useradd
```

**Managing User Passwords**
====================


```
[root@server1 ~]# passwd user1
Changing password for user user1.
New password:
BAD PASSWORD: The password is shorter than 7 characters
Retype new password:
passwd: all authentication tokens updated successfully
```

```
[root@server1 ~]# grep user1 /etc/shadow
user1:$6$XA/
pQtyv$rZPpvkJKidkyDwFPu3j1TPqFh9XoOjXUwI9rLUhhI1wJSQTHt6tDe27
Z0AhGo6xZ39jNwRAH4nXAefvtSucN6/:18483:0:99999:7:::
                    // by default sha512 also


[root@server1 ~]# grep user. /etc/shadow
rpcuser:!!:18480::::::
user1:$6$XA/
pQtyv$rZPpvkJKidkyDwFPu3j1TPqFh9XoOjXUwI9rLUhhI1wJSQTHt6tDe27Z0Ah
Go6xZ39jNwRAH4nXAefvtSucN6/:18483:0:99999:7:::       /password set
user2:!!:18483:0:99999:7:::                                         // no
password set, password change after this days 18483
user3:!!:18483:0:99999:7:::                                         // no
password set


[root@server1 ~]# echo 'user2:Password1' | chpasswd
                        // sending Password1 for user2 using chpasswd


[root@server1 ~]# grep user2 /etc/shadow
user2:$6$a4yjy/aOVUs/$Sz7i7tvIUbaab.Mfn2S28QVdk5PzcSEFUMN/
vEQpW0k9ph/jA4n1/o63E/
TUBgmx7qQsbE3GyfeCpPNdI0.mf1:18483:0:99999:7:::


[root@server1 ~]# echo Password1 | passwd user3 --stdin
Changing password for user user3.
passwd: all authentication tokens updated successfully.


[root@server1 ~]# grep user3 /etc/shadow
user3:$6$m8Fkujl1$QflFXNbaFOqvYTSLHjnfqdqdYoFaf85.pHBWwt1.Qi82kVxP
HAKflY1dq5SyZue36mwGcy.BTc3lcIqALS29S/:18483:0:99999:7:::
```

```
[root@server1 ~]# grep user. /etc/shadow
rpcuser:!!:18480::::::
user1:$6$XA/
pQtyv$rZPpvkJKidkyDwFPu3j1TPqFh9XoOjXUwI9rLUhhI1wJSQTHt6tDe27Z0Ah
Go6xZ39jNwRAH4nXAefvtSucN6/:18483:0:99999:7:::
user2:$6$a4yjy/aOVUs/$Sz7i7tvIUbaab.Mfn2S28QVdk5PzcSEFUMN/
vEQpW0k9ph/jA4n1/o63E/
TUBgmx7qQsbE3GyfeCpPNdI0.mf1:18483:0:99999:7:::
user3:$6$m8FkujI1$QflFXNbaFOqvYTSLHjnfqdqdYoFaf85.pHBWwt1.Qi82kVxP
HAKflY1dq5SyZue36mwGcy.BTc3lcIqALS29S/:18483:0:99999:7:::
```

**Password age data**

==================

```
[root@server1 ~]# chage -l student
Last password change                          : Aug 09, 2020
Password expires                              : never
Password inactive                             : never
Account expires                               : never
Minimum number of days between password change        : 0
Maximum number of days between password change        : 99999
Number of days of warning before password expires    : 7



[root@server1 ~]# chage -l user1
```

```
Last password change                        : Aug 09, 2020
Password expires                            : never
Password inactive                           : never
Account expires                             : never
Minimum number of days between password change     : 0
Maximum number of days between password change     : 99999
Number of days of warning before password expires  : 7
```

```
[root@server1 ~]# grep user1 /etc/passwd
user1:x:1004:1004::/home/user1:/bin/bash            // second field X means ,
password in shadow data
```

```
[root@server1 ~]# pwunconv                                         //
convert password from shadow file
[root@server1 ~]# grep user1 /etc/passwd
user1:$6$XA/
pQtyv$rZPpvkJKidkyDwFPu3j1TPqFh9XoOjXUwI9rLUhhI1wJSQTHt6tDe27
Z0AhGo6xZ39jNwRAH4nXAefvtSucN6/:1004:1004::/home/user1:/bin/bash
```

```
[root@server1 ~]# pwconv
[root@server1 ~]# grep user1 /etc/passwd
user1:x:1004:1004::/home/user1:/bin/bash
```

```
[root@server1 ~]# chage -M 40 user1

[root@server1 ~]# chage -l user1
Last password change                        : Aug 09, 2020
Password expires                            : Sep 18, 2020
Password inactive                           : never
Account expires                             : never
Minimum number of days between password change     : 0
Maximum number of days between password change     : 40
Number of days of warning before password expires  : 7
```

```
[root@server1 ~]# grep user1 /etc/shadow
user1:$6$XA/
pQtyv$rZPpvkJKidkyDwFPu3j1TPqFh9XoOjXUwI9rLUhhI1wJSQTHt6tDe27Z0Ah
Go6xZ39jNwRAH4nXAefvtSucN6/:18483:0:40:7:::
```

```
[root@server1 ~]# passwd -l user1                                        //
locking user
Locking password for user user1.
passwd: Success
```

```
[root@server1 ~]# grep user1 /etc/shadow
user1:!!$6$XA/
pQtyv$rZPpvkJKidkyDwFPu3j1TPqFh9XoOjXUwI9rLUhhI1wJSQTHt6tDe27Z0Ah
Go6xZ39jNwRAH4nXAefvtSucN6/:18483:0:40:7:::
```

```
[root@server1 ~]# passwd -u user1
Unlocking password for user user1.
passwd: Success
```

```
user1:$6$XA/
pQtyv$rZPpvkJKidkyDwFPu3j1TPqFh9XoOjXUwI9rLUhhI1wJSQTHt6tDe27Z0Ah
Go6xZ39jNwRAH4nXAefvtSucN6/:18483:0:40:7:::              // no !! Sign
```

**Account Defaults**
====================

```
[user1@server1 ~]$ less /etc/login.defs
```

```
[root@server1 ~]# useradd -D
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes




[root@server1 ~]# useradd -Ds /bin/sh

[root@server1 ~]# useradd -D
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/sh
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes




[root@server1 ~]# cat /etc/default/useradd
# useradd defaults file
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/sh
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes




[root@server1 ~]# vim /etc/default/useradd

SHELL=/bin/sh
```

Change to

SHELL=/bin/bash

## Modify and delete accounts
====================

```
[root@server1 ~]# su - student                          //manage sudores
file

[student@server1 ~]$ sudo usermod -c "user one"  user1

[student@server1 ~]$ grep user1 /etc/passwd
user1:x:1004:1004:user one:/home/user1:/bin/bash



[student@server1 ~]$ chsh -l
/bin/sh
/bin/bash
/sbin/nologin
/usr/bin/sh
/usr/bin/bash
/usr/sbin/nologin
/bin/tcsh
/bin/csh
```

```
[student@server1 ~]$ sudo chsh -s /bin/sh user2
Changing shell for user2.
Shell changed.

[student@server1 ~]$ grep user2 /etc/passwd
user2:x:1005:100::/home/user2:/bin/sh

[student@server1 ~]$ sudo usermod -s /bin/bash user2

[student@server1 ~]$ grep user2 /etc/passwd
user2:x:1005:100::/home/user2:/bin/bash
```

```
[student@server1 ~]$ ls /home/
maximus  mivaan  sanjeev  student  user1  user2  user3


[student@server1 ~]$ sudo userdel -r user2
      //-r deletes home dir as well as corncobs and mails of user acc

[student@server1 ~]$ ls /home/
maximus  mivaan  sanjeev  student  user1  user3


[student@server1 ~]$ sudo userdel user3
[student@server1 ~]$ ls /home/
maximus  mivaan  sanjeev  student  user1  user3


[student@server1 ~]$ sudo find /home/ -uid 1003 -delete
[student@server1 ~]$ ls /home/
```

===================================================================
=====

## Managing Local Groups

```
***************************************************************
********
```

**Creating local Groups**
```
===================
```

Objectives
```
```````````
```

Create, delete  and modify local groups and group membership
Configure set-GID directories for collaboration

LAB
```
`````
```

Create local group
Modify group membership
Set GID permission on directory
Group password

Creating groups
```
```````````
```

[student@server1 ~]$ grep student /etc/group
**student**:x:1005:

[student@server1 ~]$ id
uid=1005(student) gid=1005(student) groups=1005(student)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023

[student@server1 ~]$ sudo newgrp user1

[student@server1 ~]$ id

uid=1005(student) gid=1005(student) groups=1005(student)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023

```
[student@server1 ~]$ sudo newgrp user1
[
root@server1 /home/student]# pwd
/home/student

[root@server1 /home/student]# touch file1

[root@server1 /home/student]# ls -l file1
-rw-r--r--. 1 root user1 0 Aug  9 18:45 file1

[root@server1 /home/student]#

[root@server1 /home/student]# exit
exit

[student@server1 ~]$ touch file2

[student@server1 ~]$ ls -l file
file1  file2

[student@server1 ~]$ ls -l file*
-rw-r--r--. 1 root    user1   0 Aug  9 18:45 file1
-rw-rw-r--. 1 student student 0 Aug  9 18:45 file2
```

```
[student@server1 ~]$ sudo groupadd sales

[student@server1 ~]$ grep sales /etc/group
sales:x:1006:
```

```
[student@server1 ~]$ sudo grep sales /etc/gshadow
sales:!::                                        //invalid group
password
```

**Manage Group Membership**
====================

```
[student@server1 ~]$ id –Gn
student
```



```
[student@server1 ~]$ id –gn
student
```

```
[student@server1 ~]$ sudo usermod –G sales,sanjeev student
```

**Making the use of SGID Permission**
====================

**Group Password**
====================

**Abc**
====================

====================================================================
=====
# Using PAM to Control User Access
********************************************************
********

**Abc**
====================

**Abc**
====================

**Abc**
====================

**Abc**
====================

**Abc**
====================

**Abc**
====================

**Abc**
==================

**Abc**
==================

=================================================================
=====
# Implementing Open LDAP Directories
*********************************************************
********

**Abc**
==================

**Abc**
==================

**Abc**
==================

**Abc**
==================

**Abc**
==================

=================================================================
=====
# Implementing Open LDAP Authentication
*********************************************************
********

**Abc**
==================

**Abc**

==================

**Abc**

==================

**Abc**

==================

**Abc**

==================

==============================================================
=====

# Implementing Kerberos Authentication

**************************************************************
********

**Abc**

==================

**Abc**

==================

**Abc**

==================

**Abc**

==================

**Abc**

==================