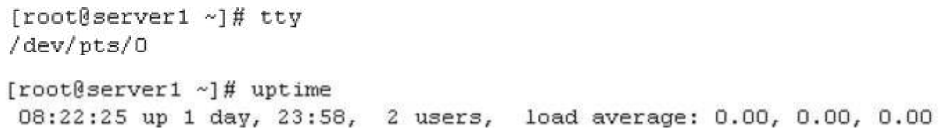
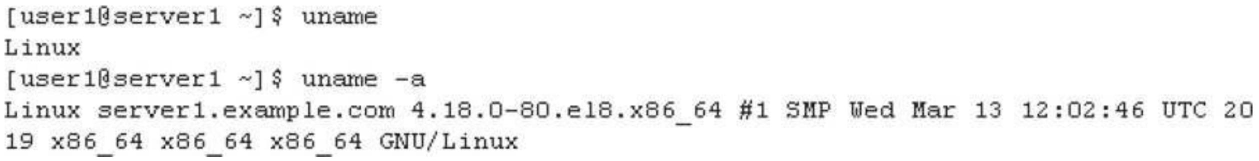
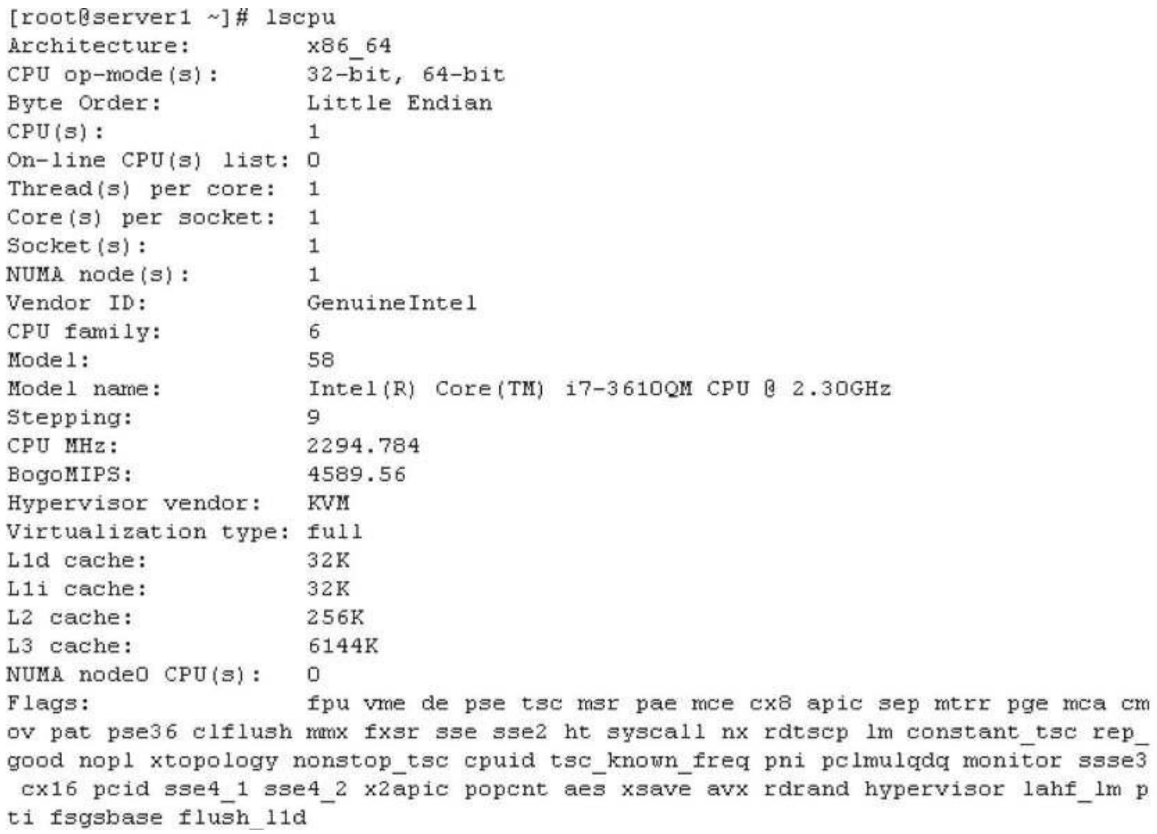
Important Linux



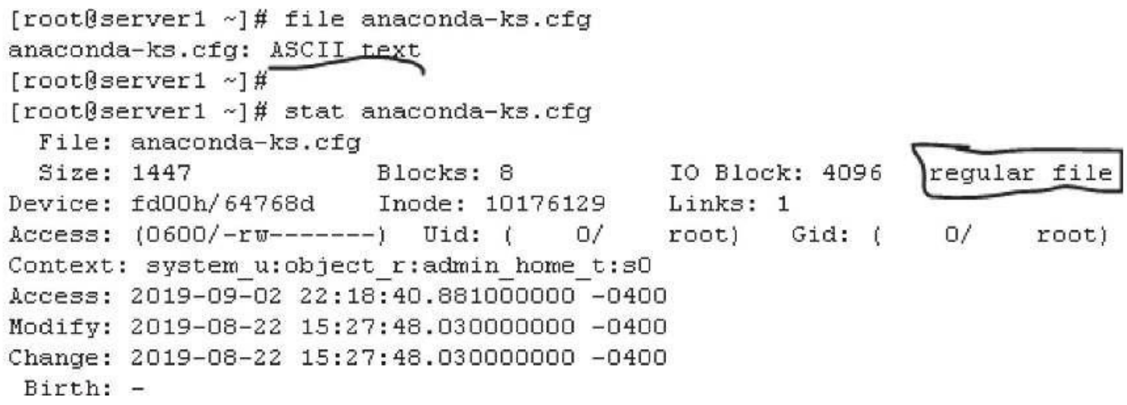
```
[root@server1 ~]# tty
/dev/pts/0
[root@server1 ~]# uptime
 08:22:25 up 1 day, 23:58,  2 users,  load average: 0.00, 0.00, 0.00
```



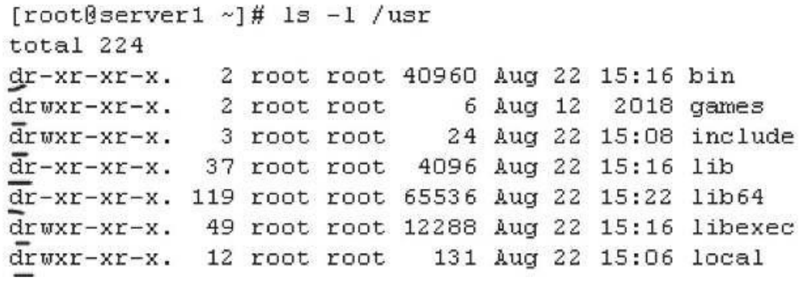
```
[user1@server1 ~]$ uname
Linux
[user1@server1 ~]$ uname -a
Linux server1.example.com 4.18.0-80.el8.x86_64 #1 SMP Wed Mar 13 12:02:46 UTC 20
19 x86_64 x86_64 x86_64 GNU/Linux
```



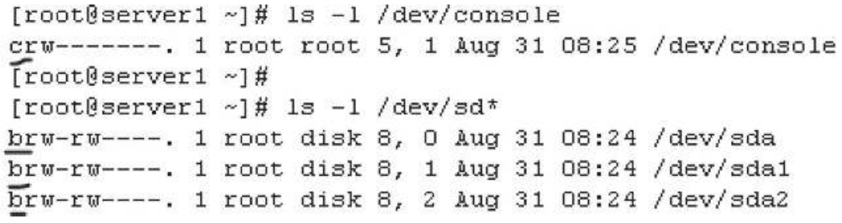
```
[root@server1 ~]# lscpu
Architecture:        x86_64
CPU op-mode(s):      32-bit, 64-bit
Byte Order:          Little Endian
CPU(s):              1
On-line CPU(s) list: 0
Thread(s) per core:  1
Core(s) per socket:  1
Socket(s):           1
NUMA node(s):        1
Vendor ID:           GenuineIntel
CPU family:          6
Model:               58
Model name:          Intel(R) Core(TM) i7-3610QM CPU @ 2.30GHz
Stepping:            9
CPU MHz:             2294.784
BogoMIPS:            4589.56
Hypervisor vendor:   KVM
Virtualization type: full
L1d cache:           32K
L1i cache:           32K
L2 cache:            256K
L3 cache:            6144K
NUMA node0 CPU(s):   0
Flags:               fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cm
ov pat pse36 clflush mmx fxsr sse sse2 ht syscall nx rdtscp lm constant_tsc rep_
good nopl xtopology nonstop_tsc cpuid tsc_known_freq pni pclmulqdq monitor ssse3
 cx16 pcid sse4_1 sse4_2 x2apic popcnt aes xsave avx rdrand hypervisor lahf_lm p
ti fsgsbase flush_l1d
```



```
[root@server1 ~]# file anaconda-ks.cfg
anaconda-ks.cfg: ASCII text
[root@server1 ~]#
[root@server1 ~]# stat anaconda-ks.cfg
  File: anaconda-ks.cfg
  Size: 1447            Blocks: 8          IO Block: 4096   regular file
Device: fd00h/64768d    Inode: 10176129    Links: 1
Access: (0600/-rw-------)  Uid: (    0/    root)   Gid: (    0/    root)
Context: system_u:object_r:admin_home_t:s0
Access: 2019-09-02 22:18:40.881000000 -0400
Modify: 2019-08-22 15:27:48.030000000 -0400
Change: 2019-08-22 15:27:48.030000000 -0400
 Birth: -
```

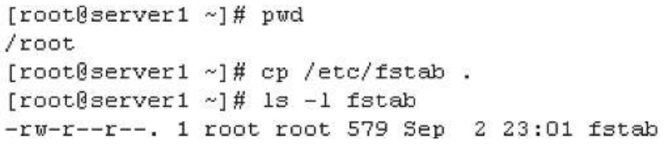


```
[root@server1 ~]# ls -l /usr
total 224
dr-xr-xr-x.   2 root root 40960 Aug 22 15:16 bin
drwxr-xr-x.   2 root root     6 Aug 12  2018 games
drwxr-xr-x.   3 root root    24 Aug 22 15:08 include
dr-xr-xr-x.  37 root root  4096 Aug 22 15:16 lib
dr-xr-xr-x. 119 root root 65536 Aug 22 15:22 lib64
drwxr-xr-x.  49 root root 12288 Aug 22 15:16 libexec
drwxr-xr-x.  12 root root   131 Aug 22 15:06 local
```

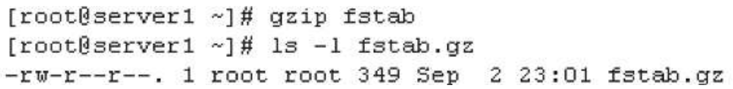


```
[root@server1 ~]# ls -l /dev/console
crw-------. 1 root root 5, 1 Aug 31 08:25 /dev/console
[root@server1 ~]#
[root@server1 ~]# ls -l /dev/sd*
brw-rw----. 1 root disk 8, 0 Aug 31 08:24 /dev/sda
brw-rw----. 1 root disk 8, 1 Aug 31 08:24 /dev/sda1
brw-rw----. 1 root disk 8, 2 Aug 31 08:24 /dev/sda2
```

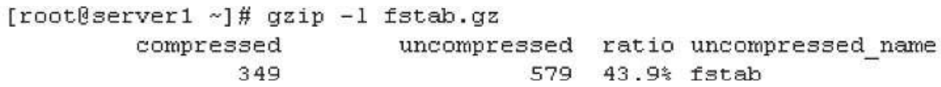
Using gzip and gunzip



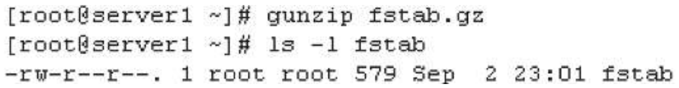
```
[root@server1 ~]# pwd
/root
[root@server1 ~]# cp /etc/fstab .
[root@server1 ~]# ls -l fstab
-rw-r--r--. 1 root root 579 Sep  2 23:01 fstab
```



```
[root@server1 ~]# gzip fstab
[root@server1 ~]# ls -l fstab.gz
-rw-r--r--. 1 root root 349 Sep  2 23:01 fstab.gz
```

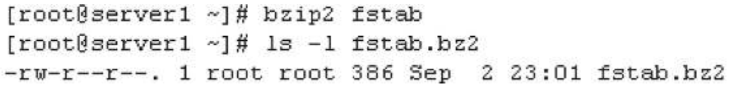


```
[root@server1 ~]# gzip -l fstab.gz
         compressed        uncompressed  ratio uncompressed_name
                349                 579  43.9% fstab
```

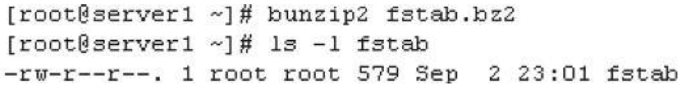


```
[root@server1 ~]# gunzip fstab.gz
[root@server1 ~]# ls -l fstab
-rw-r--r--. 1 root root 579 Sep  2 23:01 fstab
```

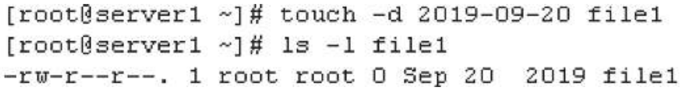
Using bzip2 and bunzip2



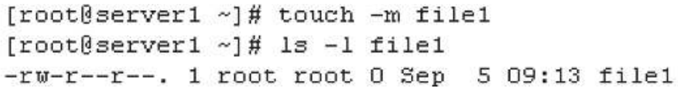
```
[root@server1 ~]# bzip2 fstab
[root@server1 ~]# ls -l fstab.bz2
-rw-r--r--. 1 root root 386 Sep  2 23:01 fstab.bz2
```



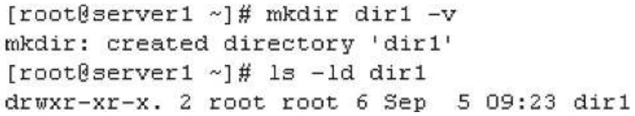
```
[root@server1 ~]# bunzip2 fstab.bz2
[root@server1 ~]# ls -l fstab
-rw-r--r--. 1 root root 579 Sep  2 23:01 fstab
```



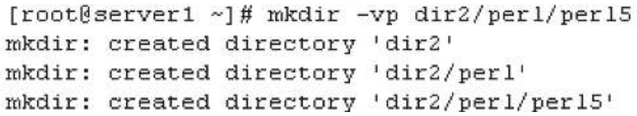
```
[root@server1 ~]# touch -d 2019-09-20 file1
[root@server1 ~]# ls -l file1
-rw-r--r--. 1 root root 0 Sep 20  2019 file1
```



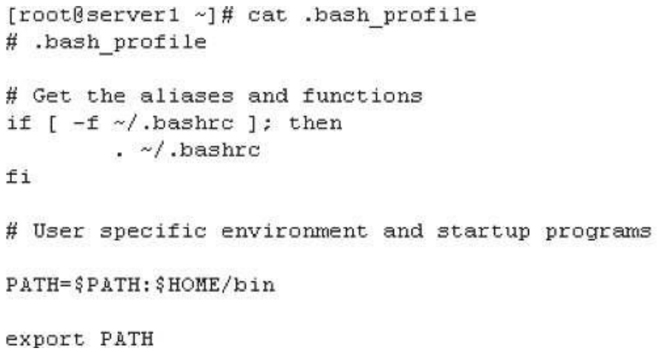
```
[root@server1 ~]# touch -m file1
[root@server1 ~]# ls -l file1
-rw-r--r--. 1 root root 0 Sep  5 09:13 file1
```



```
[root@server1 ~]# mkdir dir1 -v
mkdir: created directory 'dir1'
[root@server1 ~]# ls -ld dir1
drwxr-xr-x. 2 root root 6 Sep  5 09:23 dir1
```



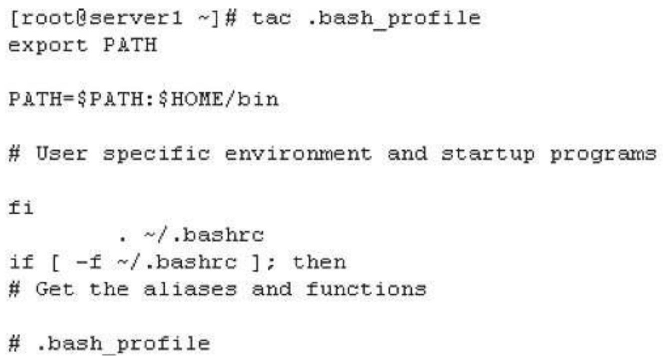
```
[root@server1 ~]# mkdir -vp dir2/perl/perl5
mkdir: created directory 'dir2'
mkdir: created directory 'dir2/perl'
mkdir: created directory 'dir2/perl/perl5'
```



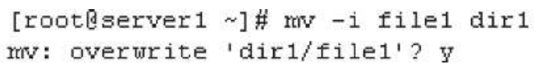
```
[root@server1 ~]# cat .bash_profile
# .bash_profile

# Get the aliases and functions
if [ -f ~/.bashrc ]; then
        . ~/.bashrc
fi

# User specific environment and startup programs

PATH=$PATH:$HOME/bin

export PATH
```

Using tac

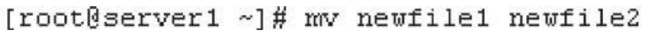
tac displays the contents of a text file in reverse. In the example below, the *.bash_profile* file in the *root* user’s home directory is displayed with the *tac* command:



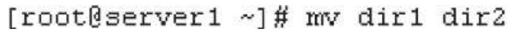
```
[root@server1 ~]# tac .bash_profile
export PATH

PATH=$PATH:$HOME/bin

# User specific environment and startup programs

fi
        . ~/.bashrc
if [ -f ~/.bashrc ]; then
# Get the aliases and functions

# .bash_profile
```



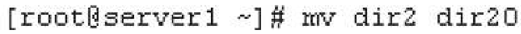
```
[root@server1 ~]# mv -i file1 dir1
mv: overwrite 'dir1/file1'? y
```



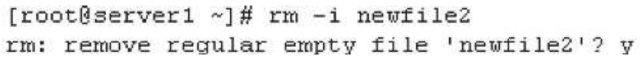
```
[root@server1 ~]# mv newfile1 newfile2
```



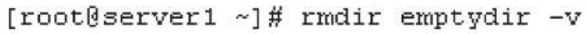
```
[root@server1 ~]# mv dir1 dir2
```



```
[root@server1 ~]# mv dir2 dir20
```

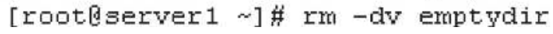


```
[root@server1 ~]# rm -i newfile2
rm: remove regular empty file 'newfile2'? y
```

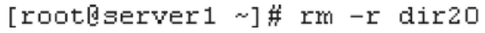


```
[root@server1 ~]# rmdir emptydir -v
```

or

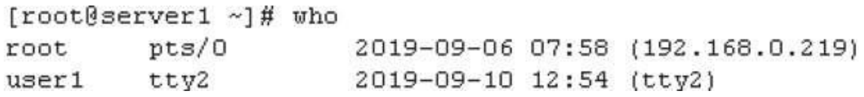


```
[root@server1 ~]# rm -dv emptydir
```

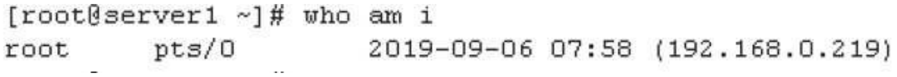


```
[root@server1 ~]# rm -r dir20
```

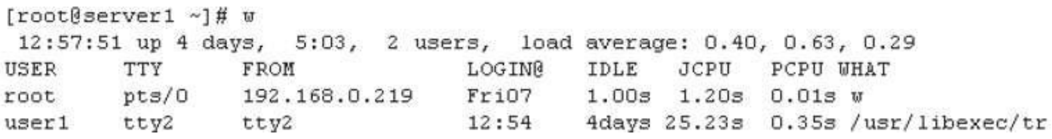
User Login Activity and Information



```
[root@server1 ~]# who
root      pts/0        2019-09-06 07:58 (192.168.0.219)
user1     tty2         2019-09-10 12:54 (tty2)
```

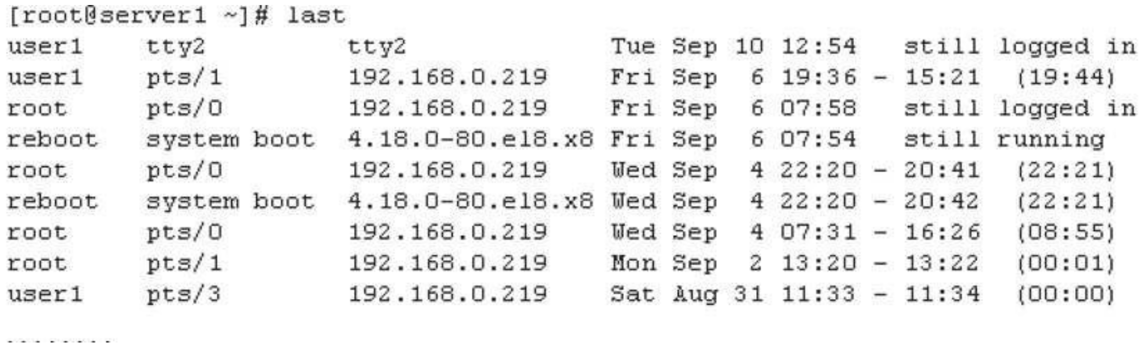


```
[root@server1 ~]# who am i
root      pts/0        2019-09-06 07:58 (192.168.0.219)
```

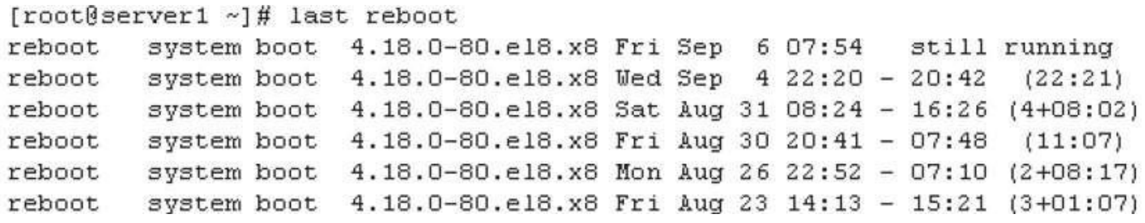


```
[root@server1 ~]# w
 12:57:51 up 4 days,  5:03,  2 users,  load average: 0.40, 0.63, 0.29
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     pts/0    192.168.0.219    Fri07    1.00s  1.20s  0.01s w
user1    tty2     tty2             12:54    4days 25.23s  0.35s /usr/libexec/tr
```

Inspecting History of Successful L Attempts and System Reboots

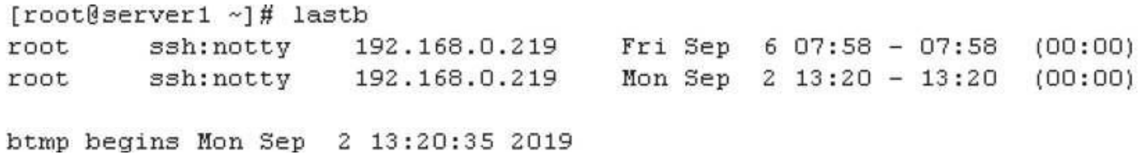


```
[root@server1 ~]# last
user1     tty2         tty2              Tue Sep 10 12:54   still logged in
user1     pts/1        192.168.0.219     Fri Sep  6 19:36 - 15:21  (19:44)
root      pts/0        192.168.0.219     Fri Sep  6 07:58   still logged in
reboot    system boot  4.18.0-80.el8.x8 Fri Sep  6 07:54   still running
root      pts/0        192.168.0.219     Wed Sep  4 22:20 - 20:41  (22:21)
reboot    system boot  4.18.0-80.el8.x8 Wed Sep  4 22:20 - 20:42  (22:21)
root      pts/0        192.168.0.219     Wed Sep  4 07:31 - 16:26  (08:55)
root      pts/1        192.168.0.219     Mon Sep  2 13:20 - 13:22  (00:01)
user1     pts/3        192.168.0.219     Sat Aug 31 11:33 - 11:34  (00:00)

........
```



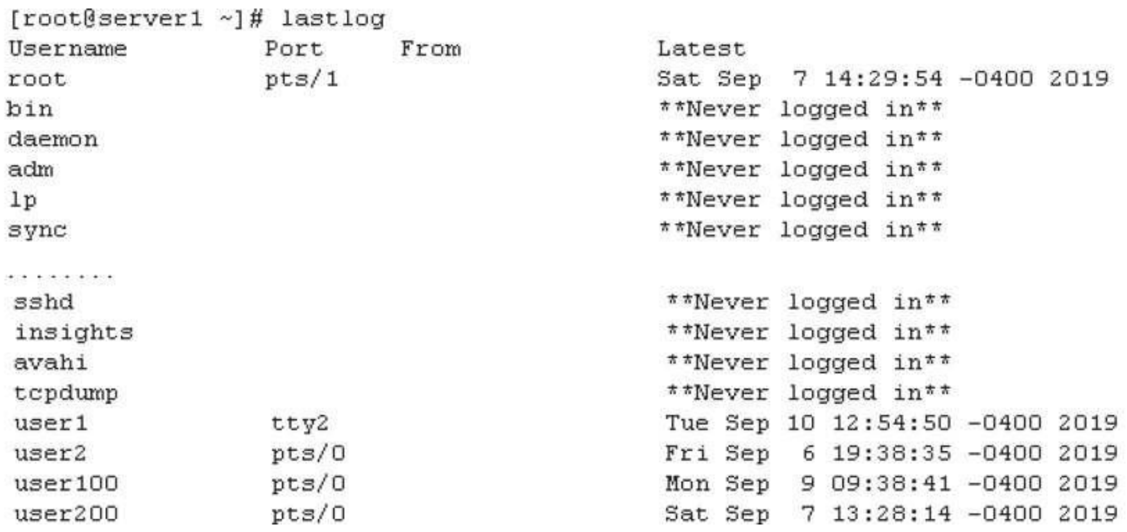
```
[root@server1 ~]# last reboot
reboot    system boot  4.18.0-80.el8.x8 Fri Sep  6 07:54   still running
reboot    system boot  4.18.0-80.el8.x8 Wed Sep  4 22:20 - 20:42   (22:21)
reboot    system boot  4.18.0-80.el8.x8 Sat Aug 31 08:24 - 16:26 (4+08:02)
reboot    system boot  4.18.0-80.el8.x8 Fri Aug 30 20:41 - 07:48   (11:07)
reboot    system boot  4.18.0-80.el8.x8 Mon Aug 26 22:52 - 07:10 (2+08:17)
reboot    system boot  4.18.0-80.el8.x8 Fri Aug 23 14:13 - 15:21 (3+01:07)
```

Viewing History of Failed User Login Attempts



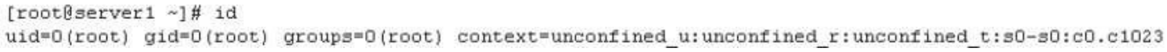
```
[root@server1 ~]# lastb
root      ssh:notty     192.168.0.219     Fri Sep  6 07:58 - 07:58  (00:00)
root      ssh:notty     192.168.0.219     Mon Sep  2 13:20 - 13:20  (00:00)

btmp begins Mon Sep  2 13:20:35 2019
```

Reporting Recent User Login Attempts

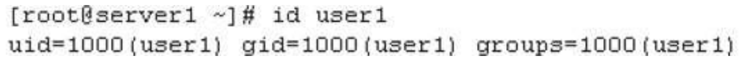


```
[root@server1 ~]# lastlog
Username         Port     From             Latest
root             pts/1                     Sat Sep  7 14:29:54 -0400 2019
bin                                        **Never logged in**
daemon                                     **Never logged in**
adm                                        **Never logged in**
lp                                         **Never logged in**
sync                                       **Never logged in**
.........
sshd                                       **Never logged in**
insights                                   **Never logged in**
avahi                                      **Never logged in**
tcpdump                                    **Never logged in**
user1            tty2                      Tue Sep 10 12:54:50 -0400 2019
user2            pts/0                     Fri Sep  6 19:38:35 -0400 2019
user100          pts/0                     Mon Sep  9 09:38:41 -0400 2019
user200          pts/0                     Sat Sep  7 13:28:14 -0400 2019
```

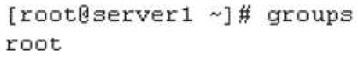
Examining User and Group Information



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

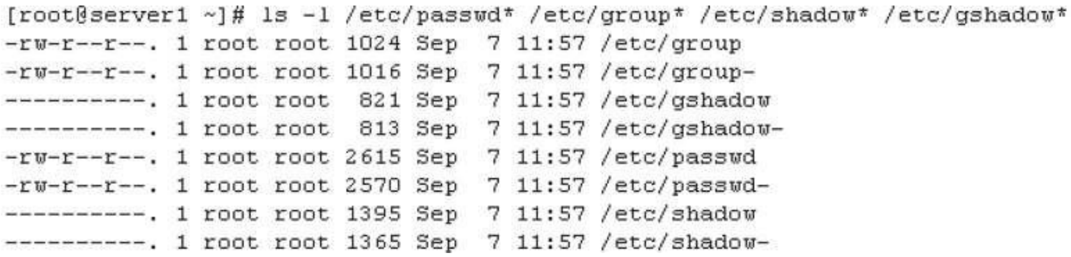


```
[root@server1 ~]# id user1
uid=1000(user1) gid=1000(user1) groups=1000(user1)
```



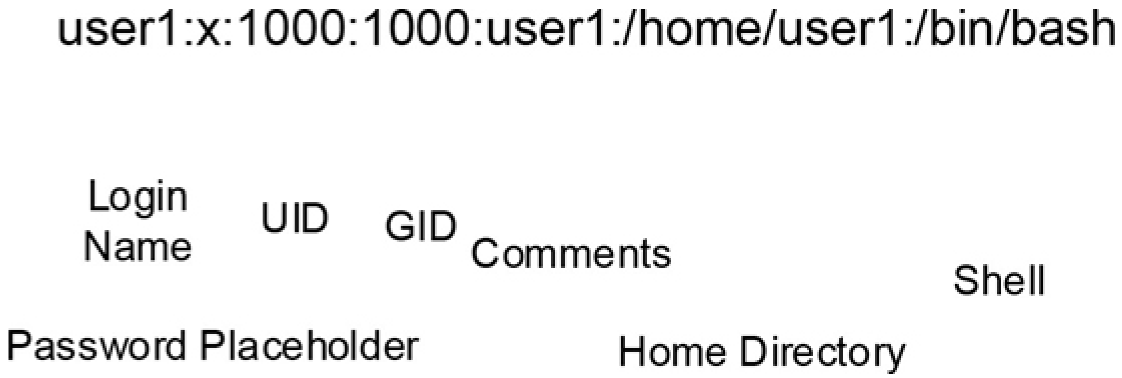
```
[root@server1 ~]# groups
root
```

Local User Authentication Files



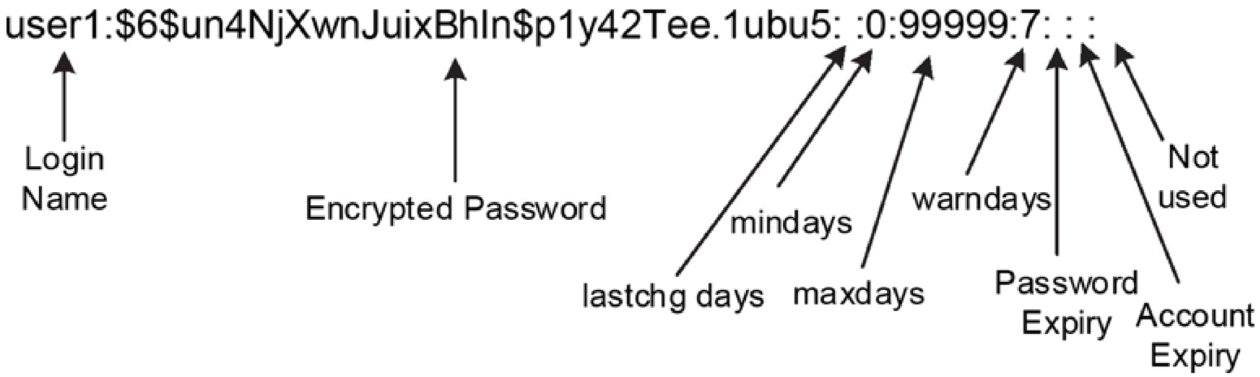
```
[root@server1 ~]# ls -l /etc/passwd* /etc/group* /etc/shadow* /etc/gshadow*
-rw-r--r--. 1 root root 1024 Sep  7 11:57 /etc/group
-rw-r--r--. 1 root root 1016 Sep  7 11:57 /etc/group-
----------. 1 root root  821 Sep  7 11:57 /etc/gshadow
----------. 1 root root  813 Sep  7 11:57 /etc/gshadow-
-rw-r--r--. 1 root root 2615 Sep  7 11:57 /etc/passwd
-rw-r--r--. 1 root root 2570 Sep  7 11:57 /etc/passwd-
----------. 1 root root 1395 Sep  7 11:57 /etc/shadow
----------. 1 root root 1365 Sep  7 11:57 /etc/shadow-
```

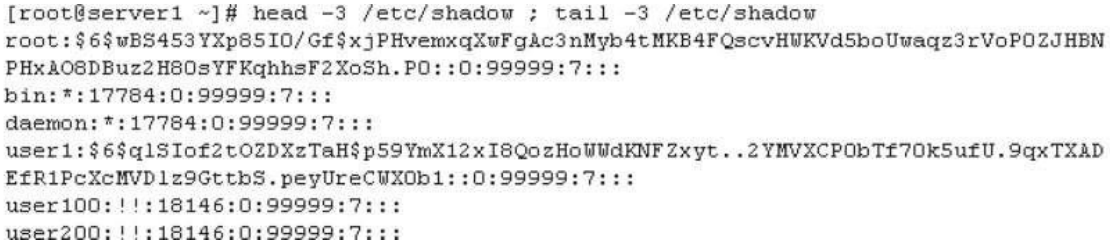
/etc/passwd



```
user1:x:1000:1000:user1:/home/user1:/bin/bash
```

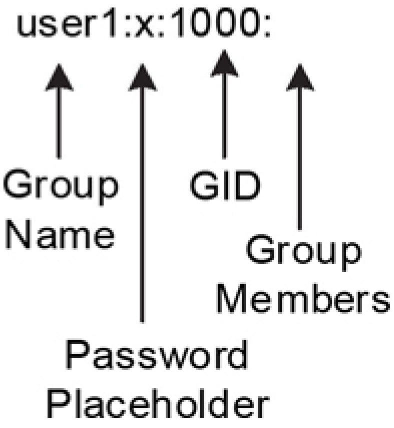
/etc/shadow

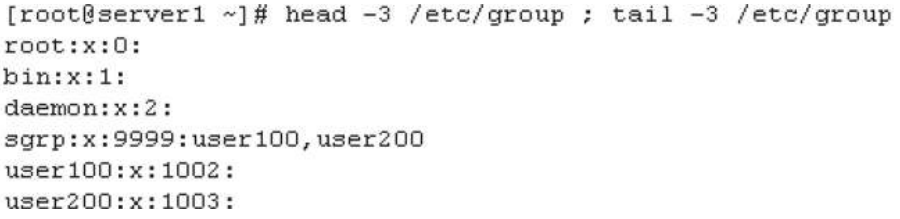




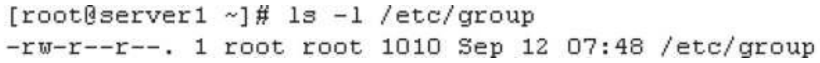
```
[root@server1 ~]# head -3 /etc/shadow ; tail -3 /etc/shadow
root:$6$wBS453YXp85IO/Gf$xjPHvemxqXwFgAc3nMyb4tMKB4FQscvHWKVd5boUwaqz3rVoPOZJHBN
PHxAO8DBuz2H8OsYFKqhhsF2XoSh.PO::0:99999:7:::
bin:*:17784:0:99999:7:::
daemon:*:17784:0:99999:7:::
user1:$6$qlSIof2tOZDXzTaH$p59YmX12xI8QozHoWWdKNFZxyt..2YMVXCPObTf7Ok5ufU.9qxTXAD
EfR1PcXcMVDlz9GttbS.peyUreCWXOb1::0:99999:7:::
user100:!!:18146:0:99999:7:::
user200:!!:18146:0:99999:7:::
```

The group File



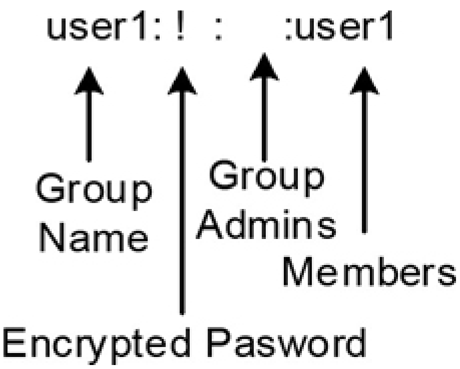


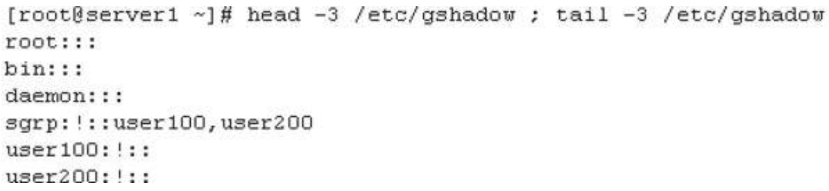
```
[root@server1 ~]# head -3 /etc/group ; tail -3 /etc/group
root:x:0:
bin:x:1:
daemon:x:2:
sgrp:x:9999:user100,user200
user100:x:1002:
user200:x:1003:
```



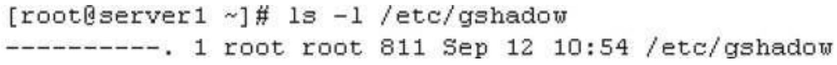
```
[root@server1 ~]# ls -l /etc/group
-rw-r--r--. 1 root root 1010 Sep 12 07:48 /etc/group
```

The gshadow File



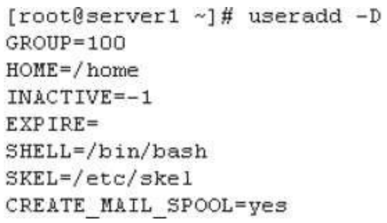


```
[root@server1 ~]# head -3 /etc/gshadow ; tail -3 /etc/gshadow
root:::
bin:::
daemon:::
sgrp:!::user100,user200
user100:!::
user200:!::
```

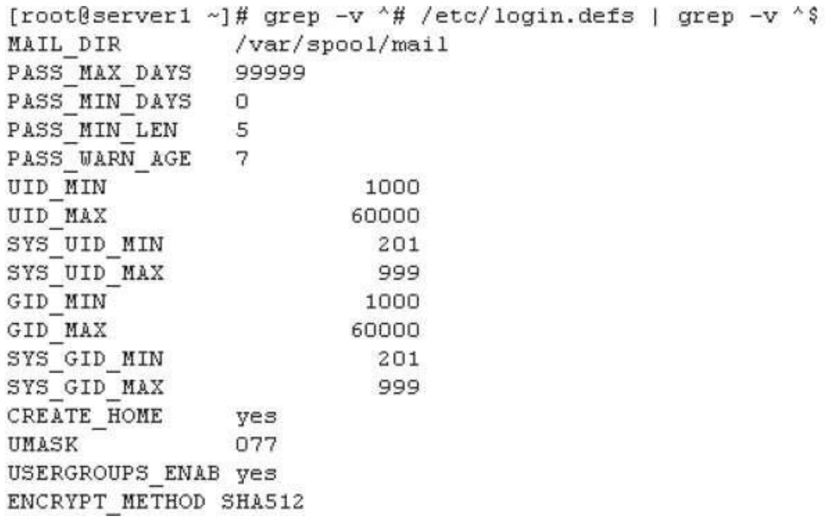


```
[root@server1 ~]# ls -l /etc/gshadow
----------. 1 root root 811 Sep 12 10:54 /etc/gshadow
```

The useradd and login.defs Configuration Files

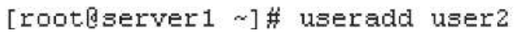


```
[root@server1 ~]# useradd -D
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes
```

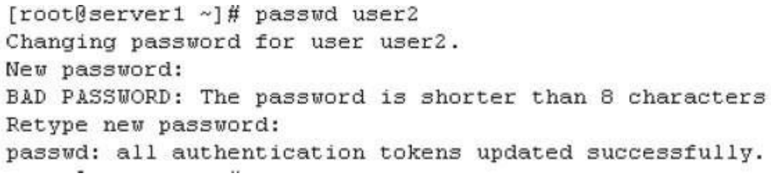


```
[root@server1 ~]# grep -v ^# /etc/login.defs | grep -v ^$
MAIL_DIR        /var/spool/mail
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_MIN_LEN    5
PASS_WARN_AGE   7
UID_MIN                  1000
UID_MAX                 60000
SYS_UID_MIN               201
SYS_UID_MAX               999
GID_MIN                  1000
GID_MAX                 60000
SYS_GID_MIN               201
SYS_GID_MAX               999
CREATE_HOME     yes
UMASK           077
USERGROUPS_ENAB yes
ENCRYPT_METHOD SHA512
```

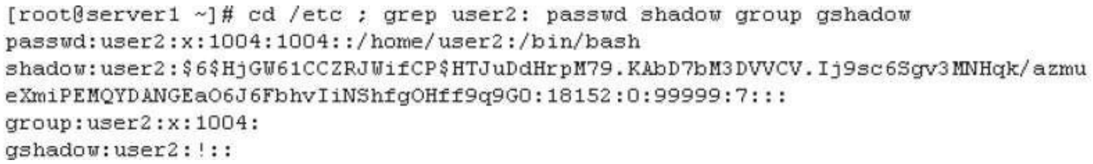
The useradd, usermod, and userdel Commands



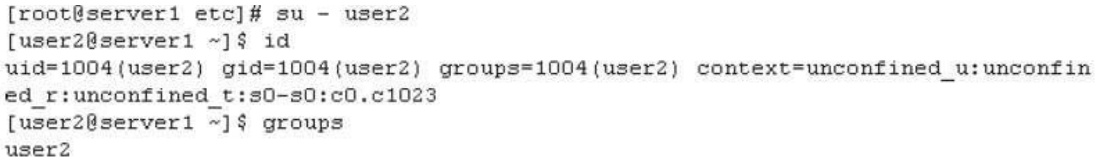
```
[root@server1 ~]# useradd user2
```



```
[root@server1 ~]# passwd user2
Changing password for user user2.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
```

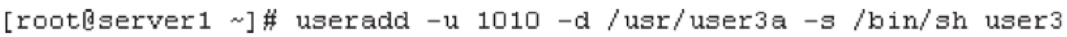


```
[root@server1 ~]# cd /etc ; grep user2: passwd shadow group gshadow
passwd:user2:x:1004:1004::/home/user2:/bin/bash
shadow:user2:$6$HjGW61CCZRJWifCP$HTJuDdHrpM79.KAbD7bM3DVVCV.Ij9sc6Sgv3MNHqk/azmu
eXmiPEMQYDANGEaO6J6FbhvIiNShfgOHff9q9G0:18152:0:99999:7:::
group:user2:x:1004:
gshadow:user2:!::
```

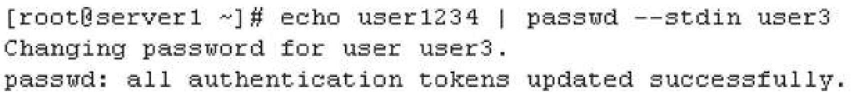


```
[root@server1 etc]# su - user2
[user2@server1 ~]$ id
uid=1004(user2) gid=1004(user2) groups=1004(user2) context=unconfined_u:unconfin
ed_r:unconfined_t:s0-s0:c0.c1023
[user2@server1 ~]$ groups
user2
```

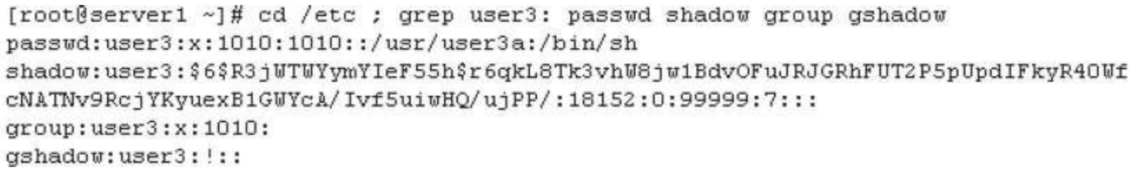
Create a User Account with Custom Values



```
[root@server1 ~]# useradd -u 1010 -d /usr/user3a -s /bin/sh user3
```

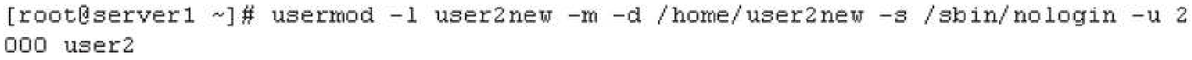


```
[root@server1 ~]# echo user1234 | passwd --stdin user3
Changing password for user user3.
passwd: all authentication tokens updated successfully.
```

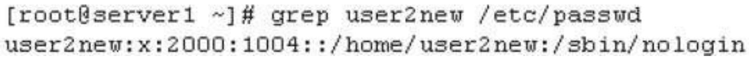


```
[root@server1 ~]# cd /etc ; grep user3: passwd shadow group gshadow
passwd:user3:x:1010:1010::/usr/user3a:/bin/sh
shadow:user3:$6$R3jWTWYymYIeF55h$r6qkL8Tk3vhW8jw1BdvOFuJRJGRhFUT2P5pUpdIFkyR4OWf
cNATNv9RcjYKyuexB1GWYcA/Ivf5uiwHQ/ujPP/:18152:0:99999:7:::
group:user3:x:1010:
gshadow:user3:!::
```

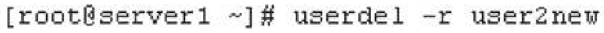
Modify and Delete a User Account



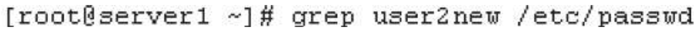
```
[root@server1 ~]# usermod -l user2new -m -d /home/user2new -s /sbin/nologin -u 2
000 user2
```



```
[root@server1 ~]# grep user2new /etc/passwd
user2new:x:2000:1004::/home/user2new:/sbin/nologin
```

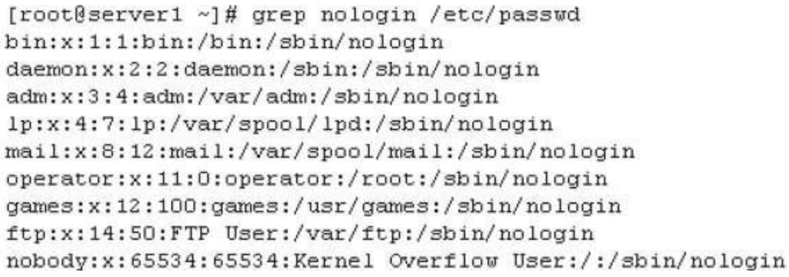


```
[root@server1 ~]# userdel -r user2new
```



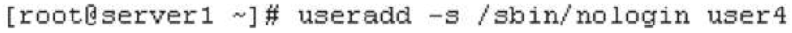
```
[root@server1 ~]# grep user2new /etc/passwd
```

No-Login (Non-Interactive) User Account

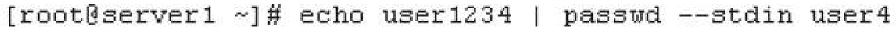


```
[root@server1 ~]# grep nologin /etc/passwd
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
```

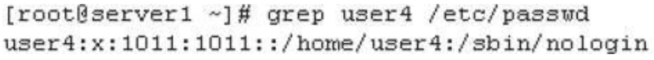
Create a User Account with No-Login Access



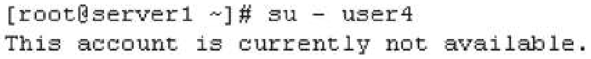
```
[root@server1 ~]# useradd -s /sbin/nologin user4
```



```
[root@server1 ~]# echo user1234 | passwd --stdin user4
```



```
[root@server1 ~]# grep user4 /etc/passwd
user4:x:1011:1011::/home/user4:/sbin/nologin
```



```
[root@server1 ~]# su - user4
This account is currently not available.
```