

251 lines (241 sloc) 11 KB

Chapter 2. Managing Users

```
root@3499a534b086:/# cat /etc/shadow | grep root
root:*:17847:0:99999:7:::
root@3499a534b086:/#
```

Understanding when to use `root`

```
apt install tmux
```

```
E: Could not open lock file /var/lib/dpkg/lock - open (13: Permission denied)
```

```
E: Unable to lock the administration directory (/var/lib/dpkg/), are you root?
```

```
sudo apt install tmux
```

Creating and removing users

```
sudo useradd -d /home/jdoe -m jdoe
```

```
ls -l /home
```

```
nano /usr/sbin/ adduser
```

```
sudo userdel dscully
```

```
ls -l /home
```

```
passwd
```

```
sudo mv /home/dscully /store/file_archive
```

```
sudo mkdir -p /store/file_archive
```

```
sudo userdel -r dscully
```

```
sudo rm -r /home/dscully
```

```
sudo rm -r / ( space ) home/dscully
```

Understanding the `/etc/passwd` & `/etc/shadow` files

```
cat /etc/passwd
```

```
sudo cat /etc/shadow
```

```
sudo cat /etc/shadow | grep root
```

```
mulder:$6$TPxx8Z.:16809:0:99999:7:::
```

```
sudo passwd -S <username>
```

```
root@u1804:/# adduser jane_doe
```

```
root@u1804:/# cat /etc/shadow | grep root
```

any password ?

```
user: * :password changed:7days between changes:max:warning:disable:8thN:9?
```

encrypted password

```
user: x :password changed:7days between changes:max:warning:disable:8thN:9?
```

lockout login

```
user: ! :password changed:7days between changes:max:warning:disable:8thN:9?
```

add a user to sudo as a secondary group

```
jane_doe@u1804:~$ sudo usermod -aG sudo jane_doe
```

switch user

```
root@u1804:/# su - jane_doe list all files in long form
```

```
jane_doe@u1804:~$ ls -al
```

add user group

```
jane_doe@u1804:~$ sudo groupadd admins
```

modify secondary group to include user

```
jane_doe@u1804:~$ sudo usermod -aG admins jane_doe
```

lock password - will not affect SSH (see ch 15)

```
jane_doe@u1804:~$ sudo passwd -l root
```

```
jane_doe@u1804:~$ sudo cat /etc/shadow | grep root
```

```
root@u1804:/# su - root
```

unlock password

```
jane_doe@u1804:~$ sudo passwd -u <username>
```

/etc/shadow

```
jane_doe@u1804:~$ sudo chage -l root
```

Distributing default configuration files with /etc/skel

```
ls -la /etc/skel
```

force password change - should move this into /etc/skel ?, for default configuration (see ch 1)

```
jane_doe@u1804:~$ sudo chage -d 0 <username>
```

...

Switching users

```
sudo passwd
```

```
sudo su -
```

```
su - <username>
```

```
sudo su - <username>
```

Pluggable Authentication Module (PAM):

```
jane_doe@u1804:~$ sudo apt install libpam-cracklib
```

...

install Nano

```
jane_doe@u1804:~$ sudo apt install nano
```

...

configure password requirements in PAM

```
jane_doe@u1804:~$ sudo nano /etc/pam.d/common-password
```

! (use a 2nd TTY to prevent lock out)

Managing groups

```
-rw-r--r-- 1 root bind 490 2013-04-15 22:05 named.conf
```

```
ls -l
```

```
groups jane_doe
```

```
cat /etc/group
```

```
sudo groupadd admins
```

```
sudo groupdel admins
```

```
sudo usermod -aG admins myuser
```

```
sudo usermod -g <group-name> <username>
```

```
man usermod
```

```
sudo usermod -d /home/jsmith jdoe -m
```

```
sudo usermod -l jsmith jdoe
```

```
sudo gpasswd -d <username> <group>
```

```
sudo gpasswd -a <username> <group>
```

add a user to sudo as a secondary group

```
jane_doe@u1804:~$ sudo usermod -aG sudo <username>
```

```
jane_doe@u1804:~$ sudo usermod -aG sudo jane_doe
```

may use another group (such as wheel)

configure sudo group or user access

```
jane_doe@u1804:~$ sudo visudo
```

checks to make sure your changes follow the correct syntax */etc/sudoers*

```
jane_doe    ALL=(ALL:ALL) ALL
```

```
charlie ubuntu-server=(jane_doe:admins) /usr/bin/apt,/usr/sbin/reboot,/usr/sbin/shutdown
```

(root or username) TTY IP=(USER:GROUP) COMMANDS

! It's always a good idea to use full paths when editing sudo command permissions

Managing passwords and password policies

lock password per <username>

```
jane_doe@u1804:~$ sudo passwd -l <username>
```

unlock password per <username>

```
jane_doe@u1804:~$ sudo passwd -u <username>
```

...

list expiration of a user's password

```
jane_doe@u1804:~$ sudo chage -l <username>
```

(set to zero would force a password change)

```
jane_doe@u1804:~$ sudo chage -d 0 <username>
```

(review changes)

```
jane_doe@u1804:~$ sudo chage -l <username>
```

expiration of a user's password (Maximum days until a change is required)

```
jane_doe@u1804:~$ sudo chage -M 90 <username>
```

expiration of a user's password (minimum days until a change is required)

```
jane_doe@u1804:~$ sudo chage -m 5 dscully
```

Pluggable Authentication Module (PAM):

```
jane_doe@u1804:~$ sudo apt install libpam-cracklib
```

...

install Nano

```
jane_doe@u1804:~$ sudo apt install nano
```

...

configure password requirements in PAM

```
jane_doe@u1804:~$ sudo nano /etc/pam.d/common-password
```

! (use a 2nd TTY to prevent lock out)

install Pluggable Authentication Module (PAM)

```
jane_doe@u1804:~$ sudo apt install libpam-cracklib
```

...

edit ..(/ etc / pam.d / common-password)

```
jane_doe@u1804:~$ sudo nano /etc/pam.d/common-password
```

password required pam_pwhistory.so remember=99 use_authok

difference (at least three characters have to be different)

difok=3

obscure (prevents simple passwords from being used)

obscure

Configuring administrator access with sudo

modify secondary Group to include user

```
jane_doe@u1804:~$ sudo usermod -aG sudo <username>
```

visudo

```
if an error return to nano edit
e
nano save changes
Ctrl + W
nano exit editor
Ctrl + X
configure visudo default Editor to vim
jane_doe@u1804:~$ sudo EDITOR=vim visudo
etc / sudoers
```

```
%sudo    ALL=(ALL:ALL) ALL
...
root     ALL=(ALL:ALL) ALL
```

TTY =(User : Group) Command
note that it's best to use full paths
charlie could run these : **commands**

```
charlie    ALL=(ALL:ALL) /usr/sbin/reboot,/usr/sbin/shutdown
```

but not others

```
Sorry, user charlie is not allowed to execute '/usr/bin/apt
install tmux' as root on ubuntu-server.
```

limited to certain terminal

```
charlie    ubuntu-server=(ALL:ALL) /usr/bin/apt
```

exclude (restrict) user & group options

```
charlie    ubuntu-server= /usr/bin/apt
```

restrict to certain (user : group)

```
charlie    ubuntu-server=(dscully:admins) ALL
```

Setting permissions on files and directories

```
-rw-rw-rw- 1 doctor doctor    5    Jan 11 12:52 welcome
-rw-r--r-- 1 root   root      665   Feb 19 2014 profile
-rwxr-xr-x 1 dalek  dalek    35125 Nov  7 2013 exterminate
-rw-r--r-- 1 sue    accounting 35125 Nov  7 2013 budget.txt
drwxr-x--- 1 bob    sales      35125 Nov  7 2013 annual_projects
```

Object type : User : Group : Other's

```
- ( file ), d (directory) or l ( link ) : rwx : rwx : rwx
```

```
ls -l
```

chmod

```

remove read from file permissions for other's
jane_doe@u1804:~$ sudo chmod o-r /home/sue/budget.txt
chmod o-r budget.txt
chmod o-r /home/sue/budget.txt
chmod 770 -R mydir
find /path/to/dir/ -type f -exec chmod 644 {} ;
find /path/to/dir/ -type d -exec chmod 755 {} ;
sudo chown sue myfile.txt
sudo chown -R sue mydir
sudo chown sue:sales myfile.txt
sudo chgrp sales myfile.txt

```

change ownership of directory recursively

```
jane_doe@u1804:~$ sudo chown -R jane_doe:admins dir_name
```

change group ownership

```
jane_doe@u1804:~$ sudo chgrp sales myfile.txt
```

octal permission patterns

```

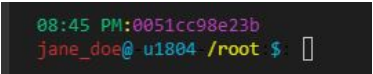
Read: 4
Write: 2
Execute: 1
$ chmod 600 filename.txt (same as) chmod -rw----- filename.txt
$ chmod 740 filename.txt (same as) chmod -rwxr----- filename.txt
$ chmod 770 filename.txt (same as) chmod -rwxrwx--- filename.txt
$ chmod 770 -R dir_name (recursive directories)

```

Q&A

1. \$ sudo
2. \$ adduser, useradd
3. \$ rm jane_doe
4. \$ /etc/passwd & /etc/shadow
5. \$ /etc/skel
6. \$ su jane_doe
7. \$ sudo groupadd accounting
8. \$ visudo
9. \$ sudo adduser jdoe
10. \$ chmod, chown

customize TTY prompt



```
08:45 PM:0051cc98e23b
jane_doe@ u1804 /root $: 
```

```

root@u1804:/# echo 'export PS1="\u@\h \w]\$ "' >> ~/.bash_profile
root@u1804:/# nano ~/.bash_profile
jane_doe@0051cc98e23b:~$ nano .bashrc
root@u1804:/# nano etc/skel.bashrc

```

```

function nonzero_return() {
    RETVAL=$?
    [ $RETVAL -ne 0 ] && echo "$RETVAL"
}

```

```

PS1='${debian_chroot:+($debian_chroot)}\n[\e[31m]\`nonzero_return\`[\e[m]\[\e[33m]:\[\e[m]\[\e[32;40m]\@\[\e[m]\[\e[33m]:\[\e[m]\[\e[35;40m]\H\[\e[m]\n\[\e[31m]\u\[\e[m]\[\e[36m]\@\[\e[m]\[\e[30m]\-\[\e[m]\[\e[36m]u1804\[\e[m]\[\e[30m]\-\[\e[m]\[\e[33;40m]\w\[\e[m]\[\e[30m]:\[\e[m]\[\e[36m]\$\[\e[m]\[\e[30m]:\[\e[m] '

```

```

PS1='${debian_chroot:+($debian_chroot)}\n[\e[32;40m]\@\[\e[m]\[\e[33m]:\[\e[m]\[\e[35;40m]\H\[\e[m]\n\[\e[31m]\u\[\e[m]\[\e[36m]\@\[\e[m]\[\e[30m]\-\[\e[m]\[\e[36m]u1804\[\e[m]\[\e[30m]\-\[\e[m]\[\e[33;40m]\w\[\e[m]\[\e[30m]:\[\e[m]\[\e[36m]\$\[\e[m]\[\e[30m]:\[\e[m] '

```