$grep - To find the text in file

$cp /etc/passwd passwd

$pwd

$ls -la

$grep <word-to-find> <FileName>

Linux is case senstive.

$grep -i <word-to-find> <FileName> - For case insenstive

**Pipeing: |**

Pipe is output of first cmd becoming input of next cmd

$head - for first 10 lines of the file

$tail - for last 10 lines of the file

$head -n 2 <filename> - for first 2 lines

$tail -n 2 <filename> - for last 2 lines

$cat <filename> | grep -n 2

**$wget - webget - to get download app link from web**

**$wget <url>**

**$curl <url> - it’s given text of terminal. it won’t download**

$cut - to cut the string baced on some delimiter

$echo <string> | cut -d <delimiter ex-/ :> -f 1

$echo <string> | cut -d <delimiter ex-/ :> -f 2

$awk -

$awk -F "/" '{print $1F}'

$awk -F "/" '{print $NF}'

**Difference between $cut and $awk?**

we can use both for the delimitation purpose. we can choose any delimiter to cut the text.

But $awk has another usage. i.e. column based.

**Editors:**

$vim (Visually Improved)

$vim <filename> - If the file doesn't exist, it will create and open. Its file is there, I will open the file.

**Esc Mode**

**Insert Mode**

when open a file by default it’s in ESC Mode

**Esc mode options:**

press i to go insert mode

press u in insert mode is undo

press yy - yank/copy the line

press p - it will paste and press 10p for paste 10 times

press dd - to cut the line

press gg - want to go top of the file

shift+g takes us to bottom

shift+: - to go column Mode:

:/<word-to-find> - It will search for the word from top. search hit bottom, continue at

:?<word-to-find> - it will search for the word from bottom

:set nu - Numbers will display/highlight

:set nonu - numbers don’t display/unhighlight

:noh - it will unhighlight the previous searched word (no highlight)

:q - quit the file or come out of the file. not saving

:q! - quit without saving

:wq - save the changes and quit

:s/<word-to-find>/<replace with another word> It will only substitute only where the cursor placed

:2ss/<word-to-find>/<replace with another word> - it will substitute a particular line word

:%s/<word-to-find>/<replace with another word>/g - replace entire file

**Permissions:**

R - Read

W - Write

X - Execute

when create user in Linux, by default a group also created on the same name of user.

$chmod u+x <filename> - Provide execute access to user

$chmod u-x <filename> - remove execute access to user

$chmod +x <filename> - to give execute access to all user, groups and others

$chmod -x <filename> - to remove execute access for all users, groups and others

**u - user**

**g - Group**

**o - others**

For changing file permissions, u should be either owner of the file or root user

**R - 4**

**W - 2**

**X - 1**

$chmod 700 - all access to user, no access to group, no access to others

$chmod 750 - all access to users, read/execute access to group, no access to others

**Public key and Private key inside the Linux will not have more than 600.**

**600 means read/write access to user, no access to group and no access to others.**

**Because the key file belongs to only you. Nobody else can read. other users can’t read your public key.**

**User Management:**

$ useradd <username> - For creating user

Linux will start creating users from 1000, Below 1000 those are system users.

/etc/passwd - for users’ info

$ getent passwd

$ passwd <username> - For creating password for user

For User login to system:

Linux disable password authentication. How to enable password authentication?

/etc/ssh/sshd\_config

sshd\_config is a crucial file. you should not do mistake here

should take backup before do changes in sshd\_config

edit the file /etc/ssh/sshd\_config

search for password /password

change No to Yes for authentication and save It

sshd -t - will check for syntax

then restart

$systemctl restart sshd

$groupadd <group-name> - For Creating Group

$usermod -g <username> <groupname> - For adding user into Primary Group

$usermod -aG <Username> <Secondary-Group>

**ssh Key Authentication to user:**

user must create his public and private keys

Share public Key to Admin

Create directory .ssh inside the home folder of user

$chmod 700 .ssh

Create a file called authorized keys and paste public key of user

give read and write access to user

no access to groups

no access to others

**Ownership:**

change ownership to user

$chown <user>:<group> .ssh

**Delete user:**

User leaving organization:

we need to remove user from group then delete user

$userdel <username> for deleting user

We can't delete user from Primary group

First need to change his primary group to his own group

$groupdel <group-name> for Deleting group

We can only delete the group if its has no users.

first, we should remove users from groups then delete.

**Process Management:**

PID

PPIAD

$ps -ef - listdown the Process

First it will create PID

1. Foreground Process

2. Background Process $sleep 10 &

$kill <PID> - Requesting to end task

$kill -9 <PID> - Forcing to end task

shouldn't kills PPID

**Package Management:**

Ubuntu - apt-get

centos - yum

aws linux 2 - amzon-linux-extras and yum

Install a package called git

$sudo amazon-linux-extras install epel -y

$yum install git -y

$yum remove git -y

$yum list all - all packages including installed packages

$yum list installed

$yum list available - all installed

**Service Management:**

Take an example Nginx Server

http server running on port 80

we should install nginx in Server in root user

$amazon-linux-extras install ngnix1 -y or $yum install nginx1 -y

we should start this Service

$systemctl start nginx

$systemctl status nginx

/usr/share/nginx/html - Folder where we keep html, CSS, JS files

If we restart server, service will not run default.

so, we should enable in Background

$systemctl enable nginx

$systemctl disable nginx

**Network Management:**

$netstat - Network statuistics

$netstat -lt - only list TCP

$netstat -ltn - to see only port numbers

$netstat -ltnp - to see process instancess ID(PID) - We can check respected port is opned or not, what is PID

$top - to check the CPU and Memory

$free -m - to check RAM Usage

$df -hT - Check the Hard disk Memory

$telnet <IP> <PORT>

$find / -name <"filename"> - To search the file