=> class-7 :- Linux -> 4

-> sudoers file :-

SED :-
users
user group

=> EC2 -> Linux -> ec2-user

Enable password based authentication for user:

==> In sshd_config file, by default PasswordBasedAuthentication is no.

We may have to enable password based authentication to yes

--> Display the sshd_config file data : $ sudo cat /etx/ssh/sshd_config

Open sshd config file : $ sudo vi /etc/ssh/sshd_config

Note : To Enable PasswordBasedAuthentication to yes we may have to go to Insert mode --> I

--> Restart sshd service : $ sudo systemctl restart sshd

Login into EC2 Linux VM as a User other than ec2-user:

--> Connected to Linux VM as ec2-user with the help of pem file

-->Create a new user : $sudo useradd harsh

--> Update the password for user harsh : $ sudo passwd harsh

--> Configure 'harsh' in sudoers file : $ sudo visudo --> harsh ALL=(ALL:ALL) ALL --> esc --> cntl+x+y+enter

--> Enable PasswordBasedAuthentication in sshd_config file : $ sudo vi /etc/ssh/sshd_config --> save :wq

--> Restart sshd service : $ sudo systemctl restart sshd

--> Connect to Linux vm as 'harsh' user using username and pwd

File permissions in Linux

- read => r
- write => w
- execute => x

In permissions every file will have 3 sections

⇒ user ⇒ (u) (owner)

⇒ group (g)

⇒ other users (o)

user	group	others
123	456	789

rwx rwx rwx f1.txt

rw- r-- r-- f1.txt

r-x --x r-- f1.txt

user → read & execute

group → execute

others → read

rwx r-- r-- file.txt

user → read, write, execute

group → read

others → read

rw- r-- r-x file.txt

own → read, write

group → read

others ⇒ read & execute.

⇒ Change file permissions

'chmod' command

$ chmod u+x f1.txt --> Gives execute permission for user

$ chmod g+w f1.txt --> Gives write permission for group

$ chmod o-x f1.txt --> Removes execute permission for others

$ chmod o+w f1.txt --> Gives write permission for others

$ chmod o-rwx f1.txt --> Remove all permissions for others

$ chmod g+rwx f1.txt --> Gives all permission for group

u g o

r w x

File Permission in Numeric Format

0 → No permission

1 → Execute

2 → write

3 ⇒ 2+1 (Execute + write)

4 ⇒ Read

5 ⇒ 4+1 (Read + Execute)

6 ⇒ 4+2 (Read + write)

---	0
--x	1
-w-	2
-wx	3
r--	4
r-x	5
rw-	6
rwx	7

7 ⇒ 6 + 1 (Read + write + execute)

⇒ • ugo+x ⇒ $ chmod 111 f.txt

ugo+w ⇒ $ chmod 222 f.txt

⇒ $ chmod 777 f.txt

0	-
1	x
2	w
3	xw
4	r
5	rx
6	rw
7	rwx

ugo+x ⇒ $ chmod 111 f.txt

ugo+r ⇒ $ chmod 444 f.txt

ugo+rwx ⇒ $ chmod 777 f.txt

u+rwx, g+rw, o+r ⇒ $ chmod 764 f.txt

u+r, g+w, o+rx ⇒ $ chmod 425 f.txt

⇒ Q) default Permissions for directory in Linux

⇒ 755 ⇒ rwx r-x r-x

Q) default Permissions for file in Linux

⇒ 644 ⇒ rw- r-- r--

Q) highest permission

777 ⇒ rwx rwx rwx

⇒ Change file/directory ownership :-

⇒ chown

⇒ $ sudo chown <newowner> file/direc ⇒ change owner

⇒ $ sudo chown :groupname file/directory ⇒ change owner group

⇒ $ sudo chown ownername:groupname file/dire ⇒ change owner & group-owner

chmod vs chown

chmod => To change file/directory permissions

chown => To change owner/group

---

find & locate => for file location search