SSH LOGIN FOR TH USER

WE ARE GOING TO GIVE READ ACCESS ONLY

1.Launch the instance in aws and log in as root user

2.Create the user

>. **adduser kalai** (user name is optional)
And set the password for the user we create
> **passwd kalai**

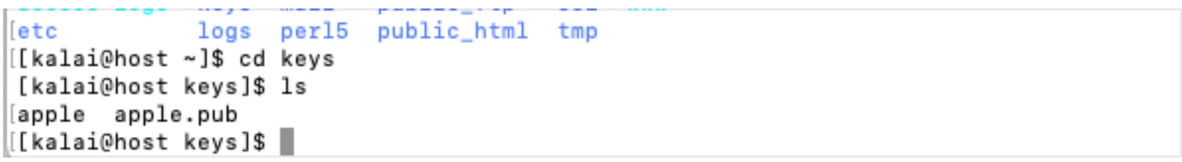
3. Create the folder called .ssh for ssh login for the user

> **mkdir /home/kalai/.ssh** 4. Then create the folder called keys
> **mkdir keys**

4. After that we need to create the public key and
private key for that move to the folder called keys and insert the command

> **ssh-keygen -b 2048 -t rsa**

Then it will ask keys name we created after that you
will public & private key in key folder . In my case I created the key called apple



```
[etc           logs  perl5  public_html  tmp
[[kalai@host ~]$ cd keys
 [kalai@host keys]$ ls
[apple  apple.pub
[[kalai@host keys]$ █
```

5. Create the file in the .ssh folder file name is (authorized_keys) don't change the name of file its manatory

6. Then open the apple.pub file and copy the content and paste into the authorized_keys we created earlier and save it

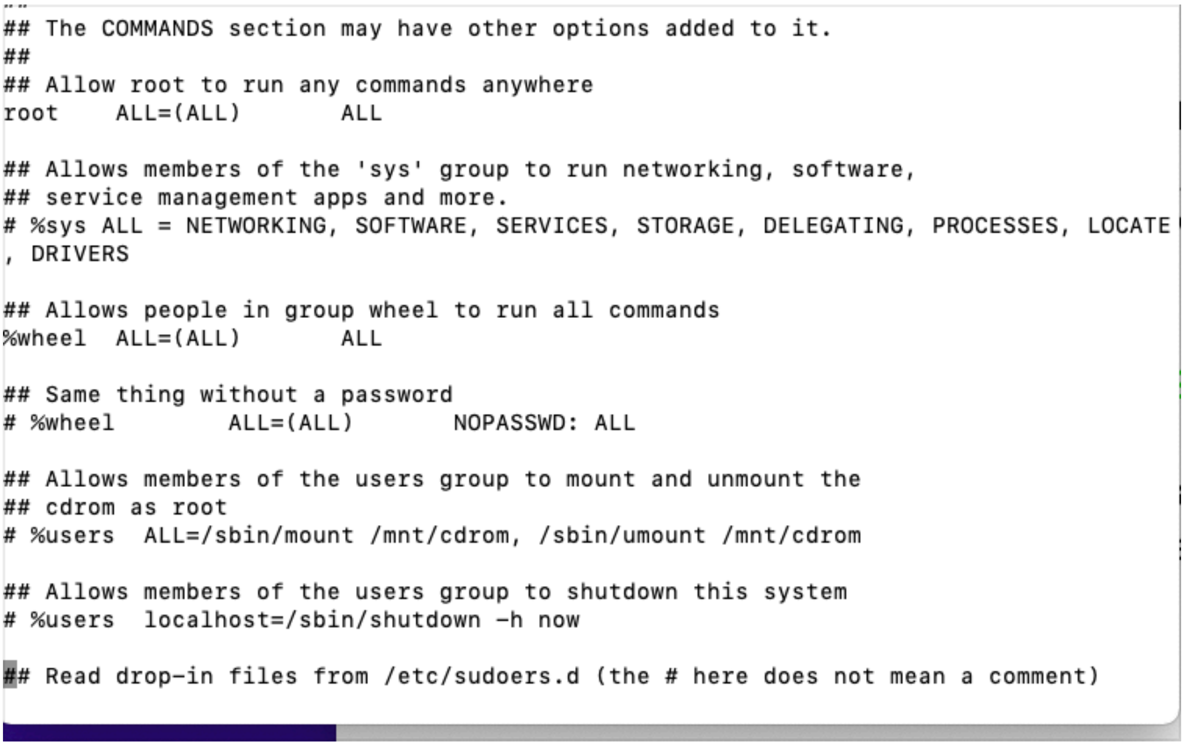
7.Then open the pub key file and copy the content and paste in to the local system because we are going to connect through the keys

8. After that restart the ssh service for that use this command
> /sbin/service sshd restart
9. Then connect to the instances with ssh login
> ssh new_user@ip_address -i private_key
private_key Is nothing but we copy the key to our local system it is called private_key
WE ARE GOING TO GIVE FULL ACCESS

1. Please follow the pervious seven steps after we going to do change the folder permission give root access for the user.

2. Then change the permission of the folder for that > chown -R kalai:kalai /home/kalai/.ssh

3. Go to the terminal and enter > visudo



```
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL

## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE
, DRIVERS

## Allows people in group wheel to run all commands
%wheel  ALL=(ALL)       ALL

## Same thing without a password
# %wheel        ALL=(ALL)       NOPASSWD: ALL

## Allows members of the users group to mount and unmount the
## cdrom as root
# %users  ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom

## Allows members of the users group to shutdown this system
# %users  localhost=/sbin/shutdown -h now

## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)
```

4. U will see the window like this .then add Search ALLOW ROOT CAN RUN search the line
and insert the value

>   kalai ALL=(ALL) NOPASSWD: ALL

5. Restart the ssh server

>   /sbin/service sshd restart

6. Then connect to the instances with ssh login

> ssh new_user@ip_address -i private_key

private_key Is nothing but we copy the key to our local system it is called private_key

chmod +rwx.