Create a User to access a specific folder in Linux

Steps to restrict the user to only have access to a single folder :

Before creating user, first login to the linux machine and switch to root account by using command **sudo su**

- Execute the command **adduser test** to add a new user, as below.

```
[root@ip-X-X-X-X home]# adduser test

[root@ip-X-X-X-X home]# ls

test
```

- Switch to new user test by executing the command **su - test**

```
[root@ip-X-X-X-X home]# su - test
```

- Change the directory to test by executing the command as **cd /home/test**

```
[test@ip-X-X-X-X ~]$ cd /home/test/
```

- Create .ssh folder inside /home/test by executing command as **mkdir .ssh** and change the execution & ownership permissions

```
[test@ip-X-X-X-X ~]$ mkdir .ssh

[test@ip-X-X-X-X ~]$ chmod 700 .ssh

[test@ip-X-X-X-X ~]$ chown test:test .ssh
```

- Change directory to .ssh by executing the command as **cd .ssh**

```
[test@ip-X-X-X-X ~]$ cd .ssh/

[test@ip-X-X-X-X .ssh]$ pwd

/home/test/.ssh
```

- Generate the SSH key pair, to login using new test user by executing the command as follows **ssh-keygen** and not required to enter the passphrase

```
[test@ip-X-X-X-X .ssh]$ ssh-keygen

Generating public/private rsa key pair.

Enter file in which to save the key (/home/test/.ssh/id_rsa):

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in /home/test/.ssh/id_rsa.

Your public key has been saved in /home/test/.ssh/id_rsa.pub.

The key fingerprint is:

SHA256:udYmwa8XuOfnvKpPau8eoNi+gsl8gtt0Z2myElND2ns test@ip-X-X-X-X.eu-west-1.compute.internal

The key's randomart image is:

+---[RSA 2048]----+

|                 |

|    .            |

|   +             |

|  . +  . .       |

|   . o S.        |

|  o .oEo.*.      |

| +.=+.B +.*.     |

|.oB.oB .o*oo.    |
|...+..oo+XB++.   |

+----[SHA256]-----+

[test@ip-X-X-X-X .ssh]$ ls

id_rsa  id_rsa.pub
```

- Create the authorized_keys file by executing the command as **touch authorized_keys**

```
[test@ip-X-X-X-X .ssh]$ touch authorized_keys

[test@ip-X-X-X-X .ssh]$ ls

authorized_keys id_rsa id_rsa.pub
```

- Change the execution & ownership permissions as below

```
[test@ip-X-X-X-X .ssh]$ chmod 600 authorized_keys

[test@ip-X-X-X-X .ssh]$ chown test:test authorized_keys

[test@ip-X-X-X-X .ssh]$ cat id_rsa.pub >> authorized_keys

[test@ip-X-X-X-X .ssh]$ ls

authorized_keys id_rsa id_rsa.pub
```

- To get the content of private key execute the command as **less id_rsa**

```
[test@ip-X-X-X-X .ssh]$ less id_rsa
```

- Copy the content and paste in notepad and save with the extension of **.pem**

```
-----BEGIN RSA PRIVATE KEY-----

***************************

-----END RSA PRIVATE KEY-------
```

- Open puttygen and load this .pem file and click on ‘Save private key’, a passphrase not required but can be used if additional security is required.
- Save the key with the extension of **.ppk**
- Again login to the linux machine and switch to the root account to grant privileges follow the below steps.
- To grant the ownership to a specific folder for test user run below command

```
chown test:test /path/to/myfolder
```

- To grant the execution permissions on specific folder run as below

```
chmod u+w /path/to/myfolder
```

- Now users can login and do their specific activities.