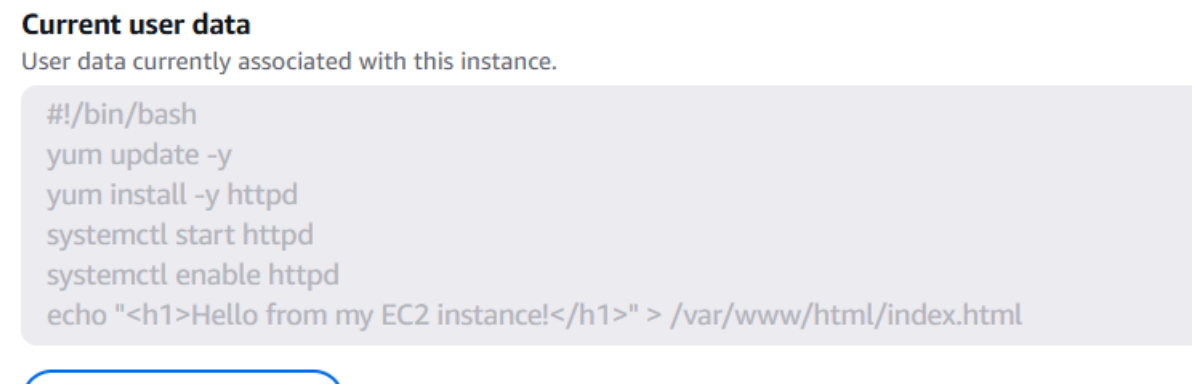
1. Launch one EC2 using Amazon Linux 2 image and add a script in user data to install Apache.

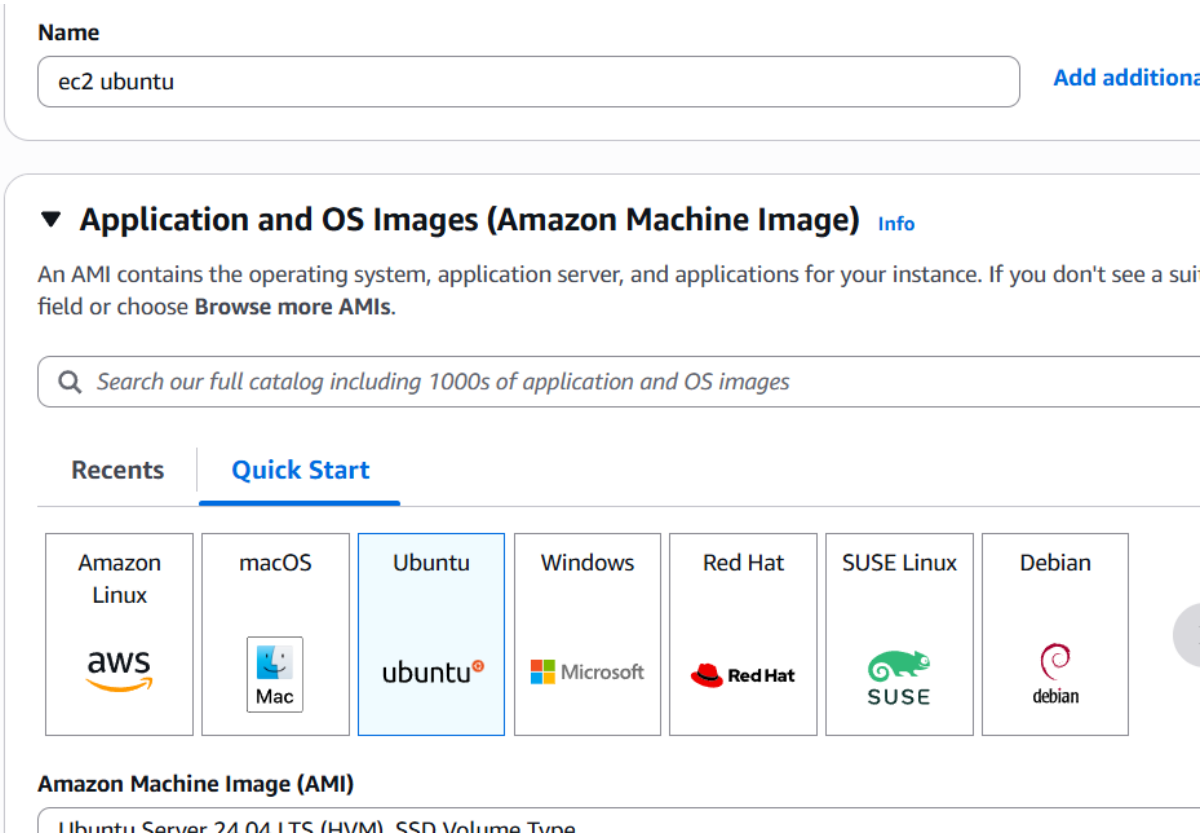
Launch a instance with linux 2 image and give all the details to create and add the script to install apache in the additional details.



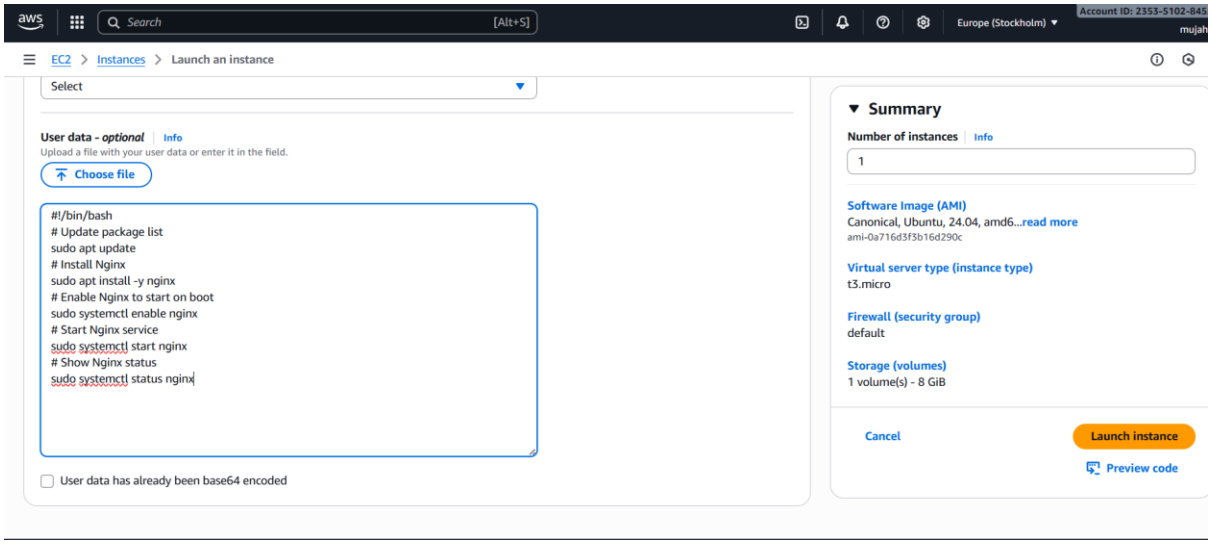
Copy the ip address and add port number 80 and run the page.

2. Launch one EC2 using Ubuntu image and add a script in user data to install Nginx.

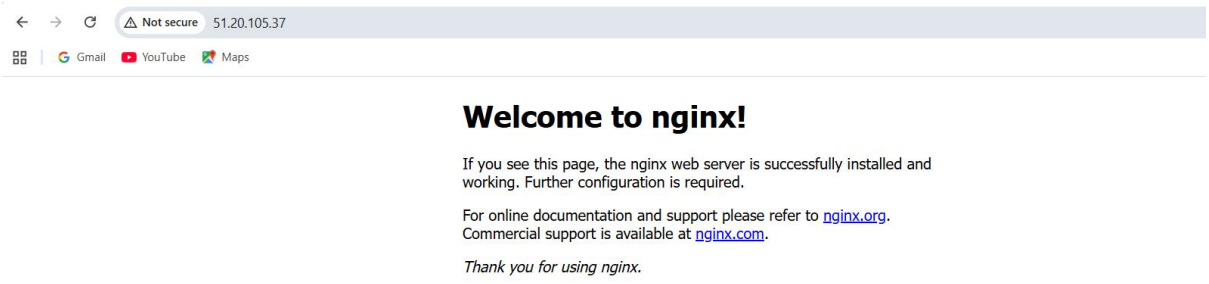
Create a instance with ubuntu image



Add the nginx installation script in the user data.



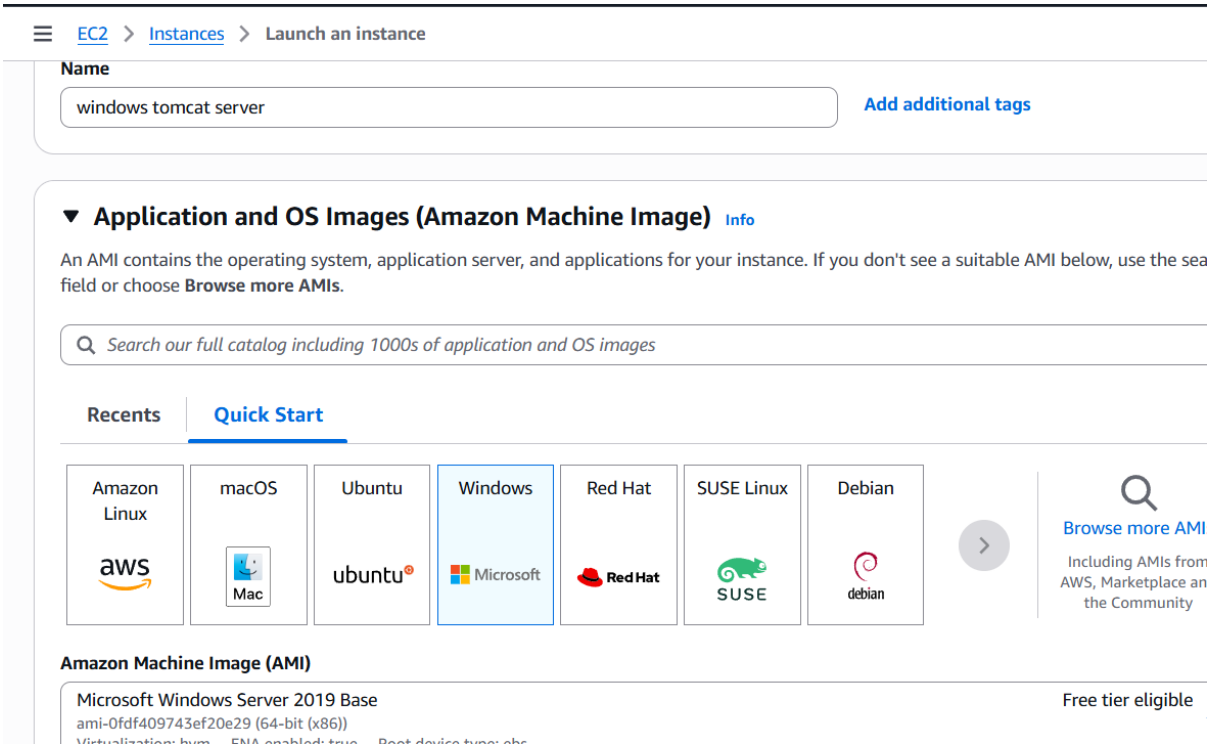
Copy the ip address and run with the port number 80.



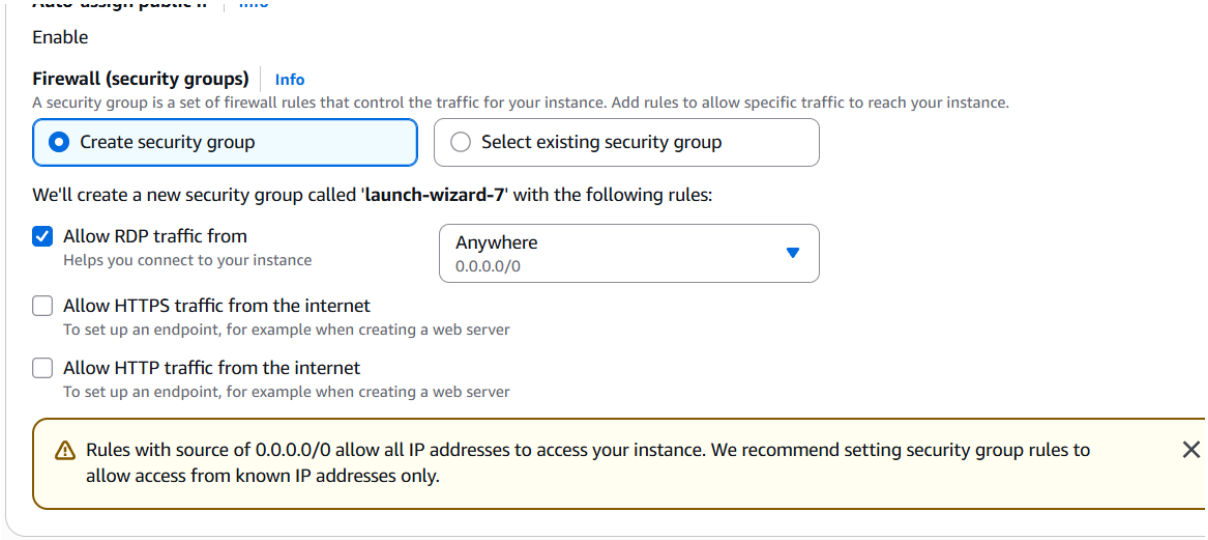
3. Launch one Windows server and install Tomcat on Windows.

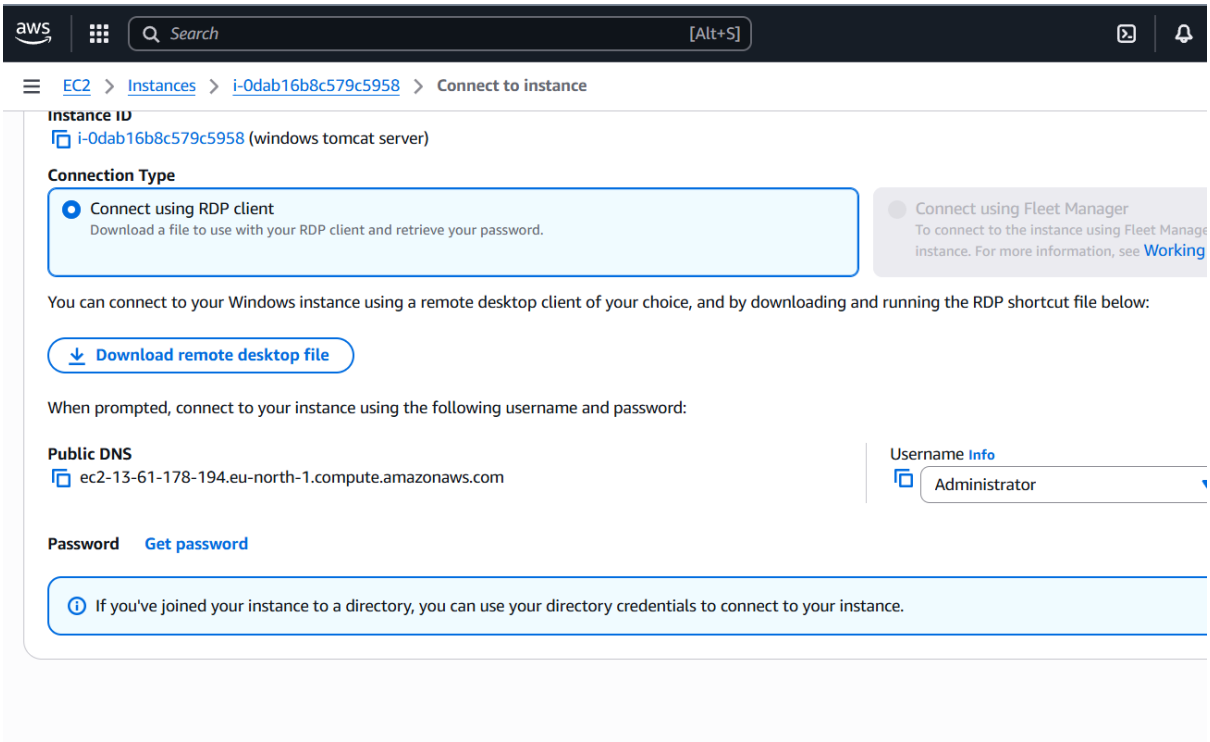
Create an instance named as windows tomcat server.

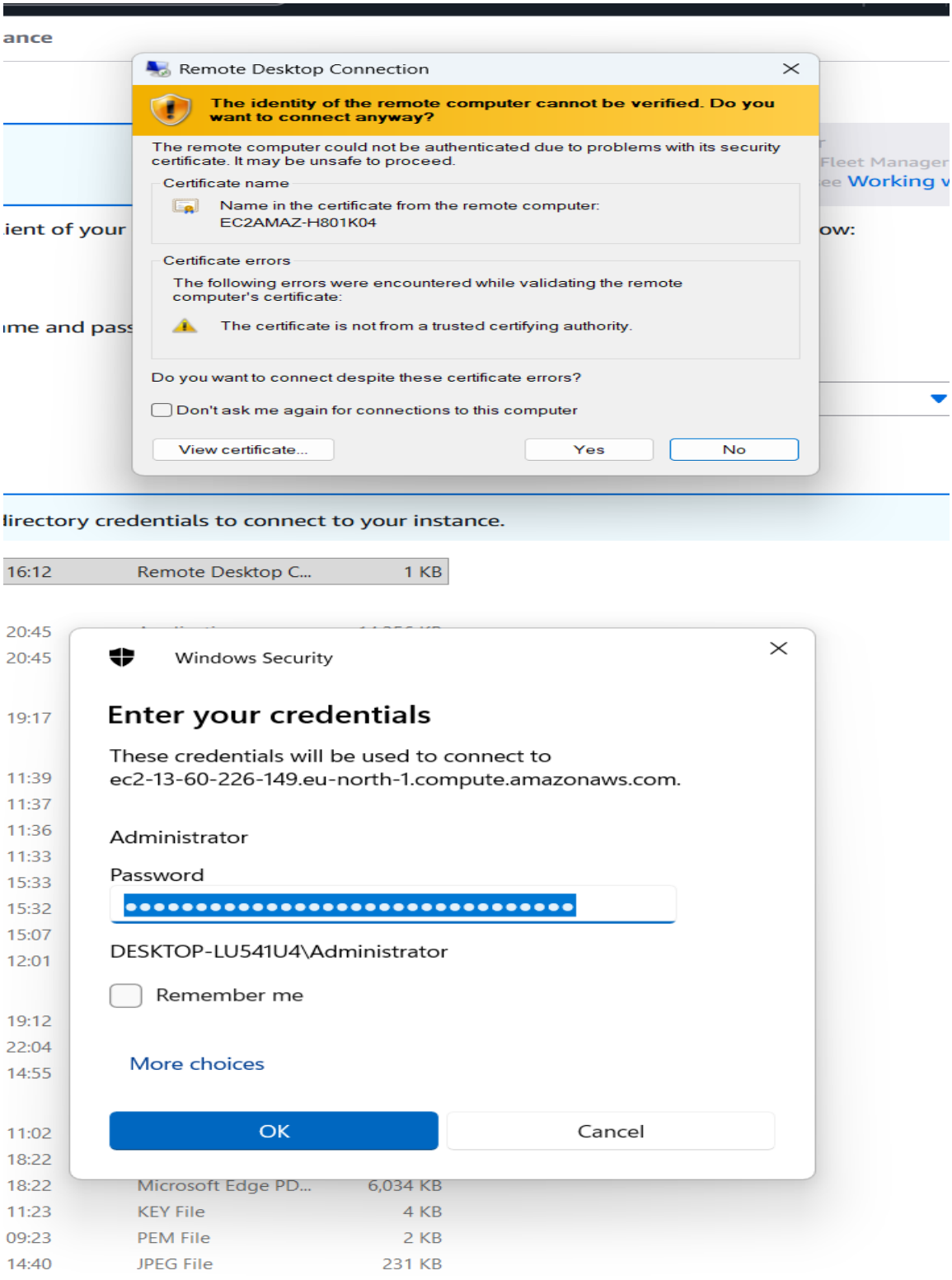
Select Microsoft windows as AMI (Amazon Machine Image)

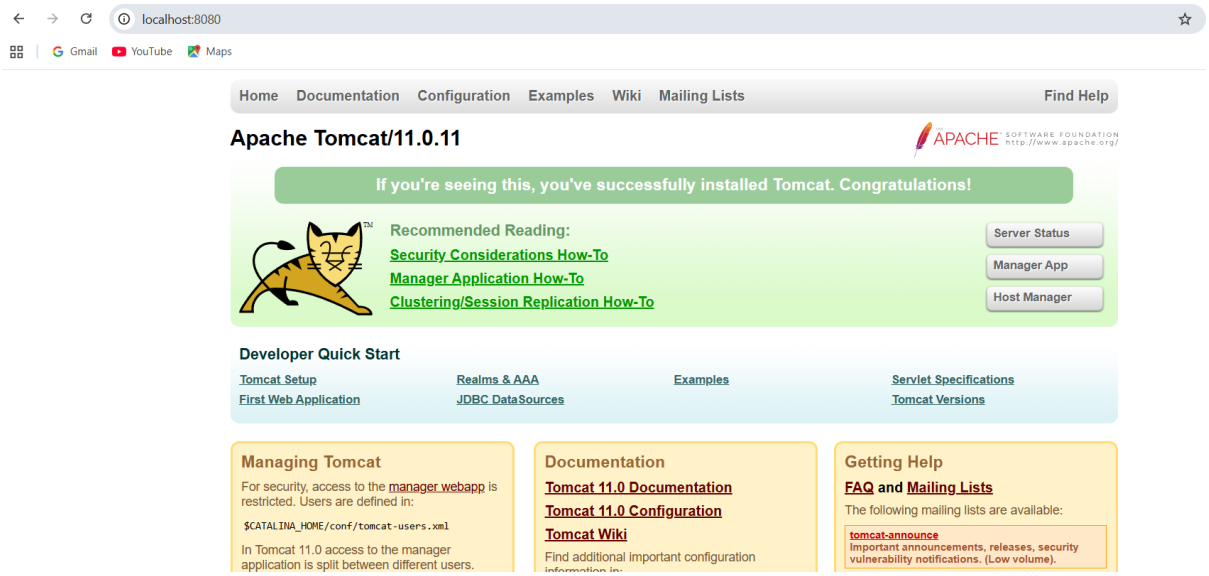


Create security group set as allow RDP traffic from


Enable
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group
We'll create a new security group called 'launch-wizard-7' with the following rules:
Allow RDP traffic from
Helps you connect to your instance
Anywhere
0.0.0.0/0
Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server
Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.


aws
Search
[Alt+S]
EC2 > Instances > i-0dab16b8c579c5958 > Connect to instance
Instance ID
i-0dab16b8c579c5958 (windows tomcat server)
Connection Type
Connect using RDP client
Download a file to use with your RDP client and retrieve your password.
Connect using Fleet Manager
To connect to the instance using Fleet Manage
instance. For more information, see Working
You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:
Download remote desktop file
When prompted, connect to your instance using the following username and password:
Public DNS
ec2-13-61-178-194.eu-north-1.compute.amazonaws.com
Username Info
Administrator
Password
Get password
If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

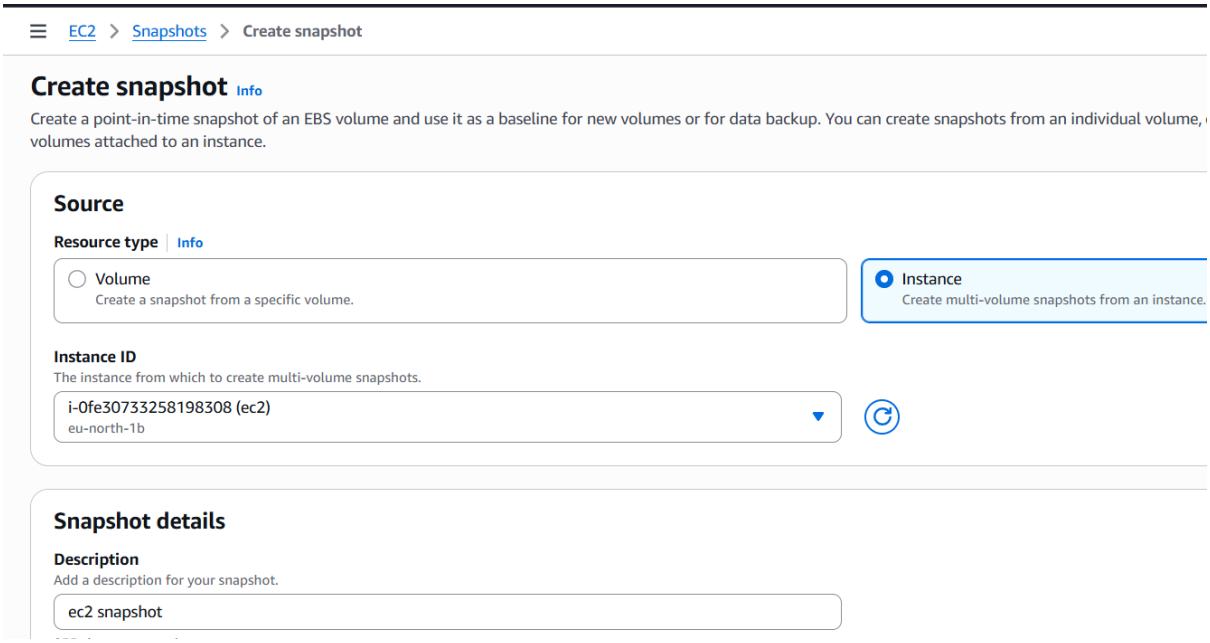

ance
Remote Desktop Connection
The identity of the remote computer cannot be verified. Do you want to connect anyway?
The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.
Certificate name
Name in the certificate from the remote computer:
EC2AMAZ-H801K04
Certificate errors
The following errors were encountered while validating the remote computer's certificate:
The certificate is not from a trusted certifying authority.
Do you want to connect despite these certificate errors?
Don't ask me again for connections to this computer
View certificate...
Yes
No
ient of your
ow:
me and pass
irectory credentials to connect to your instance.
16:12 Remote Desktop C... 1 KB
20:45
20:45
19:17
11:39
11:37
11:36
11:33
15:33
15:32
15:07
12:01
19:12
22:04
14:55
11:02
18:22
18:22 Microsoft Edge PD... 6,034 KB
11:23 KEY File 4 KB
09:23 PEM File 2 KB
14:40 JPEG File 231 KB
Windows Security
Enter your credentials
These credentials will be used to connect to
ec2-13-60-226-149.eu-north-1.compute.amazonaws.com.
Administrator
Password
DESKTOP-LU541U4\Administrator
Remember me
More choices
OK
Cancel



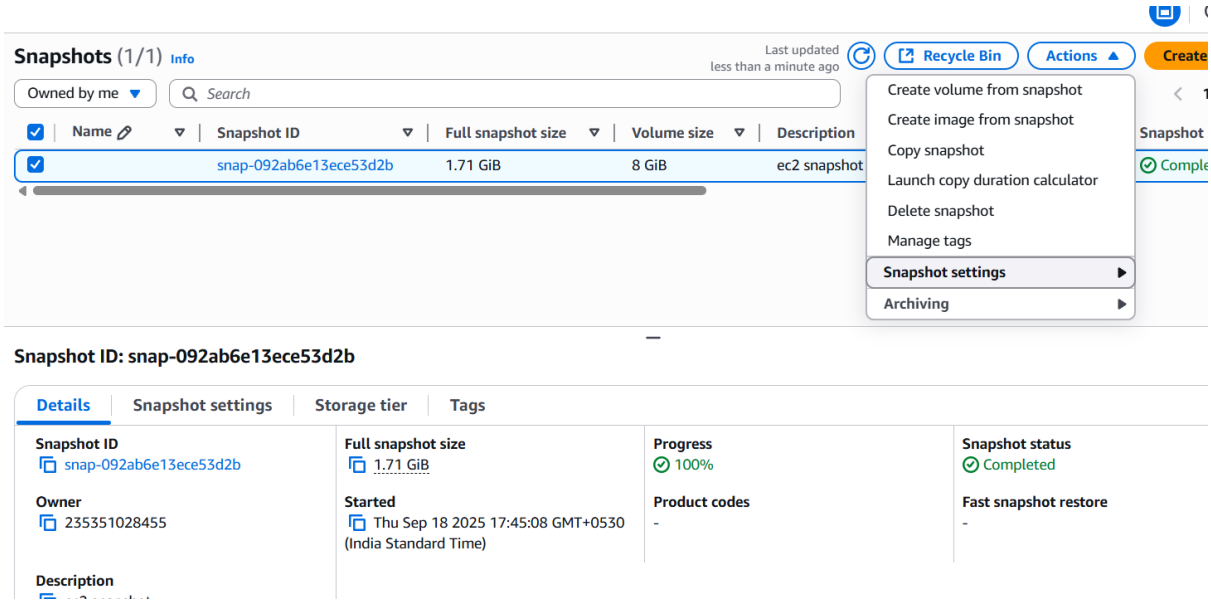
4. Take a snapshot of the instance created in Task 1.

Launch the task ec2 that we are created on the task 1.

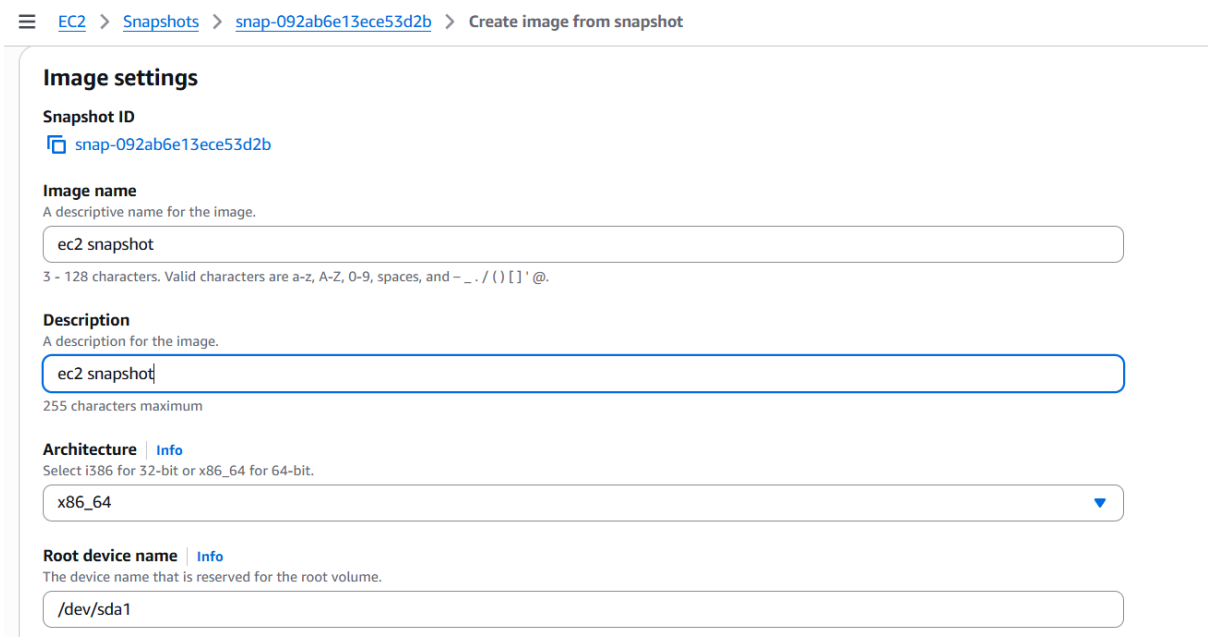
Create snapshot to that ec2 instance.

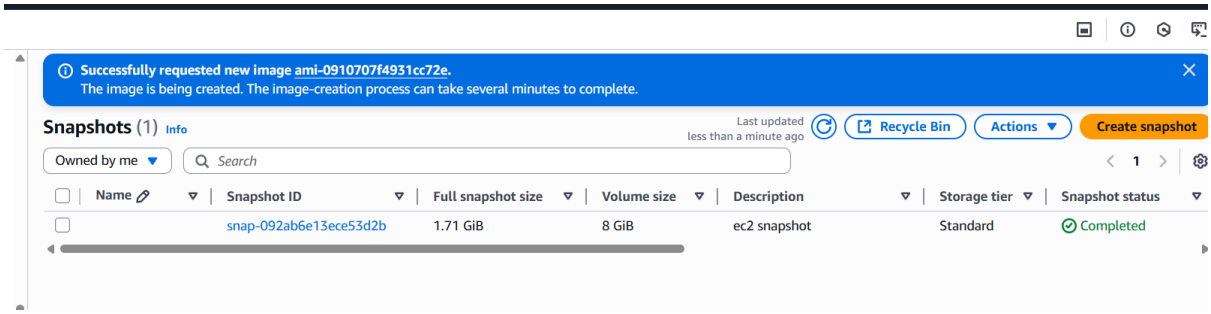


Create image from snapshot.



Give name and description for image.





5. Assign passwordless authentication for the EC2 created in Task 2.

In task 2 we have created a ec2 instance with ubuntu added nginx user data to it.

Create ssh-keygen

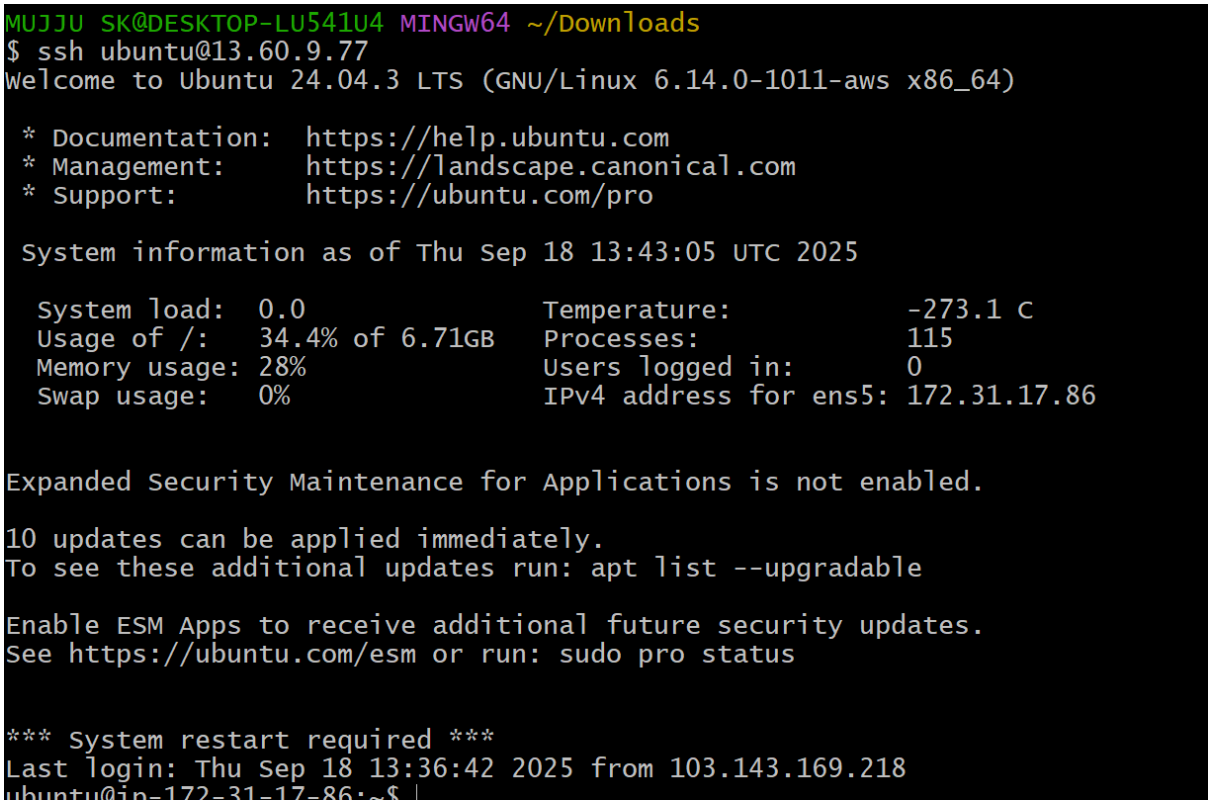
```
MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Downloads
$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/c/Users/Ashish/.ssh/id_rsa):
/c/Users/Ashish/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /c/Users/Ashish/.ssh/id_rsa
Your public key has been saved in /c/Users/Ashish/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:SR3oT15a3DH2PARRXzH/3BfV9rHUJ1VMdHp4MPDgVcU MUJJU SK@DESKTOP-LU541U4
The key's randomart image is:
+---[RSA 3072]----+
|         .. o+B@^|
|        .. o +=OE|
|       .. ...o*OX|
|       .... + .*B|
|        S+ +    *|
|          +     .|
|                 |
|                 |
|                 |
+----[SHA256]-----+

MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Downloads
$ cat /c/Users/Ashish/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDXS6RWRY5+lze8ldHGpJ5zBwMnqhEZKgidWJj6OFTbFOMFwO2daQk9nP3
EmLOnOpI6fISragy91XvbLpZPwOs73igqzaeDSEIMsHUBV2KaBHTqCPM7Mgu7wpUoErRsmUHrCk9fJai7uYvawJko+lOGag
FE7AsCBZK3O7uvONGlIvy3nWKkjmtKOKxjQ5eR/fQLZQceBXwstO5mx2GvH6O4u+Wqw2FrqD6vAYu2/WMmm8UsJirUHkWuQ
5OcpPfxkGrGvDgkCZyNiLCpZGX2ikR/roE/9FQT2zq7T6wBsxeOXJTtRKkvfLYNDMNq/lx56oF3pqLEsc3G43rCsHDYvuSX
Hlm3FZ66CAuTx49AdG8DIQi91I3fRYhFifZ/2OZj9c/T9ZGxqLPn5NYootxFXOgCzOHuyBd6cxEOvTE= MUJJU SK@DESKTO

MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Downloads
```

Copy the public key

Create a file with vi ~/.authorized_keys and copy the key and save it.

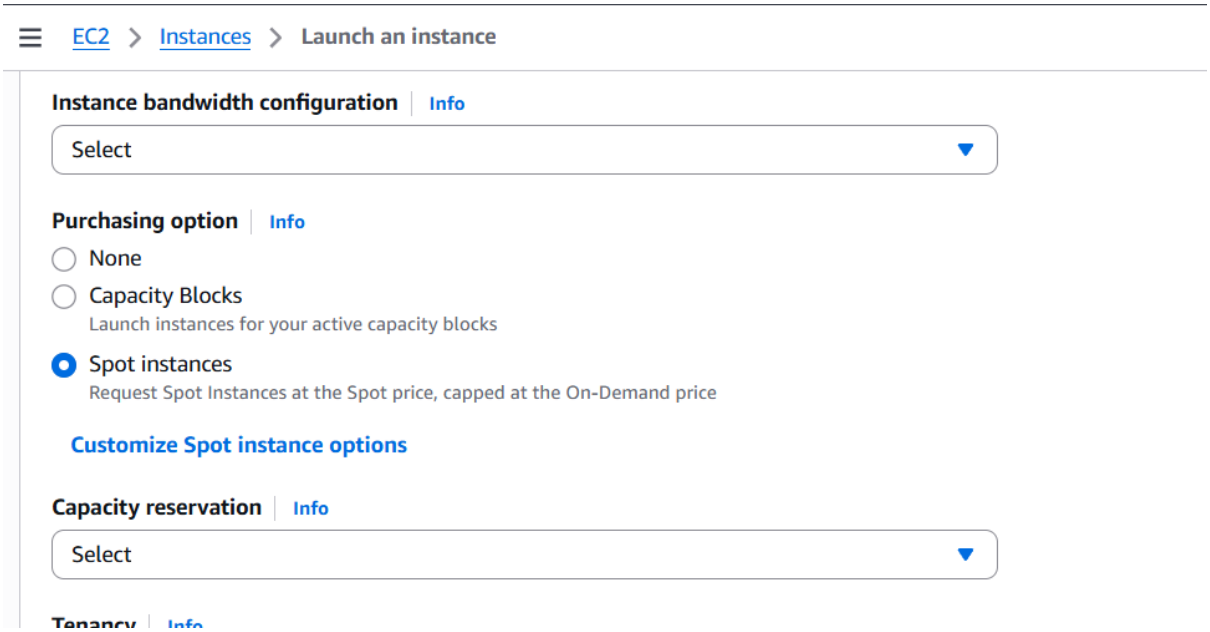
```
ubuntu@ip-172-31-17-86:~$ vi ~/.ssh/authorized_keys
ubuntu@ip-172-31-17-86:~$ ls -l
total 0
ubuntu@ip-172-31-17-86:~$ ls -l ~/.ssh/authorized_keys
-rw------- 1 ubuntu ubuntu 578 Sep 18 13:40 /home/ubuntu/.ssh/authorized_keys
ubuntu@ip-172-31-17-86:~$ exit
logout
Connection to 13.60.9.77 closed.
```

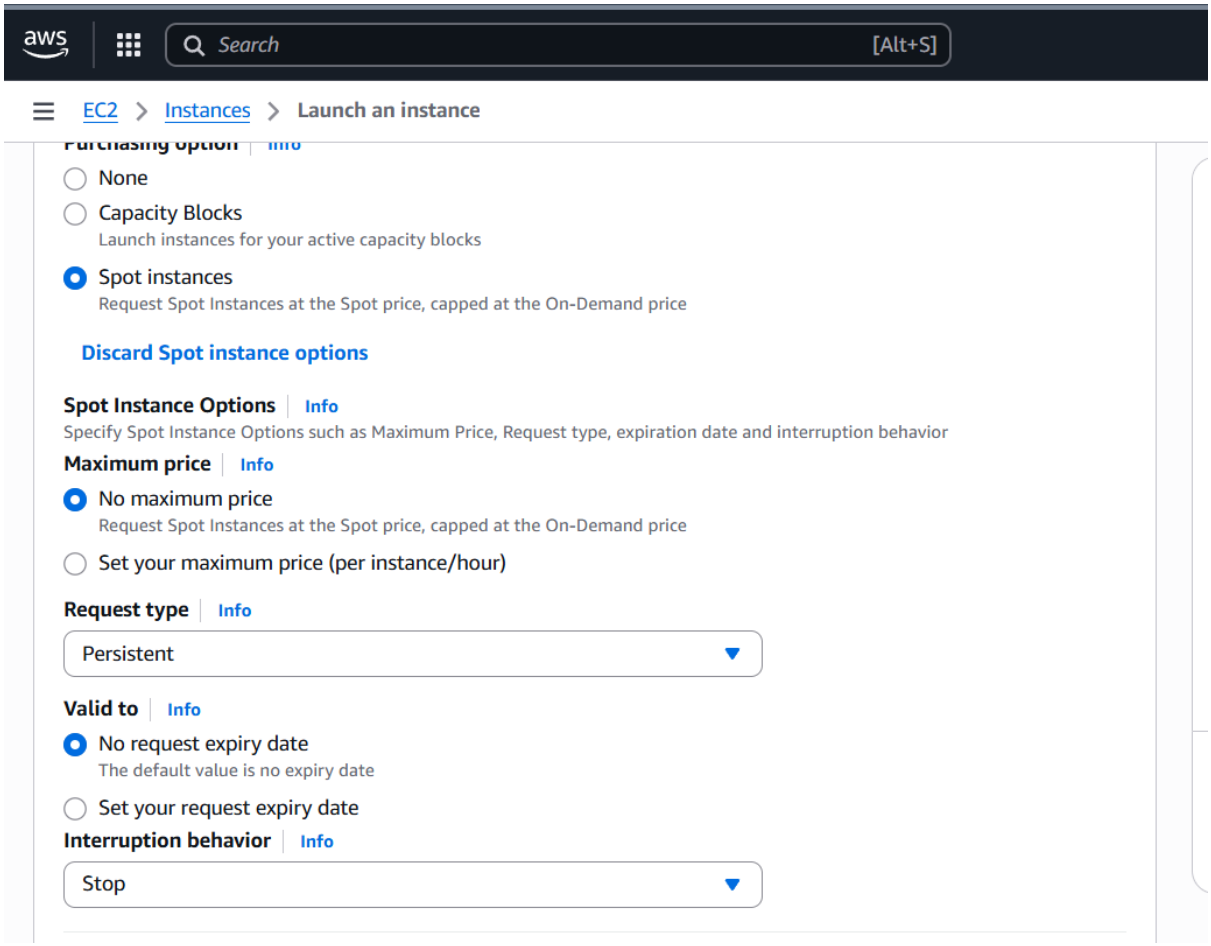
Login ssh from starting ssh ubuntu@13.60.9.77 with out pem key.



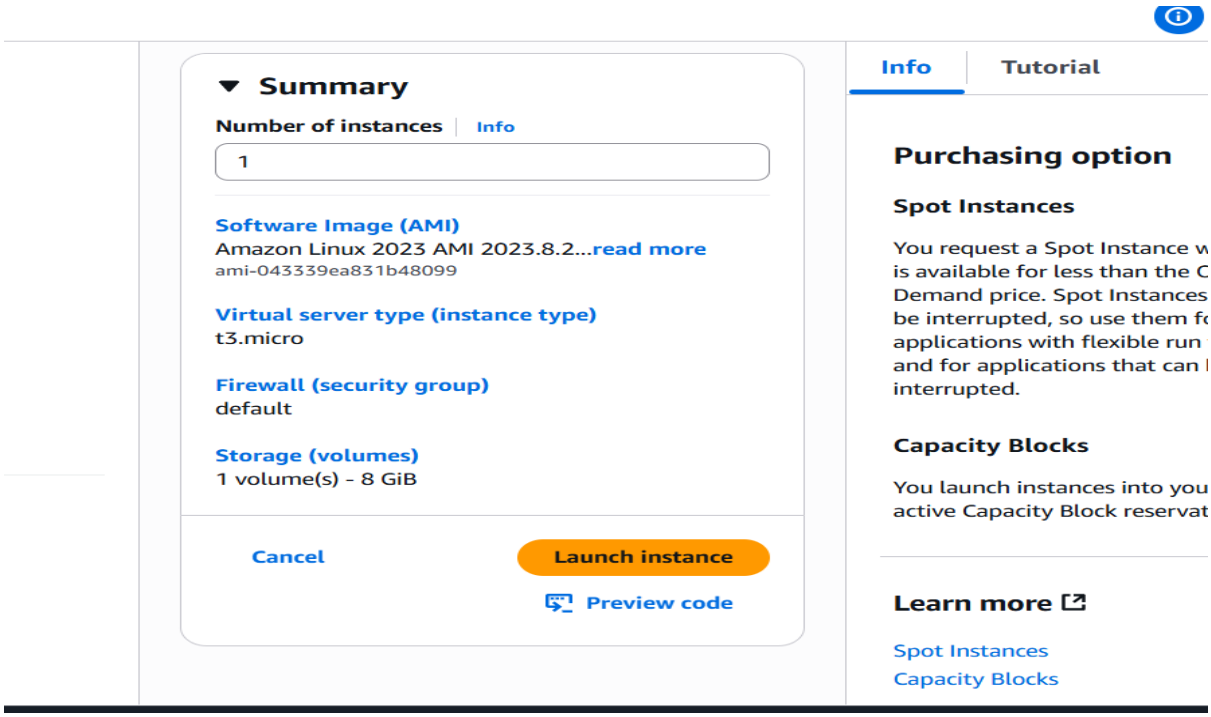
6. Launch any EC2 using the spot purchasing option.

While creating instance on additional details keep it as spot instance.



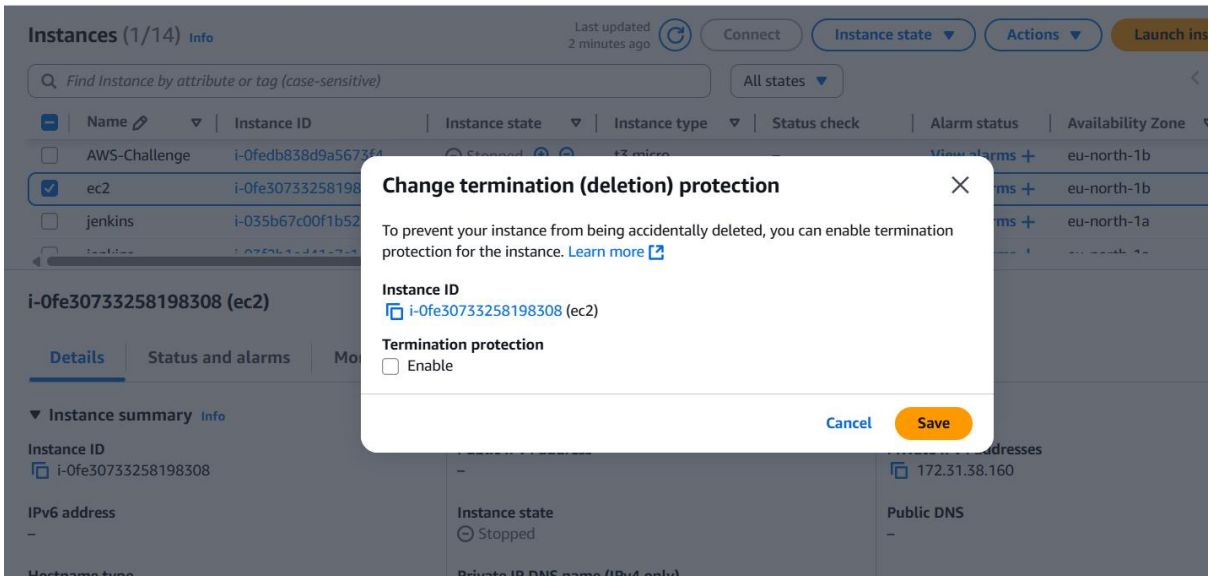


Create on launch instance then the spot instance will be created.

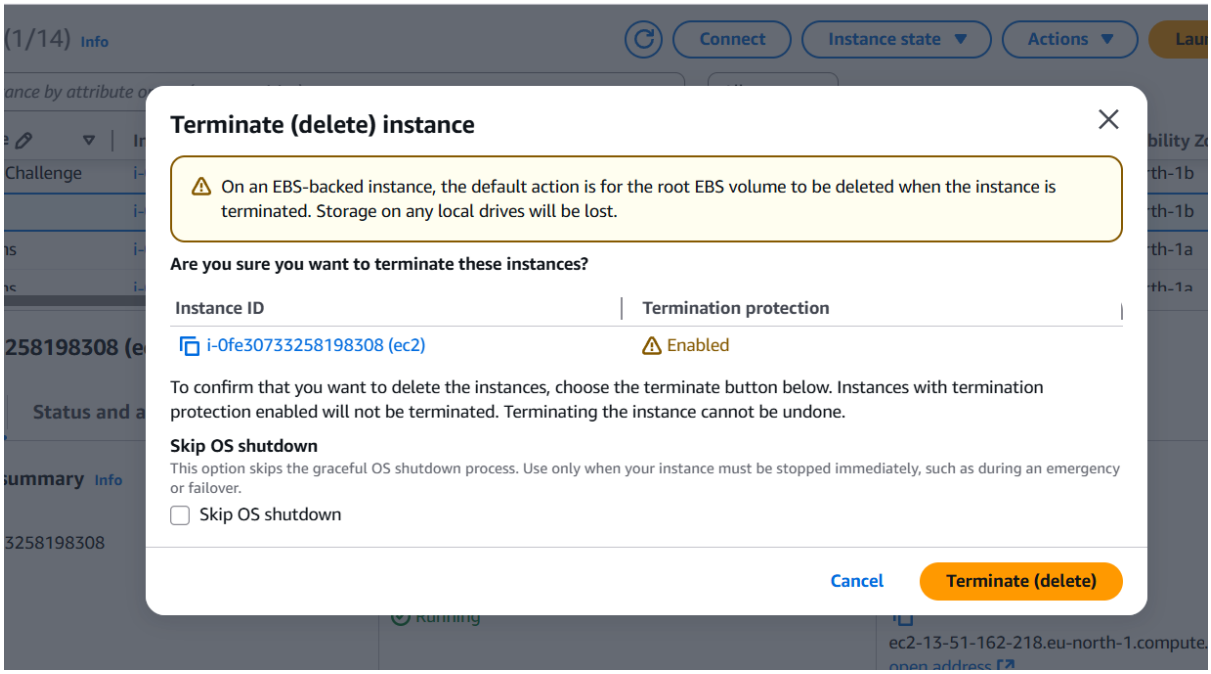


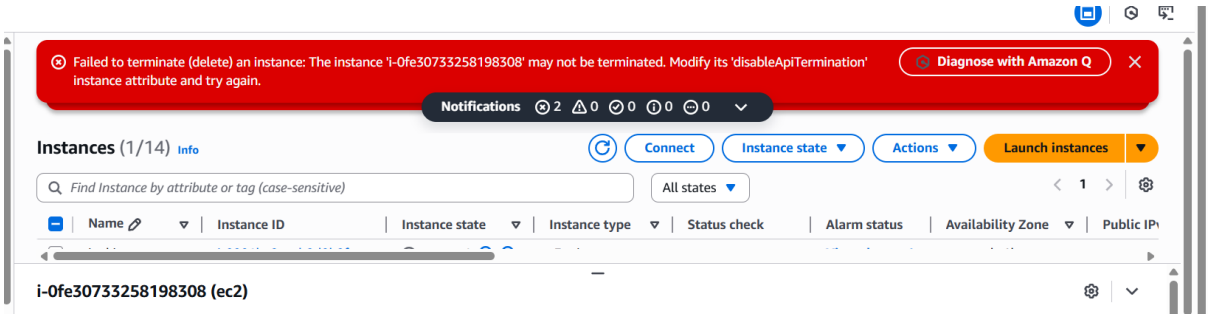
7. Enable termination policy on the EC2 created in Task .

In task 1 we created a ec2 instance with apache in user data. Select that instance and goto instance settings-termination protection-enable.



Try to terminate that instance it won't allow you to terminate.





8. Launch one EC2 using AWS CLI.

- Launch instance name with aws
- And connect to the server thenWget downlaod cli https://awscli.amazonaws.com/AWSCLIV2.msi
- Then gave a command of aws configure it will show u options like
- Access key
- Secreat access key
- Region and format

```
[root@ip-172-31-38-160 ~]# aws ec2 describe-instances
{
    "Reservations": [
        {
            "ReservationId": "r-0996a5934c75f7ecc",
            "OwnerId": "235351028455",
            "Groups": [],
            "Instances": [
                {
                    "Architecture": "x86_64",
                    "BlockDeviceMappings": [
                        {
                            "DeviceName": "/dev/xvda",
                            "Ebs": {
                                "AttachTime": "2025-09-02T09:27:33+00:00",
                                "DeleteOnTermination": true,
                                "Status": "attached",
                                "VolumeId": "vol-0c6a850661ec01030"
                            }
                        }
                    ],
                    "ClientToken": "3964d984-de4a-497c-bf8c-33f56e5d7bfb",
                    "EbsOptimized": true,
                    "EnaSupport": true,
                    "Hypervisor": "xen",
                    "NetworkInterfaces": [
```