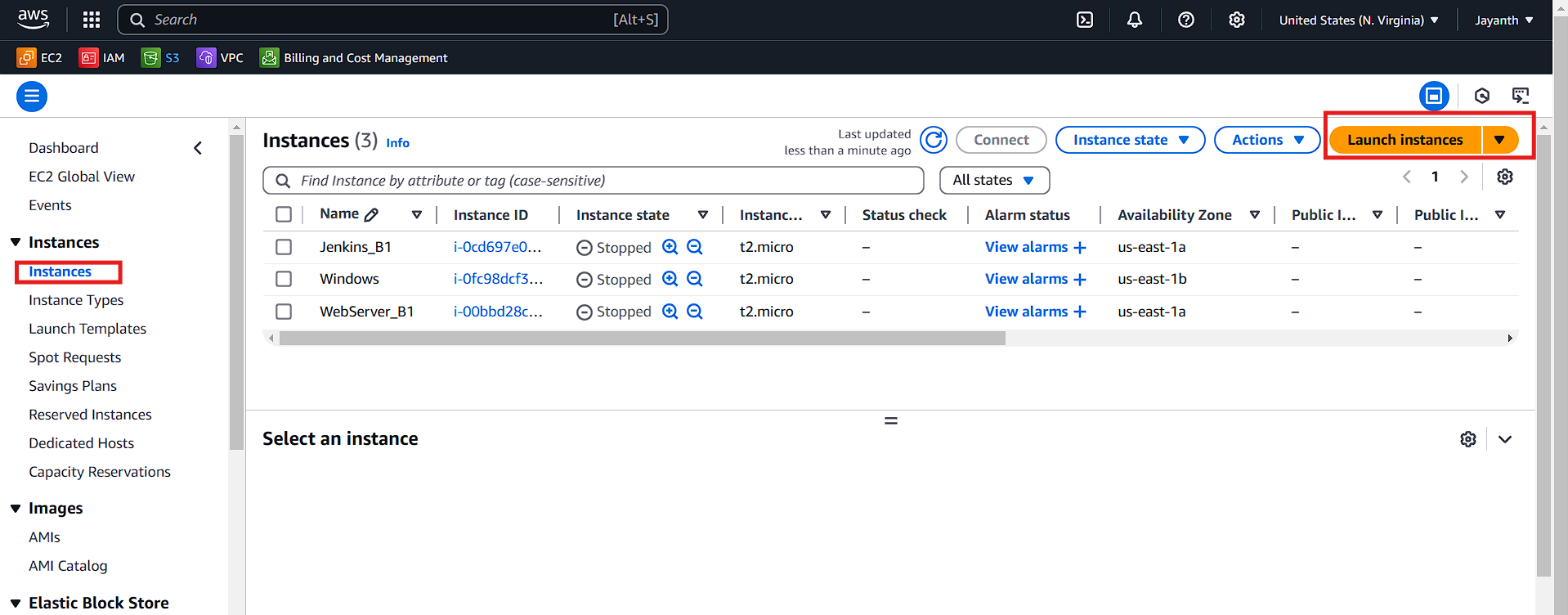
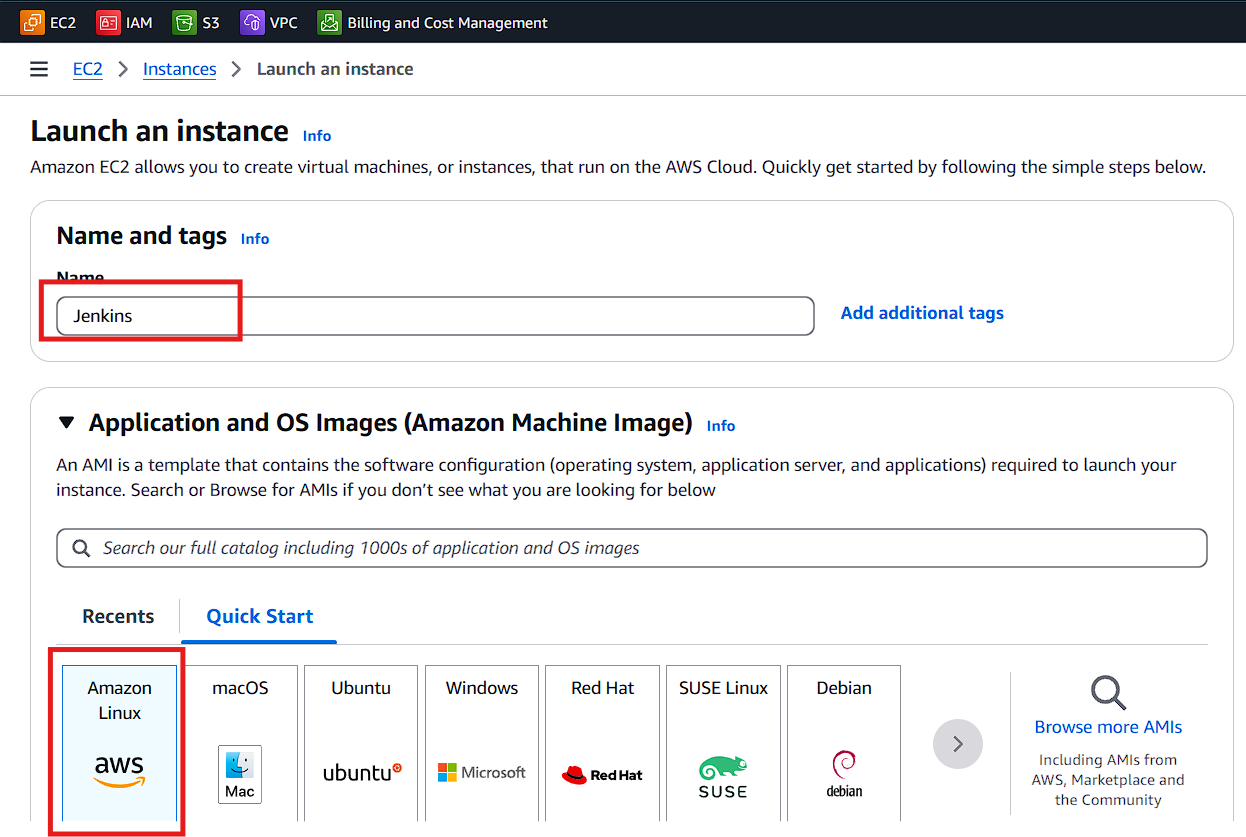
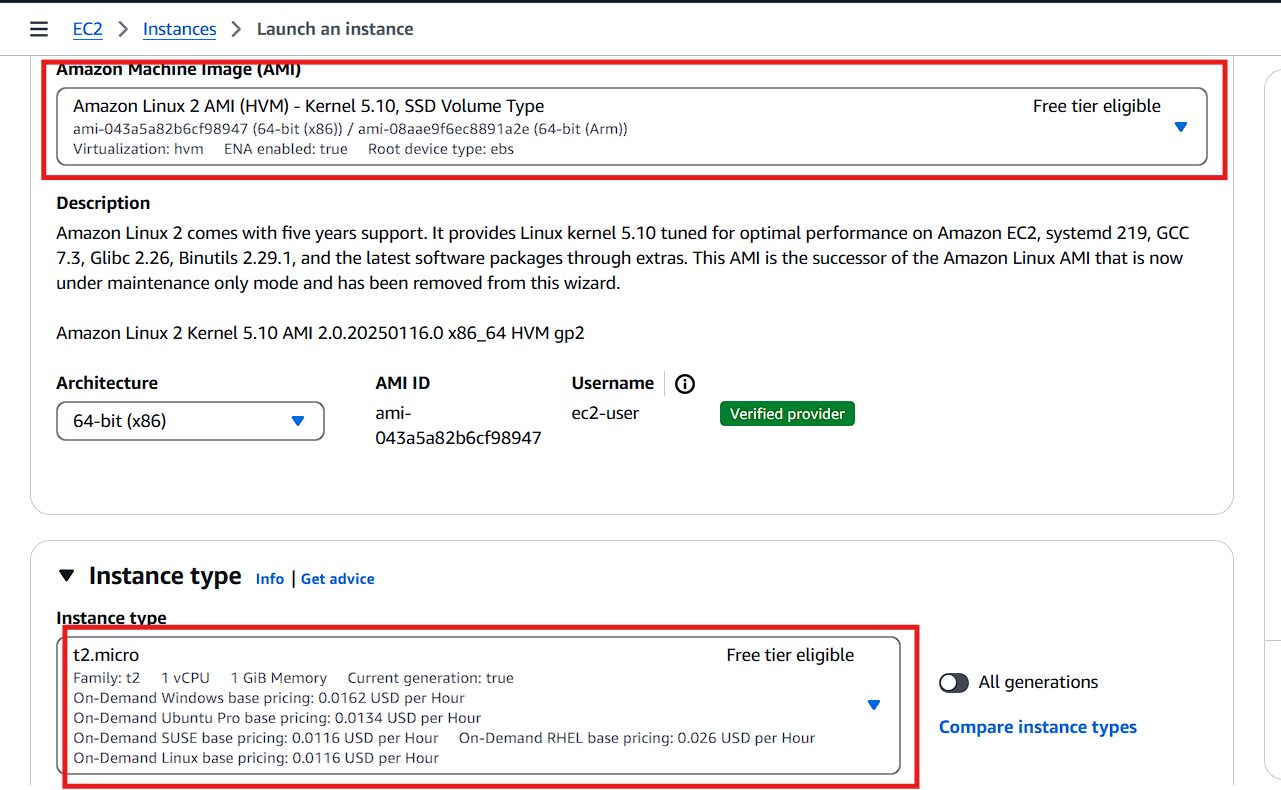
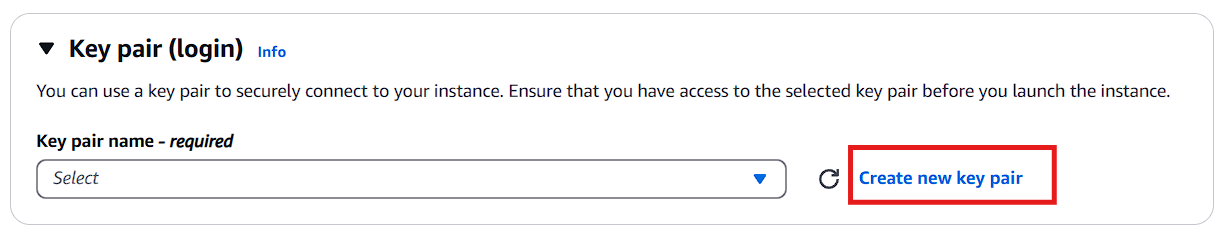
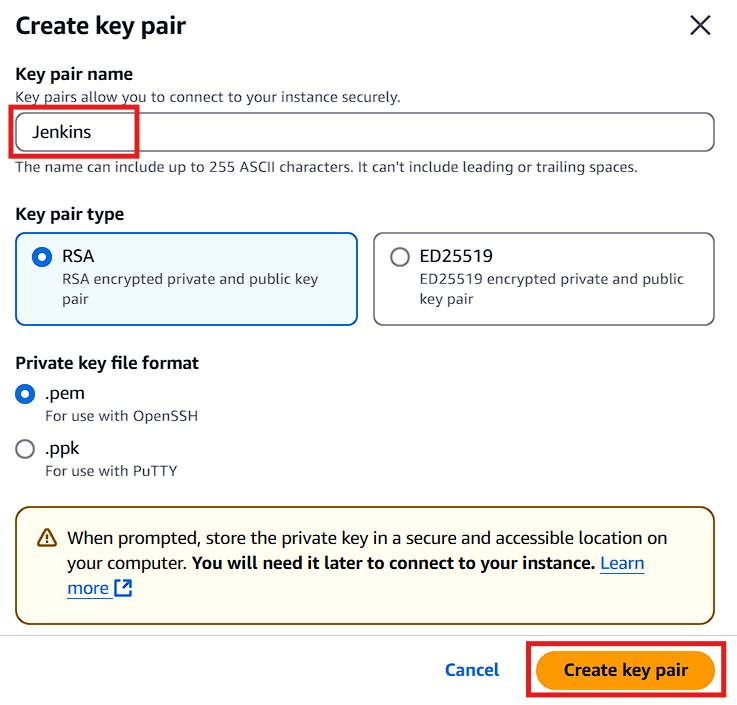
**Create a New Ec2 Instance and Install Jenkins in it**  
  
  
Go to the EC2 Dashboard, click on Instances, and then select Launch Instance.

  
  
  
Provide a name for the server and choose Amazon Linux 2 as the OS version.

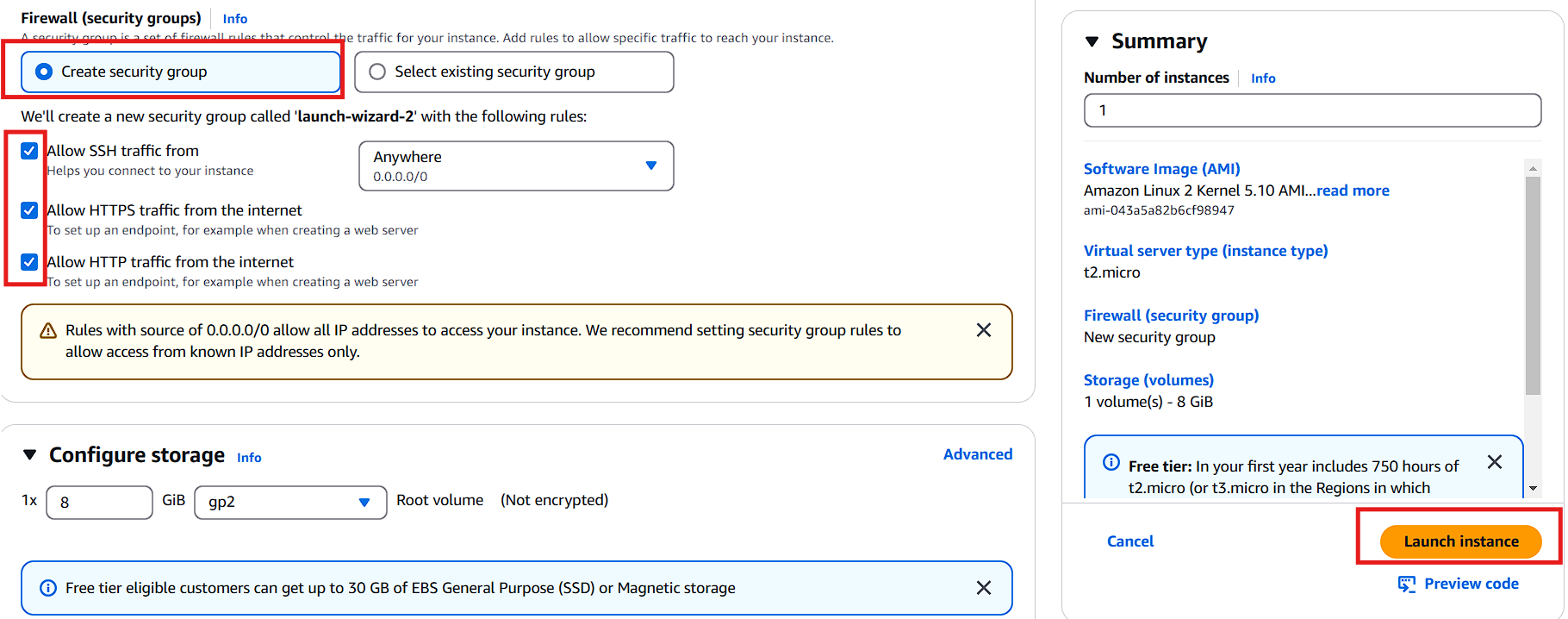
  
Select the Amazon Linux 2 AMI and t2.micro instance type.  
  
  
  
  
  
Click on Create new key pair.

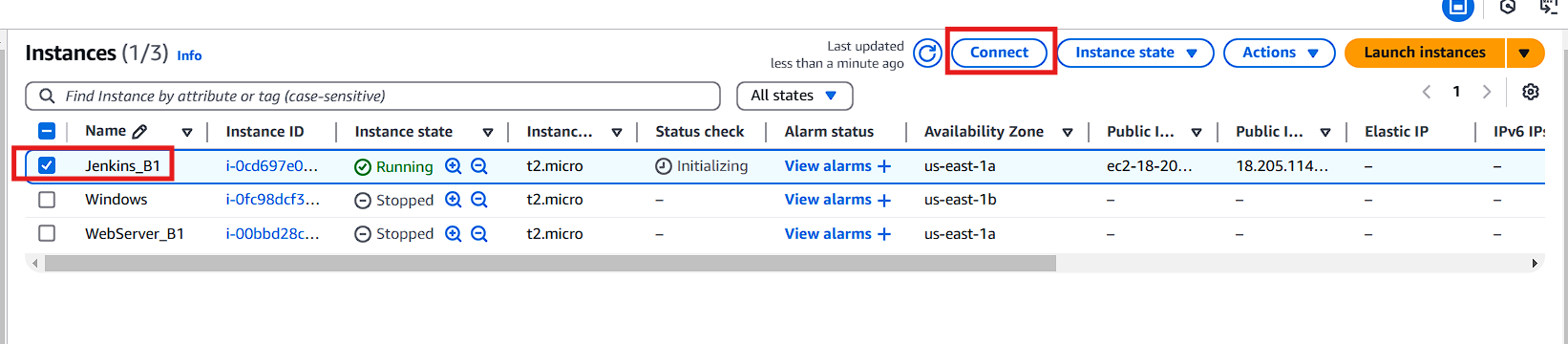
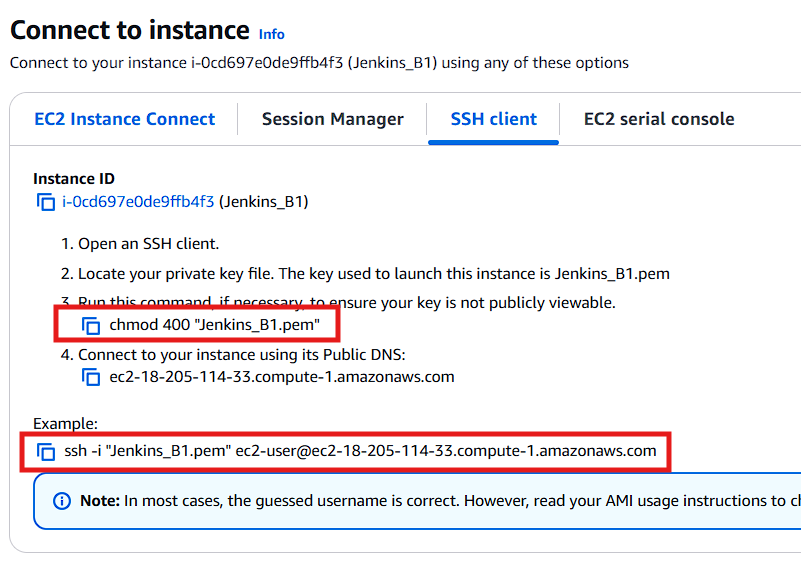
Enter a name for the key pair and click Create Key Pair.

The key pair will be automatically downloaded; store it securely for future use to log in to the instance.  


  
  
  
  
  
Click on Create security group.

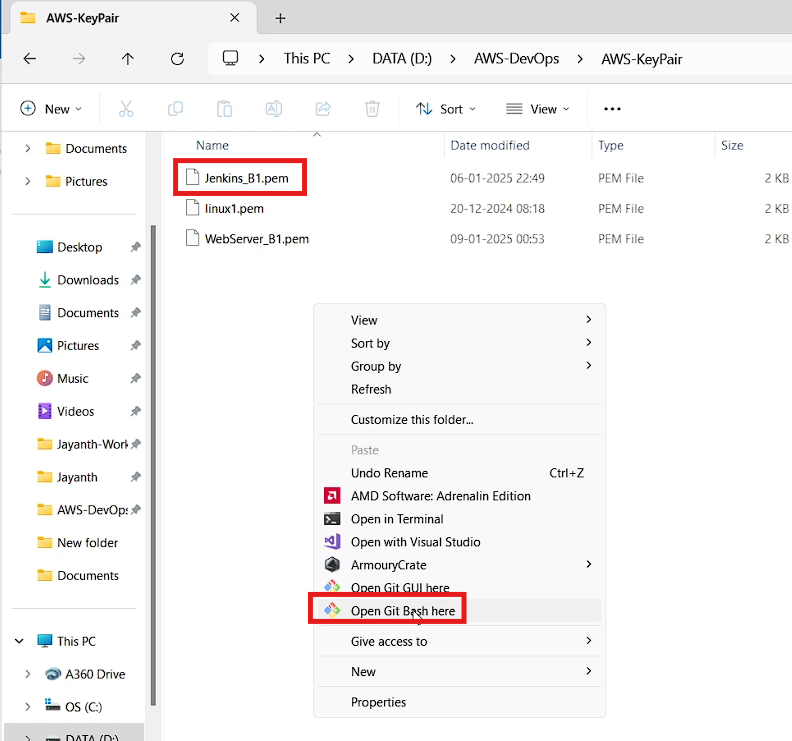
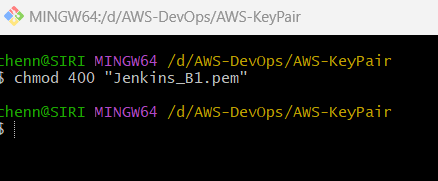
Ensure you select all the necessary options as shown.

Finally, click Launch Instance.  
  
  
  
  
Once the instance is launched, select it and click Connect.

  
  
  
  
Copy the command provided for setting up read-only permissions..  
  
  


Navigate to the path where your key pair is stored.

Right-click on the key pair file and select Git Bash.

  
  
  
  
Paste the copied command into Git Bash and press Enter.  
  
  
  
  
  
  
Copy the next command provided, paste it into Git Bash, and press Enter.

Type yes when prompted to connect to the web server instance.  
  
**Run the following commands one by one**  
  
sudo su -

wget -O /etc/yum.repos.d/jenkins.repo https://pkg.jenkins.io/redhat-stable/jenkins.repo

sudo rpm --import https://pkg.jenkins.io/redhat-stable/jenkins.io-2023.key

yum install epel-release -y

sudo amazon-linux-extras install epel -y

sudo yum install java-17-amazon-corretto-devel -y

yum install jenkins -y

systemctl start jenkins

systemctl status jenkins

systemctl enable jenkins

yum install firewall\* -y

systemctl start firewalld

systemctl status firewalld

systemctl enable firewalld

firewall-cmd --zone=public --add-port=8080/tcp --permanent

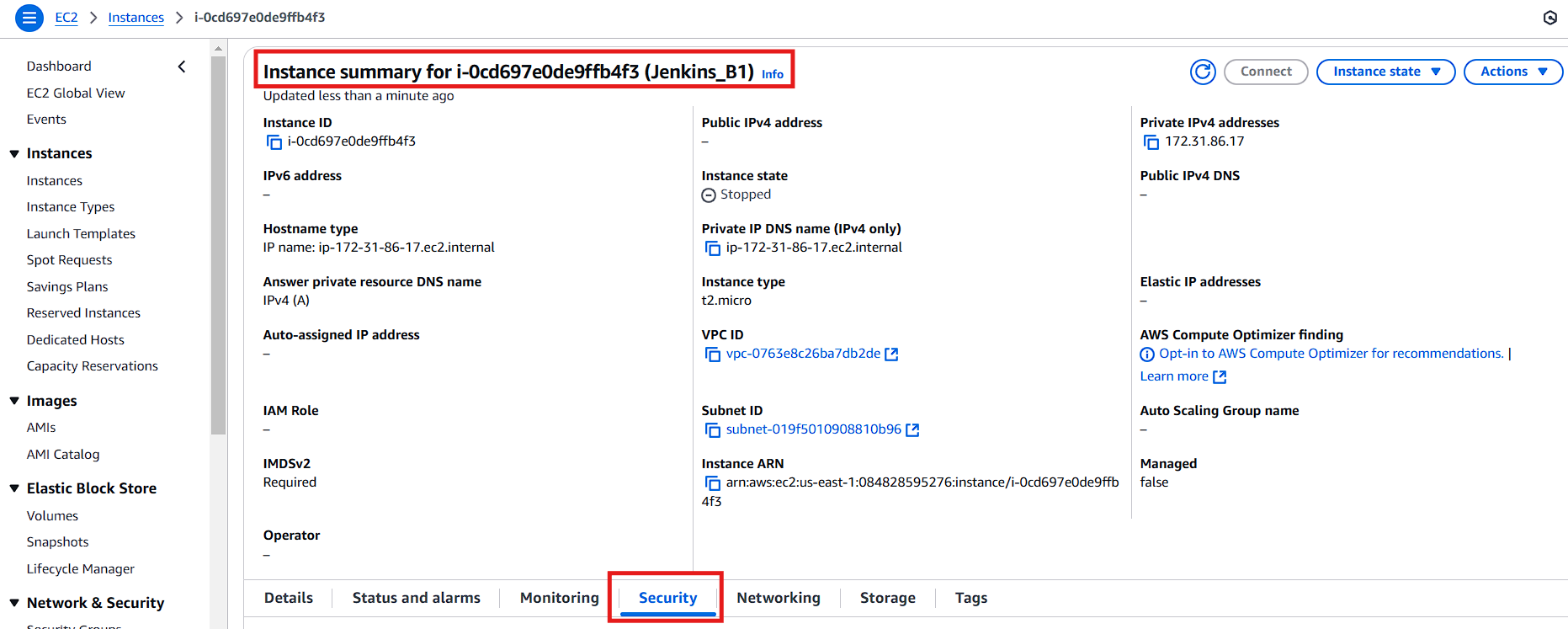
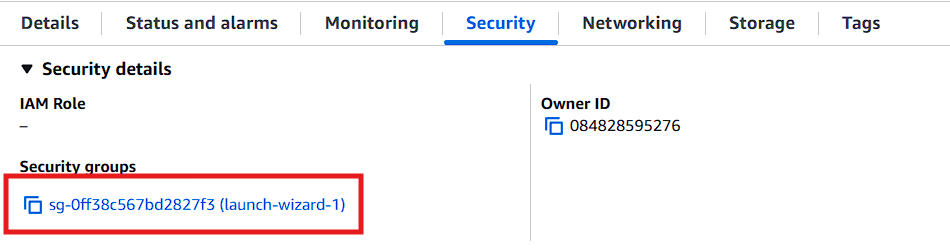
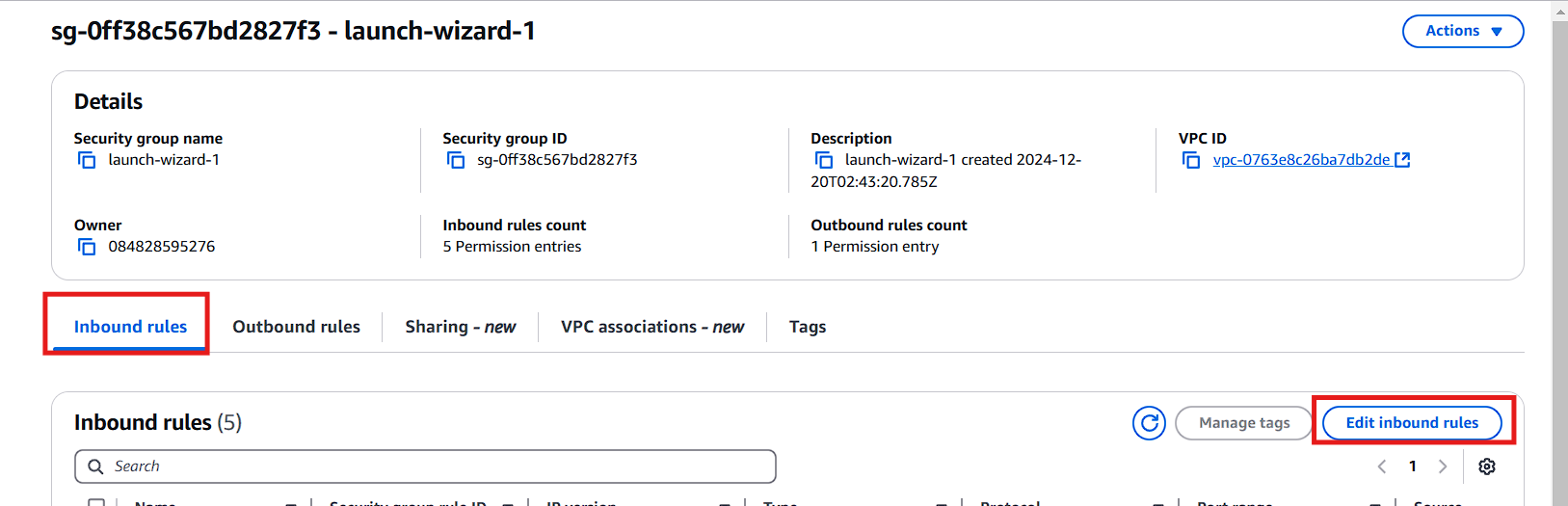
firewall-cmd --zone=public --add-service=http --permanent

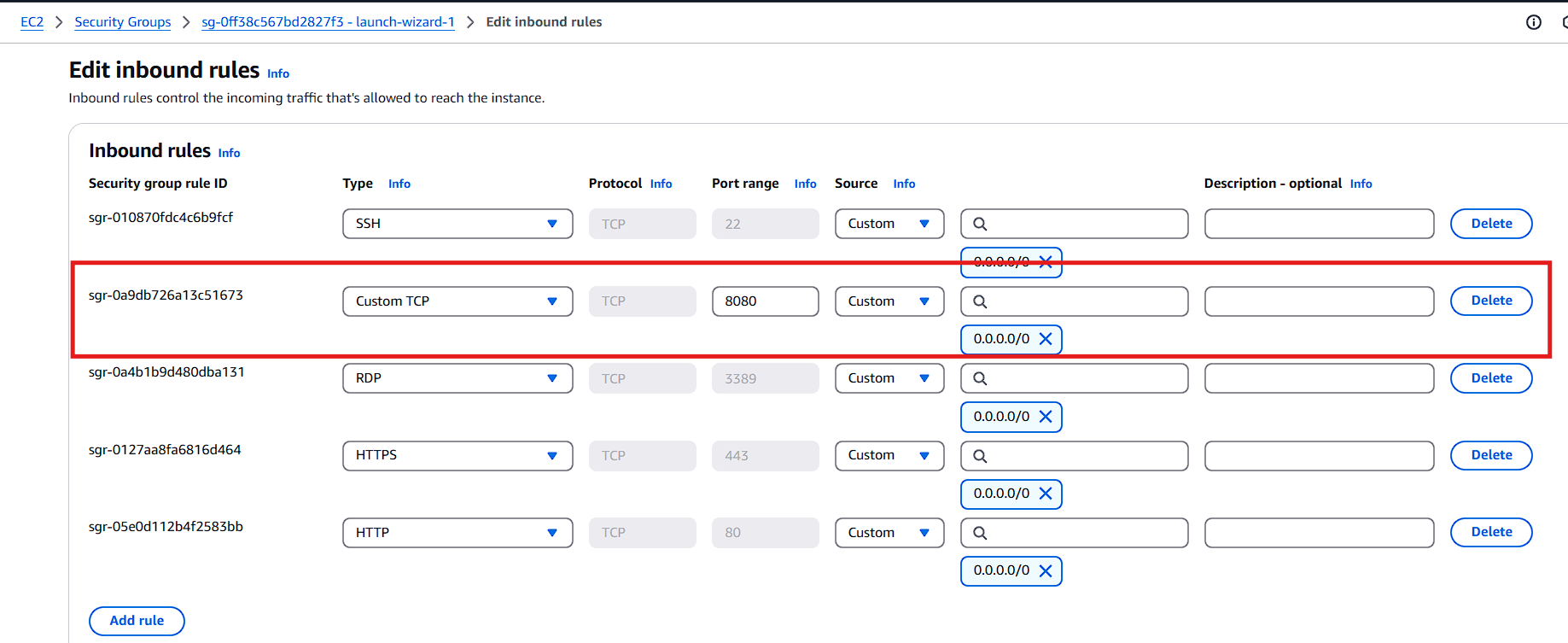
firewall-cmd --reload

firewall-cmd --list-all

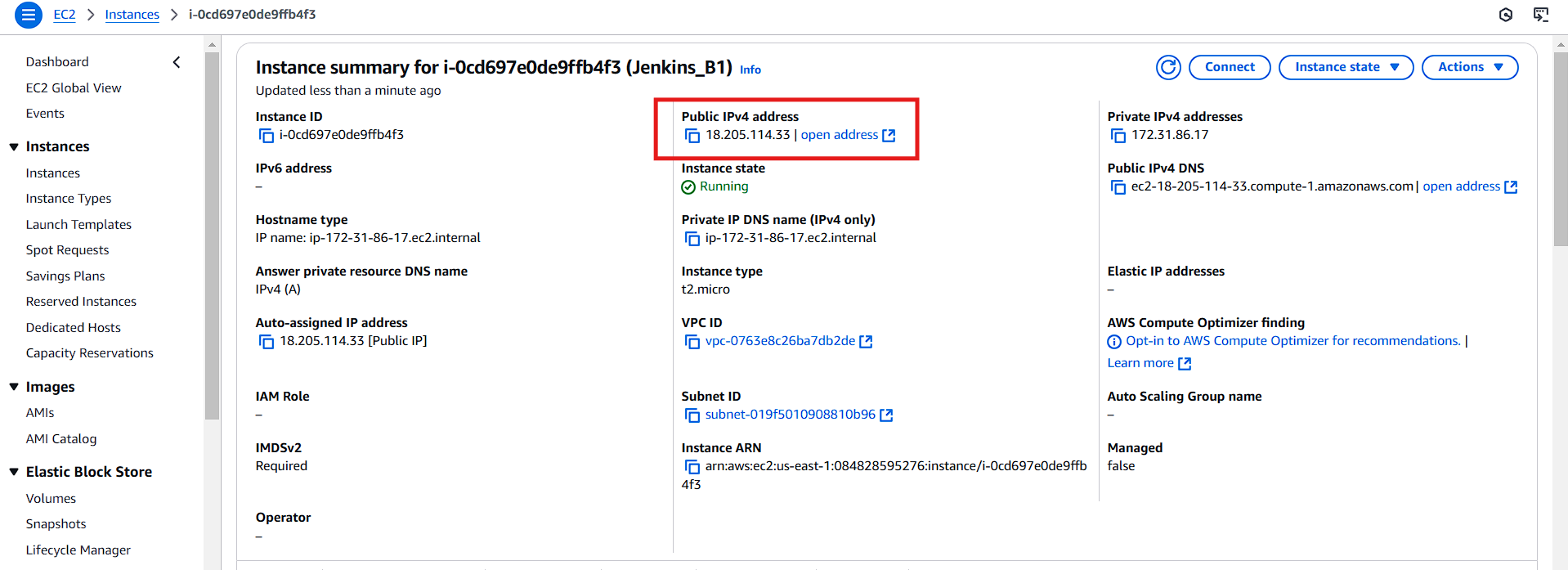
Go back to the EC2 Dashboard, select the Jenkins instance, and click on Security.

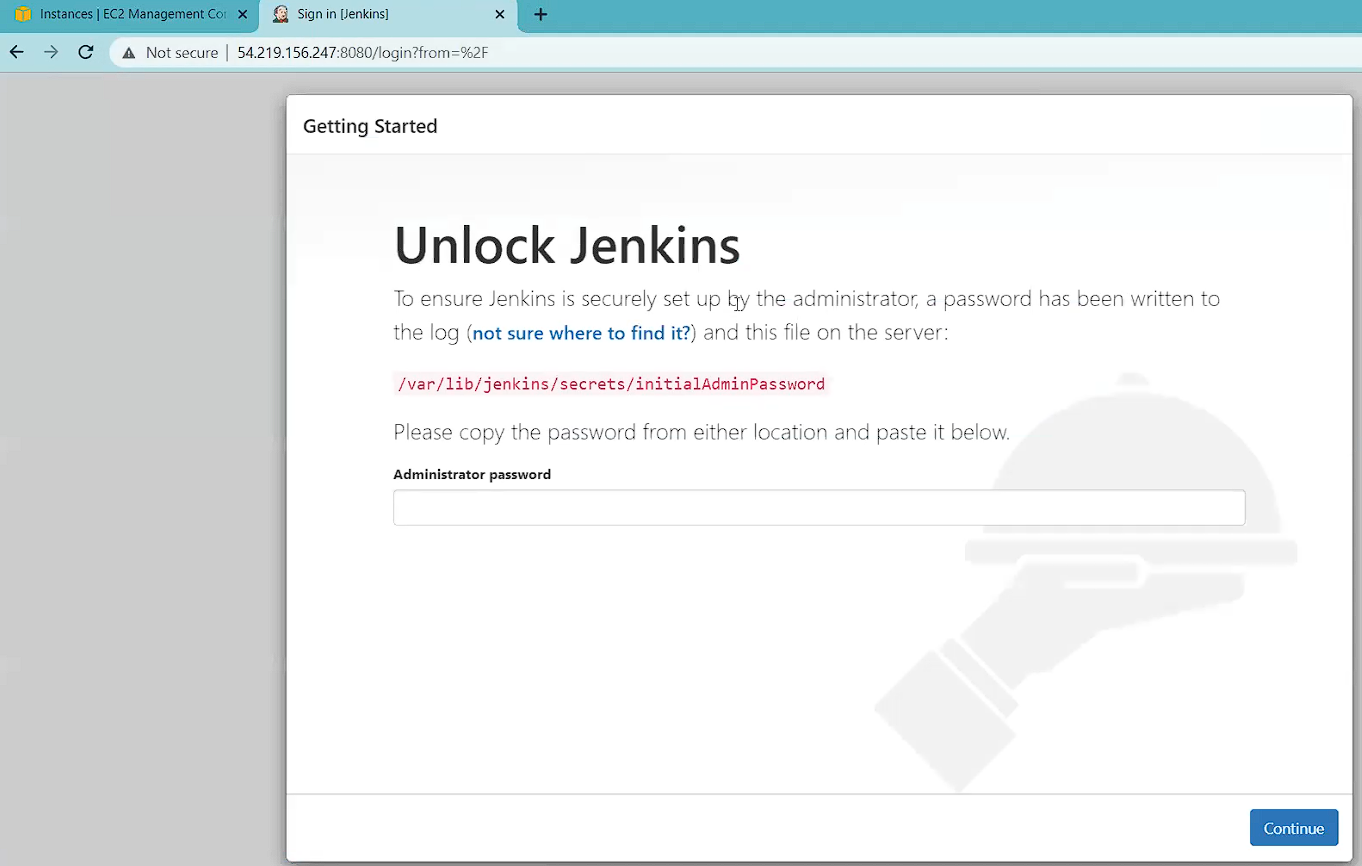
Choose the security group, click Inbound rules, and then Edit inbound rules.

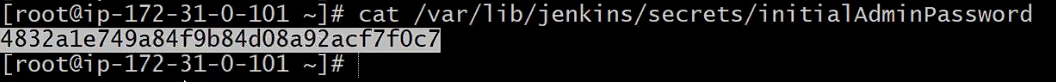
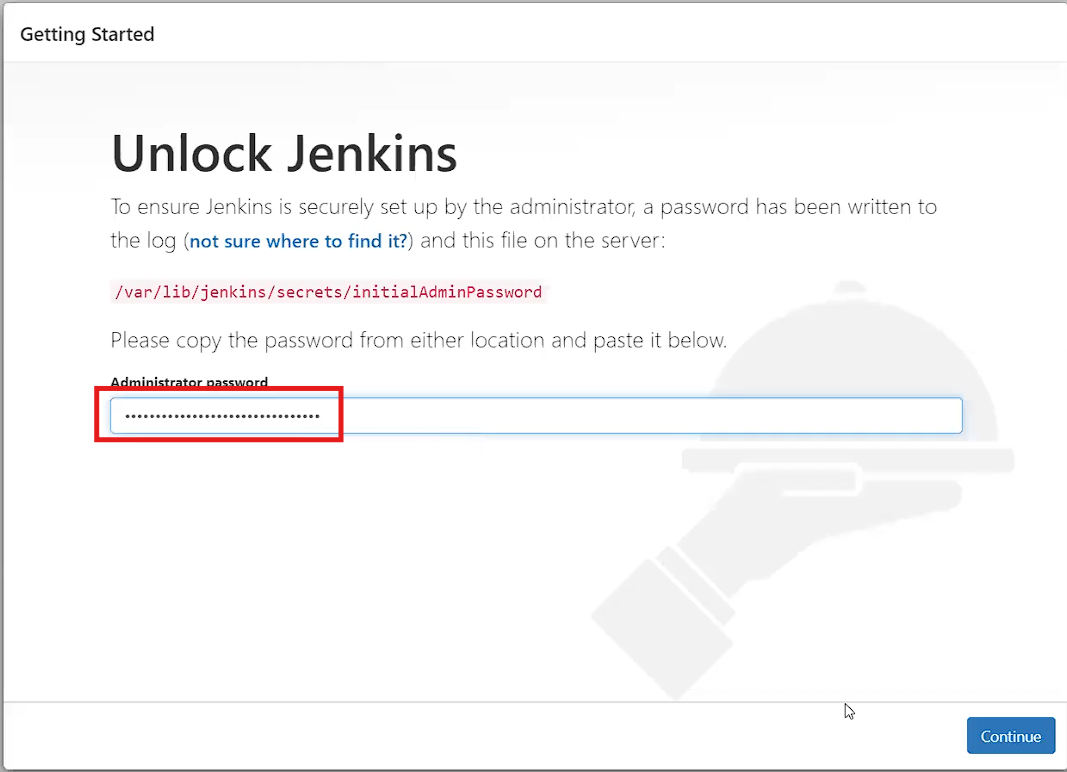
  
  


Add the necessary security rules as shown.  


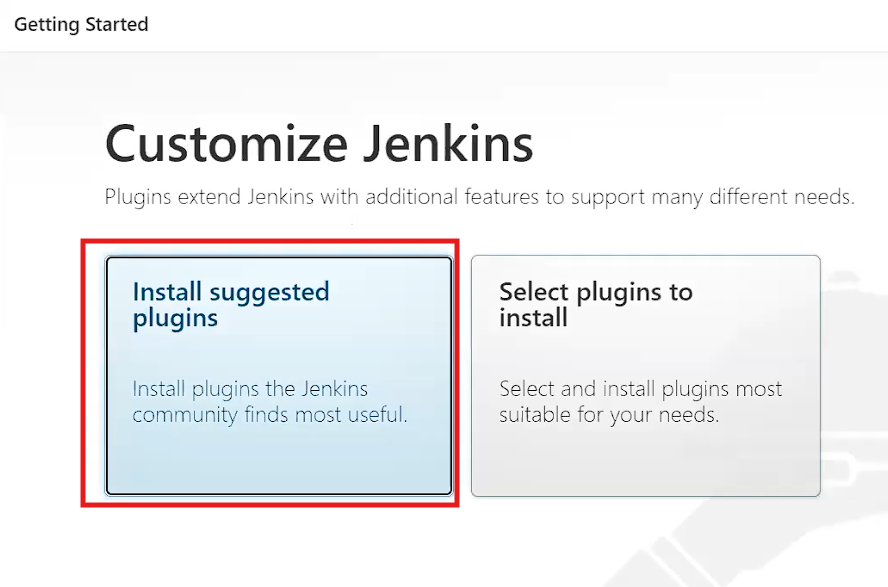
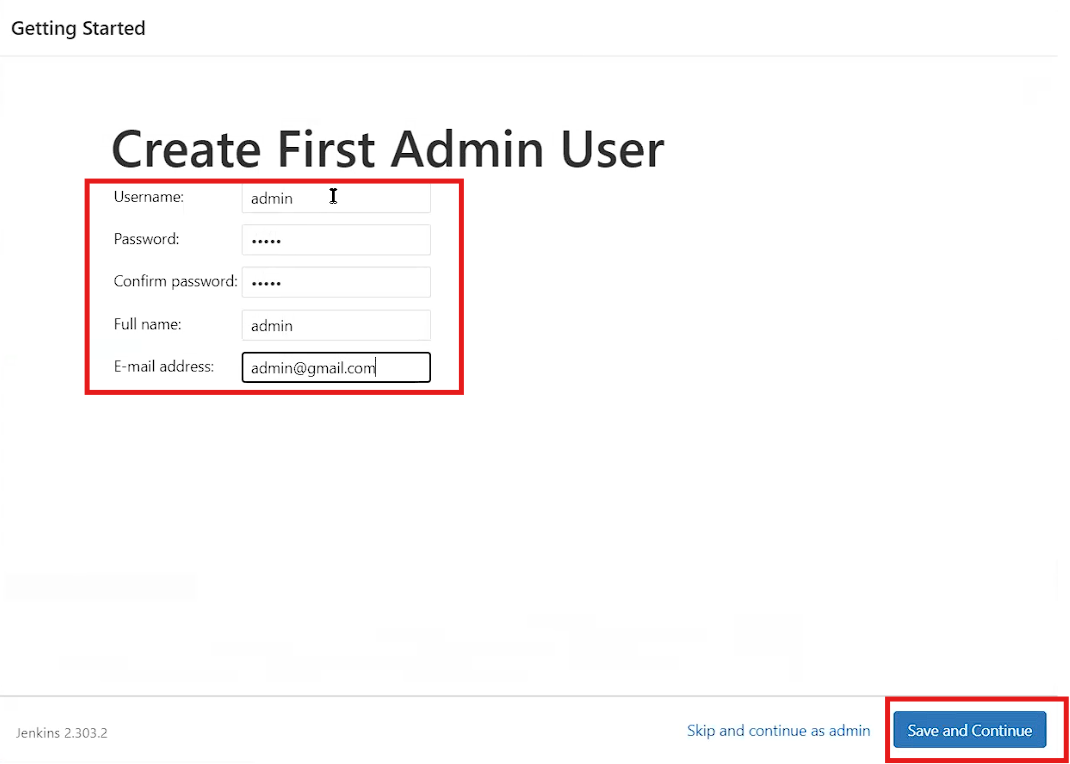
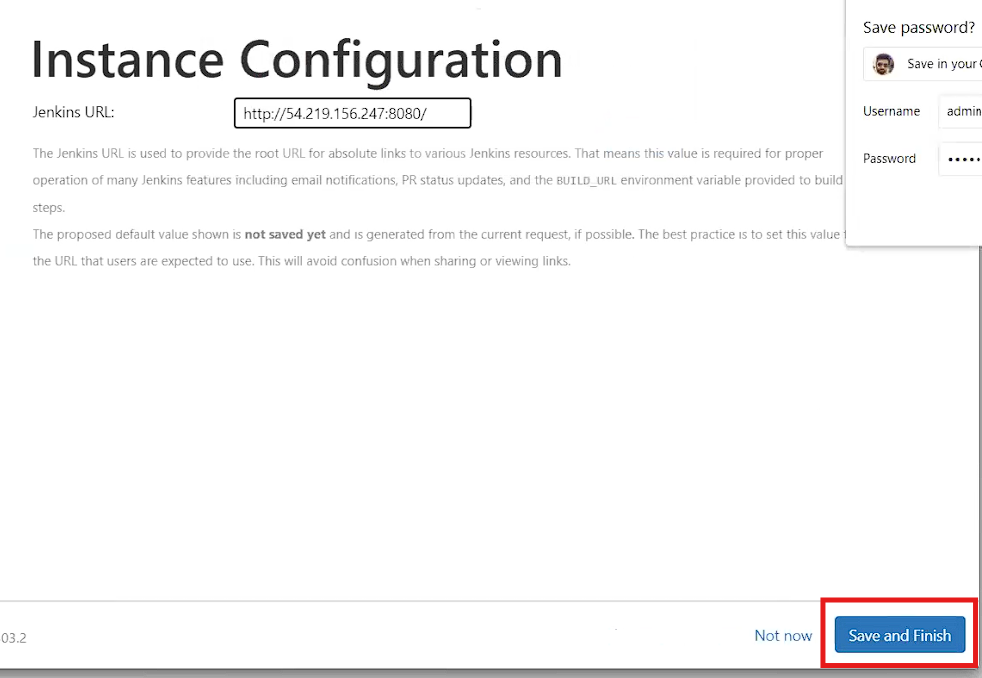
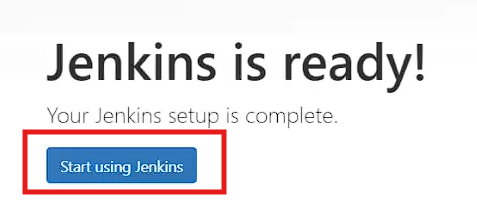
Copy the public IP address of the Jenkins instance.

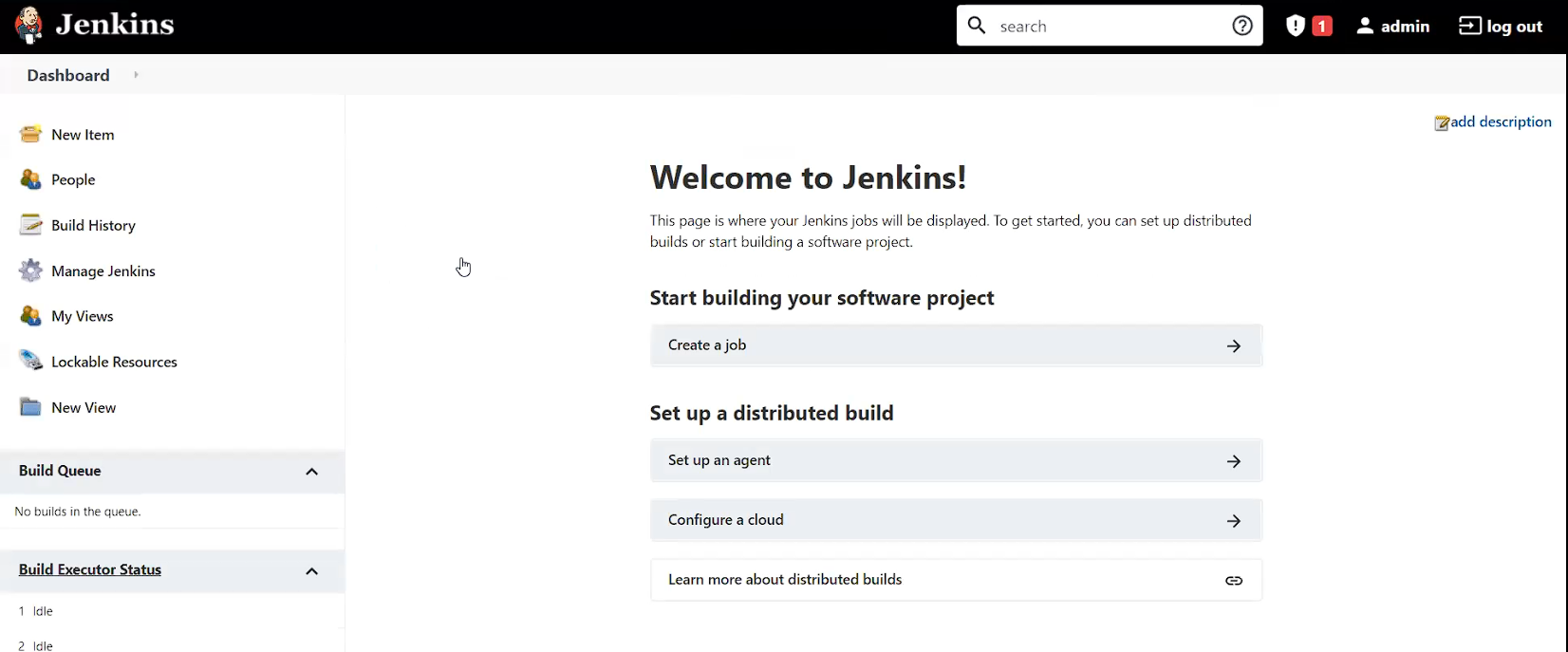
Open your browser and navigate to http://(public IP):8080.  




In Jenkins gitbash run the command to get the initial admin password  
  
  
  
Enter this password in the Jenkins setup page.  
  
  
  
  
  
  
  
Click on Install suggested plugins.

After the plugins are installed, create a user account by filling in the details and clicking Save and Continue.

Click Save and Finish.  
  
  
  
  
  
  
  
  
  
  


You will be directed to the Jenkins dashboard.  
  
  
**If the dashboard appears, you have successfully installed Jenkins, configured the firewall, and opened the necessary ports at both the server and EC2 levels.**