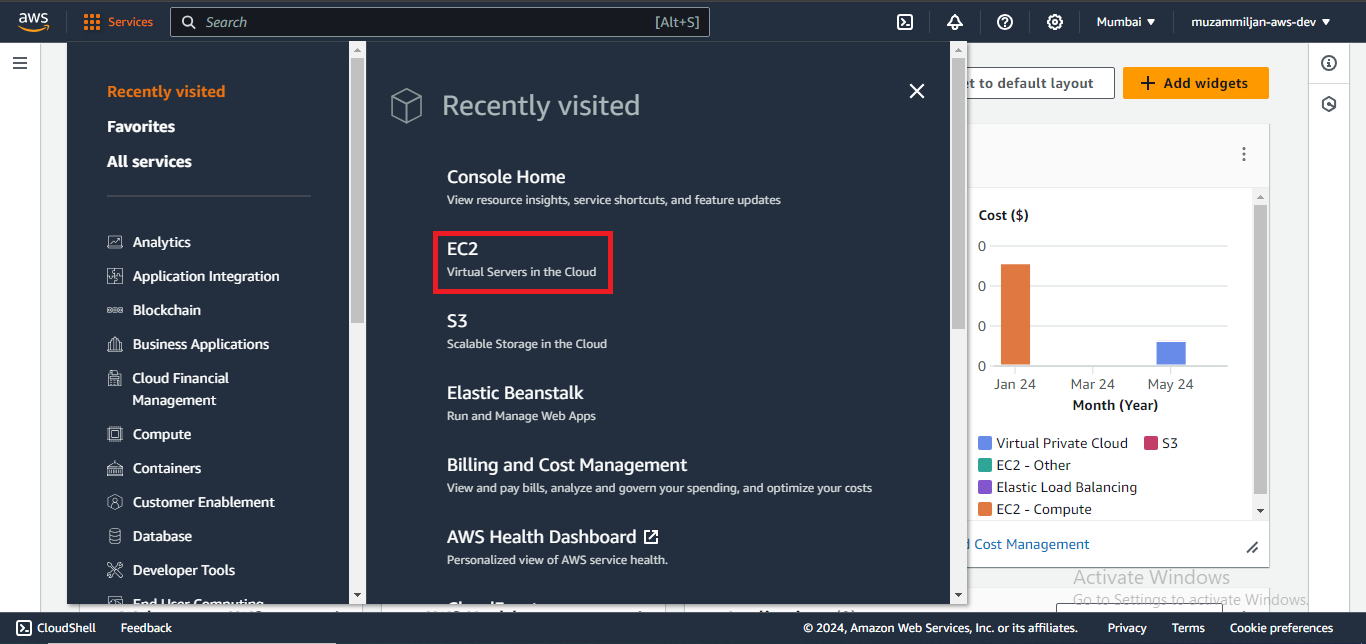


# **Executing Linux Commands with Hands-On AWS (Day 3)**

## **Ola**

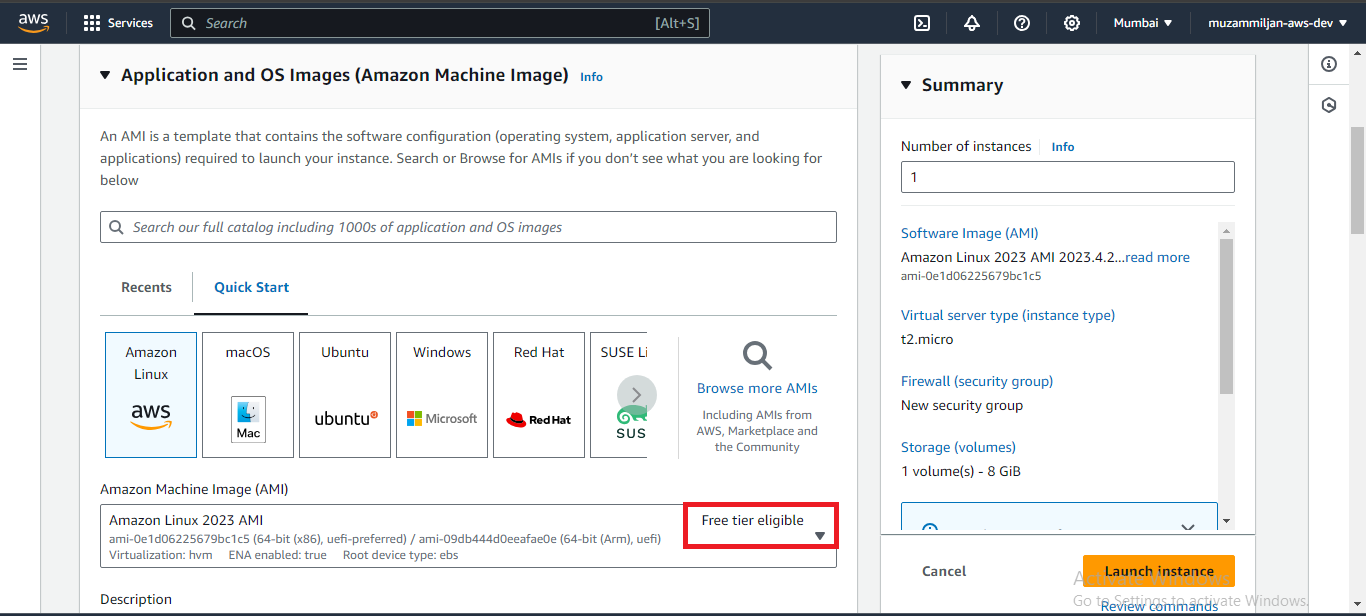
Cloud Engineer | DevOps | AWS | Linux

* Click on EC2 under Services and click on Launch Instance. A new webpage will open. Now give a name to your instance for your reference under the Name and tags heading.



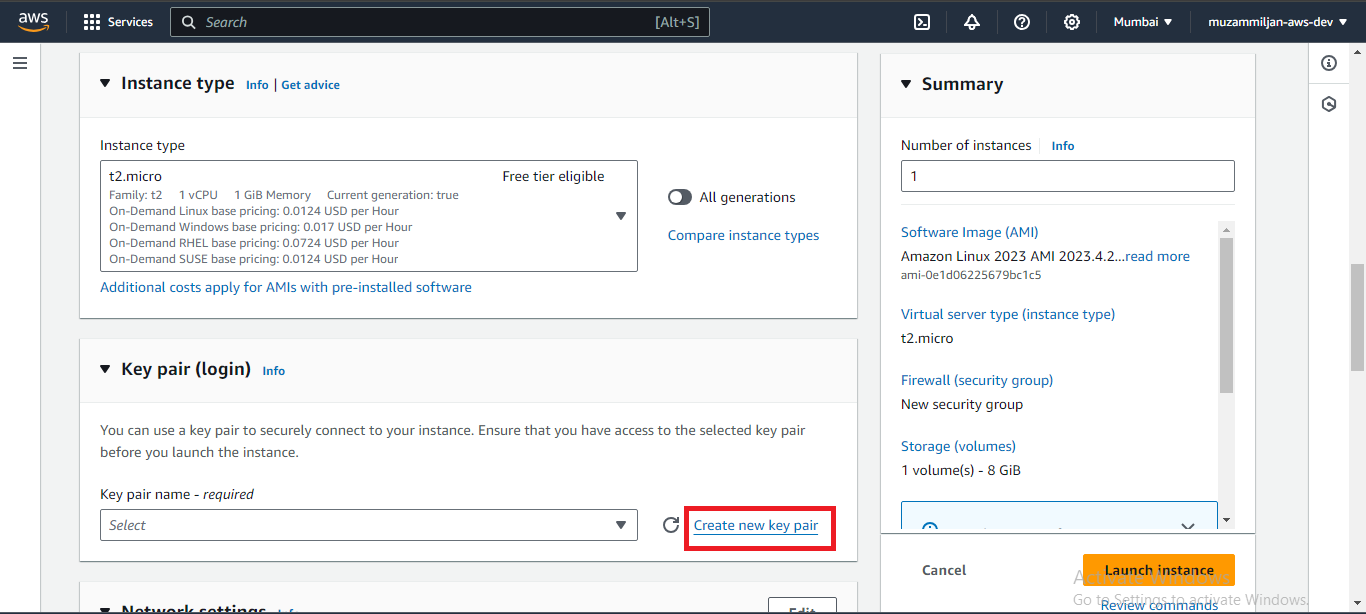
EC2

* Scroll down to Application and OS Images (Amazon Machine Image). Under Quick Start, select Amazon Linux and choose the AMI which is free tier eligible to try out this service free of charge.



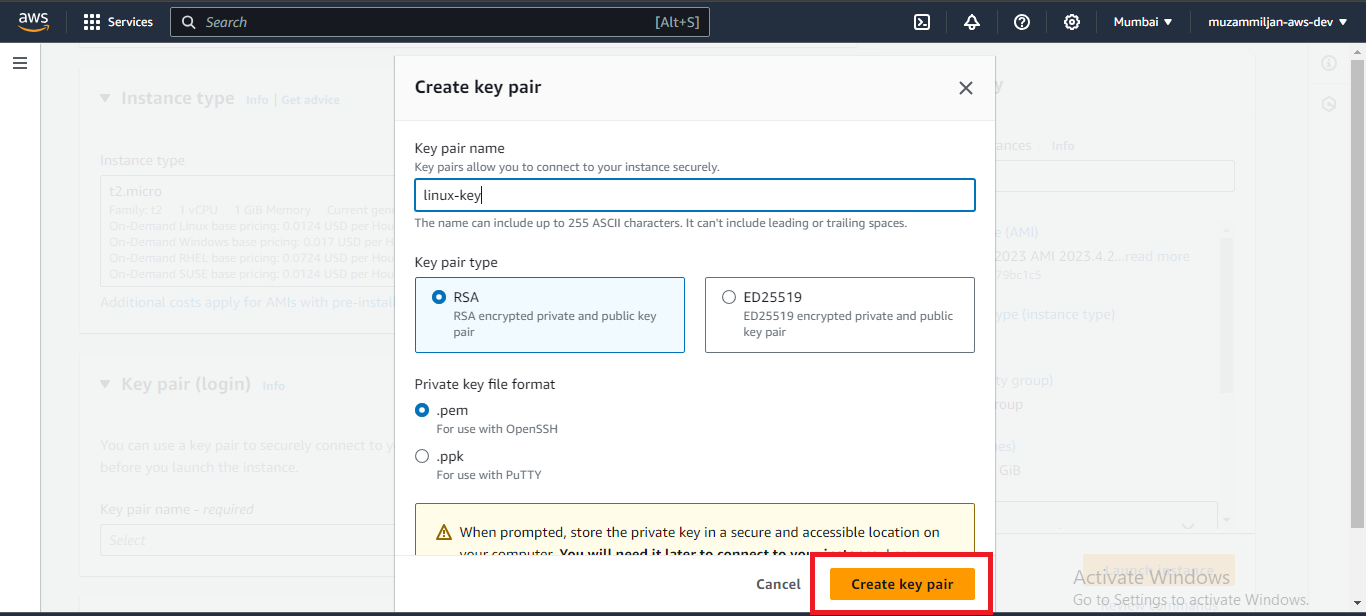
Free tier eligible

* Now move towards the Instance type and look for t2.micro. This instance type provides enough computing power to carry out the lab. Now create a new key pair for Key pair (login).



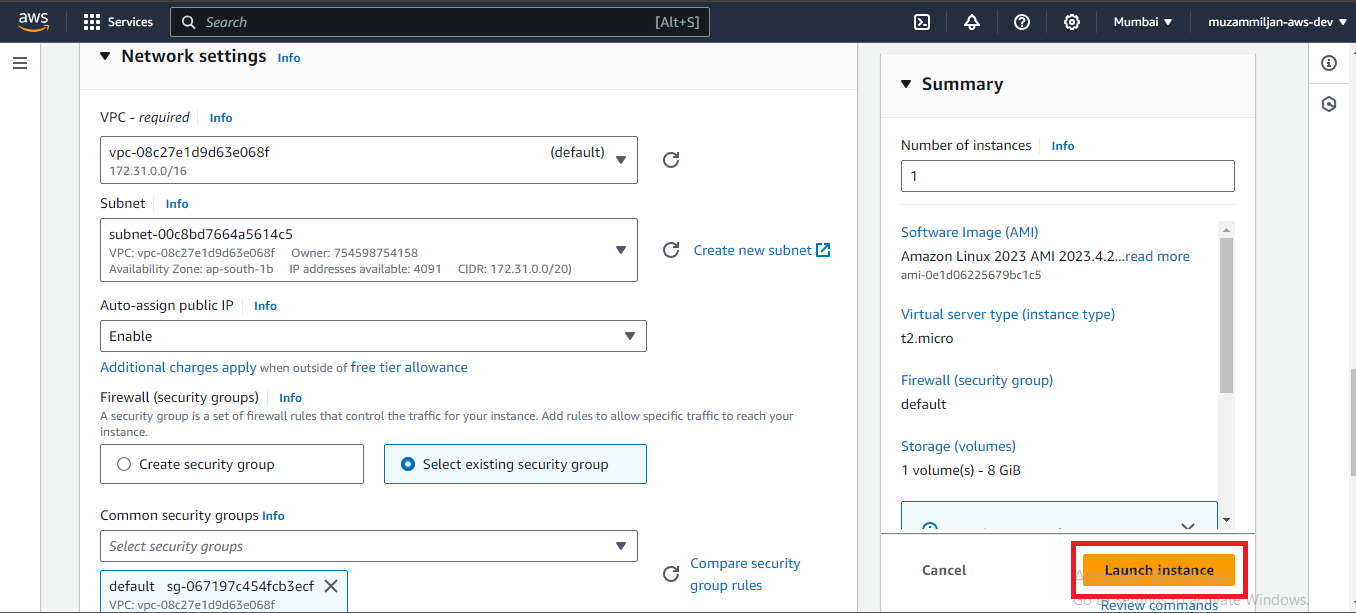
Create new key pair

* A new dialog box will appear. Enter a name for your key pair and select RSA to encrypt the public key as it is secure and based on the mathematical properties of large prime numbers, setting up a secure communication channel. Now select the .pem private key file format for secure transmission of cryptographic keys and click on Create key pair. A public key with a .pem extension will be downloaded to your computer.



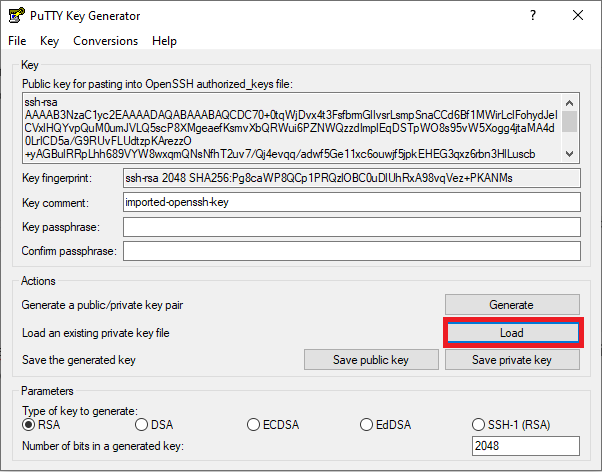
key pair type : RSA / Private Key file format: .pem

* Make sure that Auto-assign Public IP is enabled under the network settings for your instance to receive a public IP address automatically. Under Firewall and security groups, select an existing security group and choose the default VPC. Leave other settings and configurations to default and click on Launch Instance.



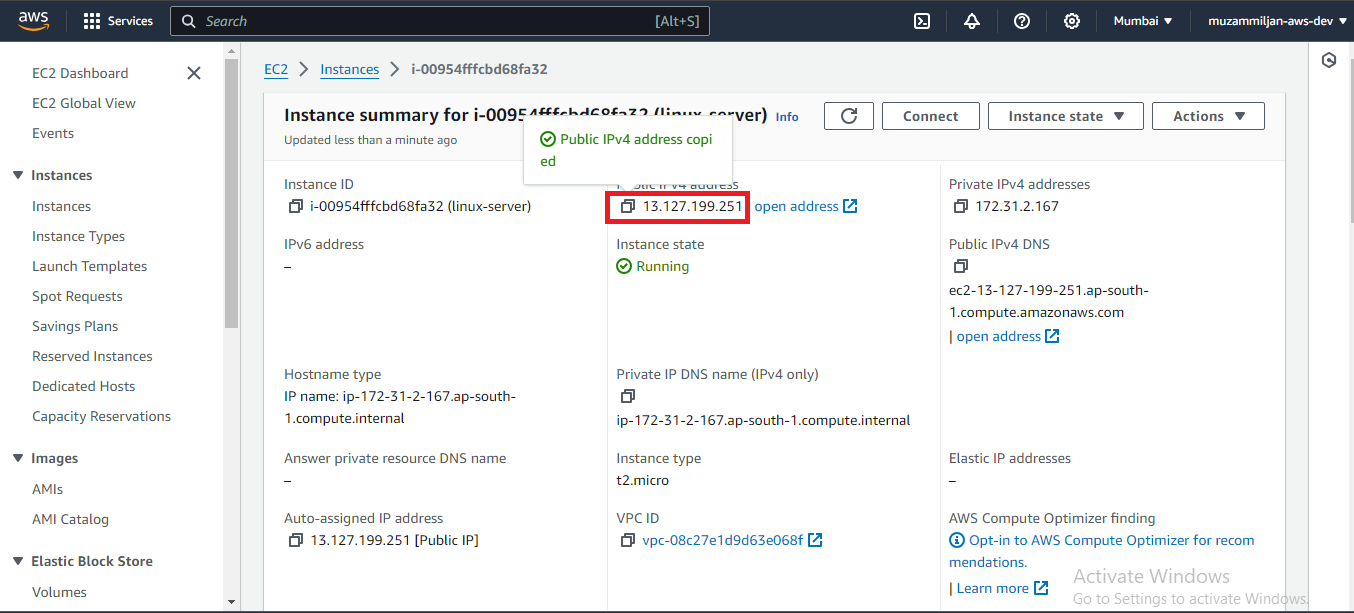
Auto Assign public ip enable

* Now open PuTTYgen and select RSA under the type of key to generate. Click on Load and select the .pem key that we generated earlier through the AWS key pair. If you cannot find your key pair, then select the file extension to All Files (\*.\*), click Open, and save the private key.



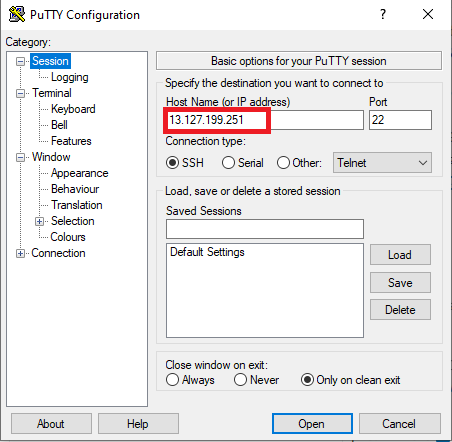
Load PuTTY Key Generator

* Go back to your AWS instance and click on the Instance ID. From there, copy the public IP address of your instance.



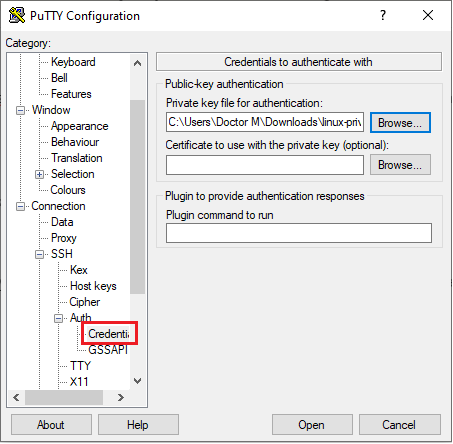
Copy Public ip adress

* Open PuTTY and paste the public IP address under the Host Name.



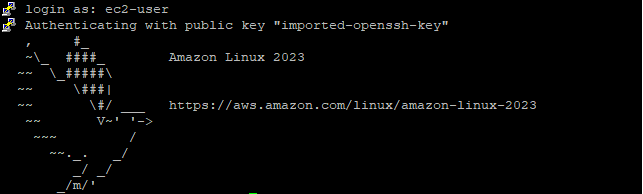
Paste public ip address

* Navigate to Category under the Connection settings and select SSH/Auth/Credentials. Attach the private key file for authentication and click Open.



attach private key

* A console version of PuTTY will open. Here, you can practice your Linux commands for today’s practical. Run your first command, ec2-user, to ensure you have the necessary permissions to configure and maintain your instance while using best practices for security and system administration.

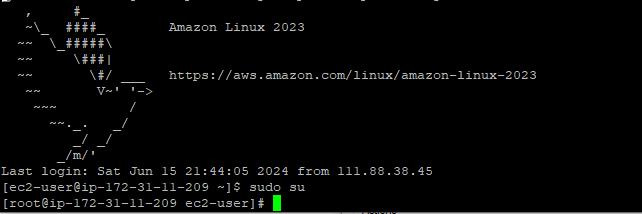


login as: ec2-user

### **Linux commands to Practice as a DevOps Engineer**

* grant's super user privileges and logs you in as the root user for the duration of your terminal session.

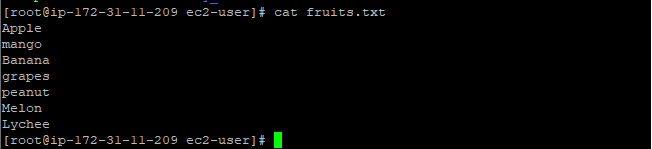
sudo su



sudo su

* To view what's written in a file.

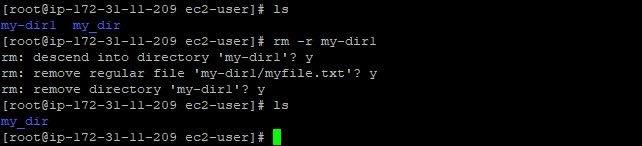
cat



cat

* To remove a directory/ Folder.

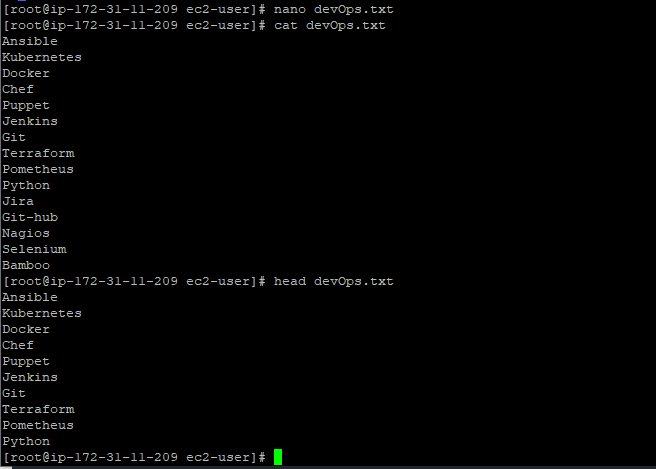
rm -r



rm -r

* To view top 10 lines of a file

head



head

* To view last 10 lines of a file

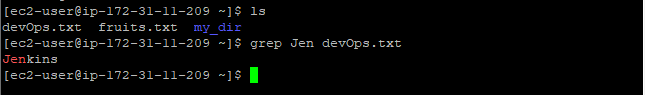
tail



tail

* To search for matching patterns in file

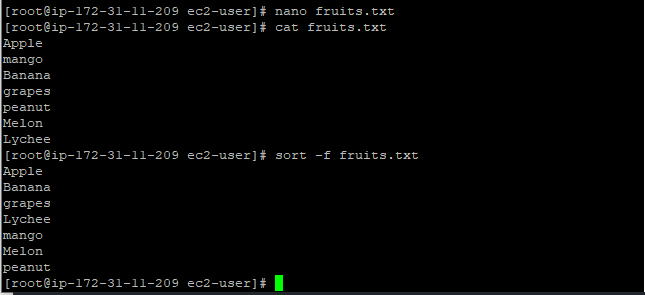
grep



grep command

* To Sort the lines in filename in a case-insensitive manner.

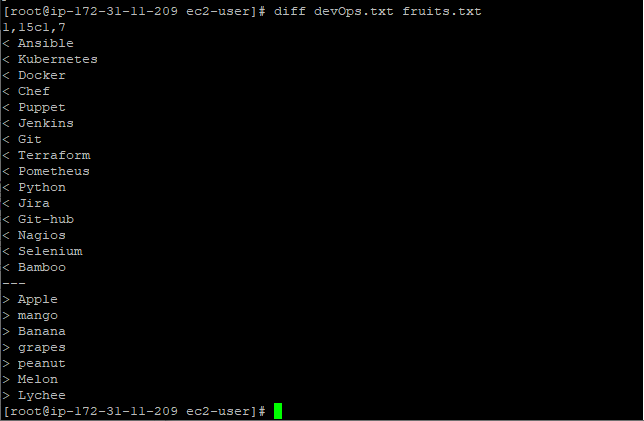
sort -f



sort -f output

* use to find the difference between two files

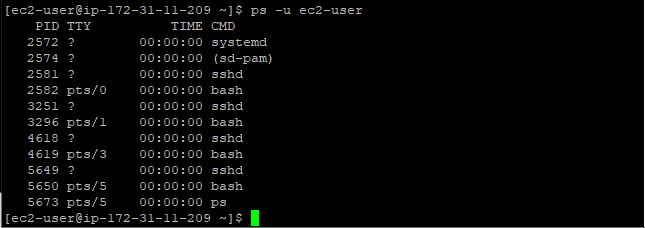
diff



diff command

* Display current processes.

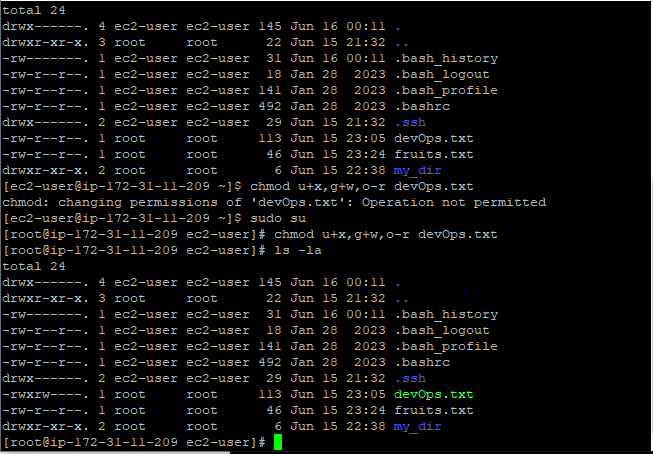
ps -u



ps command

* To change file permission for owner, group and others

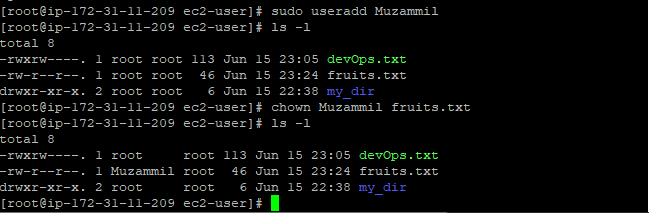
chmod



chmod

* To change the ownership of files

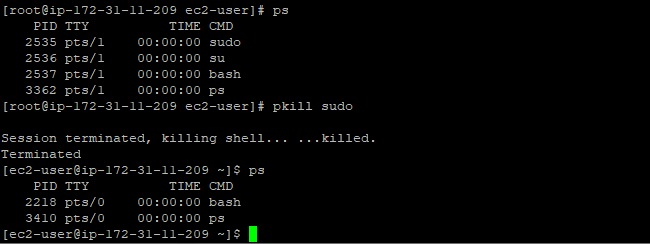
chown



chown

* Kill a process by name

pkill



pkill