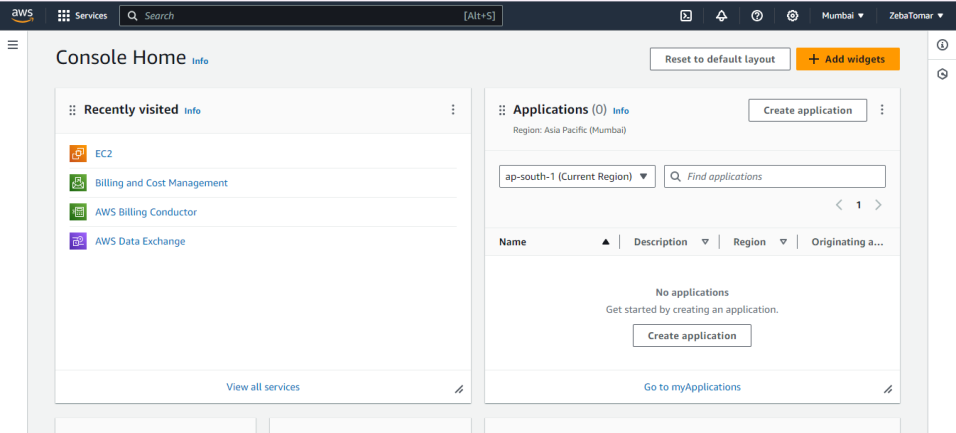
**Setting up an EC2 instance with a WireGuard VPN and configuring a client to connect to the server**

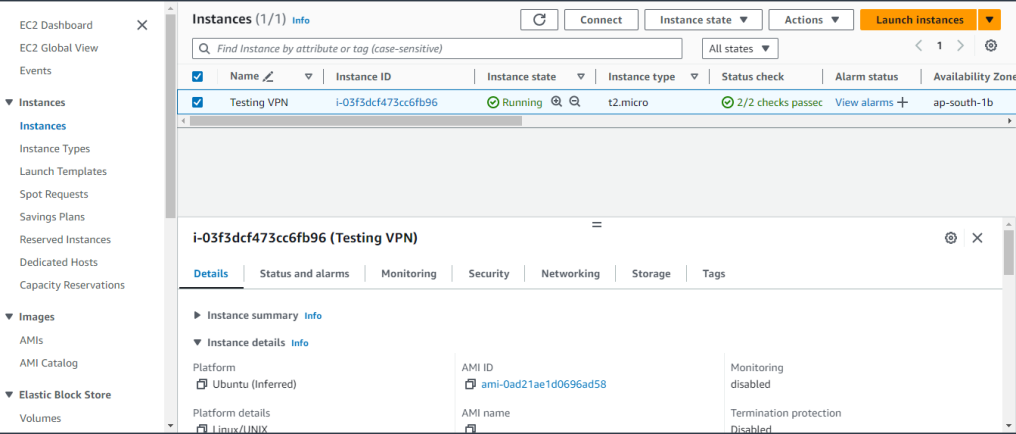
**Part 1: Launch and Configure the EC2 Instance**

**Step 1: Launch an EC2 Instance**

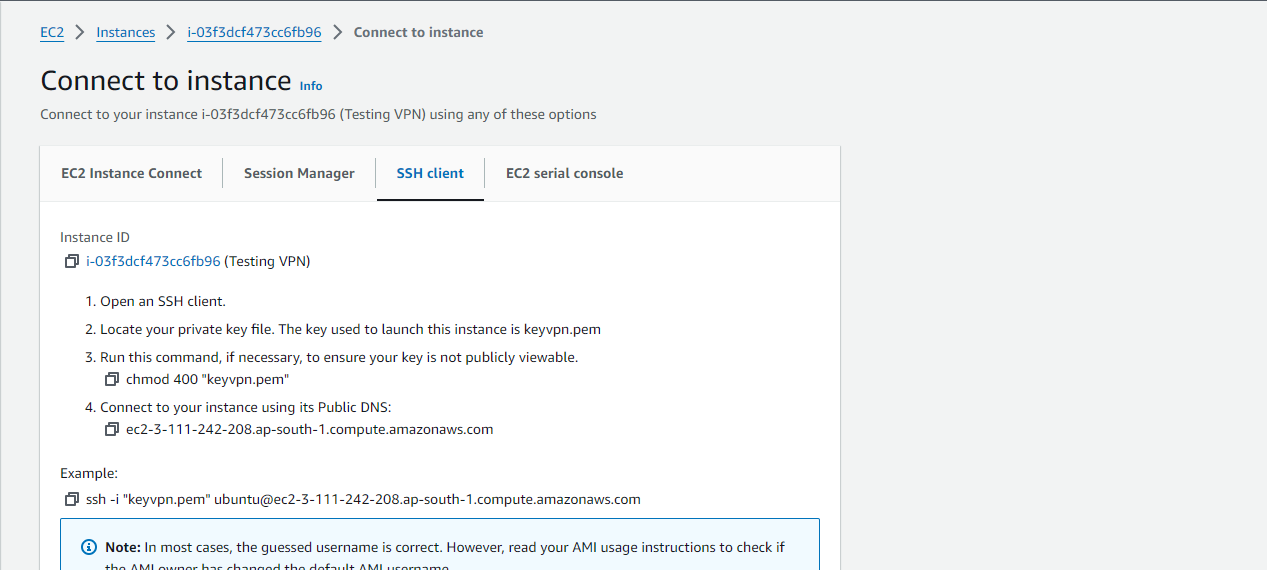
* Log in to AWS Management Console:
* Navigate to the [AWS Management Console](https://aws.amazon.com/console/) and log in.



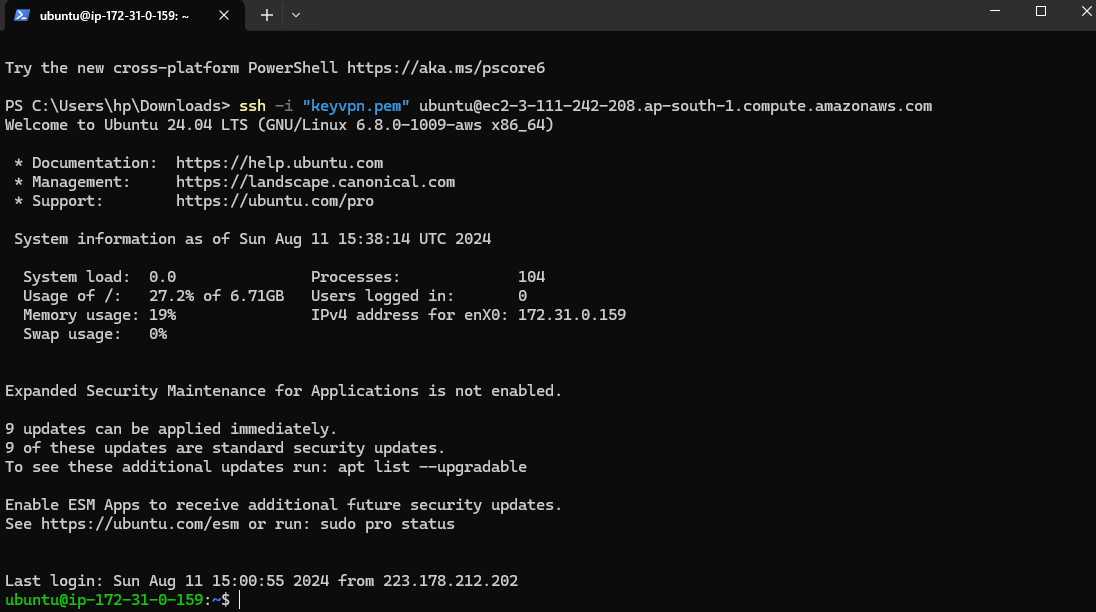
* Launch a New EC2 Instance:
* Go to the EC2 dashboard
* Click on “Launch Instance.”
* Choose an AMI: Select Ubuntu Server 24.04 LTS.
* Instance Type: Choose t2.micro (free tier eligible).
* Generate a new key pair.
* Configure Security Group: (Add a rule to allow SSH (port 22) for your IP).
* Launch a EC2 instance.



* Connect to the instance, copy the ssh key, and open the terminal to connect to the EC2 instance.

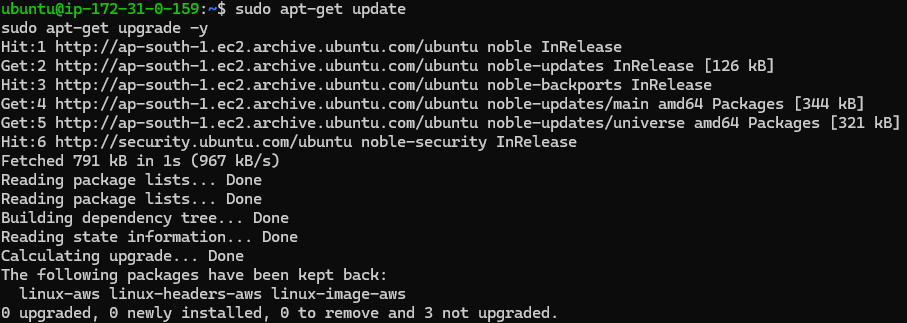


* EC2 instance is connected.

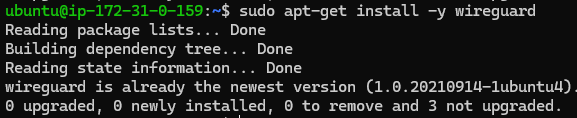


**Step 2: Install WireGuard on the EC2 Instance**

* Update the System:-Commands to update the package lists and upgrade installed packages
  + sudo apt-get update- (Updates the list of available packages and their versions.)
  + sudo apt-get upgrade –y (Upgrades all installed packages to their latest versions.)



* Install WireGuard:
  + sudo apt-get install -y wireguard-( Installs the specified package)

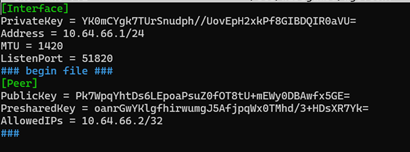


**Step 3: Configure WireGuard on the EC2 Instance**

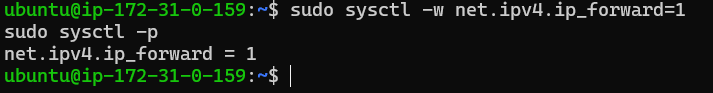
* Generate WireGuard Keys:
  + sudo mkdir -p /etc/wireguard (Creates the directory)
  + cd /etc/wireguard (change the directory)
  + umask 077- (Sets the file creation mode to ensure that the keys are only readable by the file owner.)
  + sudo wg genkey | sudo tee server\_private.key | sudo wg pubkey | sudo tee server\_public.key (Generate Wireguard key)
* Verify File permission
  + sudo ls -l /etc/wireguard/



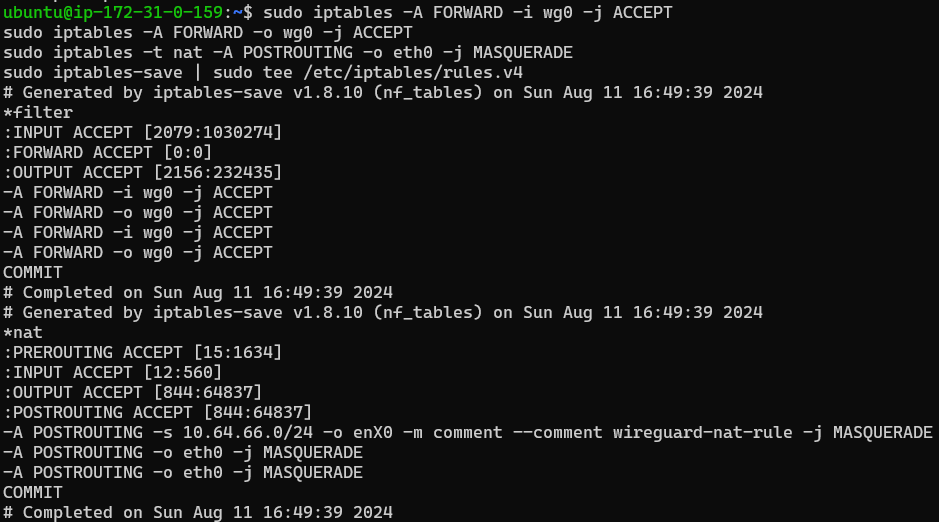
* Create the WireGuard Configuration File:
  + sudo nano /etc/wireguard/wg0.conf –(command open the file)



* Enable IP Forwarding:- to allow traffic to pass through server
* Enable the IP forwarding and loads the system configuration so that changes take effect immediately



* Set Up Firewall Rules:- Add firewall rules to allow traffic through the VPN



* Start and Enable WireGuard:
  + sudo systemctl start wg-quick@wg0 –(Start wireguard interface)
  + sudo systemctl enable wg-quick@wg0rrrr

Part 2: Configure the WireGuard Client

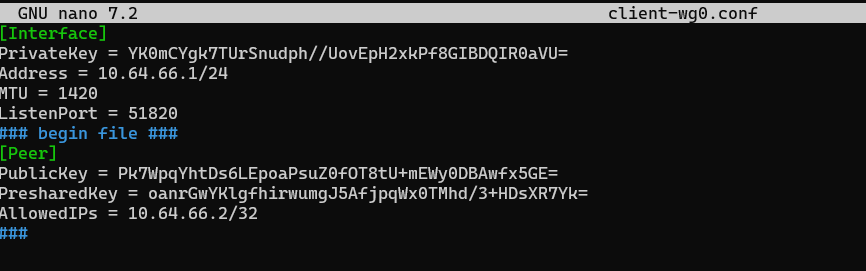
Step 4: Generate Client Keys

* Generate Keys on the Client Machine:



Step 5: Configure the WireGuard Client

* Create Client Configuration File:
  + nano client-wg0.conf



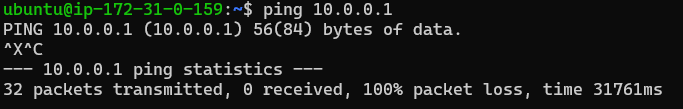
* Set Up the Client:
  + sudo cp client-wg0.conf /etc/wireguard/wg0.conf
  + sudo wg-quick up wg0

Part 3: Testing and Verification

Step 6: Test the Connection

* Ping the WireGuard Server:
  + ping 10.0.0.1





* Verify Internet Access Through VPN:
  + curl http://ifconfig.me



