**Setting Up OpenVPN on AWS**

## To Access EC2 instance private IP from the external network using VPN | AWS OpenVPN |manual installation of OpenVPN on your server.

# **Overview**

# This document offers a streamlined guide to deploying OpenVPN on Amazon Web Services (AWS). OpenVPN is strategically implemented on AWS EC2 instances, fostering a secure and encrypted conduit tailored for remote users. The configuration aims to facilitate secure access to EC2 instance private IPs from external networks through OpenVPN.

# **Prerequisites**

# The prerequisites required before starting the setup process:

- AWS account

- EC2 instance(s) for OpenVPN and test server resources

- Knowledge of OpenVPN concepts

# **Steps**

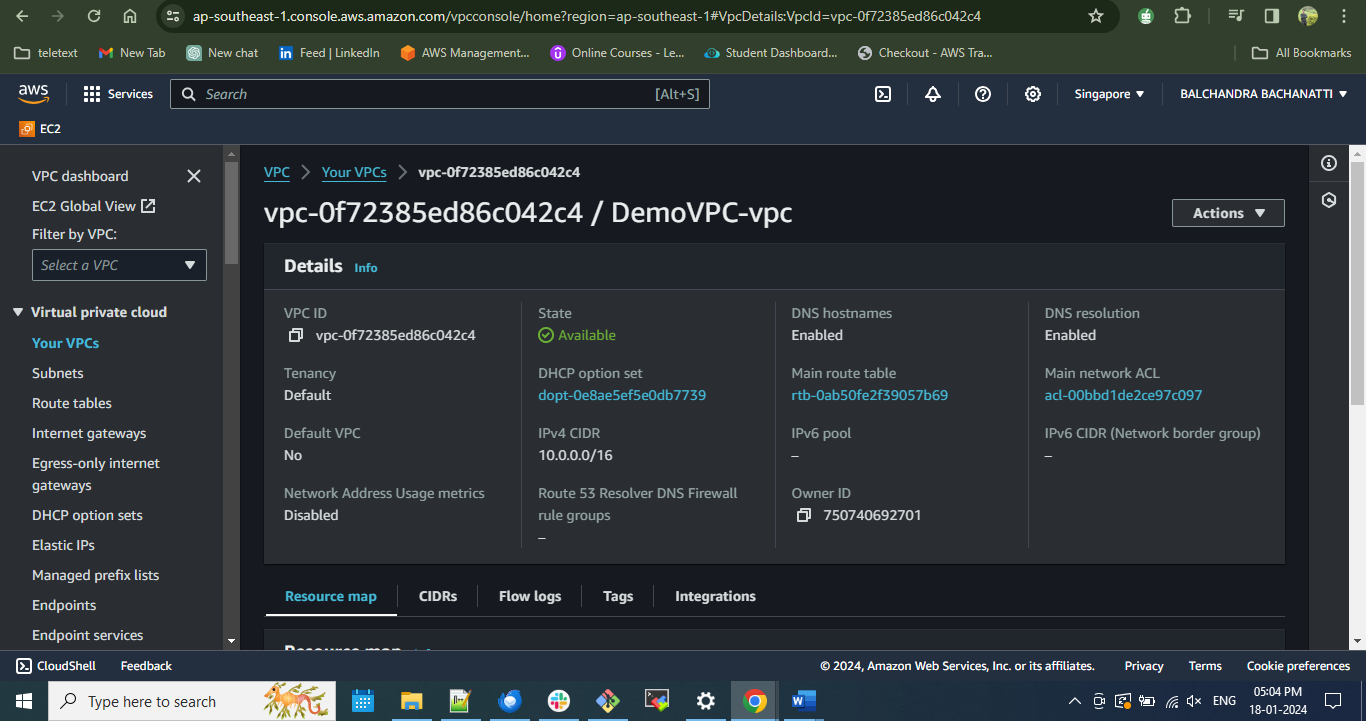
The step-by-step process involved in establishing a secure OpenVPN deployment on Amazon Web Services (AWS). The key stages include creating a Virtual Private Cloud (VPC), setting up the OpenVPN server on AWS EC2 instances to create a secure channel, configuring a test server, and performing verification steps to ensure the system's integrity.

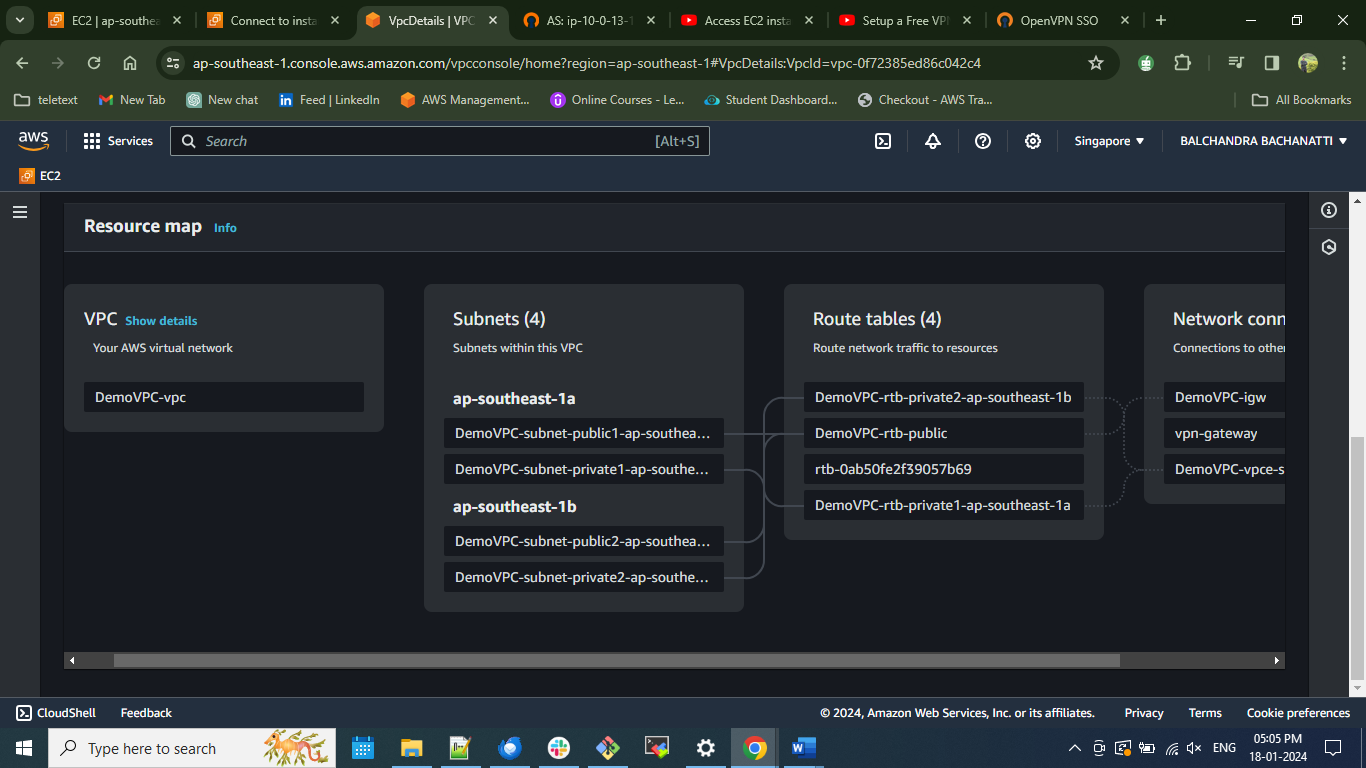
1. **VPC Creation and Configuration:**

* **Action:** Created a VPC resource and additional networking components.
* **Details:**
  + **VPC Resource Creation:** Established a Virtual Private Cloud (VPC) with specific configurations tailored to the requirements.
  + **Availability Zones (AZs):** Configured Availability Zones to ensure high availability and fault tolerance within the AWS infrastructure.
  + **Customized Subnets:** Defined private and public subnets within the VPC, strategically organizing resources based on security and accessibility needs.
  + **NAT Gateway:** Implemented a Network Address Translation (NAT) gateway to facilitate secure communication for instances in private subnets.
  + **Additional Networking Resources:** Configured various networking resources to optimize VPC functionality and enhance overall connectivity.

**Step 1.1: VPC Creation and Configuration**

*Screenshot:*





*Annotations: Established a VPC named DemoVPC, organized into two sets of private and public subnets with designated Availability Zones. Additionally, implemented a NAT Gateway to ensure secure communication within the private subnets.*

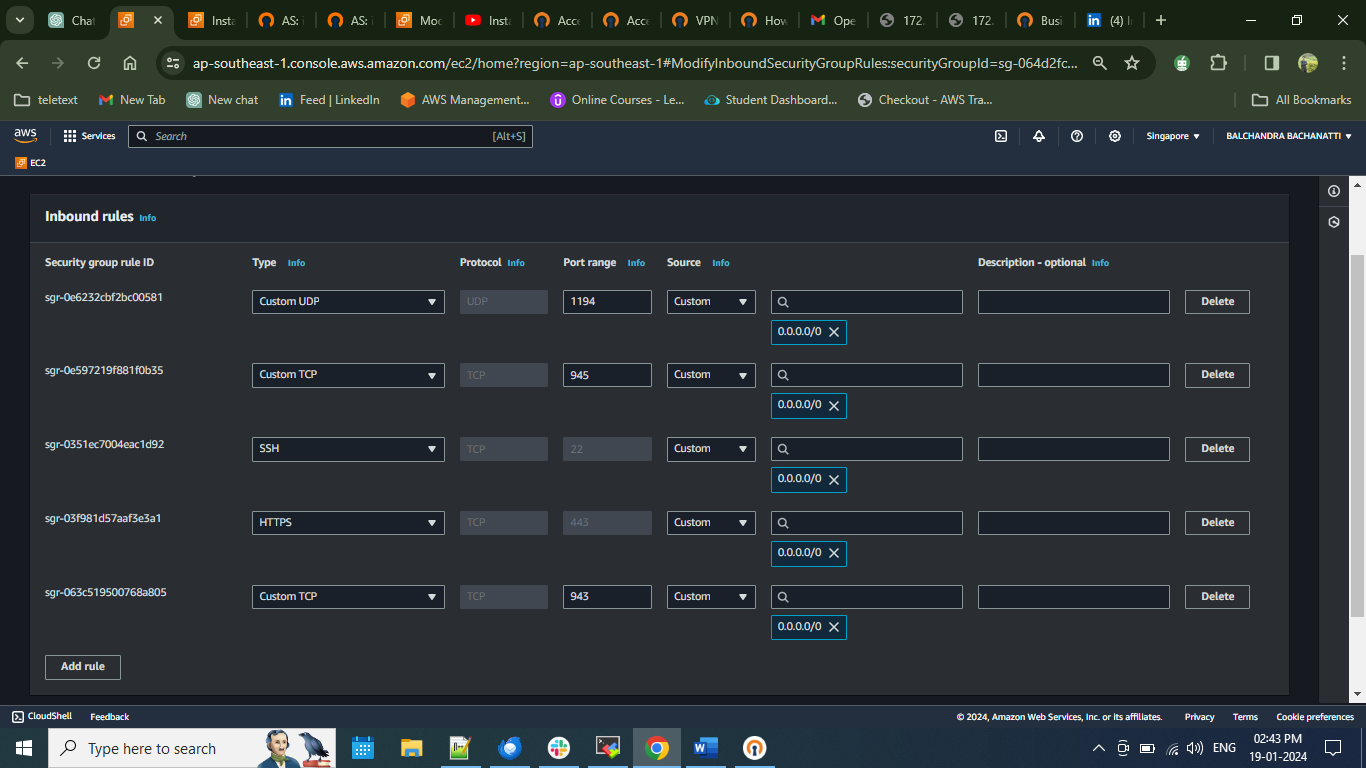
1. **To launch a new instance with OpenVPN Access Server software:**

* **Action:** Launched an Amazon EC2 instance using the AWS Marketplace AMIs with the OpenVPN Access Server.
* **Details:**

1. Select the **OpenVPN Access Server** listing in the AWS Marketplace and launch.
2. Configure the software with a 64-bit AMI, the latest version of Access Server, and your desired region.
3. Select your desired instance type. (Refer to [OpenVPN Access Server System Requirements](https://openvpn.net/vpn-server-resources/openvpn-access-server-system-requirements/) for details, if needed.)
4. Use our predefined access on ports and protocols for the security group.
5. Select a key pair for securely connecting to your instance (or click to create one).
6. You're ready to launch.

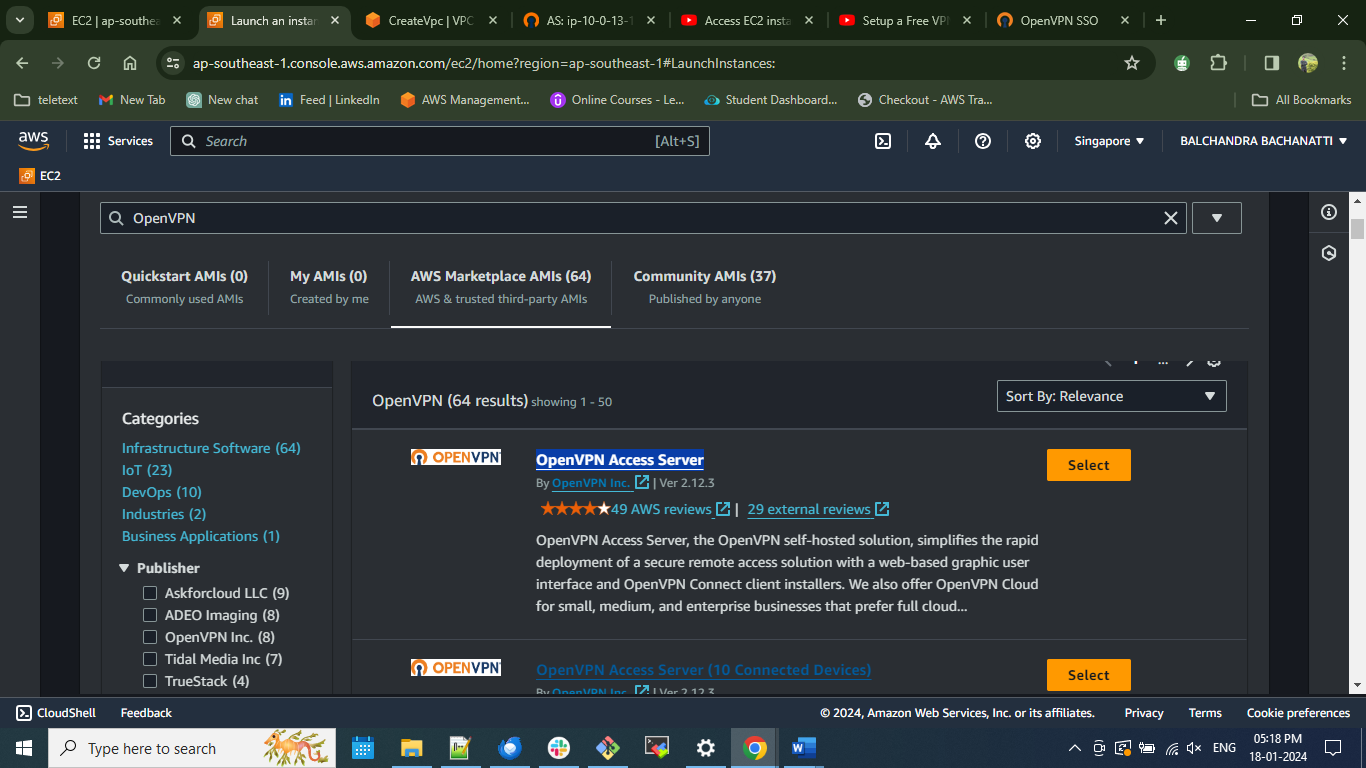
For the security group, using the default group for the marketplace instance but adjusting the sources for some ports to improve security these are the ports that need to be open:

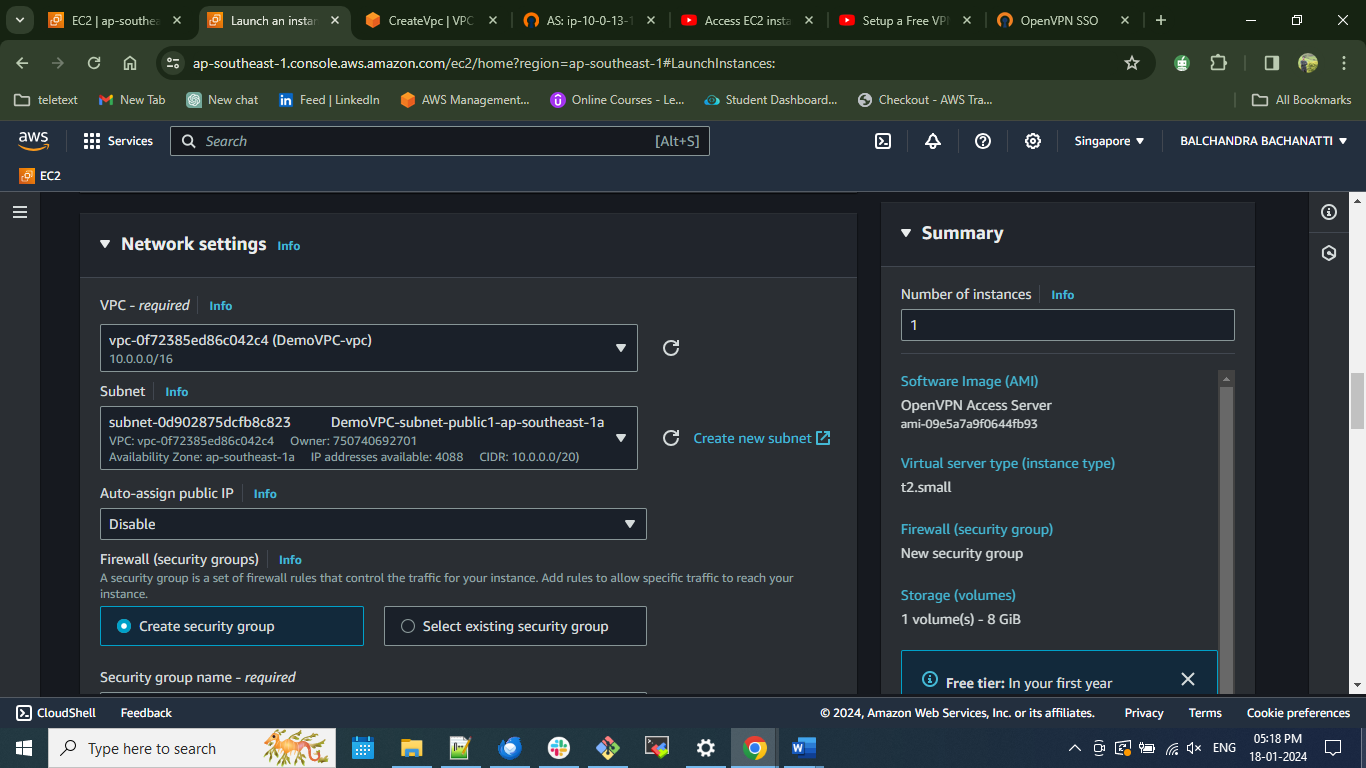
* **TCP 22:** For SSH to remotely administer your appliance.
* **TCP 943:** The Admin Web UI uses this port, which is also served on port **443** by default.
* **TCP 945:** The clustering functionality uses this port.
* **TCP 443:** For HTTPS, used by the Client Web UI, the interface where your users sign into the VPN server to retrieve client or config files leaving this port open to the source as 0.0.0.0/0.
* **UDP 1194:** For the OpenVPN UDP port used by your clients to initiate UDP-based VPN sessions to the VPN server, the preferred way for clients to communicate. Keep this port open for all clients.
* *Screenshot:*

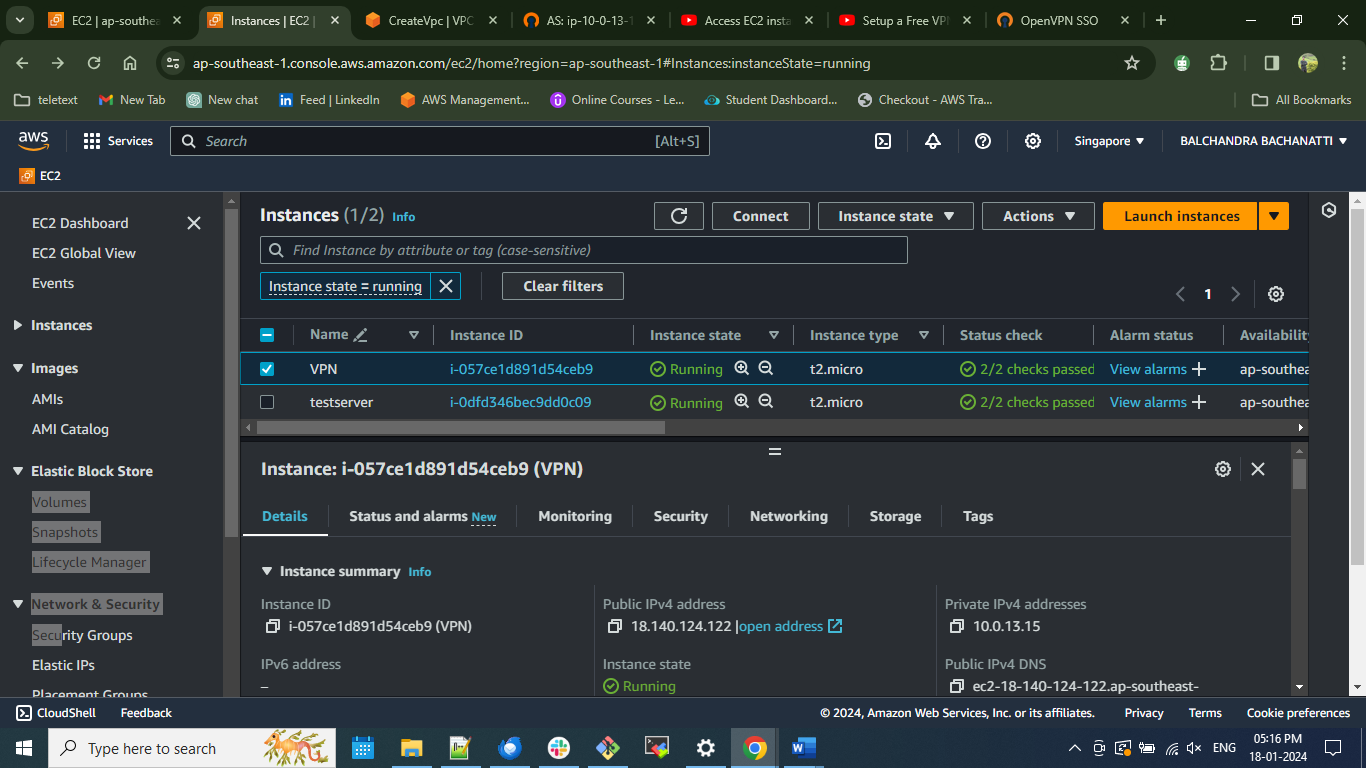


**Step 2.1: EC2 Instance Launch with OpenVPN Access Server:**

* *Screenshot:*

**

**

**

*Annotations: Established the OpenVPC using AMIs for OpenVPN, and modified the network settings, VPC, and security group configurations.*

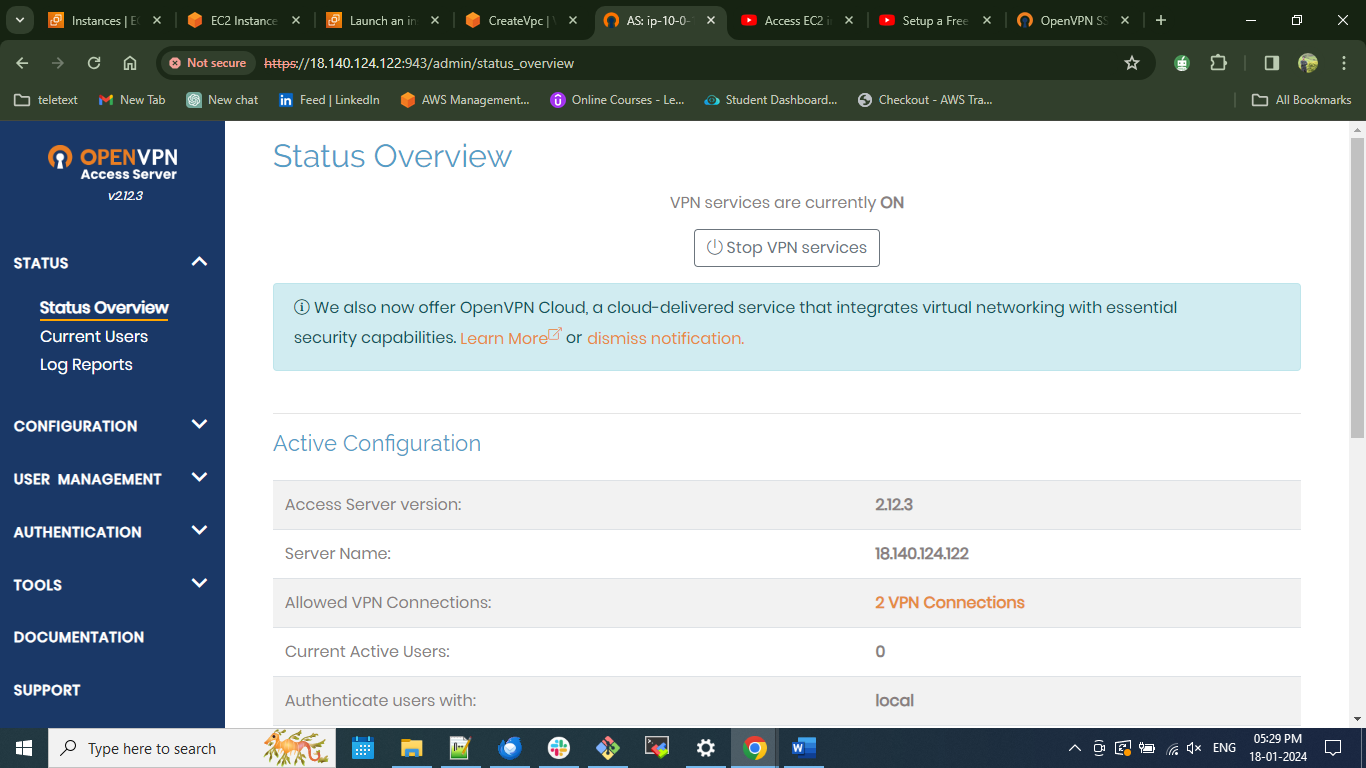
1. **SSH Access and OpenVPN Server Setup:**

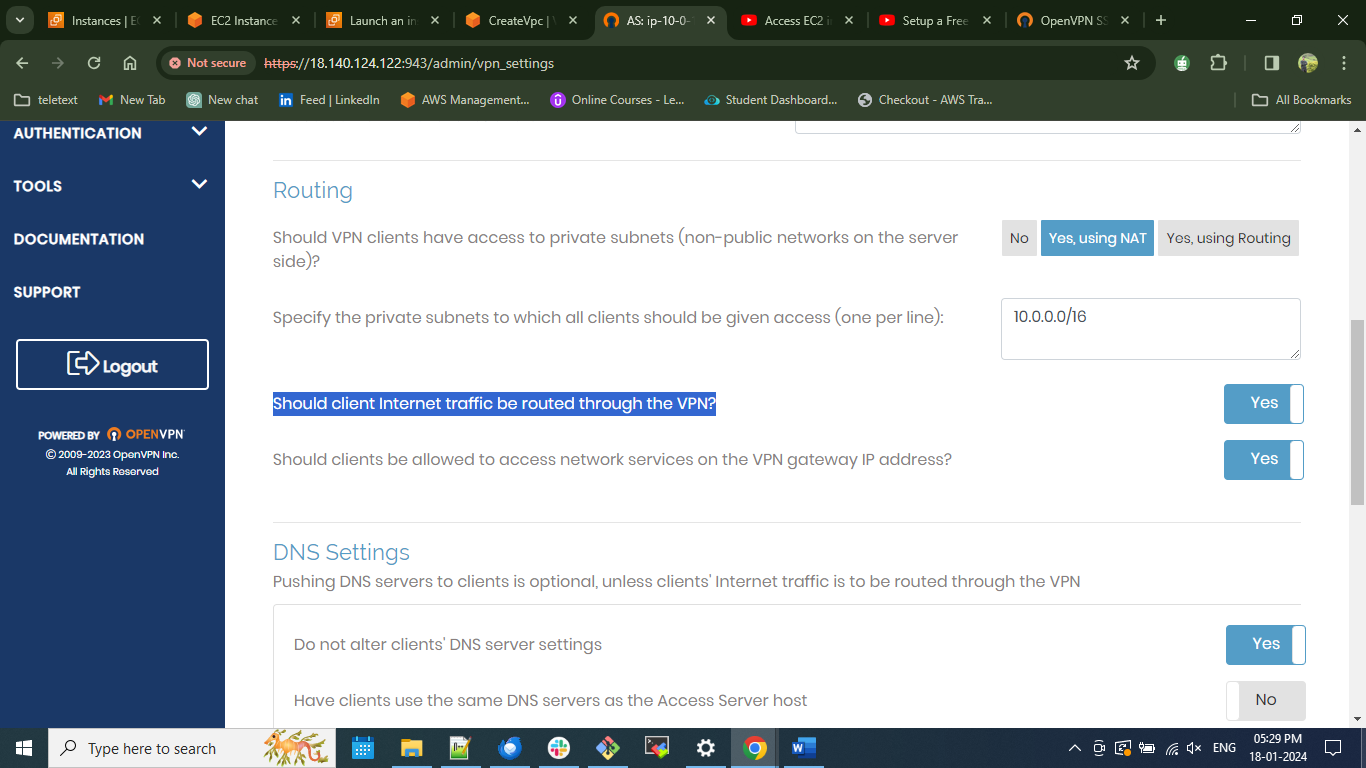
* **Action:** Accessed the EC2 instance securely through SSH and followed prescribed instructions to set up the OpenVPN server.
* **Details:**
  + **Secure Access:** Established a secure SSH connection to the EC2 instance.
  + **Configuration Steps:** Executed step-by-step instructions provided by the OpenVPN Access Server to:
    - Create VPN usernames and passwords for authorized user access.
    - Upon completion of the installation, access OpenVPN using the URL links generated during the installation process.
    - To log in, utilize the OpenVPN account credentials set during the initial setup.
    - Proceed to the admin panel to configure VPN settings. Enable the "Should client Internet traffic be routed through the VPN?" toggle under VPN settings, and set "Have clients use specific DNS servers" to "Yes." Save the settings and update the running server to apply the changes effectively.

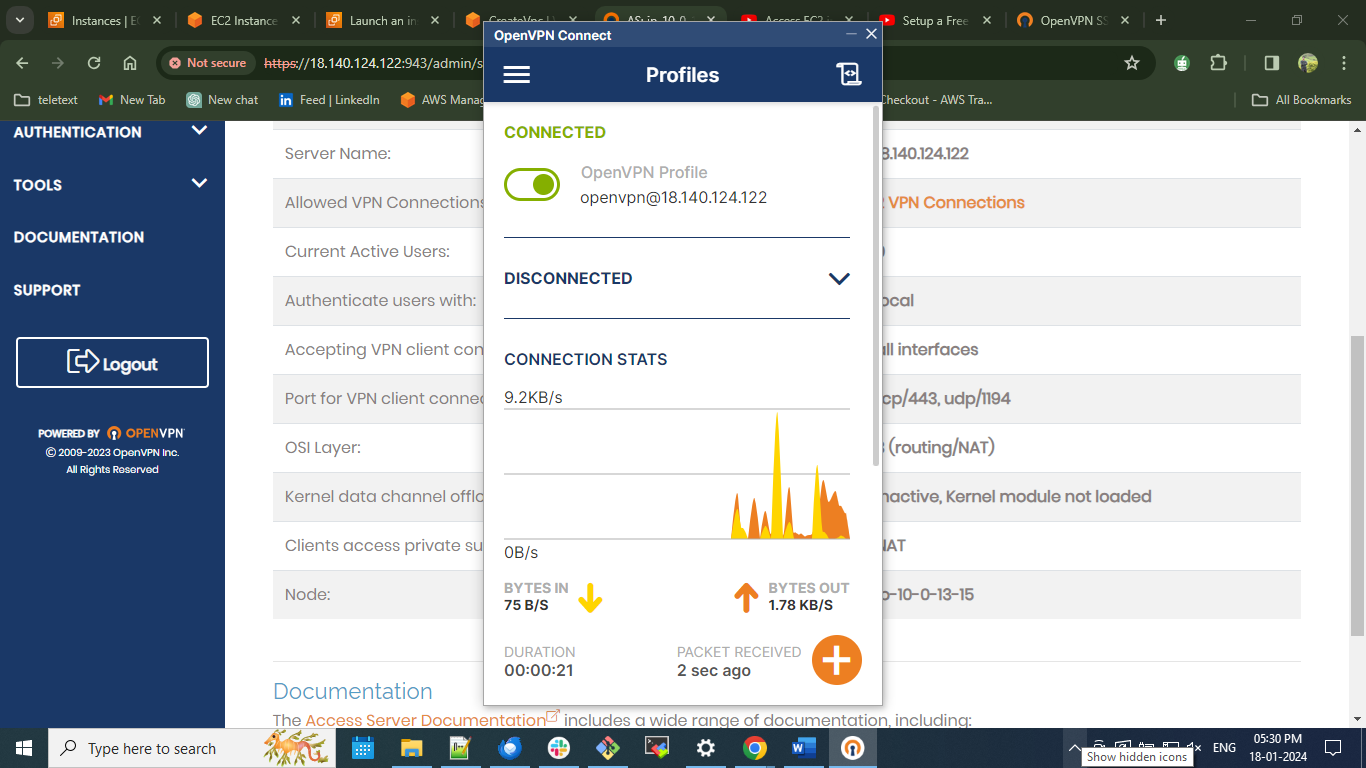
**4. Accessing VPN on Your Device**

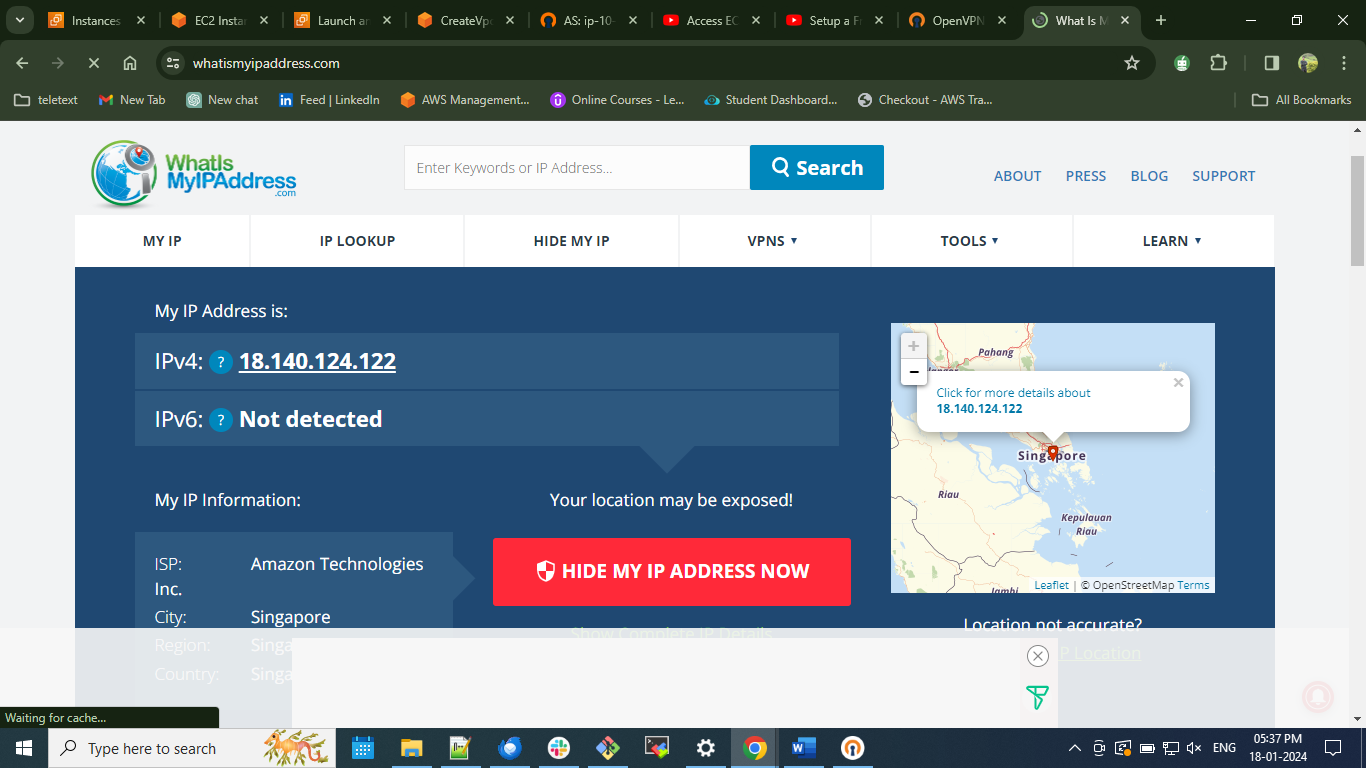
* To utilize the VPN on your device, follow these steps:
  + - Download the official OpenVPN Connect application from the official website and proceed with the installation.
    - Open the installed application and import the profile either via URL or by uploading the file.
    - Accept any prompts that appear and enter the VPN username and password configured during the setup.
    - Click the toggle to establish a connection.
* To verify its functionality:
  + - Open a web browser and search for "my IP address" to obtain your current public IP address.
    - Cross-verify this IP address with the one generated by the VPN to ensure a successful connection.
* **Step 3.1: SSH Access and OpenVPN Server Setup**

*Screenshot:*

**

**





*Annotations: 3. Successfully accessed the EC2 instance as an admin user through SSH, configured OpenVPN server settings, and established a successful connection on the device.*

**5. Post Successful VPN Connection - Creating a Test Server**

Following a successful VPN connection, proceed to create a test server to access an EC2 instance's private IP from an external network using OpenVPN.

Steps:

1. Launch an EC2 instance and configure the instance type, making adjustments in the network settings. Edit the VPC settings, selecting the same VPC created during the VPN installation.

2. Create a security group and add the private IP address of the VPN server. Disable the public IP address to ensure connectivity to the server is exclusively through OpenVPN.

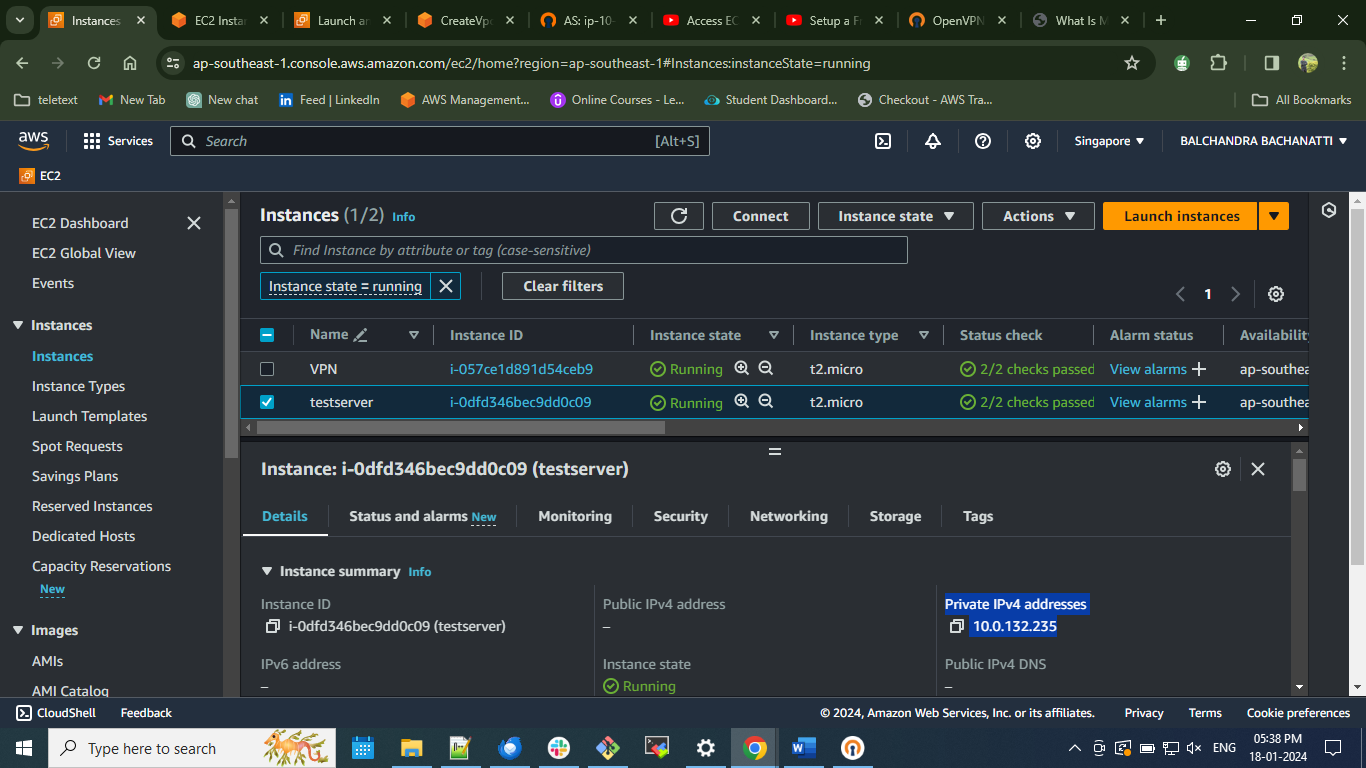
3. Launch the configured instance.

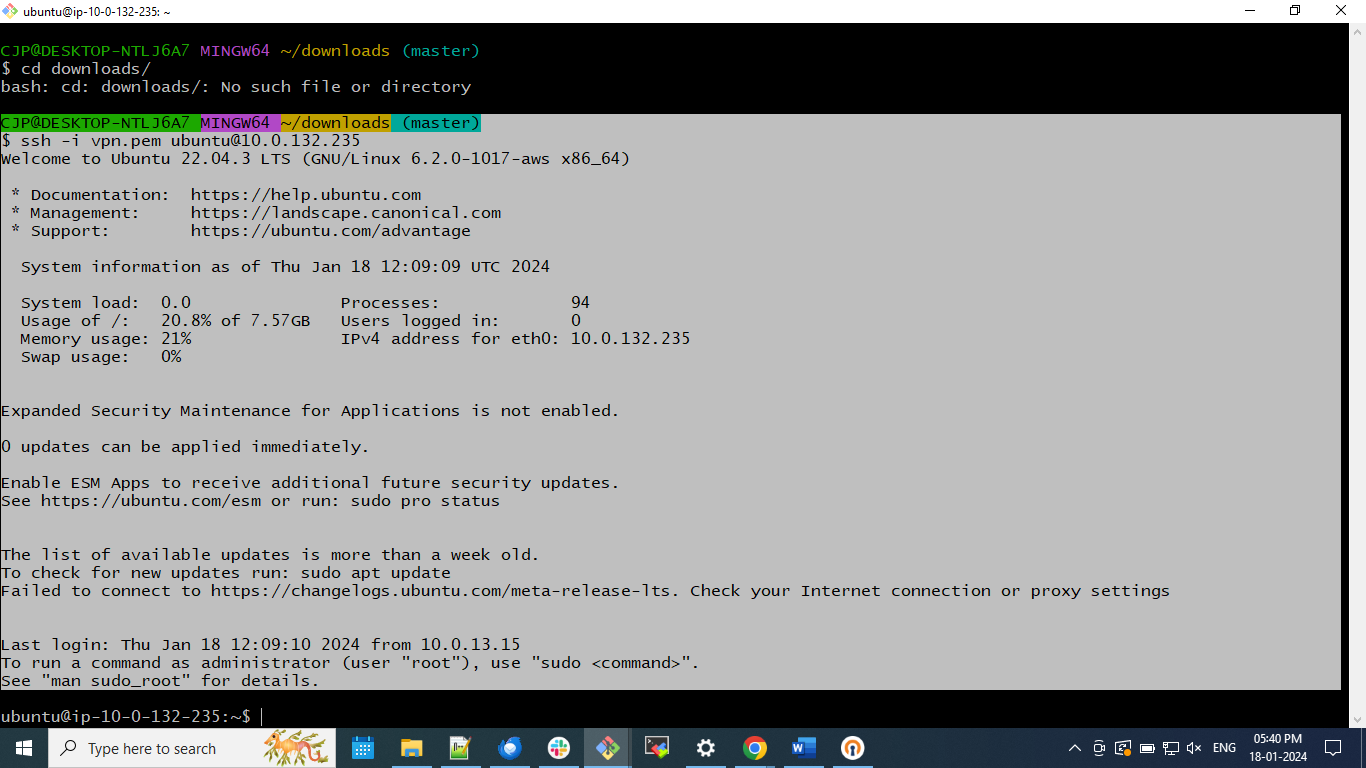
Subsequent Step to Ensure Connectivity:

4. To verify connectivity, SSH into the test server. Connect to the test server using the Public DNS of the OpenVPN server. Attempt to ping the server; a successful ping indicates that you have successfully accessed the EC2 instance's private IP from the external network using the VPN. This step ensures that the established OpenVPN connection allows secure access to the desired EC2 instance.

* **Step 5.1: . Post Successful VPN Connection - Creating a Test Server**

*Screenshot:*





*Annotations: 3.* *Post VPN success, create a test server on EC2 for secure access. Configure, launch, and verify connectivity by SSH and ping using OpenVPN.*

# Links

Referred Documentation

<https://docs.aws.amazon.com/vpn/latest/clientvpn-user/windows.html>

To acquire the OpenVPN application for Windows,

<https://openvpn.net/client/client-connect-vpn-for-windows/>

Referred Videos

<https://www.youtube.com/watch?v=R7-dj5dvpzA&t=1s>

<https://www.youtube.com/watch?v=fRIacc4mAzI&t=6s>

## **Manual installation of OpenVPN on your server.**

# Installing OpenVPN on Amazon EC2 ( Ubuntu ).

Below steps will show us how to install OpenVPN on Amazon Elastic Compute Cloud (Amazon EC2).

**Step 1: Launching an EC2 Instance**

Launching an EC2 instance is the first step to installing OpenVPN on Amazon EC2. To do this, log in to your Amazon Web Services (AWS) account and navigate to the EC2 dashboard. Then, click the "Launch Instance" button to launch a new EC2 instance.

**Step 2: Choosing an Amazon Machine Image (AMI)**

Next, you will need to choose an Amazon Machine Image (AMI) that will be the basis for your EC2 instance (ubuntu).

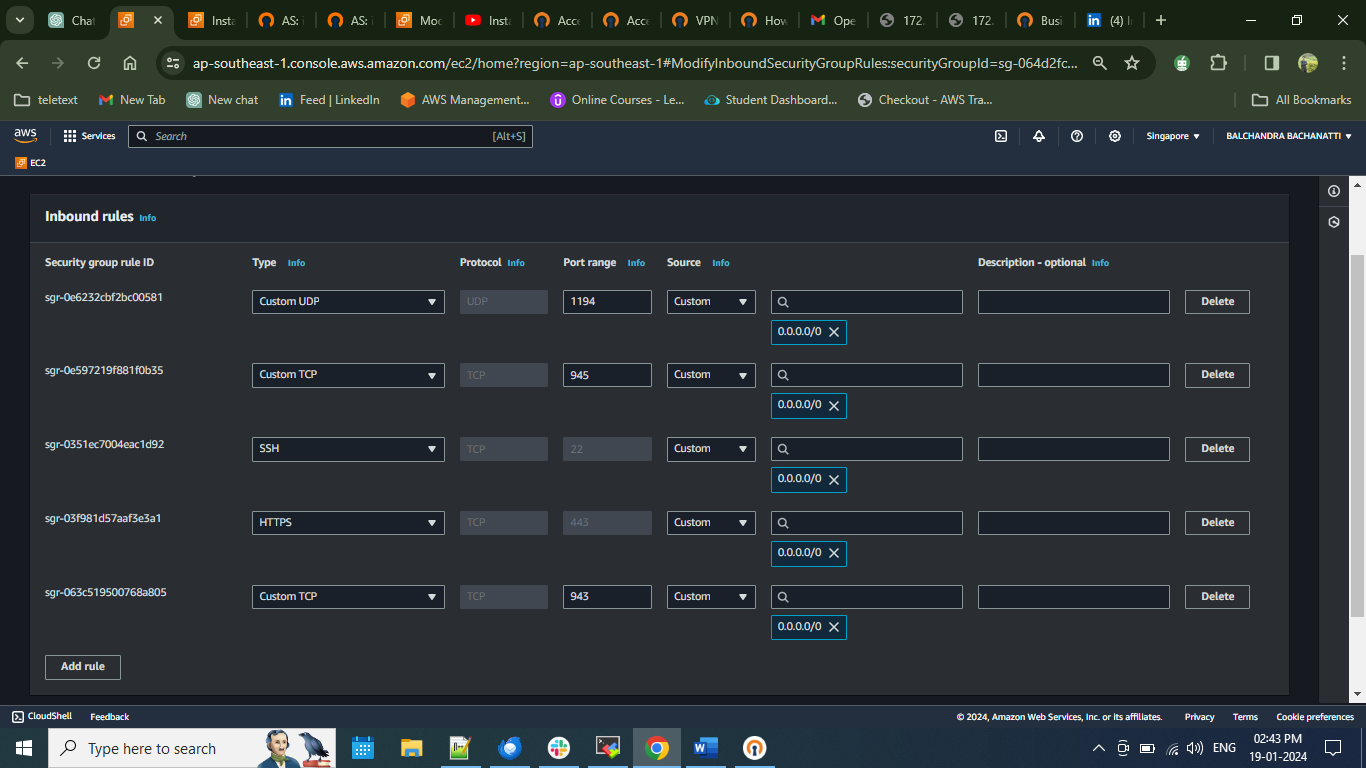
**Step 3: Configuring the Instance**

Once you have selected an AMI, you must configure your EC2 instance. This includes setting the instance type, configuring security groups, and attaching storage volumes selecting VPC which was created earlier. have set up a security group to allow incoming traffic on TCP port 22 (for SSH access) and UDP port 1194 (for OpenVPN traffic).

To make sure the connection is safe, you should now set up a firewall rule that only lets traffic from your server's OpenVPN port through. This can be done by creating an inbound security group on your EC2 instance. From the EC2 dashboard, click on the Network & Security tab and then select Security Groups from the left-hand menu. Create a new security group and name it something like "OpenVPN-Access."

Then, select the Inbound tab and add a rule as mentioned below. Once you have saved the rule, you can then assign this security group to your EC2 instance. This will make sure that only traffic from the OpenVPN port is allowed in, making for a secure connection.

* *Screenshot:*



**Step 5: Installing OpenVPN**

To connect to your newly created EC2 instance, you will need to use SSH.

To install Access Server, use the official repository. Log in to your Linux system with root privileges, and enter these commands to add the repository and install the package 'openvpn-as'. The client bundle installs automatically.

apt update && apt -y install ca-certificates wget net-tools gnupg

wget https://as-repository.openvpn.net/as-repo-public.asc -qO /etc/apt/trusted.gpg.d/as-repository.asc

echo "deb [arch=amd64 signed-by=/etc/apt/trusted.gpg.d/as-repository.asc] http://as-repository.openvpn.net/as/debian jammy main">/etc/apt/sources.list.d/openvpn-as-repo.list

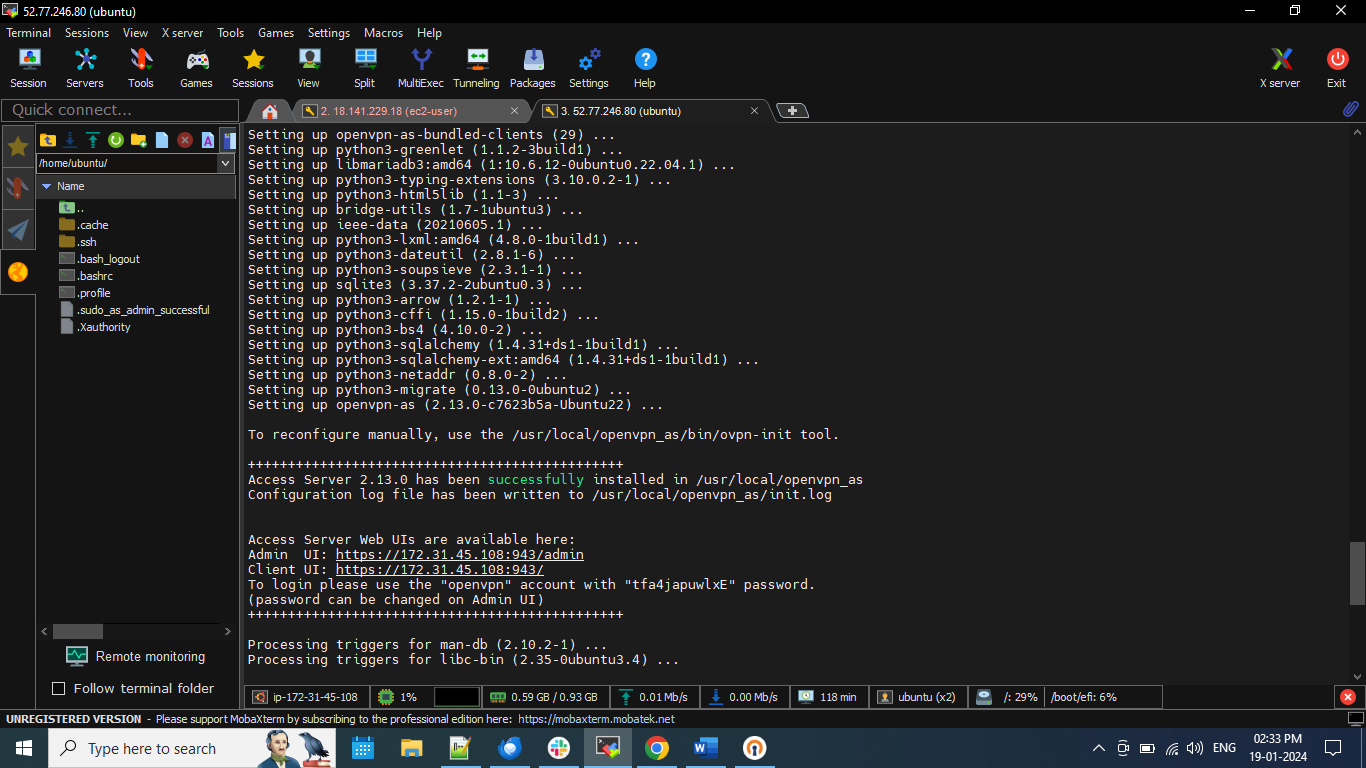
apt update && apt -y install openvpn-as

After these steps, your Access Server should be installed and awaiting further configuration.

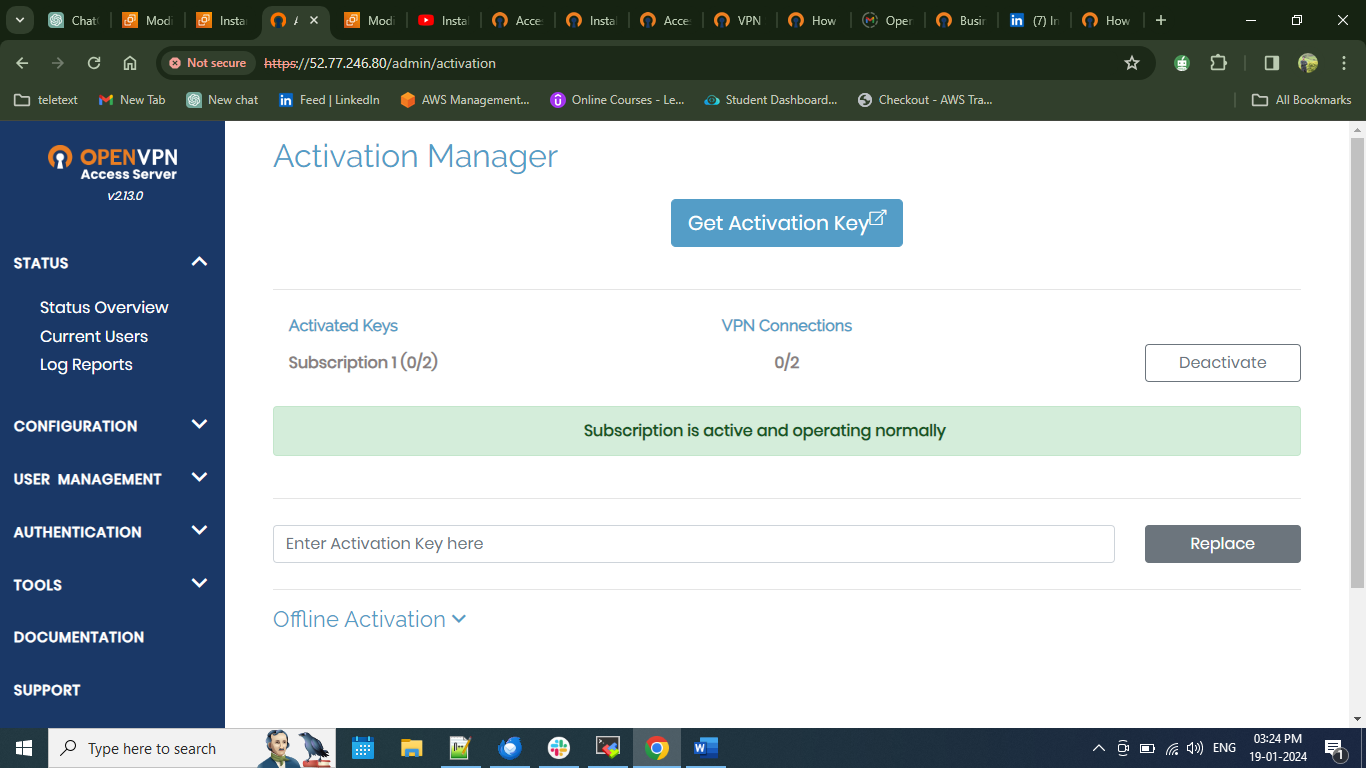
After installing, you'll receive the **URLs for your admin and client UIs** along with a randomly generated admin **username** and **password**.

To reconfigure manually, use the /usr/local/openvpn\_as/bin/ovpn-init tool.

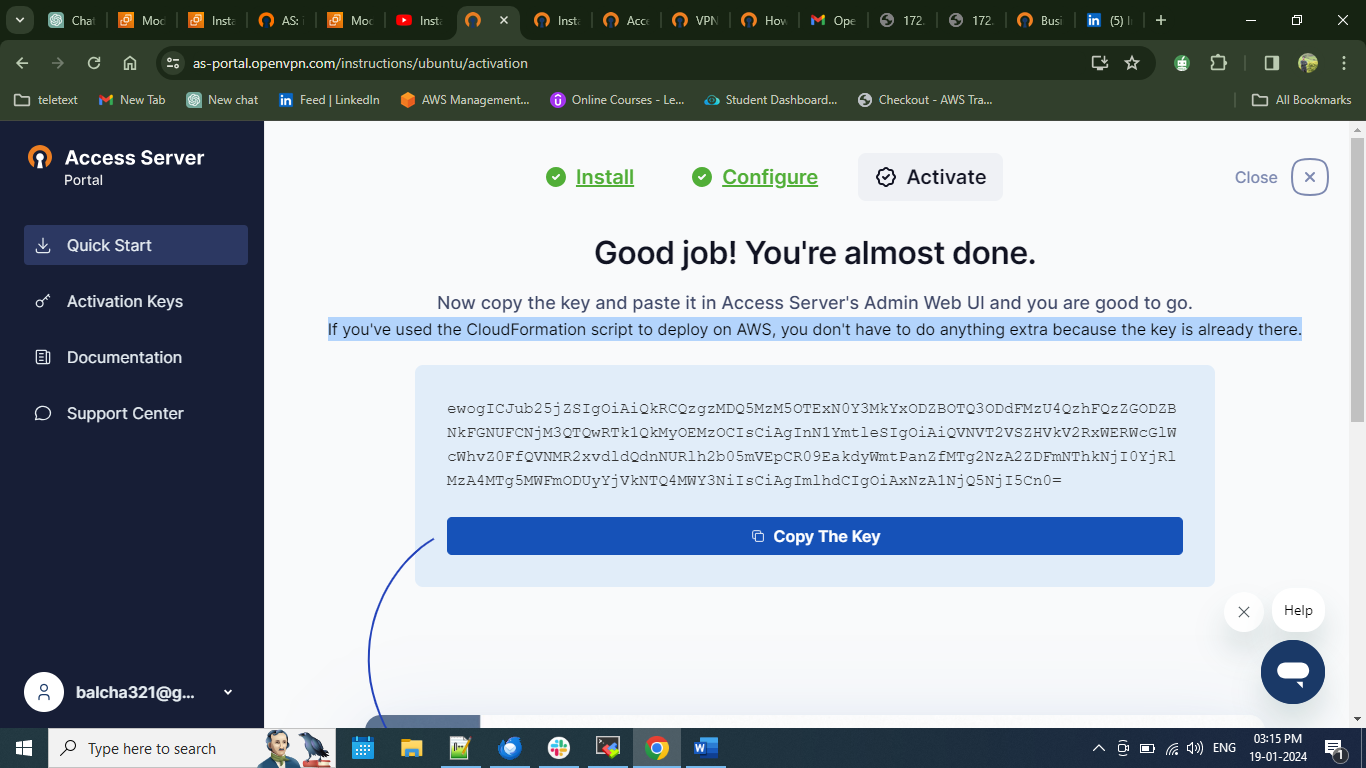
/usr/local/openvpn\_as/bin/ovpn-init tool



**To log in, utilize the OpenVPN account credentials set during the initial setup.**



Now to activate get the activation key copy the key and paste it in Access Server's Admin Web UI and you are good to go.



# Conclusion

# In conclusion, this comprehensive guide outlines the process of setting up OpenVPN on AWS for secure remote access to EC2 instances' private IPs from external networks. By meticulously creating a VPC, launching an OpenVPN server, and configuring a test server, users can establish an encrypted channel. The outlined steps, combined with detailed annotations and visual aids, offer a robust framework for successfully implementing and verifying the OpenVPN deployment on AWS.

# Links

**VPN Software Repository & Packages**

<https://openvpn.net/vpn-software-packages/>

**Configuration of Access Server**

<https://openvpn.net/vpn-server-resources/how-to-configure-the-openvpn-access-server>

<https://as-portal.openvpn.com/instructions/ubuntu/configuration>