AMAZON EC2 SERVICE

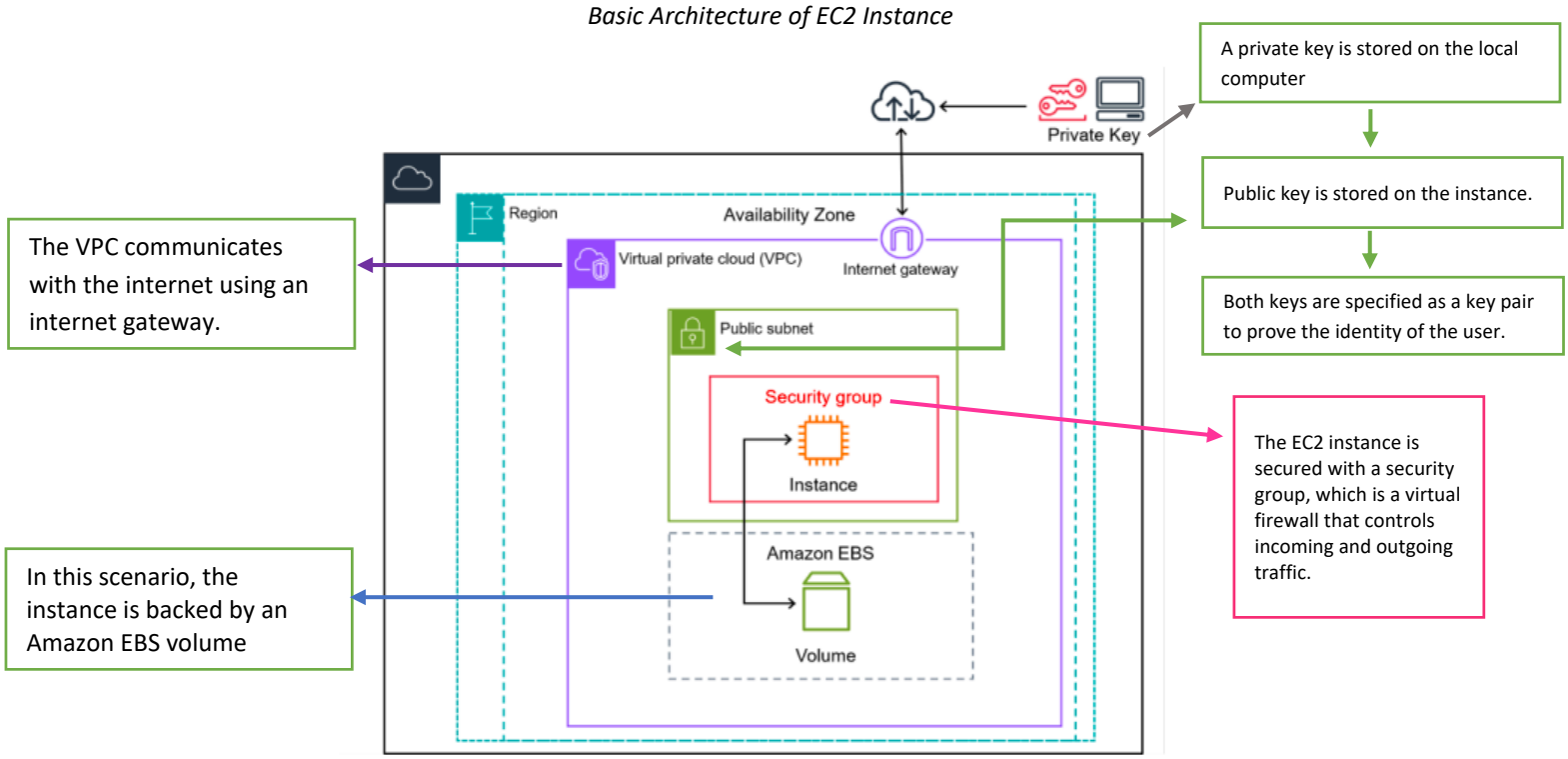
Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud.

✓Access reliable, scalable infrastructure on demand. Scale capacity within minutes with SLA commitment of 99.99% availability.

✓Provide secure compute for your applications. Security is built into the foundation of Amazon EC2 with the AWS Nitro System.

✓Optimize performance and cost with flexible options like AWS Graviton-based instances, Amazon EC2 Spot instances, and AWS Savings Plans.

Basic Architecture of EC2 Instance



The diagram shows a basic architecture of an Amazon EC2 instance deployed within an Amazon Virtual Private Cloud (VPC). In this example, the EC2 instance is within an Availability Zone in the Region. The EC2 instance is secured with a security group, which is a virtual firewall that controls incoming and outgoing traffic. A private key is stored on the local computer and a public key is stored on the instance. Both keys are specified as a key pair to prove the identity of the user. In this scenario, the instance is backed by an Amazon EBS volume. The VPC communicates with the internet using an internet gateway.

FEATURES OF AMAZON EC2 AMAZON

EC2 provides the following high-level features:

Instances: This is a Virtual server.

Amazon Machine Images (AMIs): Preconfigured templates for your instances that package the components you need for your server (including the operating system and additional software).

Instance types: Various configurations of CPU, memory, storage, networking capacity, and graphics hardware for your instances.

Key pairs: Secure login information for your instances. AWS stores the public key and you store the private key in a secure place.

Instance store volumes: Storage volumes for temporary data that is deleted when you stop, hibernate, or terminate your instance.

Amazon EBS volumes: Persistent storage volumes for your data using Amazon Elastic Block Store (Amazon EBS).

Regions, Availability Zones, Local Zones, AWS Outposts, and Wavelength Zones: Multiple physical locations for your resources, such as instances and Amazon EBS volumes.

Security groups: A virtual firewall that allows you to specify the protocols, ports, and source IP ranges that can reach your instances, and the destination IP ranges to which your instances can connect.

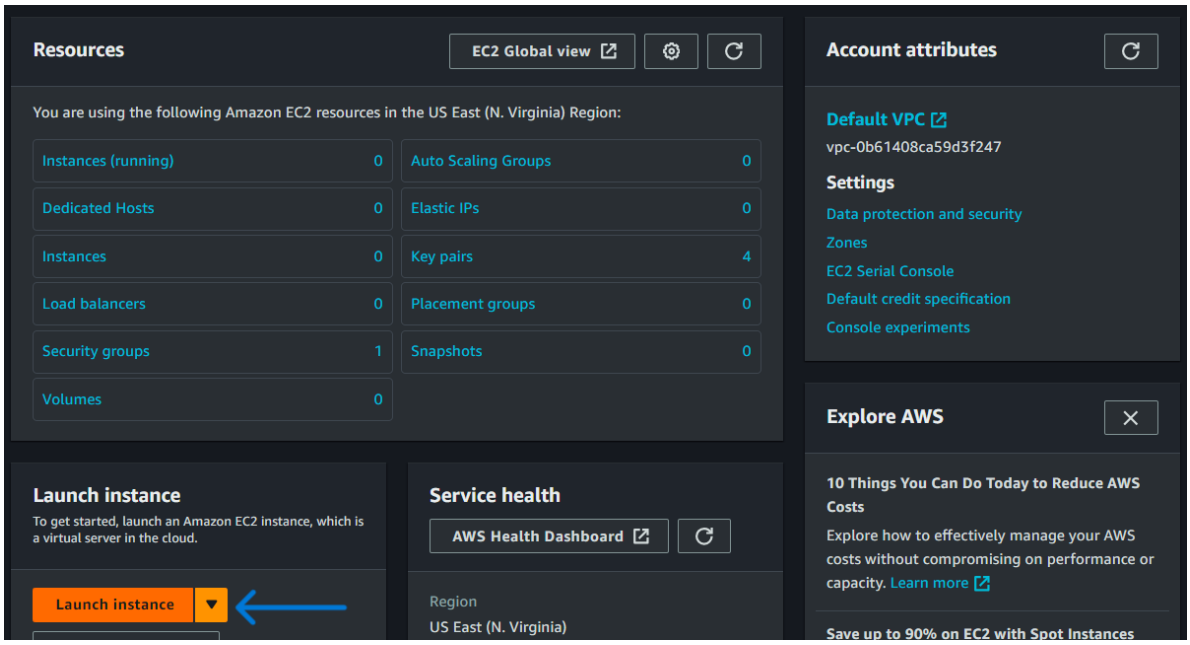
Elastic IP addresses: Static IPv4 addresses for dynamic cloud computing.

Tags: Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment.

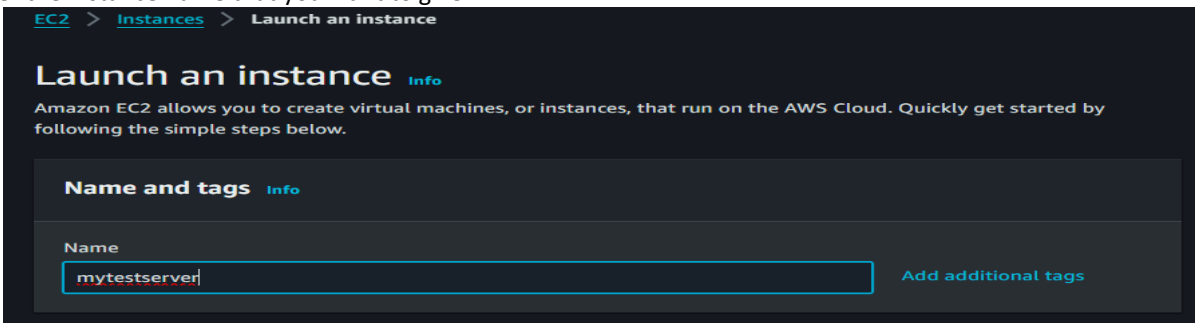
Virtual private clouds (VPCs): Virtual networks you can create that are logically isolated from the rest of the AWS Cloud. You can optionally connect these virtual networks to your own network.

EC2 INSTANCE LAUNCH STEPS

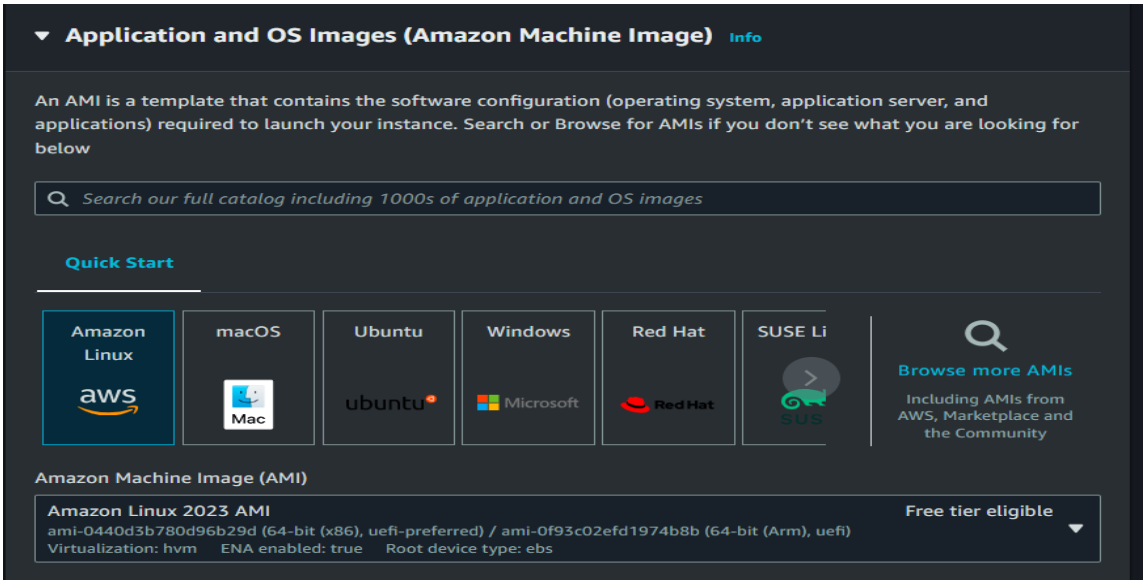
Step 1) Sing in the AWS Console and Go to EC2 Service Dashboard. And click on the Launch Instance Button.



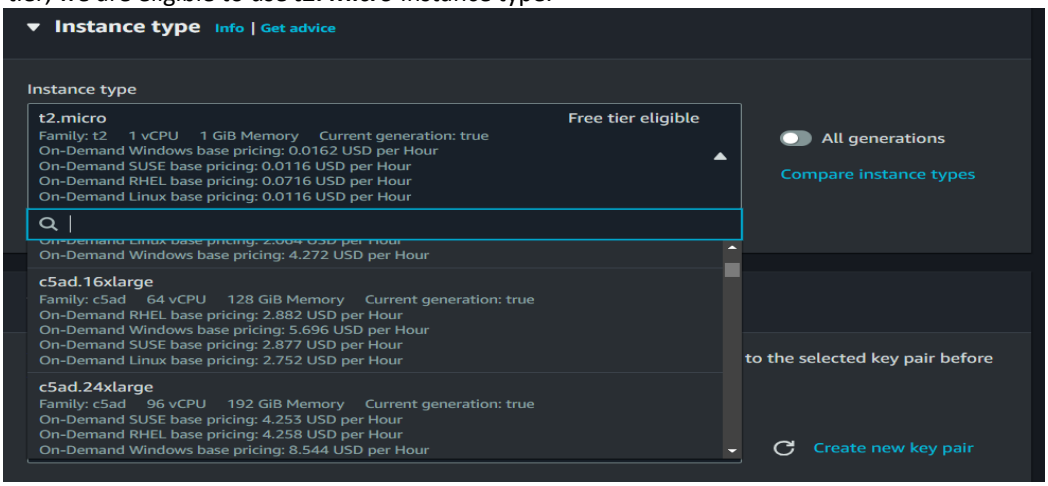
Step 2) Enter the instance name that you want to give.



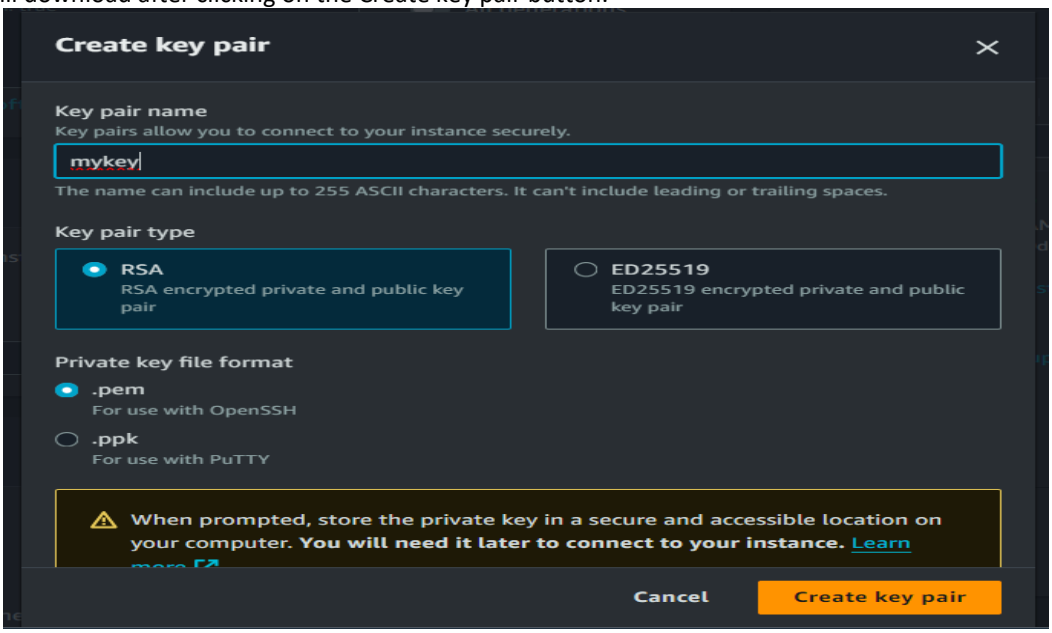
Step 3) Select AMI (Amazon Machine Image).



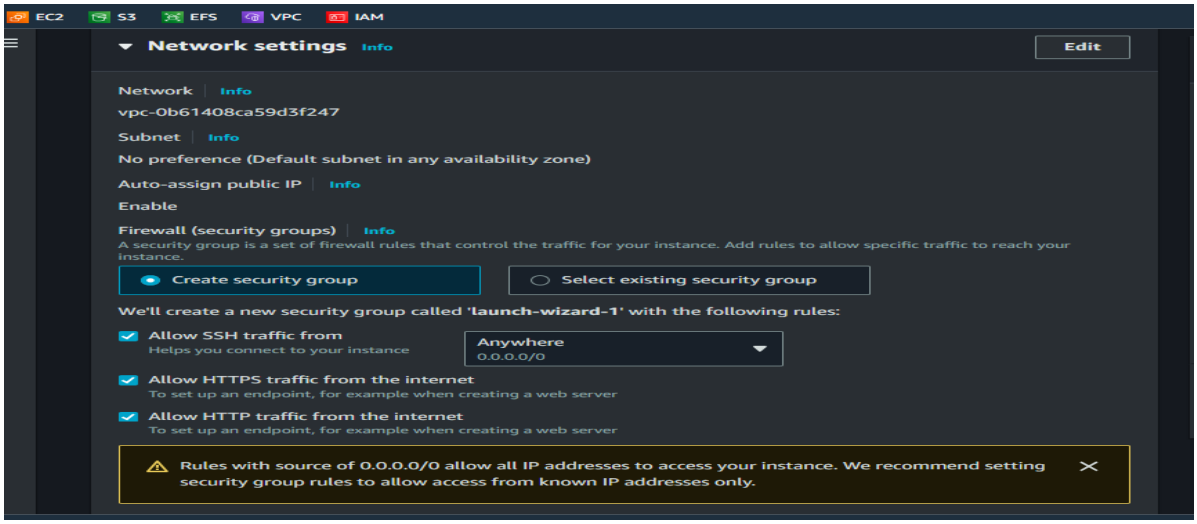
Step 4) Select the Instance type that requires your computing, memory, networking, or storage requirements.
In the free tier, we are eligible to use ***t2. Micro*** Instance type.



Step 5) Create a new Key pair (or select an existing key pair) to securely connect to your Instance.
The key will download after clicking on the Create key pair button.



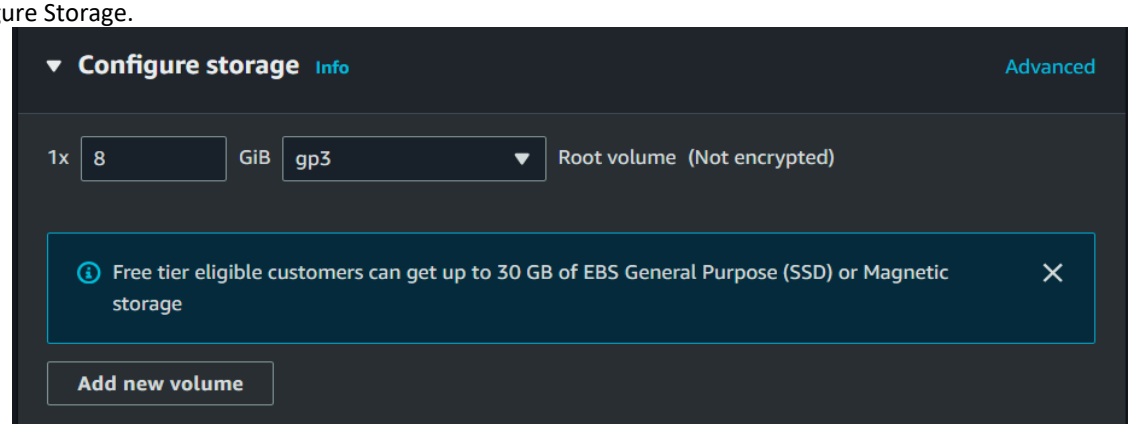
Step 6) Now in Network Setting select Create Security group and allow SSH to connect to instance or remote access, HTTPS is crucial for securely serving web content, and HTTP also transmits web pages and other web content.



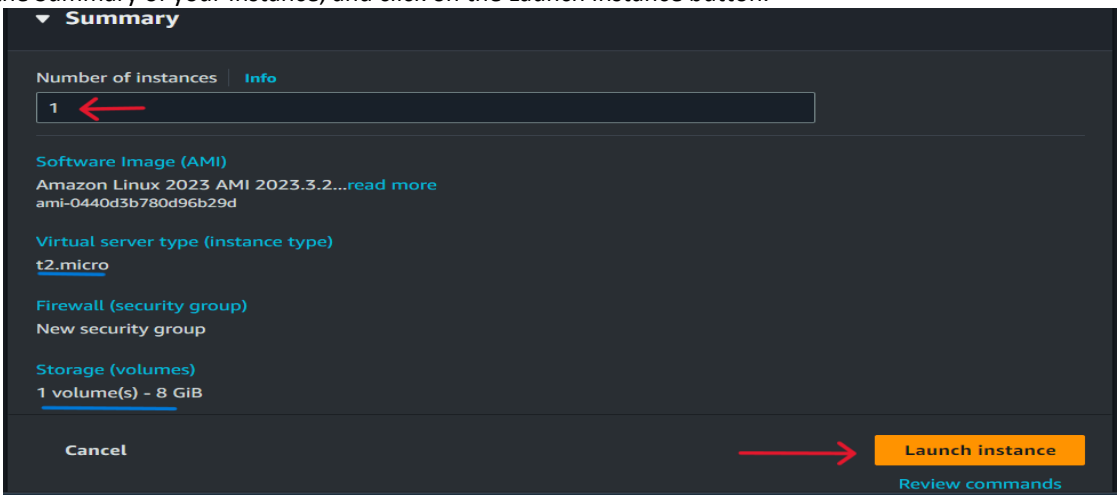
A *security group is a set of firewall rules* that controls the traffic to and from your instance. Inbound rules control the incoming traffic to your instance, and outbound rules control the outgoing traffic from your instance.

Enabling SSH, HTTPS, and HTTP on AWS instances allows them to do a lot of different things, like letting people log in remotely to manage the server (SSH), securely serve websites and web applications (HTTPS), and host web content (HTTP). But it's crucial to make sure these services are set up securely.

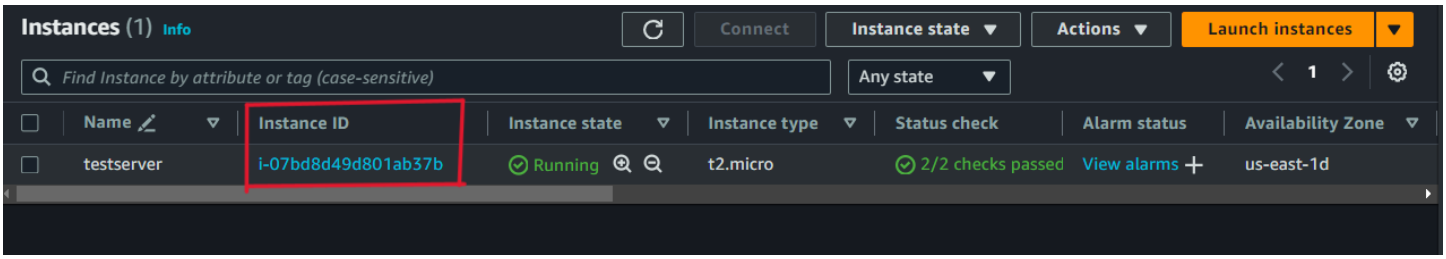
Step 7) Configure Storage.

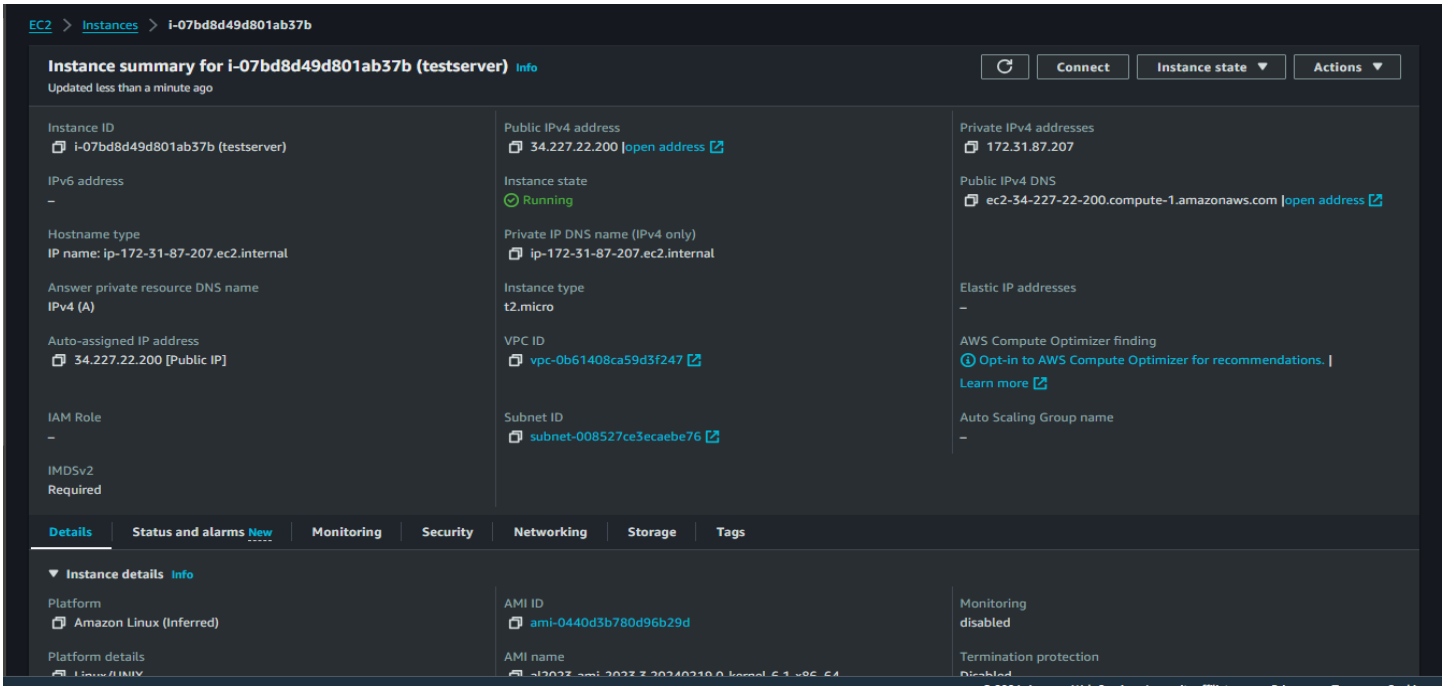


Step 8) Check the Summary of your Instance, and click on the Launch Instance button.



Now your Instance launching will start, it will take some time to launch and install. After it is done you will receive a notification with the instance ID simply click on it Instance list will open. Again click on the Instance ID then the Instance all Summary Details page will open.





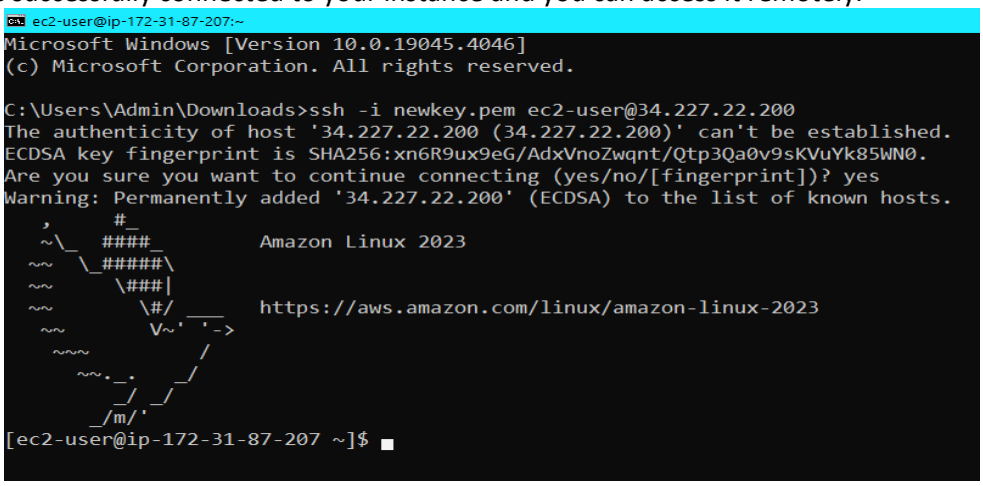
Connect to the Instance on Windows Command Prompt by SSH with Key pair

Step 1) Go to the folder where you stored your Key pair file. Open the Command Prompt at that location.

Step 2) Enter the following Command

- **ssh -i newkey.pem ec2-user@34.227.22.200** (ssh –i keypairname ec2-user@public.ip.address.of.instance)
- ask for connection type **yes** and enter

  Now you're successfully connected to your instance and you can access it remotely.



Now we Host a Static website using CLI mode by following commands

- **sudo –i** **-> switch to root user**
- **yum install httpd –y** **-> install httpd package**
- **systemctl start httpd** **-> to jerk package**
- **systemctl enable httpd** **-> to enable package**
- **systemctl status httpd** **-> to check status**

Now go to the web browser and search CSS template download, copy any template download link.

- **curl –O link of download template -> your template will be downloaded in .zip format**
- **ls** **-> list the template file**
- **unzip filename.zip** **-> to unzip your file**
- **mv filename/* /var/www/html** **-> move all content of file to a web server directory**

Now your web page is public, simply copy your Public IP address and paste it into the web browser and you will see your static website is running.