**Module 1\_ AWS\_Fundamentals\_Cloud**

==================================================================================

Submitted to Vikul\_Sir

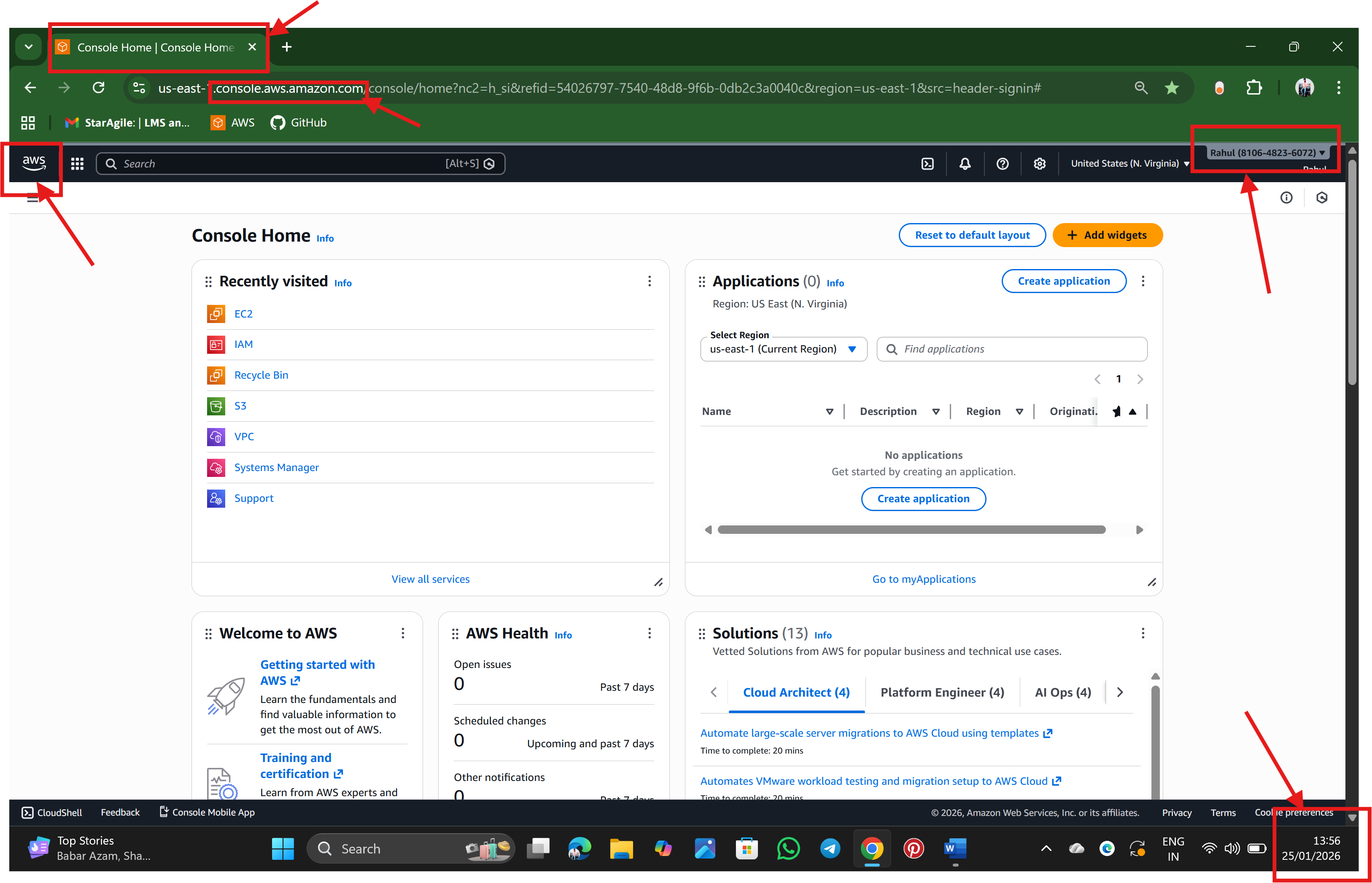
Submitted by Nalathati Rahul

Submission Date –03/Feb/2026

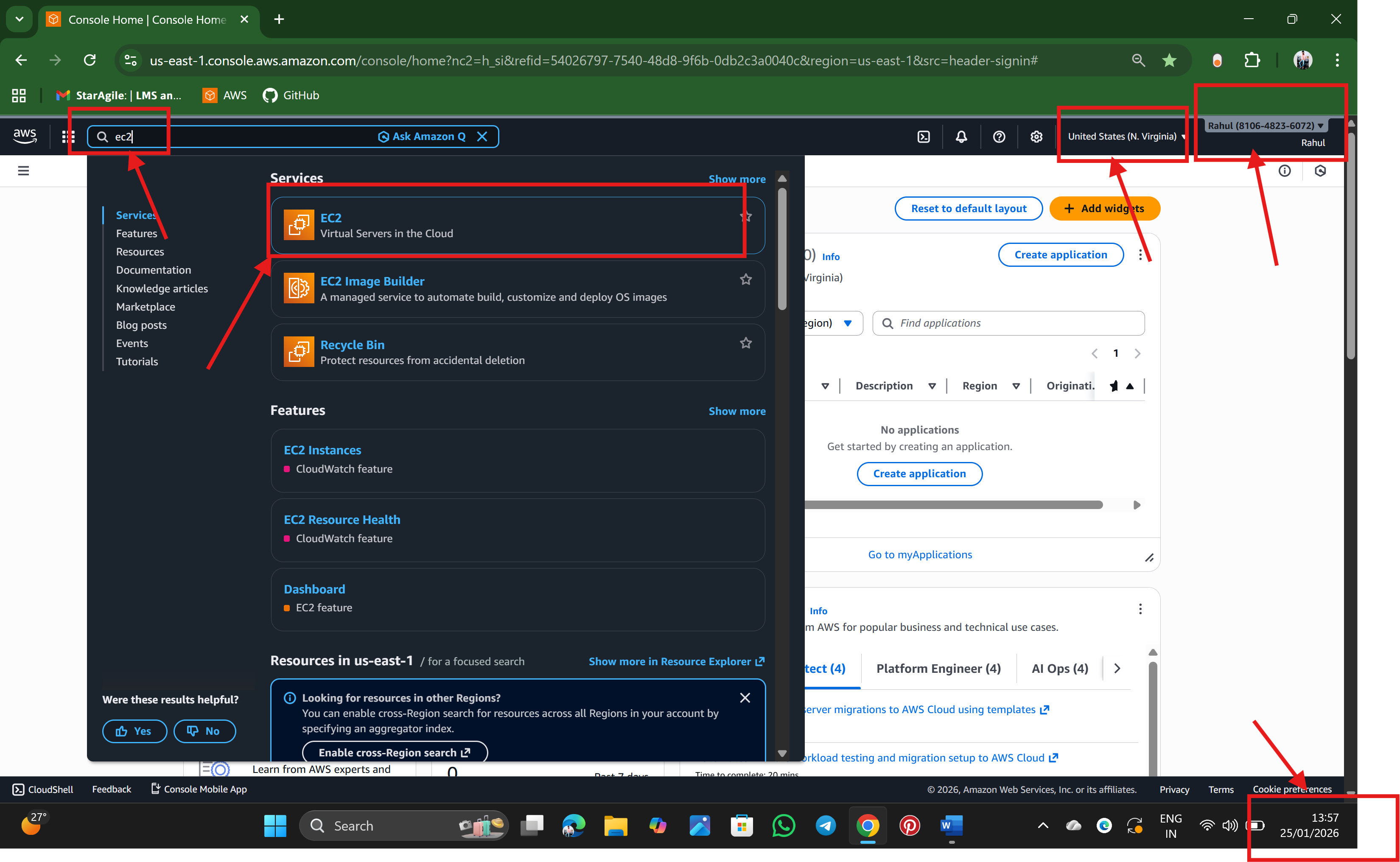
==================================================================================

L3 - Launch AWS EC2 Ubuntu Instance and configure the Security Group - Inbound Rule: 8080. Justify the usage of Inbound Rules

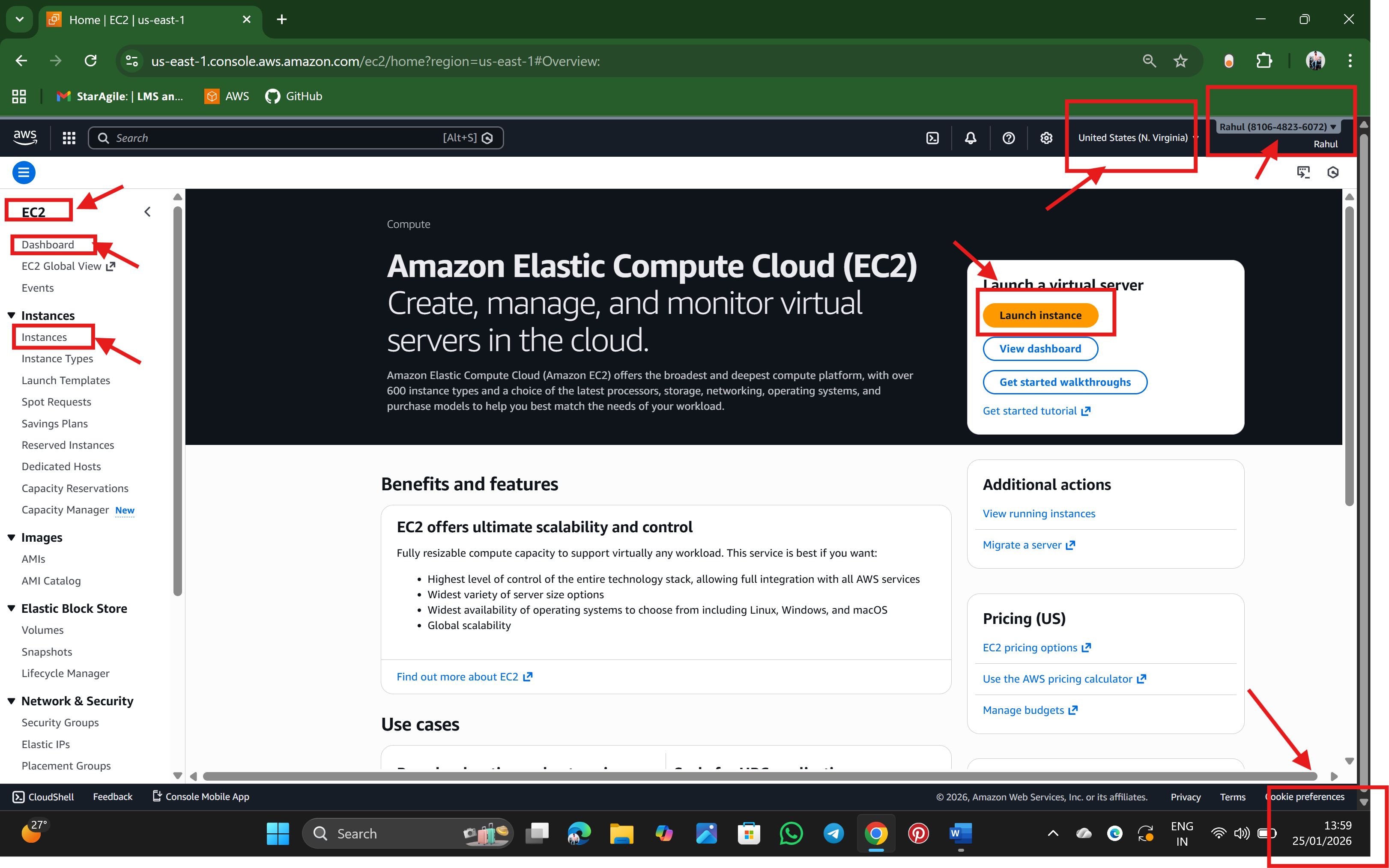
Step 1: Go to AWS URL 🡪 <https://aws.amazon.com/console/> 🡪and login with Credentials



Step 2: Search EC2 Servers in the search bar of AWS 🡪 EC2 is Virtual computer that provide by AWS



Step 3: This the interface of EC2 server Dashboard, so click the option launch instance



Step 4:

🡪 after, Enter Name the server

🡪 select AMI (Amazon Machine Image) which is free tier eligible, AMI is an operation system.

🡪 Select type of instance

🡪 create key pair

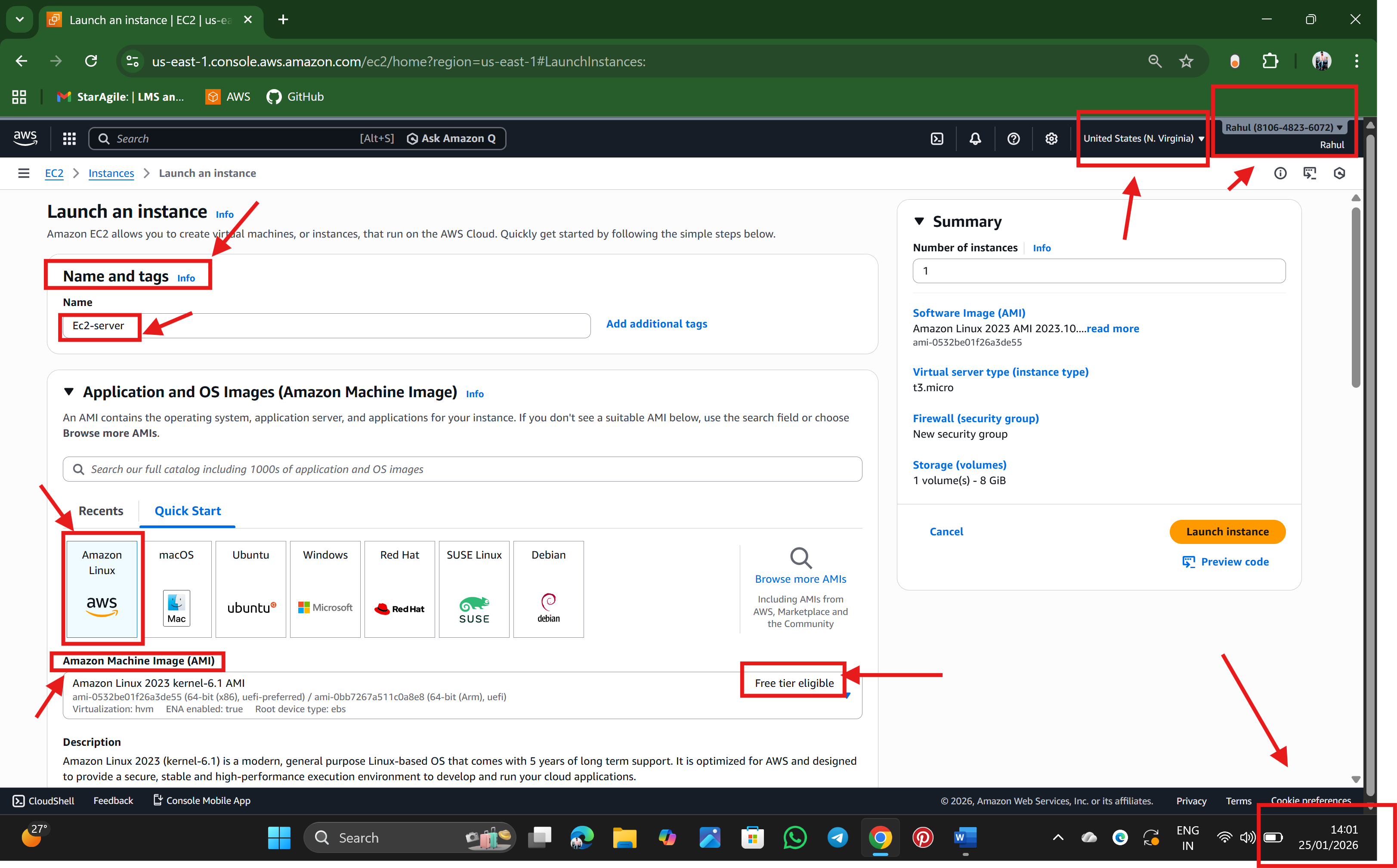
🡪Confirm Network settings by clicking Edit option

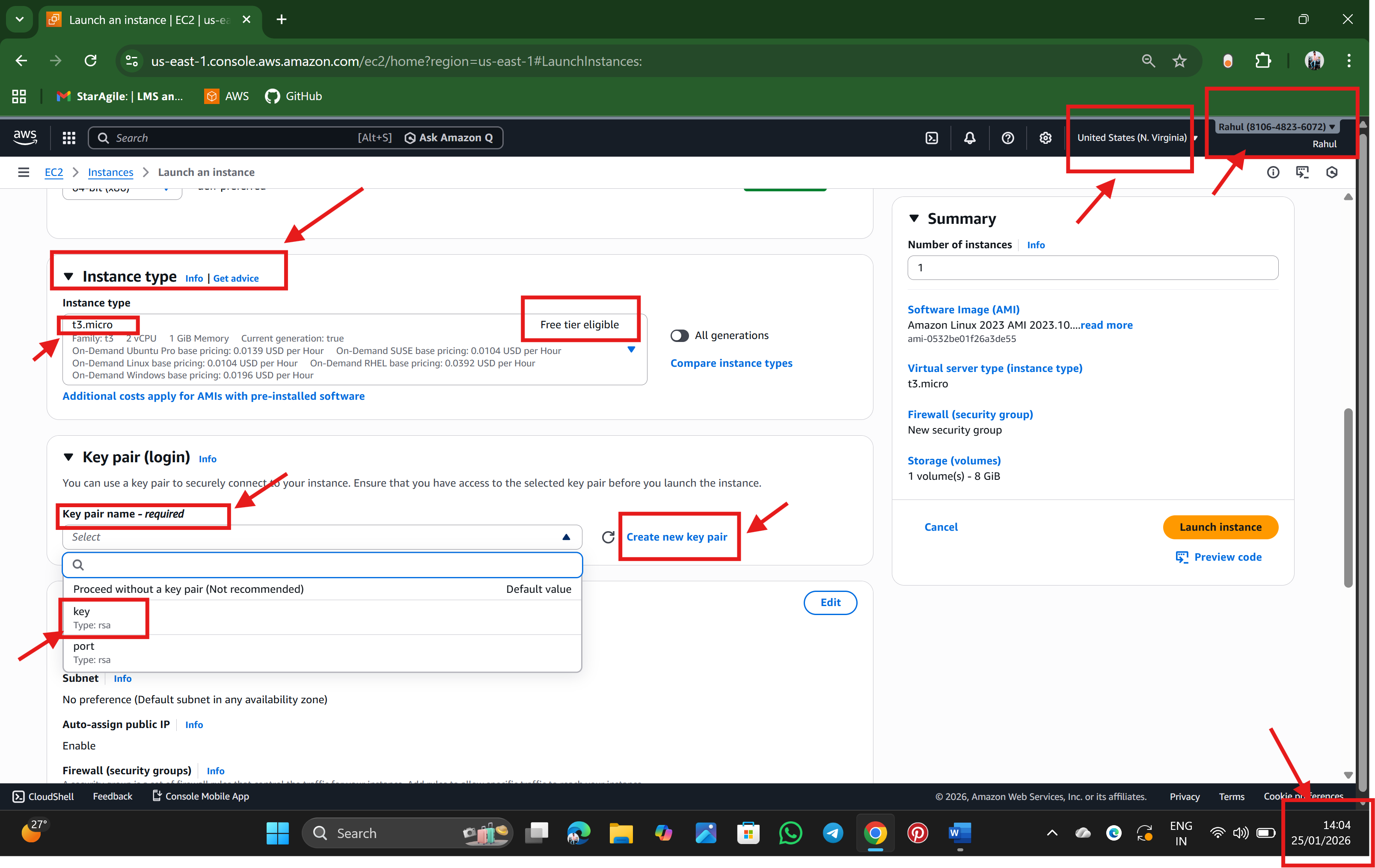
* In edit, makes changes like for SSH (default port no:22) give source type: My IP (103.120.51.46/32) which is Private IP)
* for custom TCP (with port no: 8080) give source type: Anywhere (0.0.0.0/0) which is public IP

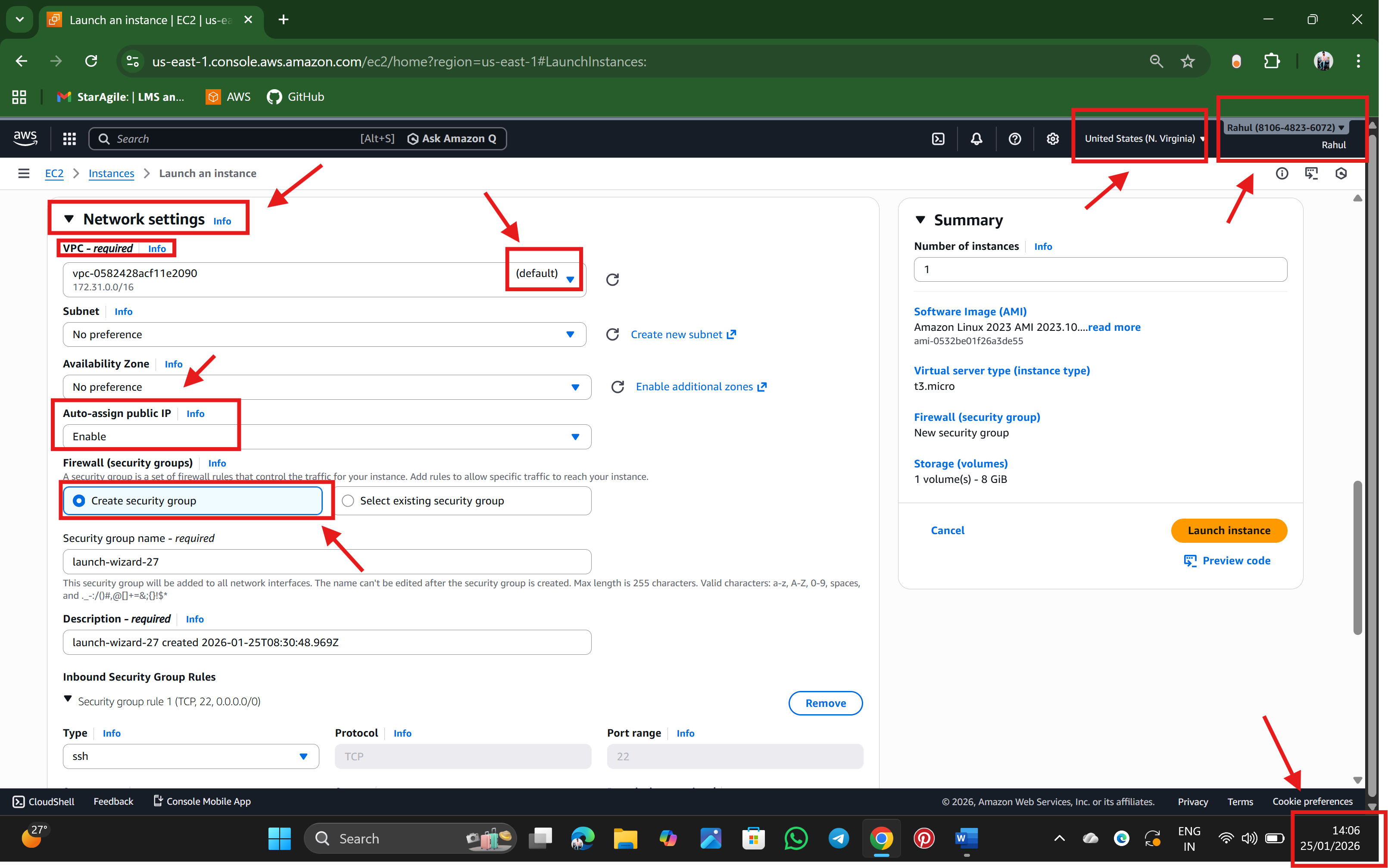
🡪check Configure storage

* default 8 GiB and gp3

🡪 Click launch instance





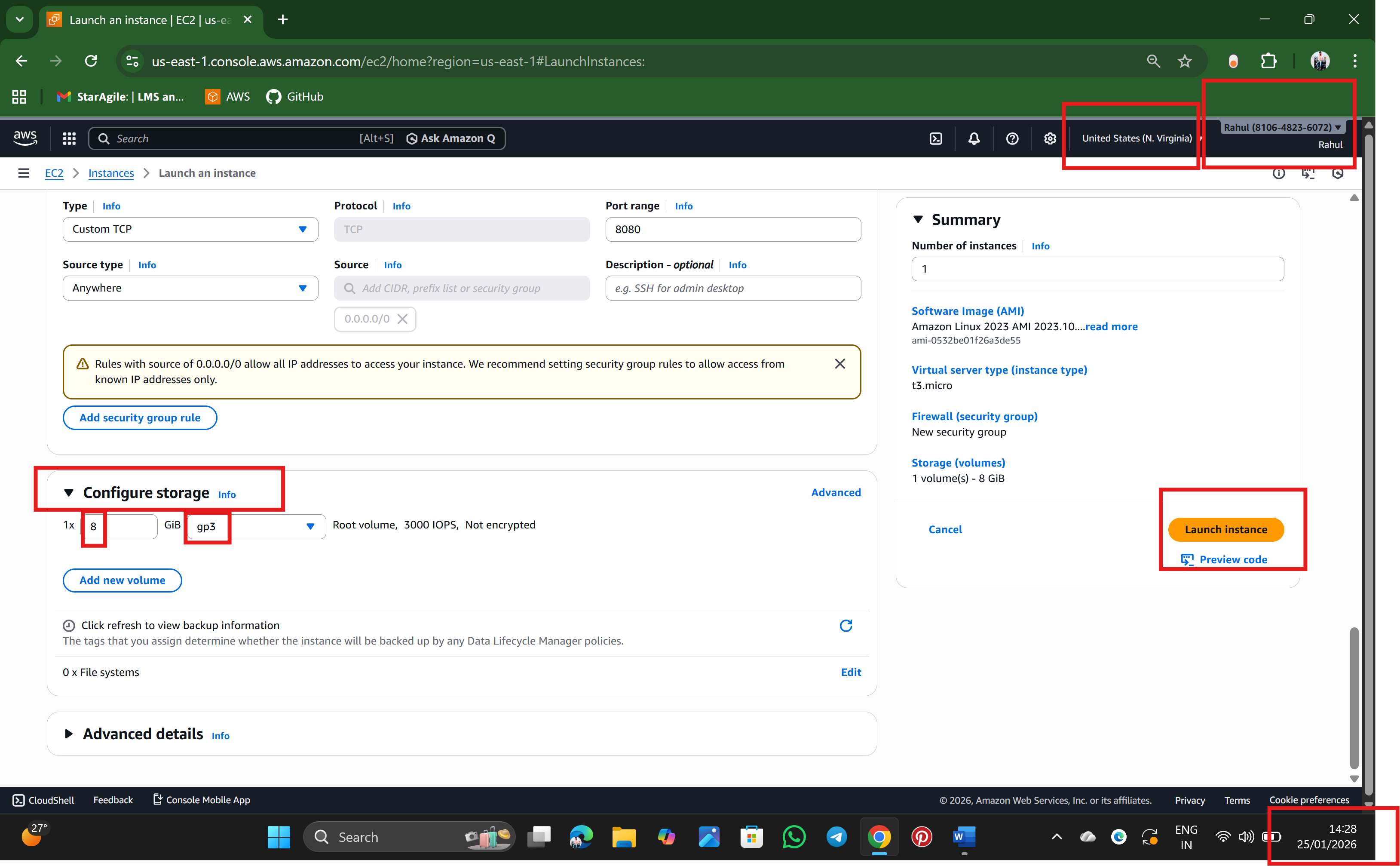




**Inbound rules are firewall rules in AWS Security Group.**

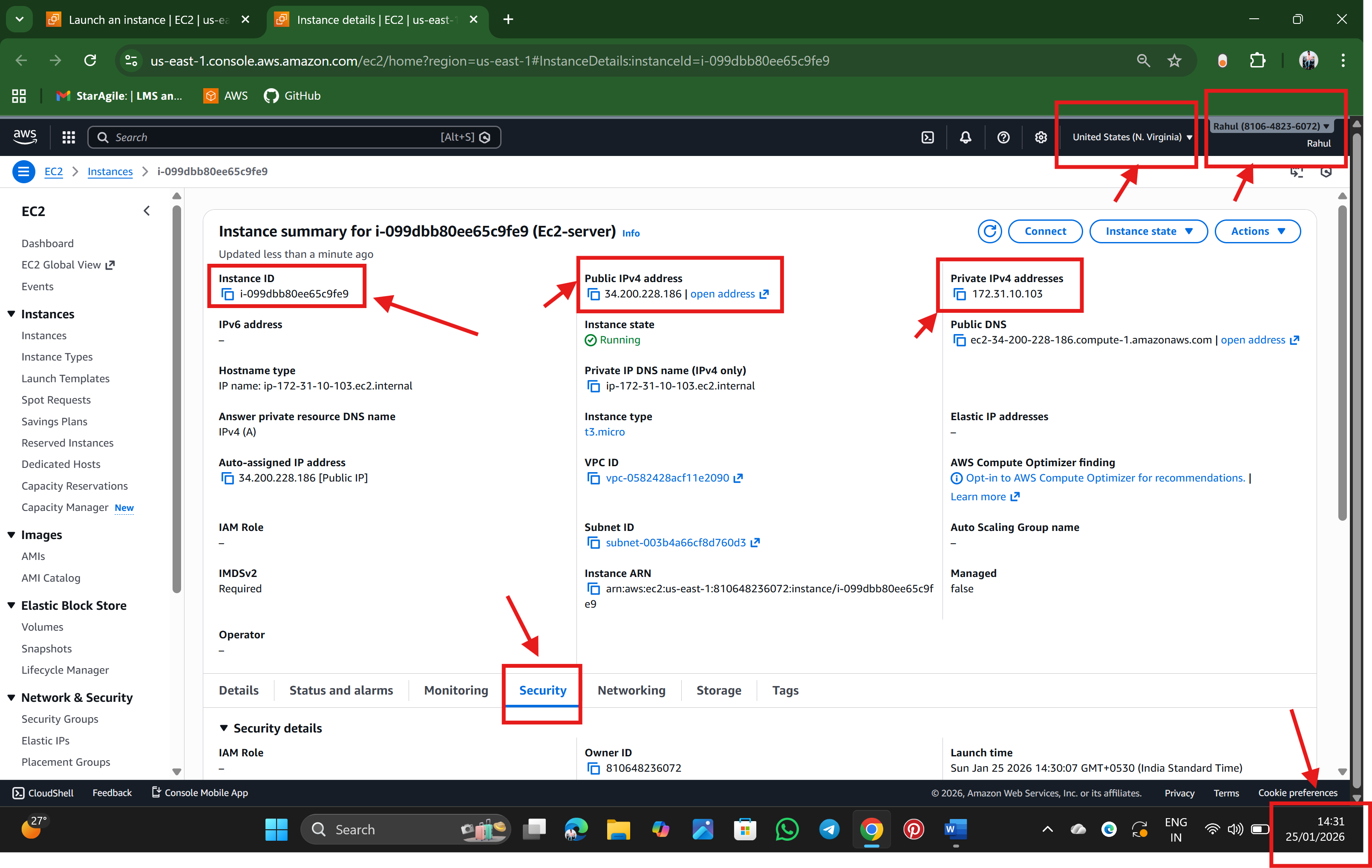
SSH = **Secure Shell** It is used to Login to your EC2 server, Run Linux commands, install software and Manage server. Without SSH rule, we cannot connect to your EC2 server. We selected **My IP** → means only we can connect via SSH (very secure)

8080 is a web application port,it is used to **access websites or applications running on the server**. Or Website or app access

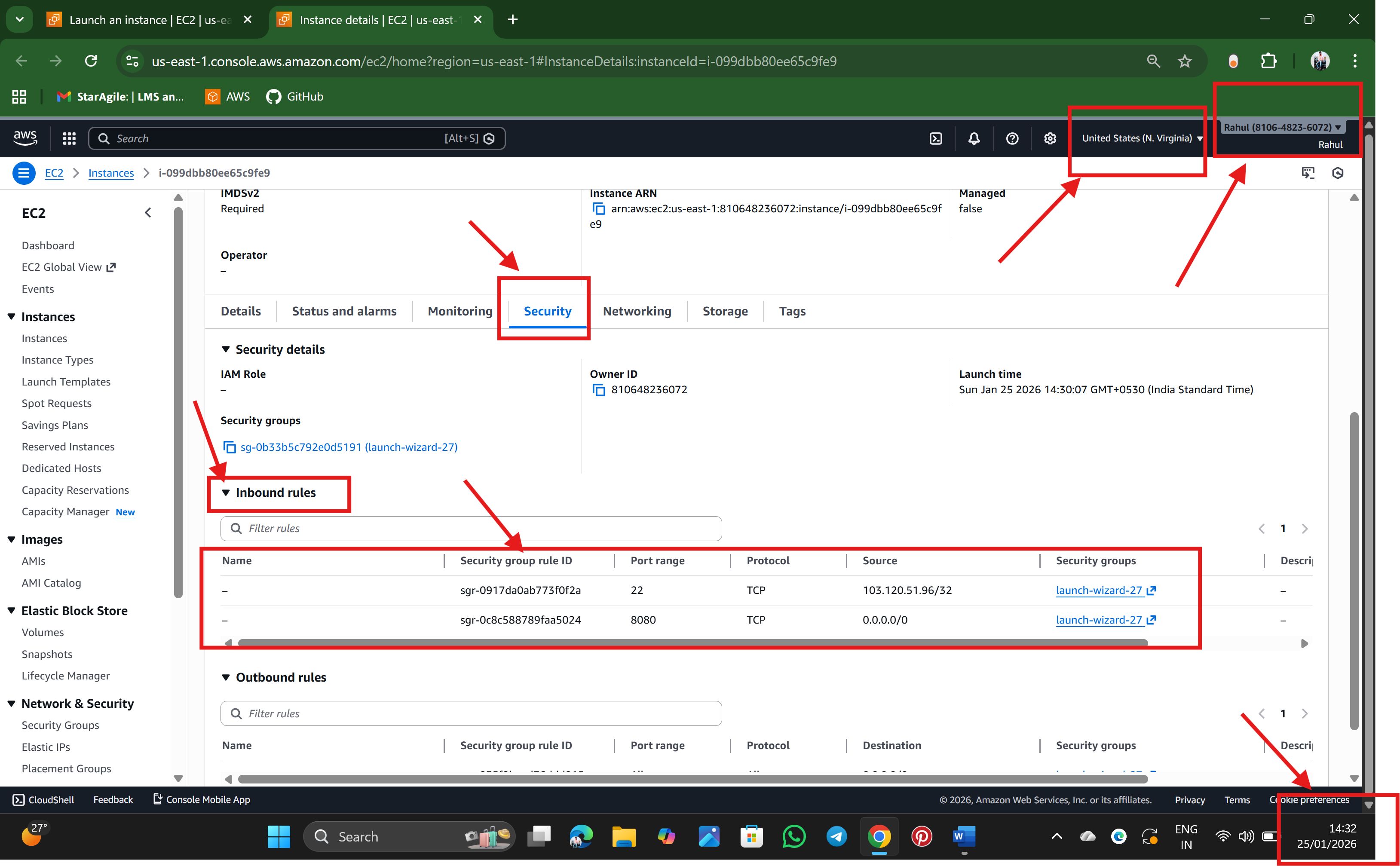




Step :5 Ater launching the instance, check summary of the server and click connect



Step 6: finally, Inbound Rule: 8080 in security



Q: Justify the usage of Inbound Rules?

ANS: - Inbound rules refer to Incoming Traffic (or)data packets or network requests that come *into* a system, server, or network from external sources.

1. Enhance Security (prevent unauthorized access by blocking unwanted connections.)
2. Improve Network Performance (Blocking unnecessary traffic reduces network congestion and resource usage.)
3. **Control Access to Services,** they ensure only specific services are reachable.  
   Example: Allow SSH (22) only from admin IP and Allow database ports only from application servers

**==================================================================================**

**🡪Rahul Nalathati**