

**Placement Empowerment Program**

***Cloud Computing and DevOps Centre***

**Set Up a Virtual Machine in the Cloud**

Create a free-tier AWS, Azure, or GCP account. Launch a virtual machine and SSH into it.

Name: Rathipriya S Department: CSE



**Introduction and Overview**

Setting up a virtual machine (VM) in AWS allows you to run applications, test environments, or host services in the cloud. AWS provides **Amazon EC2 (Elastic Compute Cloud)** instances, which can be used as virtual machines. After launching an EC2 instance, users can remotely connect to it using SSH (Secure Shell) to manage the server, deploy applications, and monitor the system. This document outlines the process of setting up a virtual machine in AWS, launching it, and accessing it through SSH.

**Objectives**

* To create and launch a virtual machine (EC2 instance) in AWS.
* To configure the instance with necessary settings and security measures.
* To establish SSH connectivity to the EC2 instance for remote management.

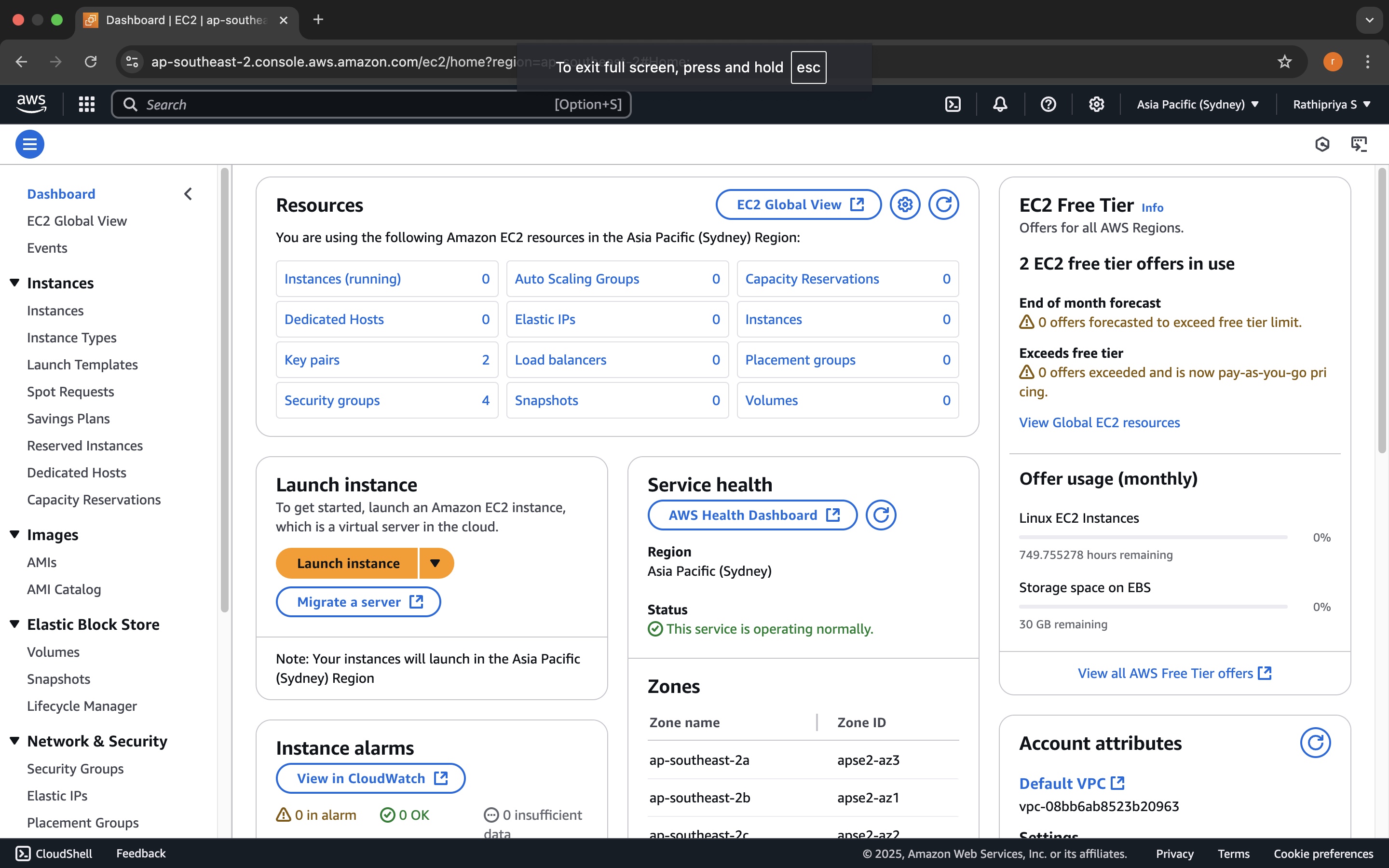
**Importance**

* **Remote Management:** SSH access enables users to manage their virtual machines remotely, ensuring flexibility in administration and troubleshooting.
* **Scalability:** AWS provides the ability to launch and scale virtual machines based on your needs, allowing businesses to adapt quickly.
* **Security:** By configuring secure SSH access, you ensure that only authorized users can connect to your virtual machine.
* **Cost Efficiency:** AWS EC2 allows you to choose the instance type that best suits your workload, providing cost-effective solutions for running virtual machines in the cloud.

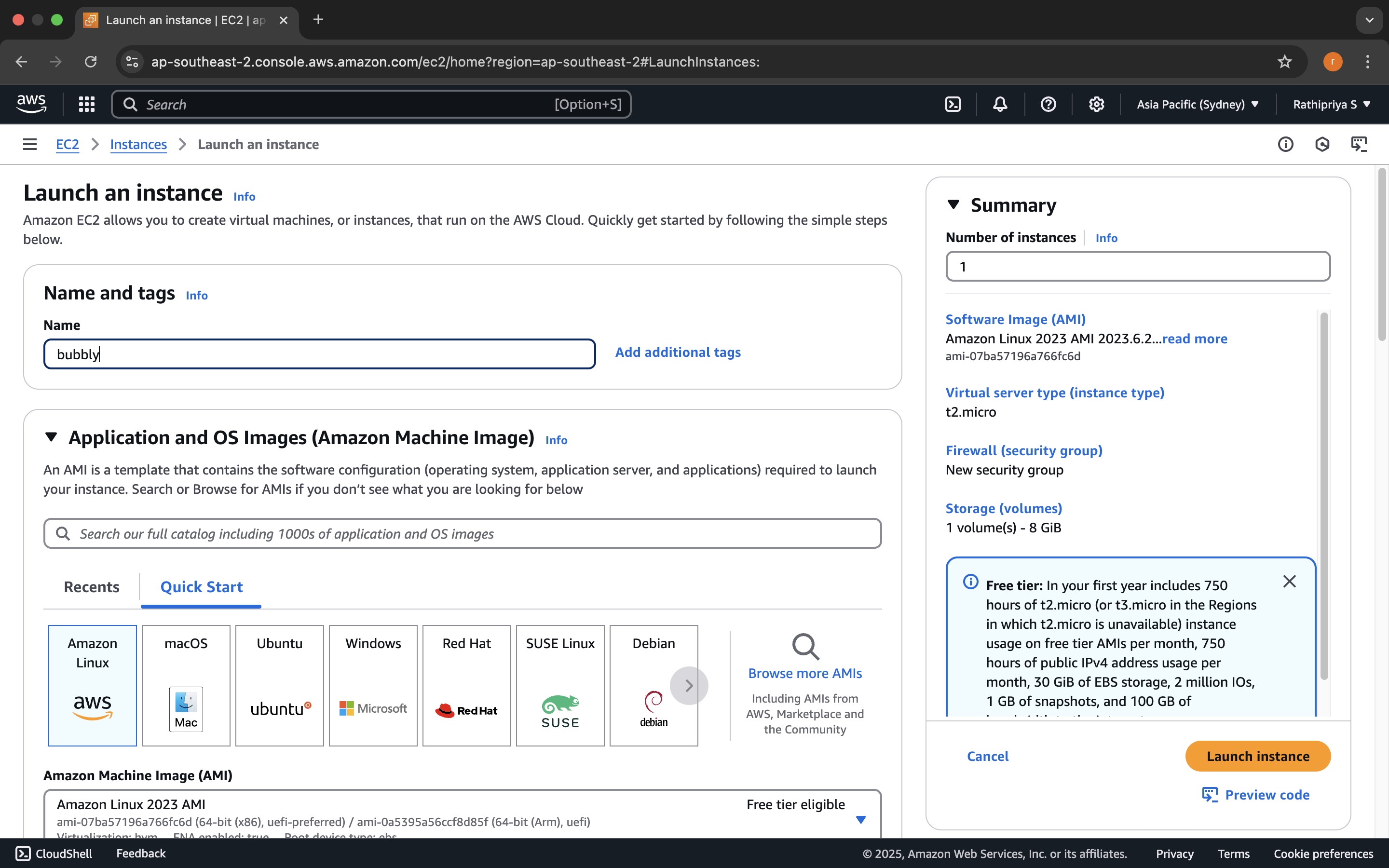
**STEPS:**

**STEP 1:** Launch an EC2 Instance (Virtual Machine)

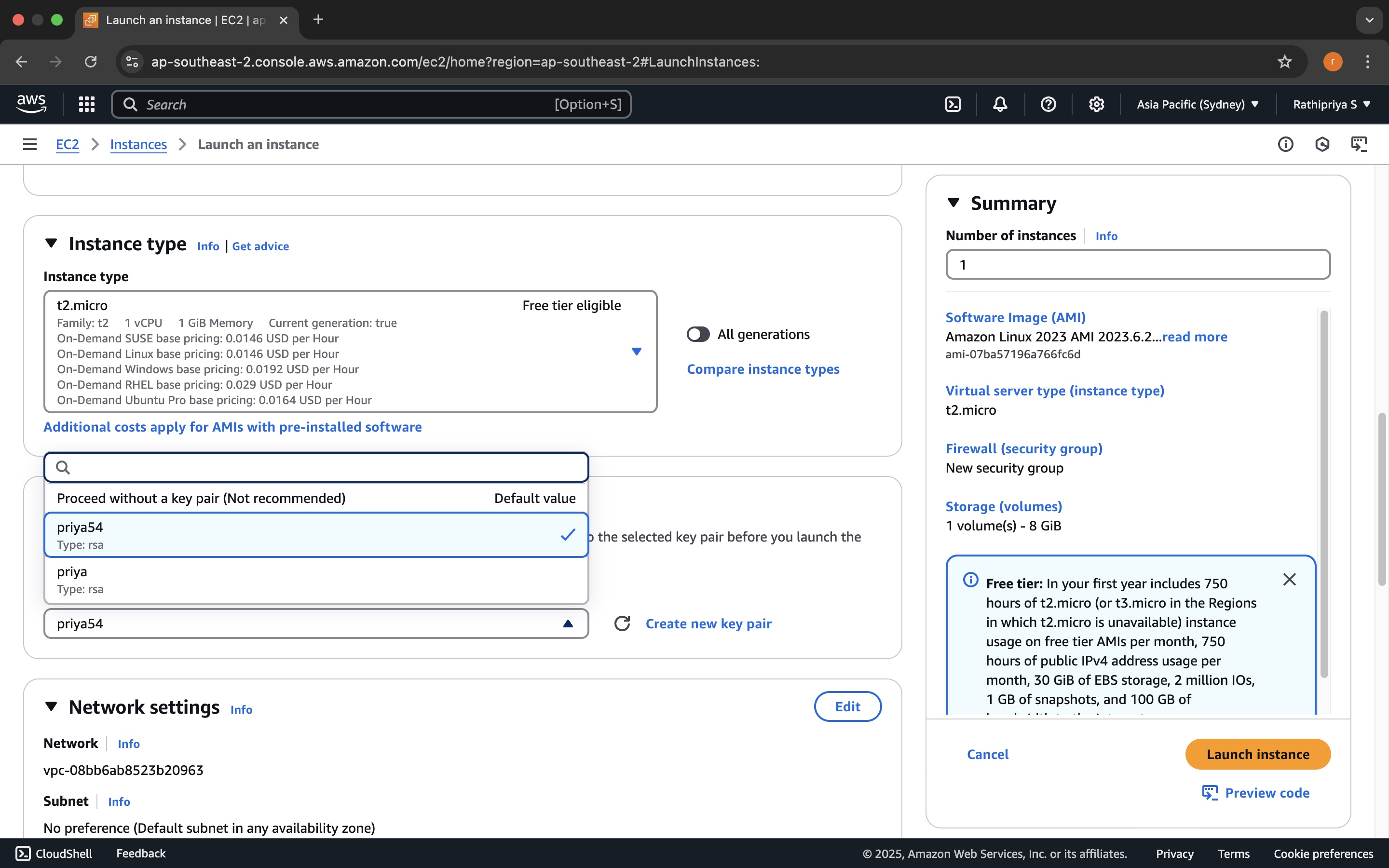
* Log in to AWS Management Console and navigate to the EC2 Dashboard.



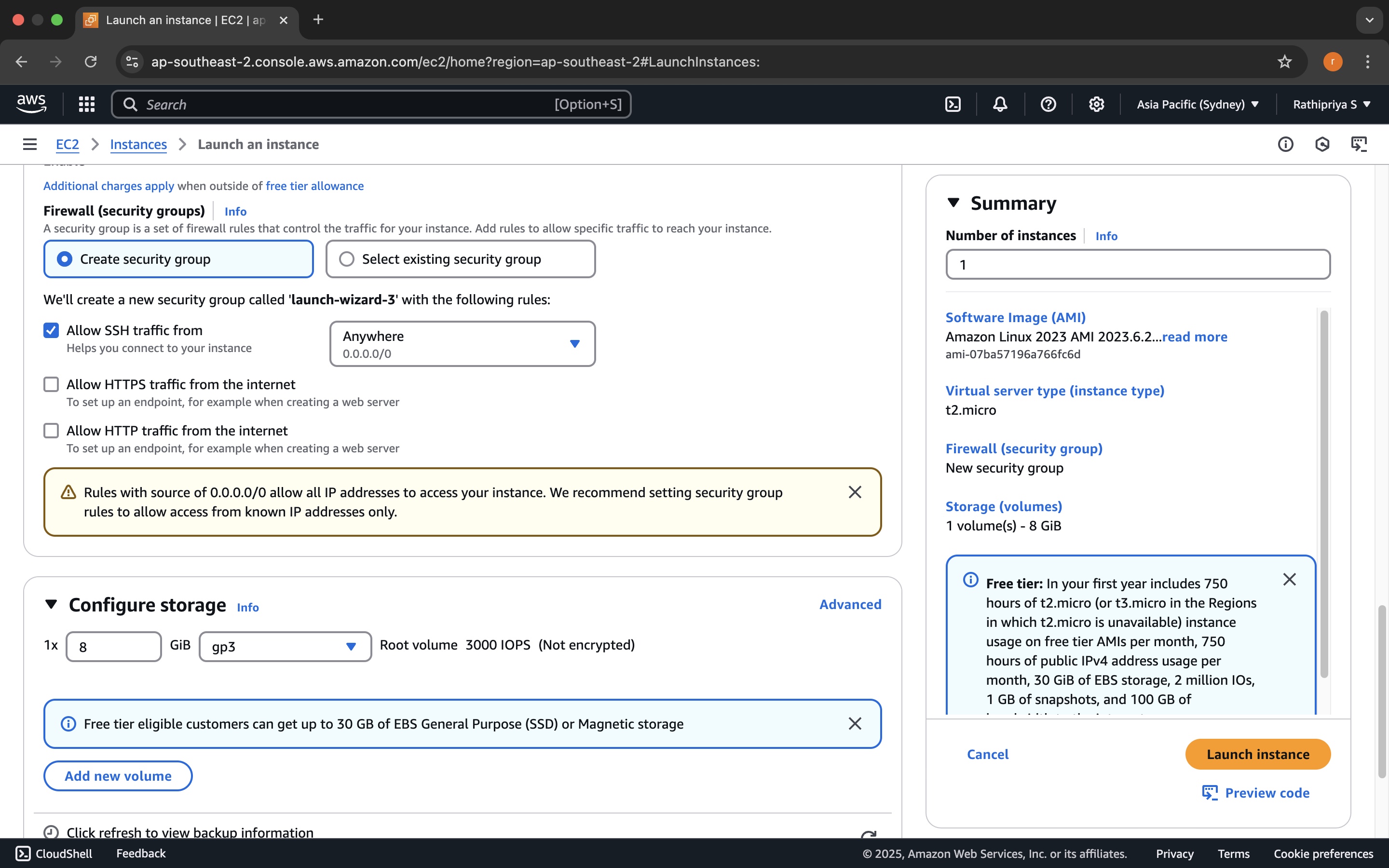
* Click Launch Instance to start the process of creating a new EC2 instance.
* Select an Amazon Machine Image (AMI) for your VM. Choose an OS like Ubuntu, Amazon Linux, or Windows based on your requirements.



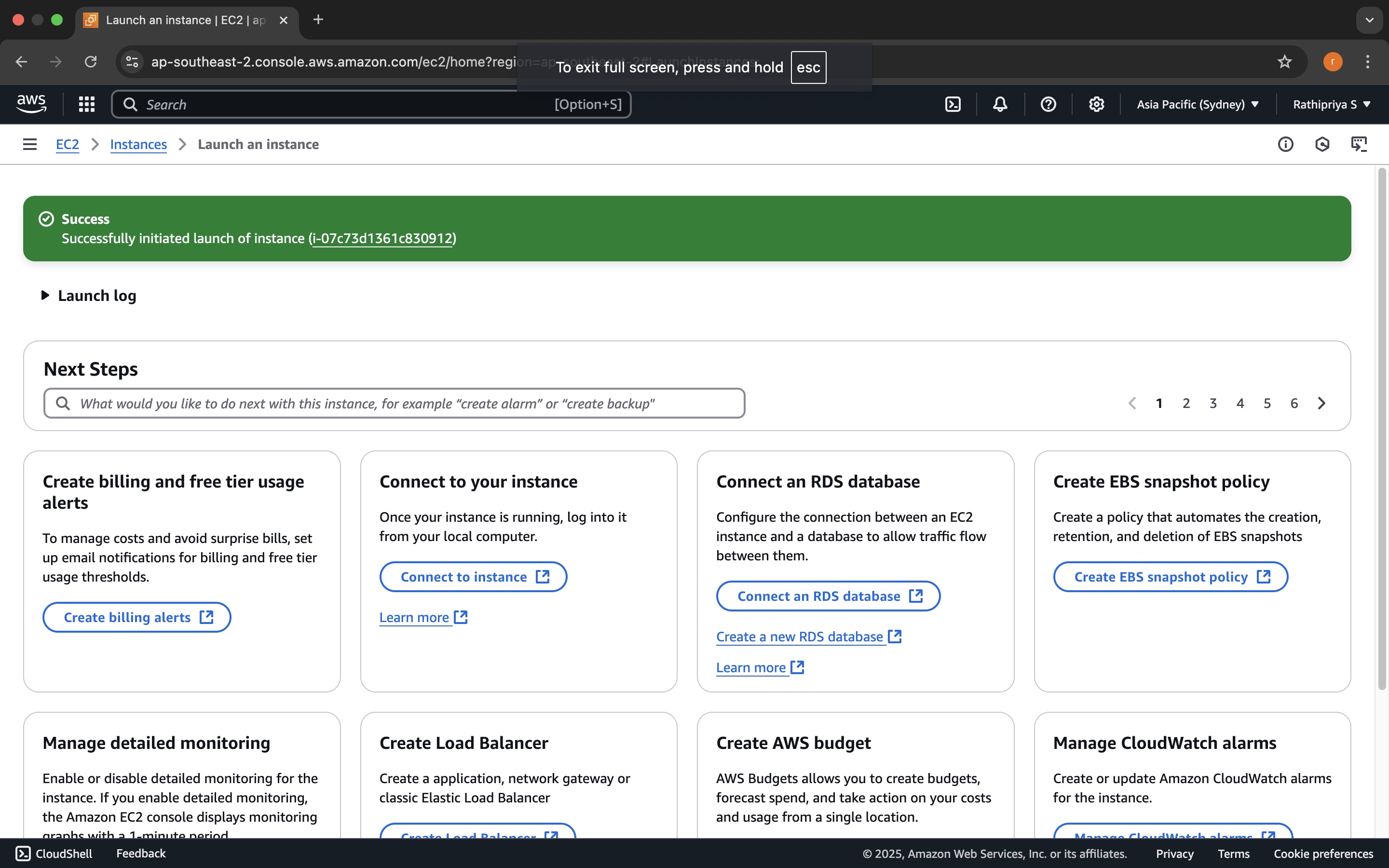
* Select an Instance Type (e.g., t2.micro for a small VM).



* Add Storage: You can modify the storage size here (e.g., add an EBS volume if necessary).
* Configure Security Group: Set up a security group to allow SSH (port 22) access to the instance.
  + Select Create a new security group and ensure that SSH is allowed from your IP address.



* Review your configurations and click Launch.



* When prompted, select Create a new key pair, download the key pair, and store it safely (this will be used to access your VM via SSH).

**Step 2: Access the EC2 Instance via SSH**

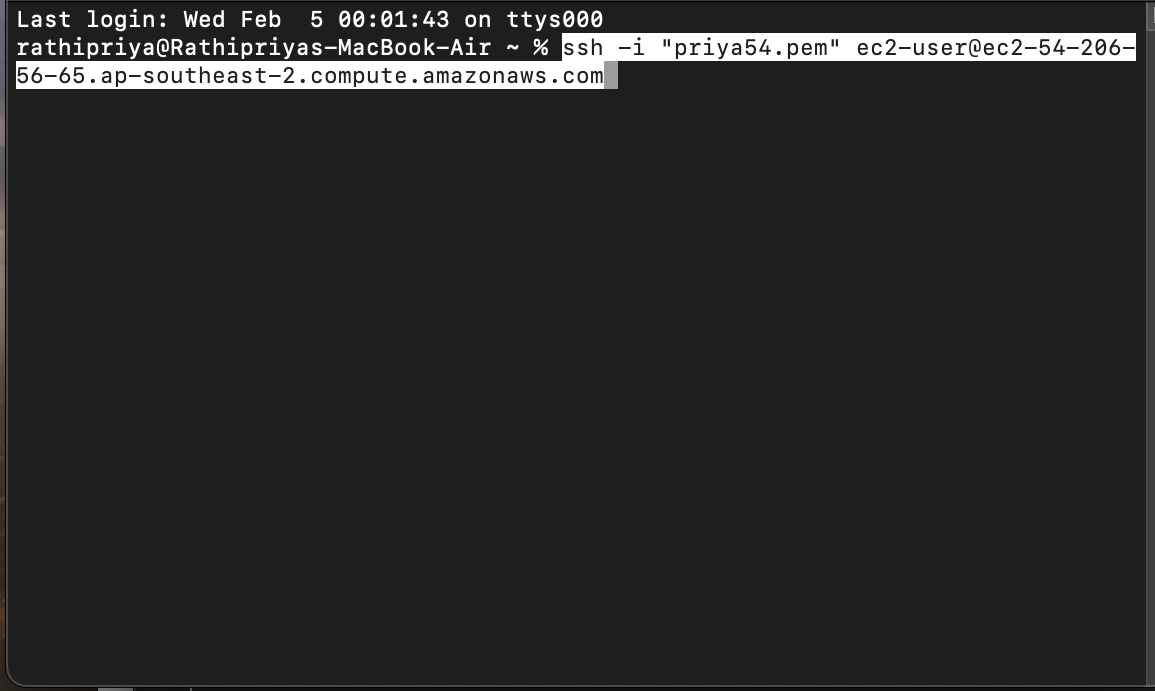
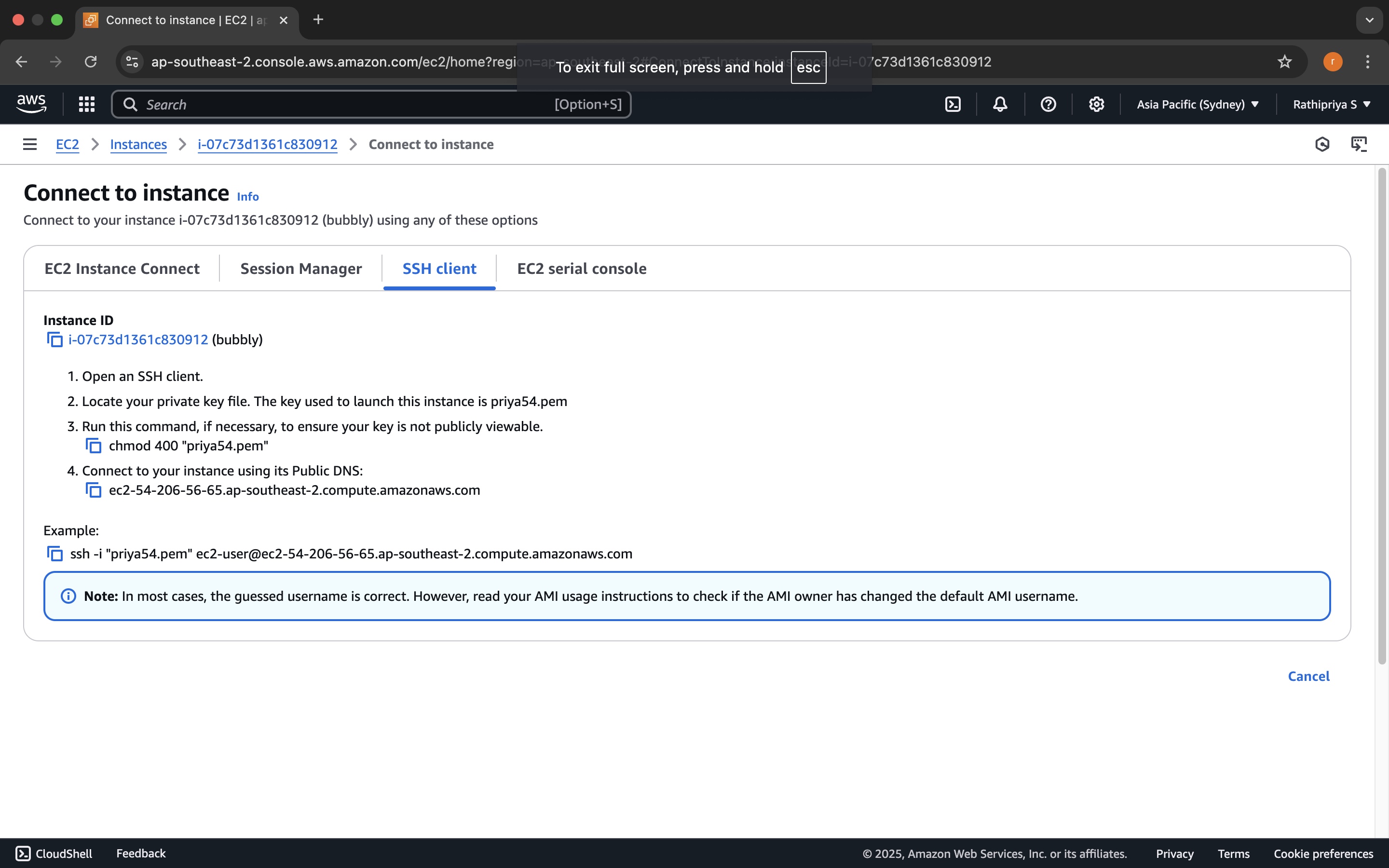
* Navigate to the directory where your .pem key pair file is located (the one you downloaded when launching the EC2 instance).



* Open a terminal (Linux/macOS) or use PuTTY (Windows).
* Use SSH to connect to your EC2 instance using its Public IP Address. The command format is:

ssh -i <your-key-file.pem> ec2-user@<your-ec2-public-ip>

For Ubuntu instances, replace ec2-user with ubuntu in the command.



* Accept the SSH fingerprint if prompted and you should be logged into your EC2 instance.

**Step 3: Verifying Connection and System Access**

* Once logged in, you can run commands like top, df -h, or uptime to verify the instance's status and check system performance.
* You can now install software, configure settings, and manage the instance remotely.

