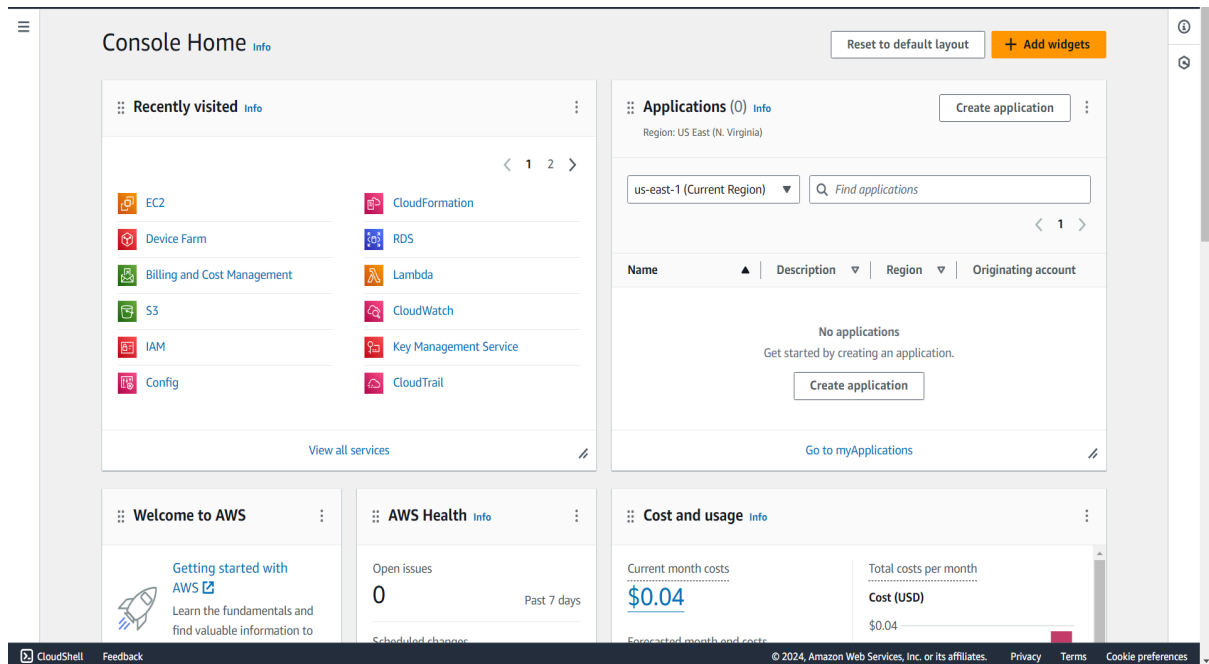
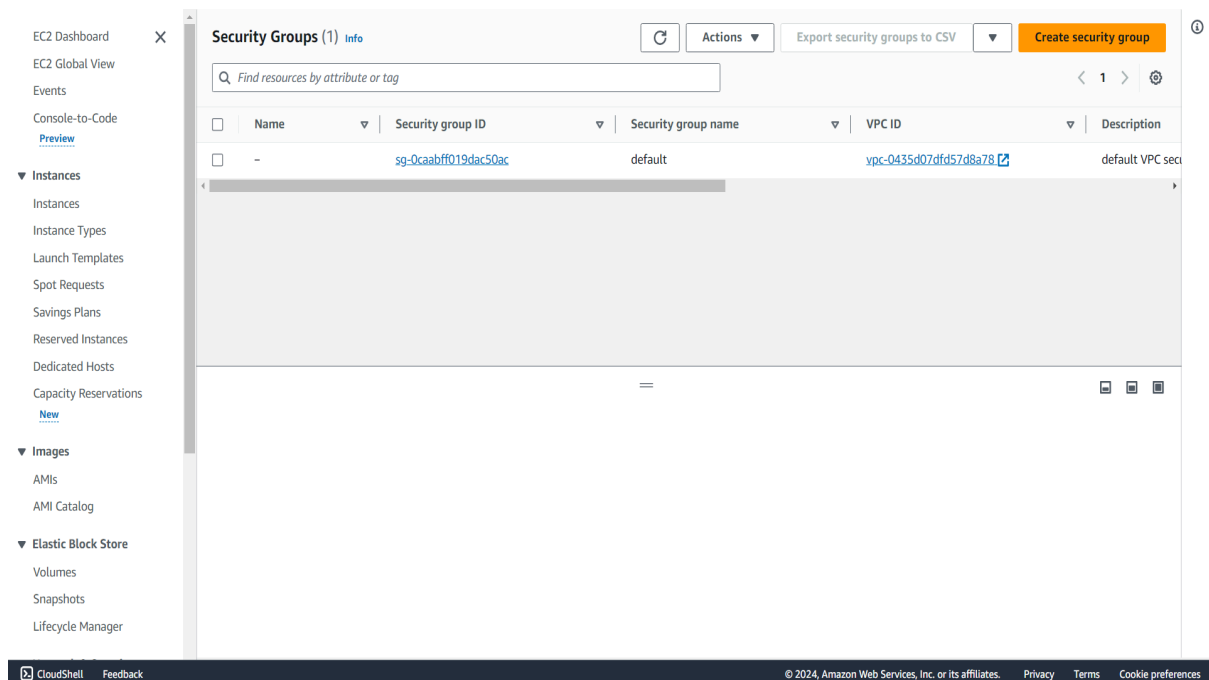


Starting AWS EC2 instance

Step 1: Sign in to aws account



Step 2: Go to EC2 dashboard and go to security groups and click on 'Create Security group'



Step 3: Give a name and description to the security group

EC2 > Security Groups > Create security group

Create security group

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name

sg_tanmayvaij_ec2docker

Name cannot be edited after creation.

Description

security group for my ec2 docker instance

VPC

vpc-0dbe7bc3f6036f9b4

Inbound rules

This security group has no inbound rules.

Add rule

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Step 4: Allow access to port 22, 80, 443 from anywhere in the inbound rules and set 'All Traffic' in outbound rules and click on create

Inbound rules

Type	Protocol	Port range	Source	Description - optional	
SSH	TCP	22	Anyw... 0.0.0.0/0		Delete
HTTP	TCP	80	Anyw... 0.0.0.0/0		Delete
HTTPS	TCP	443	Anyw... 0.0.0.0/0		Delete

Add rule

Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Outbound rules

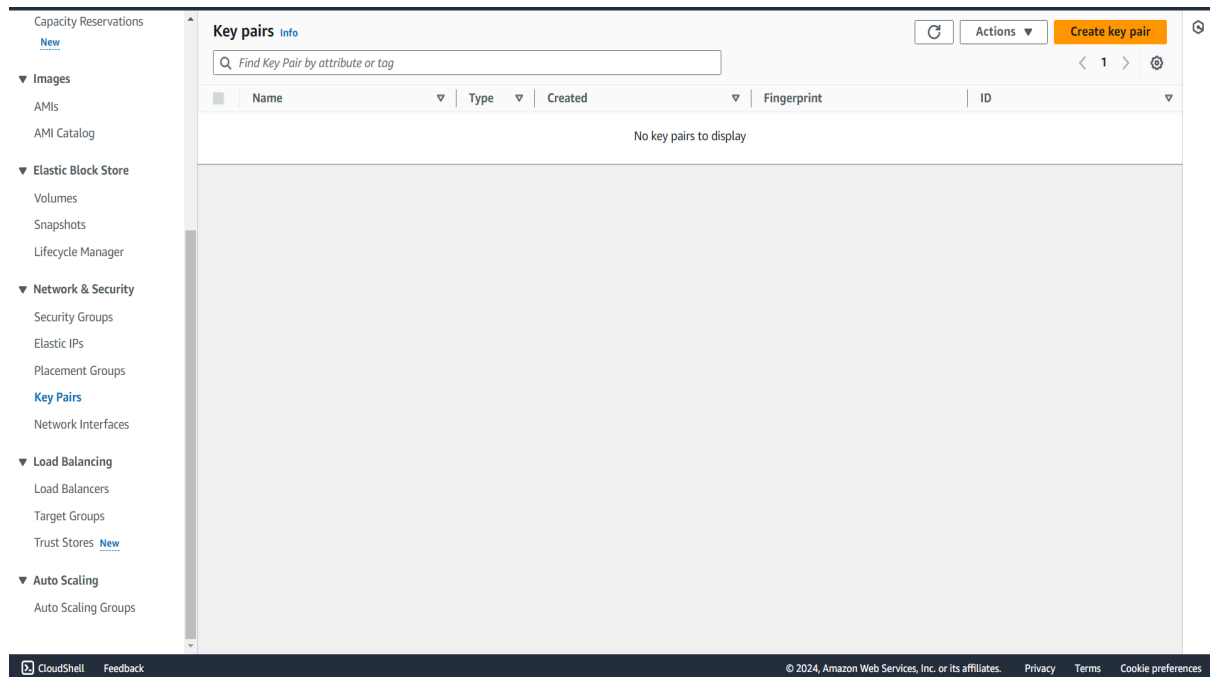
Type	Protocol	Port range	Destination	Description - optional	
All traffic	All	All	Custom 0.0.0.0/0		Delete

CloudShell

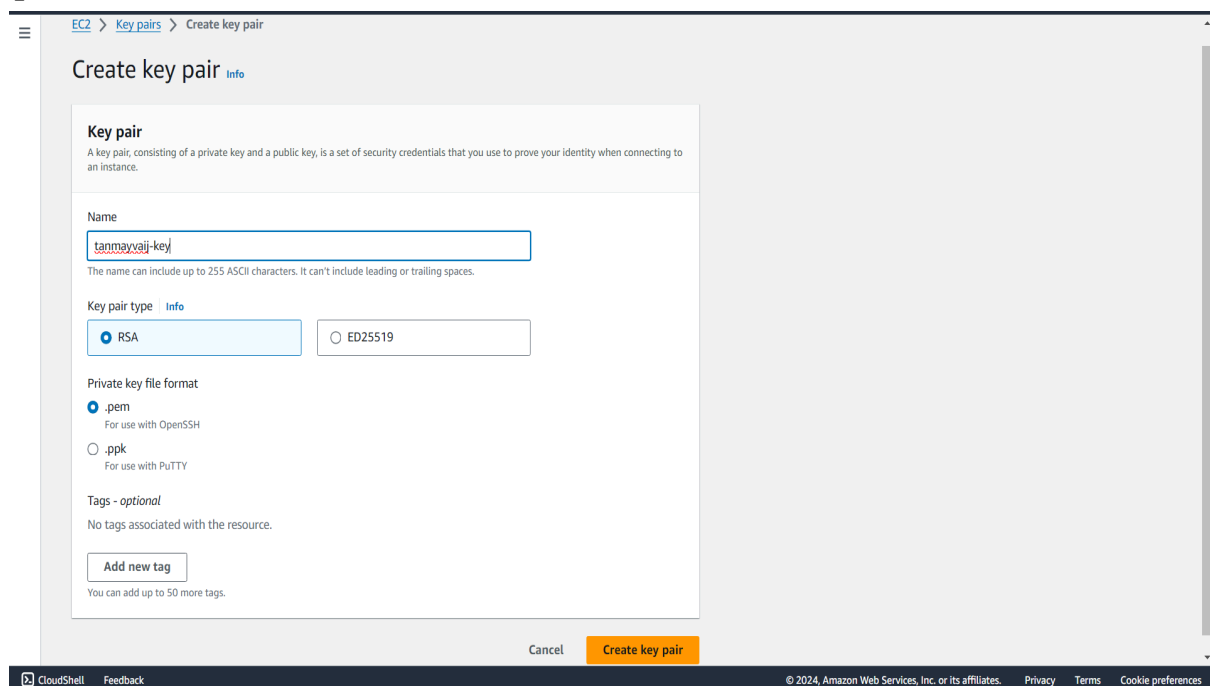
Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

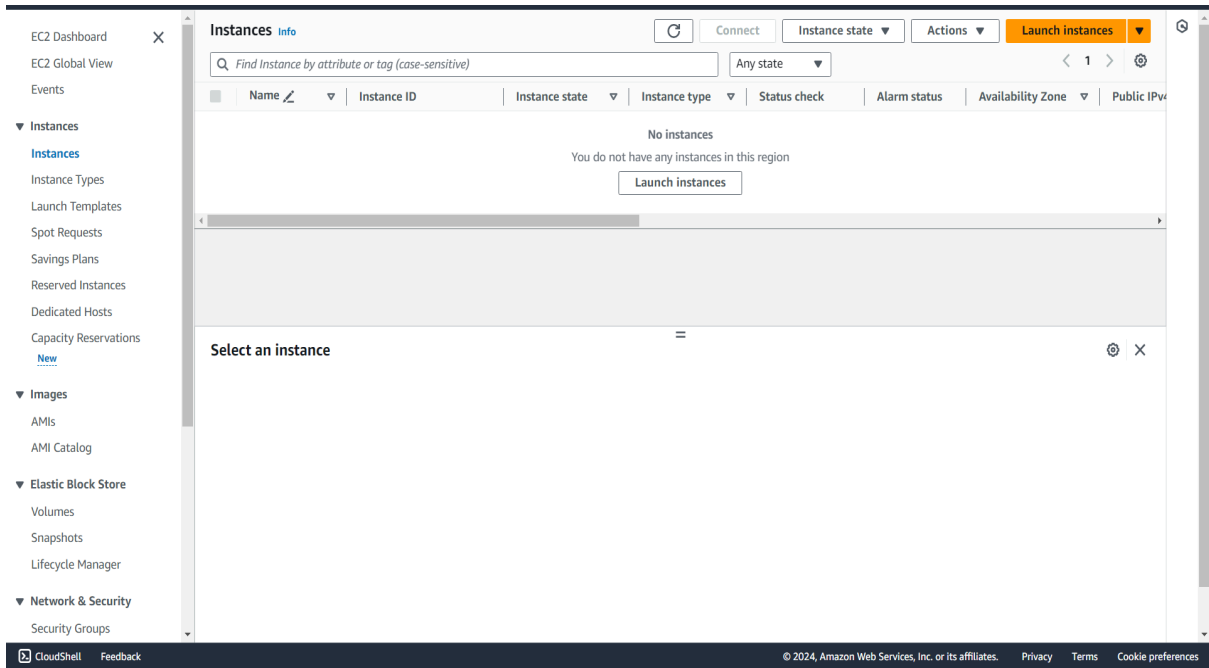
Step 5: Go the key pairs and click ‘Create key pair’



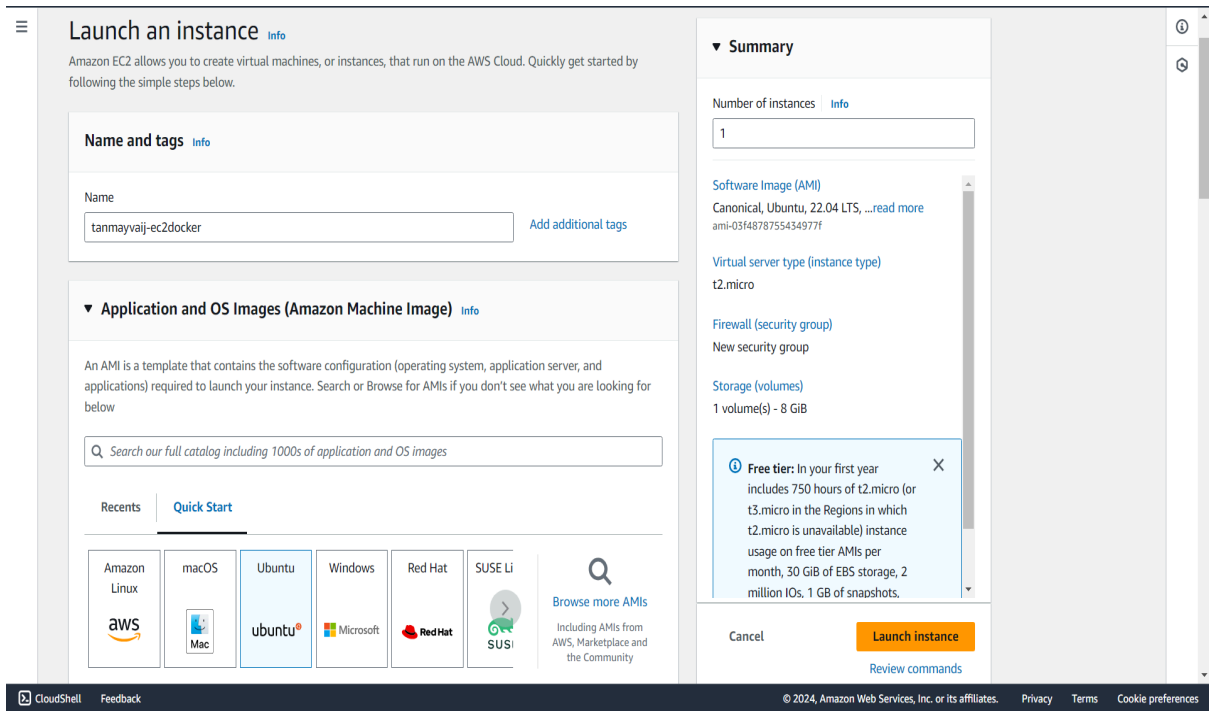
Step 6: Give a name to the key and set key pair type to RSA, file type to .pem and click on create



Step 7: Go to instances and click on ‘Launch instances’



Step 8: Give a name to the instance and select Ubuntu OS



Step 9: Select security group and key pair which was created in early steps, then click on 'Launch instance'

Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

tanmayvaj-key [Create new key pair](#)

Network settings Info [Edit](#)

Network Info

vpc-0dbe7bc3f6036f9b4

Subnet Info

No preference (Default subnet in any availability zone)

Auto-assign public IP Info

Enable

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☐ Create security group ☒ Select existing security group

Common security groups Info

Select security groups

sg_tanmayvaj_ec2docker sg-0eeae06dd24e4a332 [Compare security group rules](#)

VPC: vpc-0dbe7bc3f6036f9b4

Summary

Number of instances Info

1

Software Image (AMI)

Canonical, Ubuntu, 22.04 LTS, ...read more
ami-03f4878755434977f

Virtual server type (instance type)

t2.micro

Firewall (security group)

sg_tanmayvaj_ec2docker

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots.

Cancel [Launch instance](#) [Review commands](#)

Step 10: Click on the running EC2 instance and click on connect

EC2 Dashboard [×](#)

EC2 Global View

Events

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

[New](#)

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Network & Security

Security Groups

EC2 > Instances > i-07bc279332ecfec94

Instance summary for i-07bc279332ecfec94 (tanmayvaj-ec2docker) Info [Refresh](#) [Connect](#) [Instance state](#) [Actions](#)

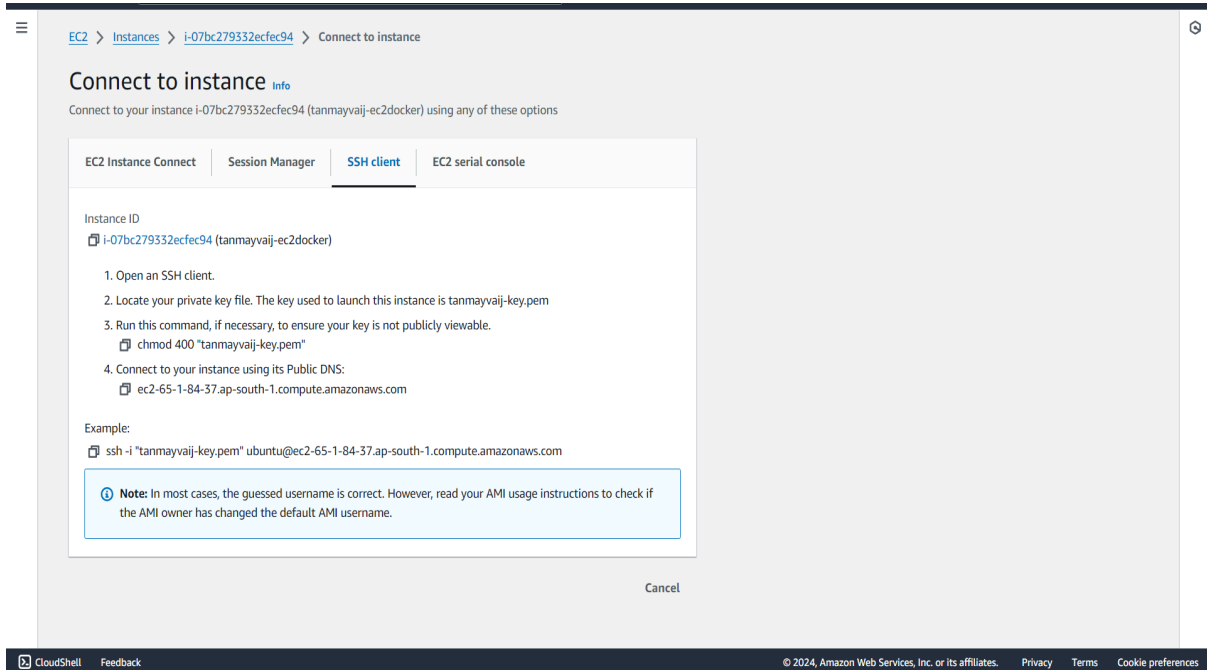
Updated less than a minute ago

Instance ID	Public IPv4 address	Private IPv4 addresses
i-07bc279332ecfec94 (tanmayvaj-ec2docker)	65.1.84.37 Open address	172.31.43.190
IPv6 address	Instance state	Public IPv4 DNS
-	Running	ec2-65-1-84-37.ap-south-1.compute.amazonaws.com Open address
Hostname type	Private IP DNS name (IPv4 only)	Elastic IP addresses
IP name: ip-172-31-43-190.ap-south-1.compute.internal	ip-172-31-43-190.ap-south-1.compute.internal	-
Answer private resource DNS name	Instance type	AWS Compute Optimizer finding
IPv4 (A)	t2.micro	Opt-in to AWS Compute Optimizer for recommendations.
Auto-assigned IP address	VPC ID	Learn more
65.1.84.37 [Public IP]	vpc-0dbe7bc3f6036f9b4	Auto Scaling Group name
IAM Role	Subnet ID	-
-	subnet-0e7d41dc412c388cd	
IMDSv2		
Required		

Details [Status and alarms](#) [Monitoring](#) [Security](#) [Networking](#) [Storage](#) [Tags](#)

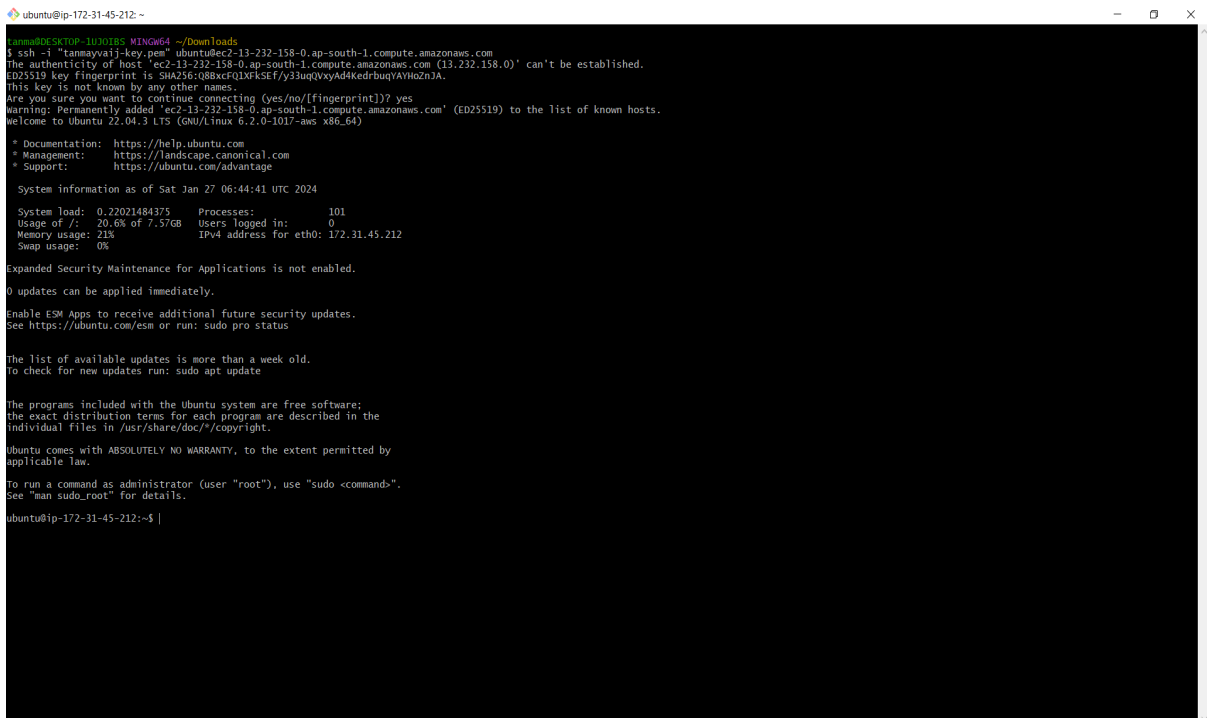
Instance details Info

Step 11: Go to SSH Client and copy the example command and run it in the local terminal to connect to the instance



The screenshot shows the AWS Management Console interface for connecting to an EC2 instance. The breadcrumb navigation at the top reads: [EC2](#) > [Instances](#) > [i-07bc279332ecfec94](#) > [Connect to instance](#). The main heading is "Connect to instance" with an "Info" link. Below the heading, a message states: "Connect to your instance i-07bc279332ecfec94 (tanmayvaji-ec2docker) using any of these options". There are four tabs: "EC2 Instance Connect", "Session Manager", "SSH client" (which is selected), and "EC2 serial console". Under the "SSH client" tab, the "Instance ID" is listed as [i-07bc279332ecfec94](#) (tanmayvaji-ec2docker). A numbered list of steps is provided: 1. Open an SSH client. 2. Locate your private key file. The key used to launch this instance is tanmayvaji-key.pem. 3. Run this command, if necessary, to ensure your key is not publicly viewable. `chmod 400 tanmayvaji-key.pem`. 4. Connect to your instance using its Public DNS: [ec2-65-1-84-37.ap-south-1.compute.amazonaws.com](#). An "Example:" section shows the command: `ssh -i tanmayvaji-key.pem ubuntu@ec2-65-1-84-37.ap-south-1.compute.amazonaws.com`. A blue note box contains the text: "Note: In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username." A "Cancel" button is located at the bottom right of the content area. The footer of the console shows "CloudShell", "Feedback", and copyright information for Amazon Web Services, Inc. or its affiliates, along with links for "Privacy", "Terms", and "Cookie preferences".

Step 12: Enter the command and instance will be connected



The screenshot shows a terminal window with the prompt `ubuntu@ip-172-31-45-212: ~`. The user has executed the command `ssh -i tanmayvaji-key.pem ubuntu@ec2-13-232-158-0.ap-south-1.compute.amazonaws.com`. The terminal output shows the SSH client's process of establishing a connection, including the host key fingerprint and a warning to add the host to the known hosts list. After confirming, the user is greeted by the Ubuntu 22.04.3 LTS login screen. The terminal displays system information, including system load, memory usage, and the list of available updates. The prompt at the bottom of the terminal is `ubuntu@ip-172-31-45-212:~$`.