

## QUESTION 2

Name tag of server and key pair as 'ec2usecase1':

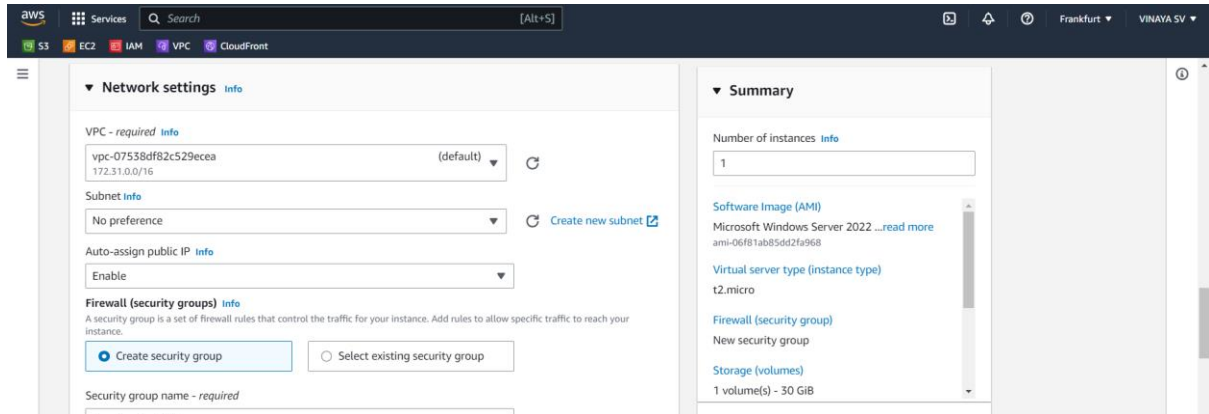
The first screenshot shows the 'Name and tags' section of the AWS EC2 console. It features a table with columns for Key, Value, and Resource types. The 'Name' key is set to 'ec2usecase1'. There is an 'Add tag' button and a note indicating 49 remaining tags out of a maximum of 50. The 'Summary' panel on the right shows 'Number of instances' set to 1, 'Software Image (AMI)' as 'Amazon Linux 2023 AMI 2023.0.2', 'Virtual server type (instance type)' as 't2.micro', and 'Firewall (security group)'.

The second screenshot shows the 'Key pair (login)' section. The 'Key pair name' is set to 'ec2usecase1'. There is a 'Create new key pair' button. The 'Summary' panel on the right shows 'Number of instances' set to 1, 'Software Image (AMI)' as 'Microsoft Windows Server 2022', and 'Virtual server type (instance type)' as 't2.micro'.

AMI as Windows OS:

The screenshot shows the 'Quick Start' section of the AWS console. It displays a grid of operating system options: Amazon Linux, macOS, Ubuntu, Windows, Red Hat, and S. The 'Windows' option is selected. Below the grid, the 'Amazon Machine Image (AMI)' section shows 'Microsoft Windows Server 2022 Base' as the selected AMI. The AMI ID is 'ami-06f81ab85dd2fa968'. The 'Description' section provides details about the AMI, including its architecture (64-bit x86) and provider status (Verified provider). The 'Summary' panel on the right shows 'Number of instances' set to 1, 'Software Image (AMI)' as 'Microsoft Windows Server 2022', 'Virtual server type (instance type)' as 't2.micro', and 'Firewall (security group)' as 'New security group'. At the bottom, there are buttons for 'Cancel', 'Launch instance', and 'Review commands'.

## Auto assigned public IP must be enabled:



**Network settings** info

VPC - *required* info  
vpc-07538df82c529ecea (default) [Refresh](#)

Subnet info  
No preference [Create new subnet](#)

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

Security group name - *required*

**Summary**

Number of instances info  
1

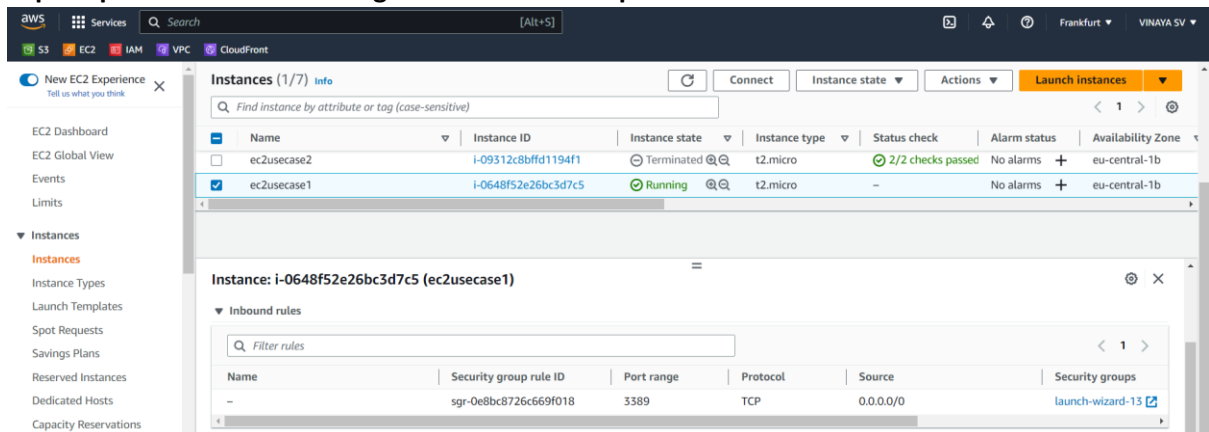
Software Image (AMI)  
Microsoft Windows Server 2022 ...[read more](#)  
ami-06f81ab85dd2fa968

Virtual server type (instance type)  
t2.micro

Firewall (security group)  
New security group

Storage (volumes)  
1 volume(s) - 30 GiB

## Expose port no. 3389 for taking the remote desktop connection:



**Instances (1/7)** info [Refresh](#) [Connect](#) [Instance state](#) [Actions](#) [Launch instances](#)

Find instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
ec2usecase2	i-09312c8bffd1194f1	Terminated	t2.micro	2/2 checks passed	No alarms	eu-central-1b
ec2usecase1	i-0648f52e26bc3d7c5	Running	t2.micro	-	No alarms	eu-central-1b

**Instance: i-0648f52e26bc3d7c5 (ec2usecase1)**

**Inbound rules**

Filter rules

Name	Security group rule ID	Port range	Protocol	Source	Security groups
-	sgr-0e8bc8726c669f018	3389	TCP	0.0.0.0/0	<a href="#">launch-wizard-13</a>

