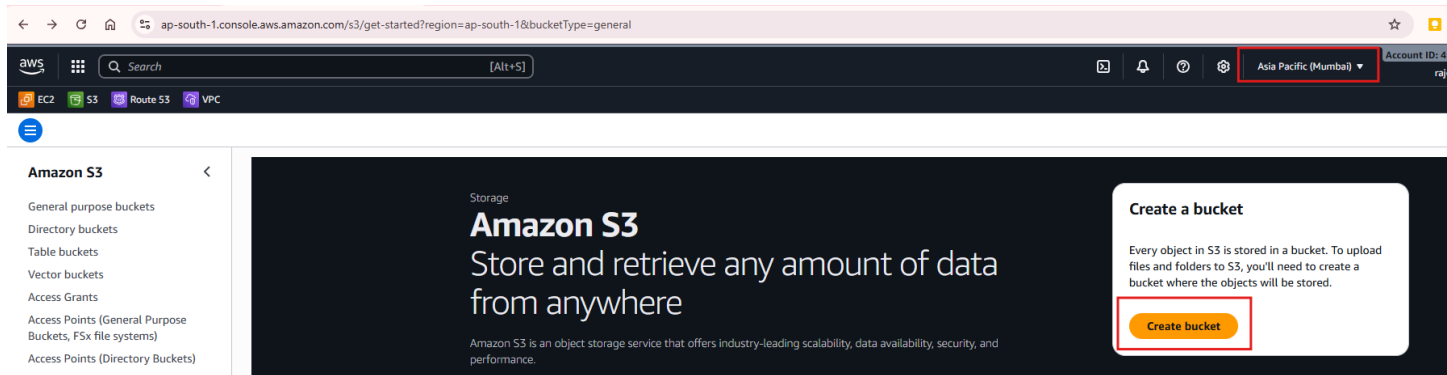Assignment - AWS July 27 2025 Batch

Question 1 : VPC Endpoint lab --> Need to connect EC2 instance with S3 bucket

1. Create S3 Bucket

1. **Open S3 Console**

   o Go to AWS Management Console → Services → S3

   o Click **"Create bucket"**

1. **Configure Bucket**

   o **Bucket name**: rajesh-s3bucket-27july

   o **AWS Region**: Asia Pacific (Mumbai) ap-south-1

   o **Block All Public Access**: Tick check

Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region

Asia Pacific (Mumbai) ap-south-1

Bucket type | Info

◉ **General purpose**
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

○ Directory
Recommended for low-latency use cases. These b
processing of data within a single Availability Zon

Bucket name | Info

rajesh-s3bucket-27july

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens

Copy settings from existing bucket - *optional*
Only the bucket settings in the following configuration are copied.

Choose bucket

Format: s3://bucket/prefix

Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to

Object Ownership

◉ **ACLs disabled (recommended)**
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

○ ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership
Bucket owner enforced

o   Click **"Create bucket"**

Amazon S3 › Buckets

⊘ **Successfully created bucket "rajesh-s3bucket-27july"**
To upload files and folders, or to configure additional bucket settings, choose **View details**.

General purpose buckets [All AWS Regions]   **Directory buckets**

General purpose buckets (1) Info   ↻   📋 Copy ARN | Empty | Delete | **Create bucket**   ▶ **Accou**
Buckets are containers for data stored in S3.   [Update]
                                                                                                 Storage
🔍 Find buckets by name   ‹ 1 › ⚙

Name ▲	AWS Region ▽	Creation date ▽
○ rajesh-s3bucket-27july	Asia Pacific (Mumbai) ap-south-1	October 10, 2025, 10:56:49 (UTC+05:30)

▶ **Exter**
[Update]
Externa
public a

2. Create VPC (if you don't have one)

1. **Open VPC Console**

o   Services → VPC

o   Click **"Your VPCs"** in left sidebar

o   Click **"Create VPC"**
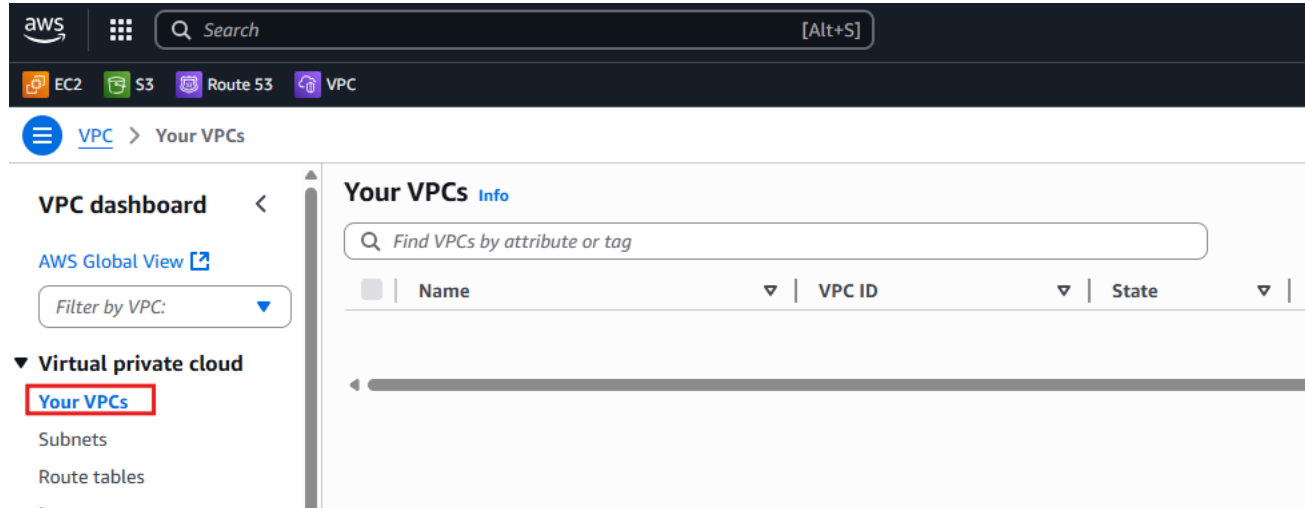
2. **Configure VPC**

o   **Resources to create**: VPC only

o   **Name tag**: rajesh-s3-vpc

o   **IPv4 CIDR**: 10.0.0.0/16   → VPC CIDR: 10.0.0.0/16 || Public Subnet: 10.0.1.0/24 || Private Subnet: 10.0.2.0/24

o   **Tenancy** "Default" - Instances run on shared hardware ,Multiple AWS customers share the same physical server, Cost-effective.

o   Click **"Create VPC"**

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create Info
Create only the VPC resource or the VPC and other networking resources.

- ◉ VPC only
- ○ VPC and more

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.

rajesh-s3-vpc

IPv4 CIDR block Info

- ◉ IPv4 CIDR manual input
- ○ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.0.0.0/16

CIDR block size must be between /16 and /28.

IPv6 CIDR block Info

- ◉ No IPv6 CIDR block
- ○ IPAM-allocated IPv6 CIDR block
- ○ Amazon-provided IPv6 CIDR block
- ○ IPv6 CIDR owned by me

Tenancy Info

Default ▼

⊘ You successfully created vpc-06b825f6ac1a5297f / rajesh-s3-vpc

vpc-06b825f6ac1a5297f / rajesh-s3-vpc

Details Info

VPC ID
⬚ vpc-06b825f6ac1a5297f

State
⊘ Available

Block Public A
⊖ Off

DNS resolution
Enabled

Tenancy
default

DHCP option s
dopt-0e0cb668

Main network ACL
acl-025b30cec390a6ec6

Default VPC
No

IPv4 CIDR
10.0.0.0/16

IPv6 CIDR (Network border group)
–

Network Address Usage metrics
Disabled

Route 53 Resol
–

Resource map | CIDRs | Flow logs | Tags | Integrations

Resource map Info

VPC
Your AWS virtual network

rajesh-s3-vpc

Subnets (0)
Subnets within this VPC

Route tables (1)
Route network traffic to resour

rtb-03ae5dca257896de6

3. Create Subnets

1. **Create Public Subnet**

   - In VPC Console → **Subnets** → **Create subnet**

   - **VPC ID**: Select your VPC

   - **Subnet name**: rajesh-public-subnet

   - **Availability Zone**: Select any AZ

   - **IPv4 CIDR**: 10.0.1.0/24 || Available IPv4 addresses – 2^8 – 5

   - Click **"Create subnet"**

subnet-0842d757f46dca09a / rajesh-public-subnet

Details

Subnet ID
subnet-0842d757f46dca09a

IPv4 CIDR
10.0.1.0/24

Availability Zone
aps1-az1 (ap-south-1a)

Network ACL
-

Auto-assign customer-owned IPv4 address
No

IPv6 CIDR reservations
–

Resource name DNS AAAA record
Disabled

Subnet ARN
arn:aws:ec2:ap-south-1:457271242412:subnet/subnet-0842d757f46dca09a

Available IPv4 addresses
251

Network border group
ap-south-1

Default subnet
No

Customer-owned IPv4 pool
–

IPv6-only
No

DNS64
Disabled

State
⊘ Available

IPv6 CIDR
–

VPC
vpc-06b825f6ac1a52

Auto-assign public I
No

Outpost ID
–

Hostname type
IP name

Owner
457271242412

2. **Create Private Subnet**

   o **Create subnet** again

   o **VPC ID**: Select your VPC

   o **Subnet name**: rajesh-private-subnet

   o **Availability Zone**: Select same AZ as public subnet

   o **IPv4 CIDR**: 10.0.2.0/24

   o Click **"Create subnet"**

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

> rajesh-private-subnet

The name can be up to 256 characters long.

Availability Zone   Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

> Asia Pacific (Mumbai) / aps1-az1 (ap-south-1a)

IPv4 VPC CIDR block   Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

> 10.0.0.0/16

IPv4 subnet CIDR block

> 10.0.2.0/24

`<` `>` `^` `v`

subnet-087a88015b1ccfc05 / rajesh-private-subnet

Details

Subnet ID 📋 subnet-087a88015b1ccfc05	**Subnet ARN** 📋 arn:aws:ec2:ap-south-1:457271242412:subnet/subnet-087a88015b1ccfc05	**State** ⊘ Available
IPv4 CIDR 📋 10.0.2.0/24	**Available IPv4 addresses** 📋 251	**IPv6 CIDR** –
Availability Zone 📋 aps1-az1 (ap-south-1a)	**Network border group** 📋 ap-south-1	**VPC** vpc-06b825f6ac1a52
Network ACL acl-025b30cec390a6ec6	**Default subnet** No	**Auto-assign public IF** No
Auto-assign customer-owned IPv4 address No	**Customer-owned IPv4 pool** –	**Outpost ID** –
IPv6 CIDR reservations –	**IPv6-only** No	**Hostname type** IP name
Resource name DNS AAAA record Disabled	**DNS64** Disabled	**Owner** 📋 457271242412

4. Create Internet Gateway

1. **VPC Console → Internet Gateways → Create internet gateway**

   o **Name tag:** rajesh-main-igw

   o Click **"Create internet gateway"**

2. **Attach to VPC**

   o Select the IGW → **Actions** → **Attach to VPC**

   o Select your VPC → **Attach internet gateway**

5. Create Route Tables

1. **Public Route Table**

   o **Route Tables** → **Create route table**

   o **Name:** rajesh-public-rt

   o **VPC:** Select your VPC

   o Click **"Create route table"**

⊘ Route table rtb-0f7c7115f7f9bd8d5 | rajesh-public-rt was created successfully.

rtb-0f7c7115f7f9bd8d5 / rajesh-public-rt

Details Info

Route table ID	Main	Explicit subnet
⧉ rtb-0f7c7115f7f9bd8d5	⧉ No	–
VPC	**Owner ID**	
vpc-06b825f6ac1a5297f | rajesh-s3-vpc	⧉ 457271242412	

Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (1)

Q Filter routes

Destination ▽	Target ▽	Status
10.0.0.0/16	local	⊘ Active

2. **Add Internet Route**

   o Select rajesh-public-rt route table → **Routes tab** → **Edit routes**

   o **Add route**:

      ▪ **Destination**: 0.0.0.0/0

      ▪ **Target**: Internet Gateway (select your IGW)

   o Click **"Save changes"**

⊘ Route table rtb-0f7c7115f7f9bd8d5 | rajesh-public-rt was created successfully.

Route tables (1/2) Info

Q Find route tables by attribute or tag

▣	Name	Route table ID ▽	Explicit subnet associ... ▽	Edge associations ▽
☐	–	rtb-03ae5dca257896de6	–	–
☑	rajesh-public-rt	rtb-0f7c7115f7f9bd8d5	–	–

Edit routes

Destination	Target	Status
10.0.0.0/16	local ▼	⊘ Active
	Q local ✕	
Q 0.0.0.0/0 ✕	Internet Gateway ▼	–
	Q igw-0bd17f88293378fa3 ✕	

(Add route)

3. **Associate Public Subnet with Route Table**

   o Select your public route table

   o Go to the Subnet associations tab below

   o Click Edit subnet associations

   o In the popup, check the box next to your public-subnet

   o Click Save associations

4. **Private Route Table**

   o **Create route table**

   o **Name:** rajesh-private-rt

- o **VPC**: Select your VPC

- o Click **"Create route table"**

✓ Route table rtb-01a30d8099a10d788 | rajesh-private-rt was created successfully.

rtb-01a30d8099a10d788 / rajesh-private-rt

Details Info

Route table ID
⎘ rtb-01a30d8099a10d788

Main
⎘ No

Explicit subnet associations
–

Edge
–

VPC
vpc-06b825f6ac1a5297f | rajesh-s3-vpc

Owner ID
⎘ 457271242412

5. **Associate Private Subnet**

- o Select private route table → **Subnet associations** → **Edit subnet associations**

- o Check private-subnet → **Save associations**

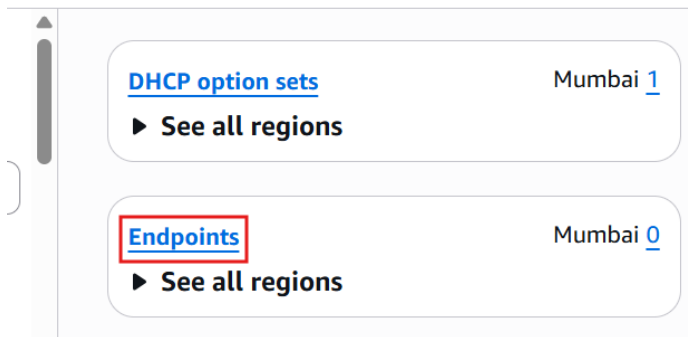| Routes | **Subnet associations** | Edge associations | Route propagation | Tags |

Explicit subnet associations (1)

🔍 Find subnet association

Name	▽	Subnet ID	▽	IPv4 CIDR	▽	IPv6 CID
rajesh-private-subnet		subnet-087a88015b1ccfc05		10.0.2.0/24		–

6. Create VPC Endpoint for S3

1. **VPC Console → Endpoints → Create Endpoint**

2. **Configure Endpoint**

   o **Service category**: AWS services

   o **Service name**: Find com.amazonaws.region.s3 (Gateway type)

   o **VPC**: Select your VPC

   o **Route tables**: Select private-rt (your private route table)

   o **Policy**: Full access (default)

   o Click **"Create endpoint"**

Services (1/2)

Search

Service Name = com.amazonaws.ap-south-1.s3   ✕ | Clear filters

Service Name	Owner	Type
● com.amazonaws.ap-south-1.s3	amazon	Gateway
○ com.amazonaws.ap-south-1.s3	amazon	Interface

Network settings
Select the VPC in which to create the endpoint

VPC
Create the VPC endpoint in the VPC in the same AWS Region from which you will access a resource.

vpc-06b825f6ac1a5297f (rajesh-s3-vpc)   ▼

7. Create EC2 Instance in Private Subnet

1. **EC2 Console → Instances → Launch instances**

2. **Configure Instance**

   o **Name**: Rajesh-EC2-private

   o **AMI**: Amazon Linux 2023 AMI Kernel 6.1

   o **Instance type**: t3.micro

   o **Key pair**: Create new

Instances (1) Info   Connect

Find Instance by attribute or tag (case-sensitive)   All states ▼

Instance state = running   ✕ | Clear filters

☐	Name ✎	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
☐	Rajesh-EC2-private	i-0bd37da725614cd8c	⊘ Running ⊕ ⊖	t3.micro	⊘ 3/3 checks passed	View alarms +	ap-south-1a

3. **Network Settings**

   o **VPC**: Select your VPC

   o **Subnet**: Select private-subnet

   o **Auto-assign Public IP**: Disable

vpc-06b825f6ac1a5297f / rajesh-s3-vpc

Details Info

VPC ID
vpc-06b825f6ac1a5297f

State
⊘ Available

Block Public Access
⊖ Off

DNS resolution
Enabled

Tenancy
default

DHCP option set
dopt-0e0cb66899dbcf823

Main network ACL
acl-025b30cec390a6ec6

Default VPC
No

IPv4 CIDR
10.0.0.0/16

IPv6 CIDR (Network border group)
–

Network Address Usage metrics
Disabled

Route 53 Resolver DNS Firewall rule groups
–

Resource map | CIDRs | Flow logs | Tags | Integrations

Resource map Info

VPC
Your AWS virtual network

rajesh-s3-vpc

Subnets (2)
Subnets within this VPC

ap-south-1a

A rajesh-public-subnet

A rajesh-private-subnet

Route tables (3)
Route network traffic to resources

rajesh-private-rt

rtb-03ae5dca257896de6

rajesh-public-rt

Network Connec
Connections to oth

rajesh-main-igw

vpce-0be2be501a

Issue : Unable to connect to the EC2 instance console. (private subnet)

Question 2 : NAT instance --> How to give internet access to my private subnet EC2 instance using NAT instance.