

School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

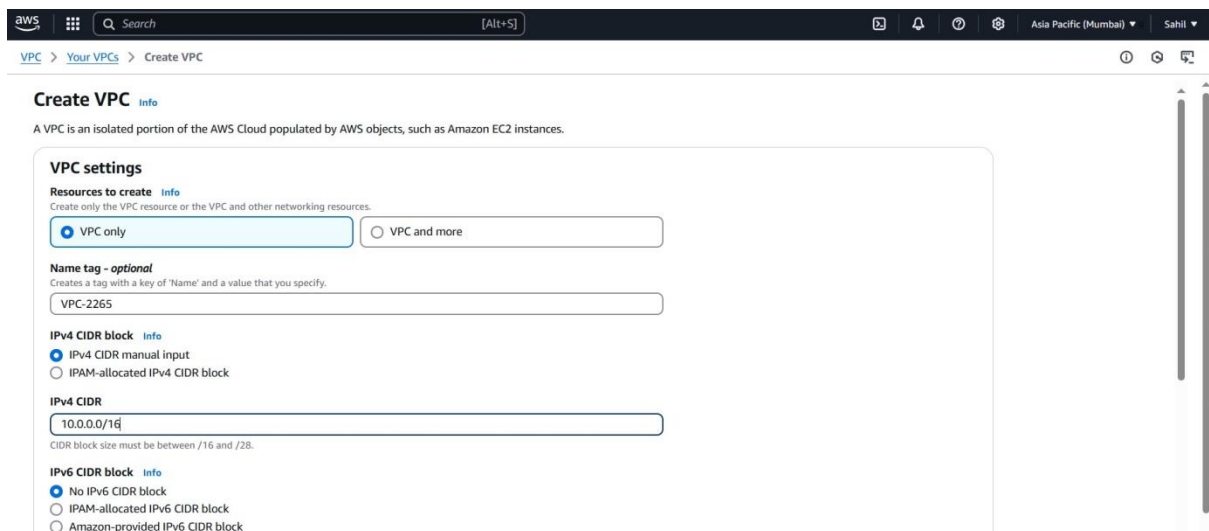
Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 4. Private Access to S3 via VPC Endpoint in a Secure VPC Architecture.

Step 1: Create a VPC and connect Internet Gateway to it.

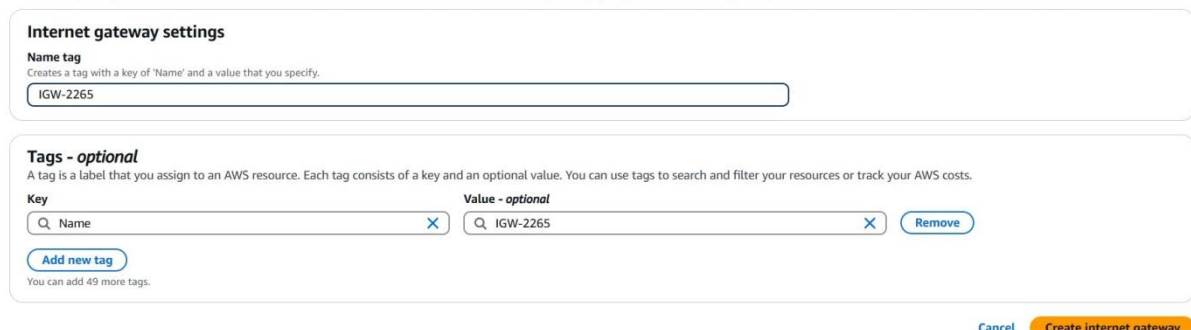
- Go to AWS console and search for VPC.
- Create VPC by selecting 'VPC Only' with valid name.
- Set IPv4 CIDR range as '10.0.0.0/16'.



- Go to Internet Gateway.
- Create an Internet Gateway.

Create internet gateway

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.



- Attach the IGW to the VPC.

School of Computer Science, Engineering and Applications (SCSEA)

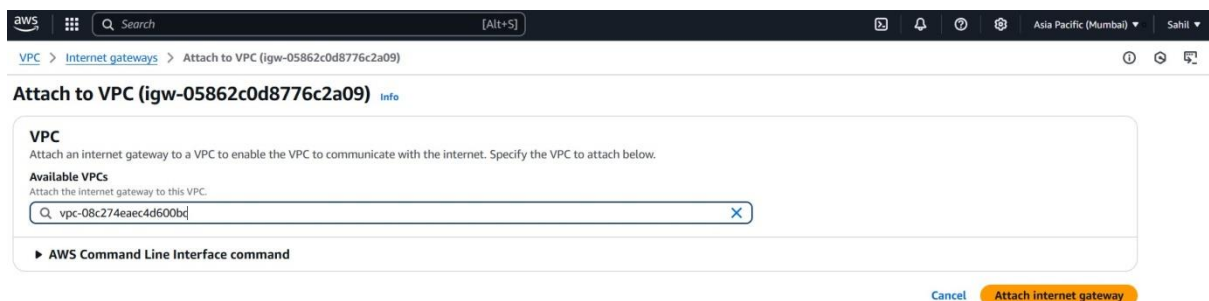
B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

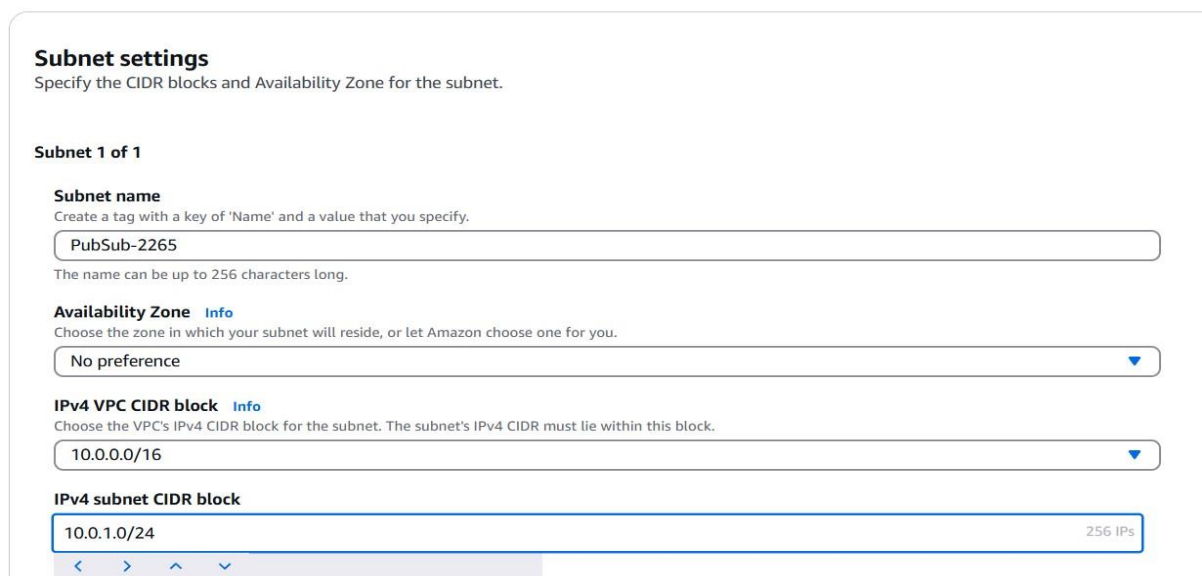
Title of Practical: 4. Private Access to S3 via VPC Endpoint in a Secure VPC Architecture.



The screenshot shows the AWS Management Console interface for the 'Attach to VPC' step. The breadcrumb trail is 'VPC > Internet gateways > Attach to VPC (igw-05862c0d8776c2a09)'. The main heading is 'Attach to VPC (igw-05862c0d8776c2a09)'. Below this, there's a section for 'VPC' with instructions: 'Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.' Under 'Available VPCs', there's a search bar with the text 'vpc-08c274eac4d600b' entered. At the bottom right, there are two buttons: 'Cancel' and 'Attach internet gateway'.

Step 2: Create a Public Subnet and a Private Subnet and Route Tables respectively.

- Create a Public Subnet and name it 'PubSub-2265'.
- Enter IPV4 subnet CIDR block as "10.0.1.0/24", then click on "Create subnet".



The screenshot shows the 'Subnet settings' page in the AWS Management Console. The heading is 'Subnet settings' with the instruction 'Specify the CIDR blocks and Availability Zone for the subnet.' Below this, it says 'Subnet 1 of 1'. The 'Subnet name' field is set to 'PubSub-2265'. The 'Availability Zone' is set to 'No preference'. The 'IPv4 VPC CIDR block' is set to '10.0.0.0/16'. The 'IPv4 subnet CIDR block' is set to '10.0.1.0/24' with a note '256 IPs'.

- Create a Private Subnet and name it 'PvtSub-2265'.
- Enter IPV4 subnet CIDR block as "10.0.2.0/24", then click on "Create subnet".

School of Computer Science, Engineering and Applications (SCSEA)
B. Tech TY (CCSA)
Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade **PRN:** 20220802265
Title of Practical: 4. Private Access to S3 via VPC Endpoint in a Secure VPC Architecture.

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.

PvtSub-2265

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.

No preference

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

256 IPs

- After creating both the subnets, go to Public Subnet – 'Actions' – 'Edit subnet settings' – Tick the 'Enable auto-assign public IPv4 address'.

Edit subnet settings [Info](#)

Subnet

Subnet ID

subnet-014856f3332e1c430

Name

PubSub-2265

Auto-assign IP settings [Info](#)

Enable AWS to automatically assign a public IPv4 or IPv6 address to a new primary network interface for an instance in this subnet.

☒ Enable auto-assign public IPv4 address [Info](#)

☐ Enable auto-assign customer-owned IPv4 address [Info](#)
Option disabled because no customer owned pools found.

- Create a Public Route Table and name it 'PublicRT-2265' and select the VPC we created.

School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 4. Private Access to S3 via VPC Endpoint in a Secure VPC Architecture.

- Associate the Public Subnet to the Route Table.

Create route table [Info](#)

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - optional

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

PublicRT-2265

VPC

The VPC to use for this route table.

vpc-0e2f1823af222ece7 (VPC-2265)

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Q Name

Value - optional

Q PublicRT-2265

Remove

Add new tag

You can add 49 more tags.

rtb-003be38a244ed9f95 / PublicRT-2265

Actions

Details [Info](#)

Route table ID

rtb-003be38a244ed9f95

Main

No

Explicit subnet associations

subnet-014856f3332e1c430 / PubSub-2265

Edge associations

-

VPC

vpc-0e2f1823af222ece7 | VPC-2265

Owner ID

908027405956

Routes

Subnet associations

Edge associations

Route propagation

Tags

Explicit subnet associations (1)

Edit subnet associations

Find subnet association

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
PubSub-2265	subnet-014856f3332e1c430	10.0.1.0/24	-

- Add a Route with Destination as '0.0.0.0/0' and Target as 'Internet Gateway' and select the internet gateway we created i.e. 'IGW-2265'.

School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 4. Private Access to S3 via VPC Endpoint in a Secure VPC Architecture.

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
<input type="text" value="0.0.0.0/0"/>	<input type="text" value="Internet Gateway"/>	-	No
	<input type="text" value="igw-0de4b2530721f9523"/>		

[Add route](#)

[Cancel](#) [Preview](#) [Save changes](#)

- Create a Private Route Table and name it 'PrivateRT-2265' and select the VPC we created.
- Associate the Private Subnet to the Route Table.

Create route table

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

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

VPC
The VPC to use for this route table.

Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key
 [Remove](#)

[Add new tag](#)
You can add 49 more tags.

[Cancel](#) [Create route table](#)

rtb-0a33a24bc85cb05b8 / PrivateRT-2265

Details

Route table ID <input type="text" value="rtb-0a33a24bc85cb05b8"/>	Main <input type="text" value="No"/>	Explicit subnet associations <input type="text" value="subnet-0a88cf83a9fed6815 / PvtSub-2265"/>	Edge associations <input type="text" value="-"/>
VPC <input type="text" value="vpc-0e2f1823af222ece7 VPC-2265"/>	Owner ID <input type="text" value="908027405956"/>		

[Routes](#) [Subnet associations](#) [Edge associations](#) [Route propagation](#) [Tags](#)

Explicit subnet associations (1)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
PvtSub-2265	subnet-0a88cf83a9fed6815	10.0.2.0/24	-

[Edit subnet associations](#)

School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 4. Private Access to S3 via VPC Endpoint in a Secure VPC Architecture.

Step 3: Create Security Groups (for public and private instances) and attach the VPC.

- Create a Public Security Group and name it 'Bastion-SG-2265'.
- Add description and attach the VPC 'VPC-2265'.

Create security group [Info](#)

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 [Info](#)

Bastion-SG-2265

Name cannot be edited after creation.

Description [Info](#)

Allow SSH, HTTP and HTTPS

VPC [Info](#)

vpc-0e2f1823af222ece7 (VPC-2265)

- Set Inbound Rules : SSH – Anywhere IPv4, HTTP – Anywhere IPv4 and HTTPS – Anywhere IPv4.

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info
SSH	TCP	22	Anyw... 0.0.0.0/0	<input type="text"/>
HTTP	TCP	80	Anyw... 0.0.0.0/0	<input type="text"/>
HTTPS	TCP	443	Anyw... 0.0.0.0/0	<input type="text"/>

[Add rule](#)

Outbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Destination Info	Description - optional Info
All traffic	All	All	Custom 0.0.0.0/0	<input type="text"/>

- Create a Private Security Group and name it 'PvtInstance-SG-2265'.

School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 4. Private Access to S3 via VPC Endpoint in a Secure VPC Architecture.

- Add description and attach the VPC 'VPC-2265'.

Create security group [Info](#)

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 [Info](#)

PvtInstance-SG-2265

Name cannot be edited after creation.

Description [Info](#)

Allow SSH

VPC [Info](#)

vpc-0e2f1823af222ece7 (VPC-2265)

- Set Inbound Rules : SSH – Source – Custom – Bastion-SG-2265.

Inbound rules [Info](#)

Type	Protocol	Port range	Source	Description - optional
SSH	TCP	22	Custom sg-0b96d9f79d4cb0! X sg-0b96d9f79d4cb05c6 X	
Add rule				

Outbound rules [Info](#)

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	Custom 0.0.0.0/0 X	
Add rule				

Step 4: Create an Endpoint.

- Create an Endpoint with name 'S3Endpoint-2265'.
- Select Type as 'AWS services'.

School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 4. Private Access to S3 via VPC Endpoint in a Secure VPC Architecture.

Create endpoint [Info](#)

Create the type of VPC endpoint that supports the service, service network or resource to which you want to connect.

Endpoint settings

Specify a name and select the type of endpoint.

Name tag - optional

Creates a tag with a key of 'Name' and a value that you specify. Tags help you find and manage your endpoint.

S3Endpoint-2265

Type [Info](#)

Select a category

☒ AWS services

Connect to services provided by Amazon with an Interface endpoint, or a Gateway endpoint

☐ PrivateLink Ready partner services

Connect to SaaS services which have AWS Service Ready designation with an Interface endpoint. Uses AWS PrivateLink

☐ AWS Marketplace services

Connect to SaaS services that you have purchased through AWS Marketplace with an Interface Endpoint

☐ EC2 Instance Connect Endpoint

An elastic network interface that allow you to connect to resources in a private subnet

☐ Resources - New

Connect to resources like Amazon Relational Database Services (RDS) with a Resource endpoint. Uses AWS PrivateLink

☐ Service networks - New

Connect to VPC Lattice service networks with a Service network endpoint. Uses AWS PrivateLink

☐ Endpoint services that use NLBs and GWLBs

Find services shared with you by service name. Connect to a Network LoadBalancer (NLB) service with an Interface endpoint or to a Gateway LoadBalancer (GWLB) service with a Gateway Load Balancer endpoint

- In Services Tab, search for 's3' and select the S3 service with the Type 'Gateway'.
- In Network settings, select our VPC 'VPC-2265'.

Services (1/5)

Search

s3

Clear filters

Service Name	Owner	Type	Service Region
<input checked="" type="radio"/> com.amazonaws.ap-south-1.s3	amazon	Gateway	-
<input type="radio"/> com.amazonaws.ap-south-1.s3	amazon	Interface	-
<input type="radio"/> com.amazonaws.ap-south-1.s3-outposts	amazon	Interface	-
<input type="radio"/> com.amazonaws.ap-south-1.s3express	amazon	Gateway	-
<input type="radio"/> com.amazonaws.s3-global.accesspoint	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-0e2f1823af222ece7 (VPC-2265)

- Next select Private Route Table i.e. 'PrivateRT-2265'.
- Keep policy as 'Full access' and click 'Create endpoint'.

School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 4. Private Access to S3 via VPC Endpoint in a Secure VPC Architecture.

Route tables (1/3) [info](#)

Q Search

Name	Route Table ID	Main	Associated Id
-	rtb-090f8242d5ed0f284	Yes	-
<input type="checkbox"/> PublicRT-2265	rtb-003be38a244ed9f95 (PublicRT-2265)	No	subnet-014856f3332e1c430 (PubSub-2265)
<input checked="" type="checkbox"/> PrivateRT-2265	rtb-0a33a24bc85cb05b8 (PrivateRT-22...	No	subnet-0a88cf83a9fed6815 (PvtSub-2265)

When you use an endpoint, the source IP addresses from your instances in your affected subnets for accessing the AWS service in the same region will be private IP addresses, not public IP addresses. Existing connections from your affected subnets to the AWS service that use public IP addresses may be dropped. Ensure that you don't have critical tasks running when you create or modify an endpoint.

rtb-0a33a24bc85cb05b8 X

Policy [info](#)

VPC endpoint policy controls access to the service.

☒ **Full access**
Allow access by any user or service within the VPC using credentials from any Amazon Web Services accounts to any resources in this Amazon Web Services service. All policies — IAM user policies, VPC endpoint policies, and Amazon Web Services service-specific policies (e.g. Amazon S3 bucket policies, any S3 ACL policies) — must grant the necessary permissions for access to succeed.

☐ **Custom**
Use the [policy creation tool](#) to generate a policy, then paste the generated policy below.

1

Step 5: Create IAM role.

- Go to IAM dashboard.
- Go to 'Roles' and click on 'Create a role'.
- Select Trusted entity type – 'AWS service' and Use case – 'EC2' and Click 'Next'.

IAM > Roles > Create role

Step 2
☐ Add permissions

Step 3
☐ Name, review, and create

Trusted entity type

☒ **AWS service**
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

☐ **AWS account**
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

☐ **Web identity**
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

☐ **SAML 2.0 federation**
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

☐ **Custom trust policy**
Create a custom trust policy to enable others to perform actions in this account.

Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case
EC2

School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

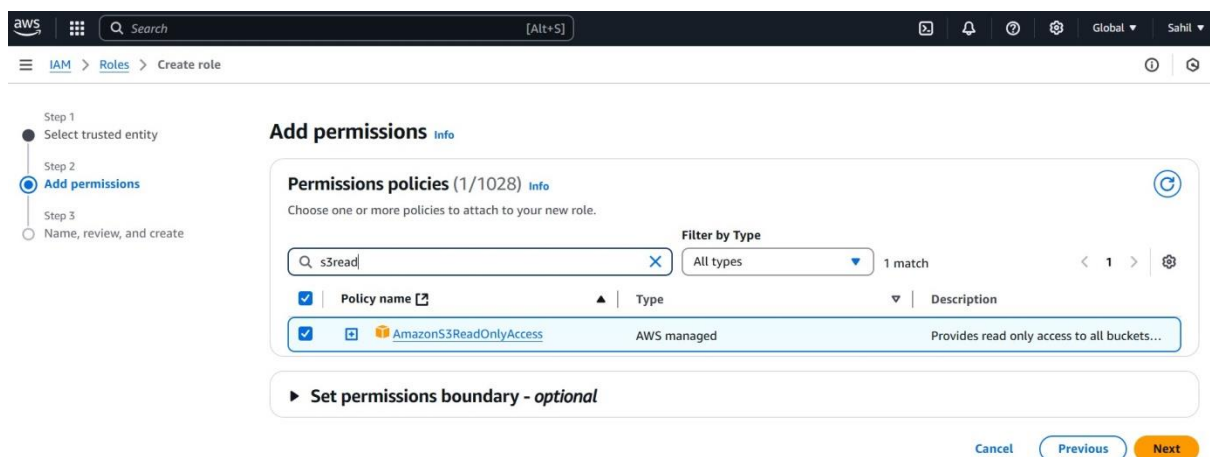
Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

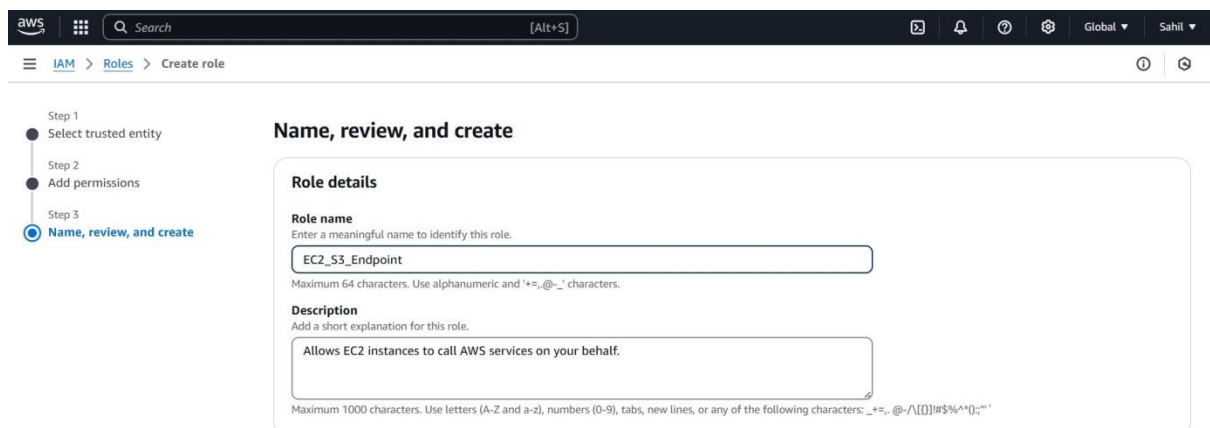
Title of Practical: 4. Private Access to S3 via VPC Endpoint in a Secure VPC Architecture.

- For permissions, search and select 'AmazonS3ReadOnlyAccess' and click on 'Next'.



The screenshot shows the AWS IAM console 'Create role' wizard, Step 2: 'Add permissions'. The left sidebar shows the progress: Step 1 (Select trusted entity), Step 2 (Add permissions), and Step 3 (Name, review, and create). The main area is titled 'Add permissions' and 'Permissions policies (1/1028)'. It instructs to 'Choose one or more policies to attach to your new role.' A search bar contains 's3read' and a dropdown shows 'All types' with '1 match'. A table lists the policy: 'AmazonS3ReadOnlyAccess' (AWS managed) with the description 'Provides read only access to all buckets...'. Below the table is a link 'Set permissions boundary - optional'. At the bottom are 'Cancel', 'Previous', and 'Next' buttons.

- Now, set role name as 'EC2_S3_Endpoint'.
- Click on Create.



The screenshot shows the AWS IAM console 'Create role' wizard, Step 3: 'Name, review, and create'. The left sidebar shows the progress: Step 1 (Select trusted entity), Step 2 (Add permissions), and Step 3 (Name, review, and create). The main area is titled 'Name, review, and create' and 'Role details'. It has two input fields: 'Role name' with the value 'EC2_S3_Endpoint' and a description 'Allows EC2 instances to call AWS services on your behalf.' Below the fields are character limits and allowed characters. At the bottom are 'Cancel', 'Previous', and 'Next' buttons.

Step 6: Launch EC2 instances (Public and Private).

- Go to EC2 console and click on 'Launch Instances'.
- Name the public instance – 'BastionHost-2265'.
- Select AMI as 'Amazon Linux' and under that select 'Amazon Linux 2 AMI (HMV)'.

School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 4. Private Access to S3 via VPC Endpoint in a Secure VPC Architecture.

EC2 > Instances > Launch an instance

Name and tags Info

Name

BastionHost-2265

[Add additional tags](#)

▼ **Application and OS Images (Amazon Machine Image)** Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Q Search our full catalog including 1000s of application and OS images

Recents

Quick Start



[Browse more AMIs](#)
Including AMIs from
AWS, Marketplace and
the Community

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type
ami-03b8adbf322415fd0 (64-bit (x86)) / ami-087856def6fa48ada (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible ▼

- Now, select Key Pair.
- Under Network settings – select VPC 'VPC-2265'.
- Subnet as 'PubSub-2265'.
- Enable auto-assign public IP.
- For Security group, select the public SG we created earlier i.e. 'Bastion-SG-2265'.
- Launch the instance.

School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 4. Private Access to S3 via VPC Endpoint in a Secure VPC Architecture.

▼ Network settings Info

VPC - required Info

vpc-0e2f1823af222ece7 (VPC-2265)
10.0.0.0/16

Subnet Info

subnet-014856f3332e1c430 PubSub-2265
VPC: vpc-0e2f1823af222ece7 Owner: 908027405956 Availability Zone: ap-south-1b
Zone type: Availability Zone IP addresses available: 251 CIDR: 10.0.1.0/24

Auto-assign public IP Info

Enable

Additional charges apply when outside of free tier allowance

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

Bastion-SG-2265 sg-0b96d9f79d4cb05c6 X
VPC: vpc-0e2f1823af222ece7

Compare security group rules

Security groups that you add or remove here will be added to or removed from all your network interfaces.

- Now, create a Private instance and name it 'PrivateInstance-2265'.
- Select AMI as 'Amazon Linux' and under that select 'Amazon Linux 2 AMI (HVM)'.

aws AWS Console Home Search [Alt+S]

EC2 > Instances > Launch an instance

Name and tags Info

Name

PrivateInstance-2265 Add additional tags

▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Recents Quick Start

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Linux Debian

aws Mac ubuntu Microsoft Red Hat SUSE debian

Browse more AMIs
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type
ami-03b8adb322415fd0 (64-bit (x86)) / ami-087856def6fa48ada (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

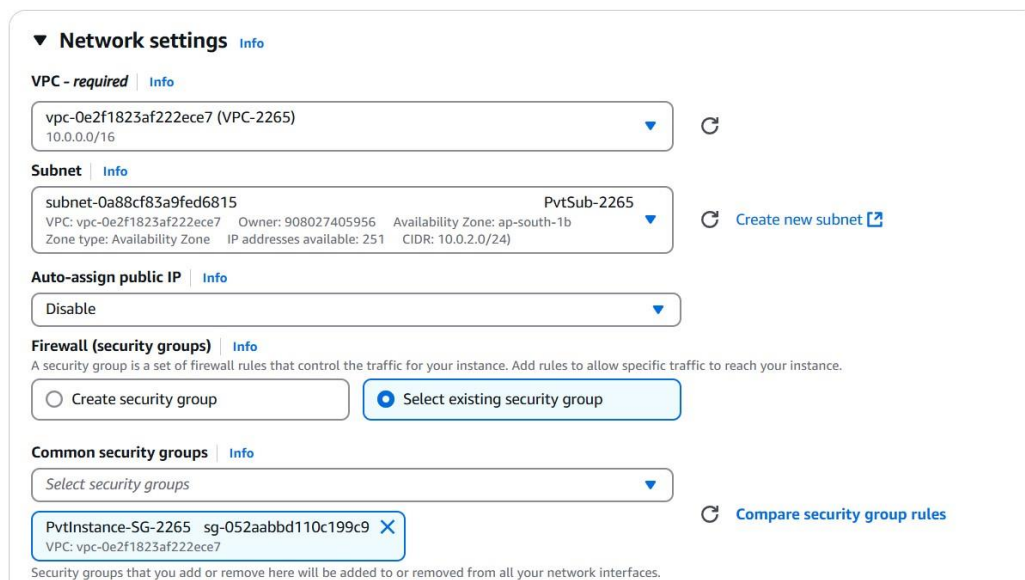
Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 4. Private Access to S3 via VPC Endpoint in a Secure VPC Architecture.

- Now, select Key Pair.
- Under Network settings – select VPC ‘VPC-2265’.
- Subnet as ‘PvtSub-2265’.
- Do not enable auto-assign public IP.
- For Security group, select the public SG we created earlier i.e. ‘PrivateInstance-SG-2265’.



The screenshot shows the 'Network settings' section of an AWS EC2 instance configuration. It includes fields for VPC (vpc-0e2f1823af222ece7), Subnet (subnet-0a88cf83a9fed6815), Auto-assign public IP (Disable), Firewall (security groups) (Select existing security group), and Common security groups (PvtInstance-SG-2265).

Network settings [Info](#)

VPC - required [Info](#)

vpc-0e2f1823af222ece7 (VPC-2265)
10.0.0.0/16

Subnet [Info](#)

subnet-0a88cf83a9fed6815 PvtSub-2265
VPC: vpc-0e2f1823af222ece7 Owner: 908027405956 Availability Zone: ap-south-1b
Zone type: Availability Zone IP addresses available: 251 CIDR: 10.0.2.0/24

Auto-assign public IP [Info](#)

Disable

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

PvtInstance-SG-2265 sg-052aabb110c199c9
VPC: vpc-0e2f1823af222ece7

Security groups that you add or remove here will be added to or removed from all your network interfaces.

- Now, in Advanced details – IAM instance profile – select the role we created earlier i.e. ‘EC2_S3_Endpoint’.
- Launch the instance.

School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 4. Private Access to S3 via VPC Endpoint in a Secure VPC Architecture.

▼ Advanced details [Info](#)

Domain join directory [Info](#)

Select ▼

[Create new directory](#)

IAM instance profile [Info](#)

EC2_S3_Endpoint
arn:aws:iam::908027405956:instance-profile/EC2_S3_Endpoint ▼

[Create new IAM profile](#)

Hostname type [Info](#)

IP name ▼

DNS Hostname [Info](#)
☒ Enable IP name IPv4 (A record) DNS requests
☐ Enable resource-based IPv4 (A record) DNS requests
☐ Enable resource-based IPv6 (AAAA record) DNS requests

Step 7: Connect Public instance in terminal.

- Go to the public instance 'BastionHost-2265' and connect it in terminal.
- Type the command 'vi KY-CCSA-TY-2265.pem' to create a Key pair in the Public instance so that we can launch the private instance inside this public instance.
- Open the Key on the device and copy the contents of the key and paste it in the terminal.
- After pasting the contents of the key in the terminal, press 'esc' key and type command ':wq' to save and exit the window.

```
root@ip-10-0-1-59:~#
Warning: Permanently added '43.204.229.8' (ED25519) to the list of known hosts.
root@ip-10-0-1-59:~#
#
#####
Amazon Linux 2
#####
AL2 End of Life is 2026-06-30.
#####
A newer version of Amazon Linux is available!
Amazon Linux 2023, GA and supported until 2028-03-15.
https://aws.amazon.com/linux/amazon-linux-2023/
[ec2-user@ip-10-0-1-59 ~]$ vi KY-CCSA-TY-2265.pem
```


School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 4. Private Access to S3 via VPC Endpoint in a Secure VPC Architecture.

- Now type the command 'chmod 400 KY-CCSA-TY-2265.pem' and press Enter button.
- Now, go to the private instance 'PrivateInstance-2265' and connect it in terminal.

```
[ec2-user@ip-10-0-1-59 ~]$ chmod 400 KY-CCSA-TY-2265.pem
[ec2-user@ip-10-0-1-59 ~]$ ssh -i "KY-CCSA-TY-2265.pem" ec2-user@10.0.2.60

#_
#####      Amazon Linux 2
#####\
\#####\
\###|      AL2 End of Life is 2026-06-30.
\#/
V~' '->
A newer version of Amazon Linux is available!
Amazon Linux 2023, GA and supported until 2028-03-15.
https://aws.amazon.com/linux/amazon-linux-2023/

_/m/'
[ec2-user@ip-10-0-2-60 ~]$
```

- Now the private instance is connected inside the public instance.
- Now, type the command 'aws s3 ls' to list the S3 buckets.
- Note: There should already be a S3 bucket created.
- If it doesn't list any bucket, type command 'aws configure' and follow these steps-
 - In Security credentials, Generate AWS Access key ID and AWS Secret key.
 - Paste these in the terminal respectively.
 - Type the Default region name.
 - Press Enter.
- Now, type the previous command for listing buckets again i.e. 'aws s3 ls'.
- It will show the buckets now (bucket-2265).
- Access the bucket using command 'aws s3 ls s3://bucket-2265'.
- Here we can see the 'HelloWorld.txt' file in the bucket.



**D Y PATIL
INTERNATIONAL
UNIVERSITY**
AKURDI PUNE

School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

**Title of Practical: 4. Private Access to S3 via VPC Endpoint in a
Secure VPC Architecture.**

```
[root@ip-10-0-2-60 ~]# aws s3 ls
^C
[root@ip-10-0-2-60 ~]# aws configure
AWS Access Key ID [None]: 
AWS Secret Access Key [None]: 
Default region name [None]: ap-south-1
Default output format [None]: 
[root@ip-10-0-2-60 ~]# aws s3 ls
2025-02-06 09:29:15 bucket-2265
[root@ip-10-0-2-60 ~]# aws s3 ls s3://bucket-2265
2025-02-06 09:31:34      12 HelloWorld.txt
[root@ip-10-0-2-60 ~]#
```