

Lab Assignment – 05

Part-1: NACL (Network Access Control List)

Task-1: Create a custom VPC in an availability zone at one region and create its necessary components like subnet, IGW and Route Table.

Create VPC Info

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

VPC settings

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

IPv4 CIDR block [Info](#)
10.0.0.0/16

IPv6 CIDR block [Info](#)
No IPv6 CIDR block

You successfully created **vpc-0504b79754a402929 / VPC_NACL**

VPC > Your VPCs > **vpc-0504b79754a402929**

Actions ▾

Details [Info](#)

VPC ID vpc-0504b79754a402929	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP options set dopt-6793dd1d	Main route table rtb-0b5e5e4eb9a29fae2	Main network ACL acl-0fa519d2dc44a5fdd
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool —	IPv6 CIDR (Network border group) —

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.

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.

IPv4 CIDR block [Info](#)

Tags - optional

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="Public Subnet - 1"/>
<input type="button" value="Remove"/>	

Feedback English (US) © 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use 14:53 12-02-2021

You have successfully created 1 subnet: subnet-0f074018a04331925

Subnets (1) [Info](#)

<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR
<input type="checkbox"/>	Public Subnet...	subnet-0f074018a043...	<input checked="" type="checkbox"/> Available	vpc-0504b79754a402...	10.0.0.0/2

Select a subnet

Feedback English (US) © 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use 14:53 12-02-2021

The screenshot shows the AWS VPC Management Console. A green notification bar at the top states: "The following internet gateway was created: igw-057c864f51da06681. You can now attach to a VPC to enable the VPC to communicate with the internet." Below this, the breadcrumb navigation shows "VPC > Internet gateways > igw-057c864f51da06681". The main area displays the details of the Internet Gateway, including its ID (igw-057c864f51da06681), State (Detached), VPC ID (-), and Owner (984668232977). A "Details" tab is selected. At the bottom right, there is a "Manage tags" button. The left sidebar shows various VPC-related options like Your VPCs, Subnets, Route Tables, and Internet Gateways.

Attach IGW to VPC

The screenshot shows the "Attach internet gateway" dialog box. It has a search bar where "vpc-0504b79754a402929" is typed. Below the search bar, there is a link to "AWS Command Line Interface command". At the bottom, there are "Cancel" and "Attach internet gateway" buttons. The background shows the same AWS VPC Management Console interface as the previous screenshot.

Workbench (5) EB03 Lab || ECSE304L || VPC Management Console +

https://console.aws.amazon.com/vpc/home?region=us-east-1#InternetGateway:internetGatewayId=igw-057c864f51da06681

90 Day GRE Study P... Deep Learning Smart Surveillance TensorRT DBMS indexing probability c++ CP Software virtual Courses traffic sign > Other favorites

AWS Services Search for services, features, marketplace products, and docs [Alt+S] vocstartsoft/user1191784-MV3451@bennett.edu.in @ 9846-6823-2977 N. Virginia Support

New VPC Experience Learn more

VPC Dashboard Filter by VPC: Select a VPC

VIRTUAL PRIVATE CLOUD Your VPCs Subnets Route Tables Internet Gateways

- Egress Only Internet Gateways
- Carrier Gateways
- DHCP Options Sets
- Elastic IPs
- Managed Prefix Lists
- Endpoints
- Endpoint Services
- NAT Gateways
- Peering Connections

Internet gateway igw-057c864f51da06681 successfully attached to vpc-0504b79754a402929

VPC > Internet gateways > igw-057c864f51da06681 igw-057c864f51da06681 / IGW_NACL Actions

Details Info

Internet gateway ID igw-057c864f51da06681	State Attached	VPC ID vpc-0504b79754a402929	Owner 984668232977
--	-------------------	---------------------------------	-----------------------

Tags Manage tags

Feedback English (US) © 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use 14:56 12-02-2021

Workbench (5) EB03 Lab || ECSE304L || Create route table | VPC Management Console +

https://console.aws.amazon.com/vpc/home?region=us-east-1#CreateRouteTable:

90 Day GRE Study P... Deep Learning Smart Surveillance TensorRT DBMS indexing probability c++ CP Software virtual Courses traffic sign > Other favorites

AWS Services Search for services, features, marketplace products, and docs [Alt+S] vocstartsoft/user1191784-MV3451@bennett.edu.in @ 9846-6823-2977 N. Virginia Support

Route Tables > Create route table

Create route table

The following Route Table was created:

Route Table ID rtb-047fccaa6c49156e04

Close

Feedback English (US) © 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use 14:56 12-02-2021



Edit route add IGW

Route Tables > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	igw-057c864f51da06681		No

Add route

* Required

Cancel Save routes

Edit Subnet association

Route Tables > Edit subnet associations

Edit subnet associations

Route table rtb-047fcc6c49156e04 (Public Route Table)

Associated subnets subnet-0f074018a04331925

Subnet ID	IPv4 CIDR	IPv6 CIDR	Current Route Table
subnet-0f074018a04331925 Public Su...	10.0.0.0/24	-	Main

* Required

Cancel Save

Task-2: Launch Window server in the public subnet and allow all traffic.

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1

Purchasing option: Request Spot instances

Network: vpc-0504b79754a402929 | VPC_NACL

Subnet: subnet-0f074018a04331925 | Public Subnet - 1 | us-east-1

Auto-assign Public IP: Enable

Placement group: Add instance to placement group

Capacity Reservation: Open

Domain join directory: No directory

IAM role: None

Buttons: Cancel, Previous, Review and Launch, Next: Add Storage

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more about Amazon EC2 security groups.](#)

Assign a security group:

- Create a new security group
- Select an existing security group

Security group name: SG_NACL

Description: launch-wizard-1 created 2021-02-12T15:00:22.862+05:30

Type	Protocol	Port Range	Source	Description
All traffic	All	0 - 65535	Anywhere	0.0.0.0/0, ::/0 e.g. SSH for Admin Desktop

Add Rule

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

Buttons: Cancel, Previous, Review and Launch, Next: Add Storage

Task-3: Create a custom Network ACL and attach the subnet to the default NACL.

The screenshot shows the AWS VPC Network ACLs management interface. A green success message at the top states: "You successfully created acl-0a31b68e2eb3633c2 / NACL_1." Below this, a table lists three Network ACLs:

Name	Network ACL ID	Associated with	Default	VPC ID
NAACL_1	acl-0a31b68e2eb3633c2	-	No	vpc-05
-	acl-92e4f0ef	6 Subnets	Yes	vpc-62
-	acl-0fa519d2dc...	subnet-0f074018a04331925 / Pub...	Yes	vpc-05

At the bottom, there is a section titled "Select a network ACL".

Note: Edit subnet association for this NACL to act as the main one. 2 NACLs cannot work on one subnet.

The screenshot shows the "Edit subnet associations" page for the NACL_1 Network ACL. The URL is https://console.aws.amazon.com/vpc/home?region=us-east-1#EditNetworkAclSubnetAssociations:networkAclId=acl-0a31b68e2eb3633c2. The page title is "Edit subnet associations" with an "Info" link. It says "Change which subnets are associated with this network ACL."

Available subnets (1/1)

Name	Subnet ID	Associated with	Availability zone	IPv4 CIDR	IPv6 CIDR
Public Subnet - 1	subnet-0f074018a04331925	acl-0a31b68e2eb3633c2 / NACL_1	us-east-1a	10.0.0.0/24	-

Selected subnets

Feedback English (US) ▾ © 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use 15:13 12-02-2021

Task-4: Set the inbound rules in NACL such as 100 for RDP.

Edit inbound rules

Inbound rules control the incoming traffic that's allowed to reach the VPC.

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	RDP (3389)	TCP (6)	3389	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Add new rule Sort by rule number

Cancel Preview changes Save changes

Task-5: Set the outbound rules in NACL such as 100 for HTTP and 200 for HTTPS.

Edit outbound rules

Outbound rules control the outgoing traffic that's allowed to leave the VPC.

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
150	RDP (3389)	TCP (6)	3389	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Add new rule Sort by rule number

Cancel Preview changes Save changes

Outbound rules control the outgoing traffic that's allowed to leave the VPC.

Rule number	Type	Protocol	Port range	Destination	Allow/Deny	Action
150	RDP (3389)	TCP (6)	3389	0.0.0.0/0	Allow	Remove
100	HTTP (80)	TCP (6)	80	0.0.0.0/0	Allow	Remove
200	HTTPS (443)	TCP (6)	443	0.0.0.0/0	Allow	Remove
*	All traffic	All	All	0.0.0.0/0	Deny	Remove

[Add new rule](#) [Sort by rule number](#)

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

Task-6: Check the connection of the server using RDP (Error would occur)

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

[Download remote desktop file](#)

When prompted, connect to your instance using the following information:

Public IP
52.207.116.70

Password
kLk)uYC(QHTE@av86)&(z(bjh2yl9*x

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

[Cancel](#)

[Feedback](#) [English \(US\)](#) [Privacy Policy](#) [Terms of Use](#)

Task-7: Go to custom VPC NACL and change the outbound rules as 250 for custom TCP and open the port range 1024 to 65535.

Rule number	Type	Protocol	Port range	Destination	Allow/Deny	Action
100	HTTP (80)	TCP (6)	80	0.0.0.0/0	Allow	Remove
150	RDP (3389)	TCP (6)	3389	0.0.0.0/0	Allow	Remove
200	HTTPS (443)	TCP (6)	443	0.0.0.0/0	Allow	Remove
250	Custom TCP	TCP (6)	1024-65535	0.0.0.0/0	Allow	Remove
*	All traffic	All	All	0.0.0.0/0	Deny	

[Add new rule](#) [Sort by rule number](#)

Task-8: Connect again using RDP.

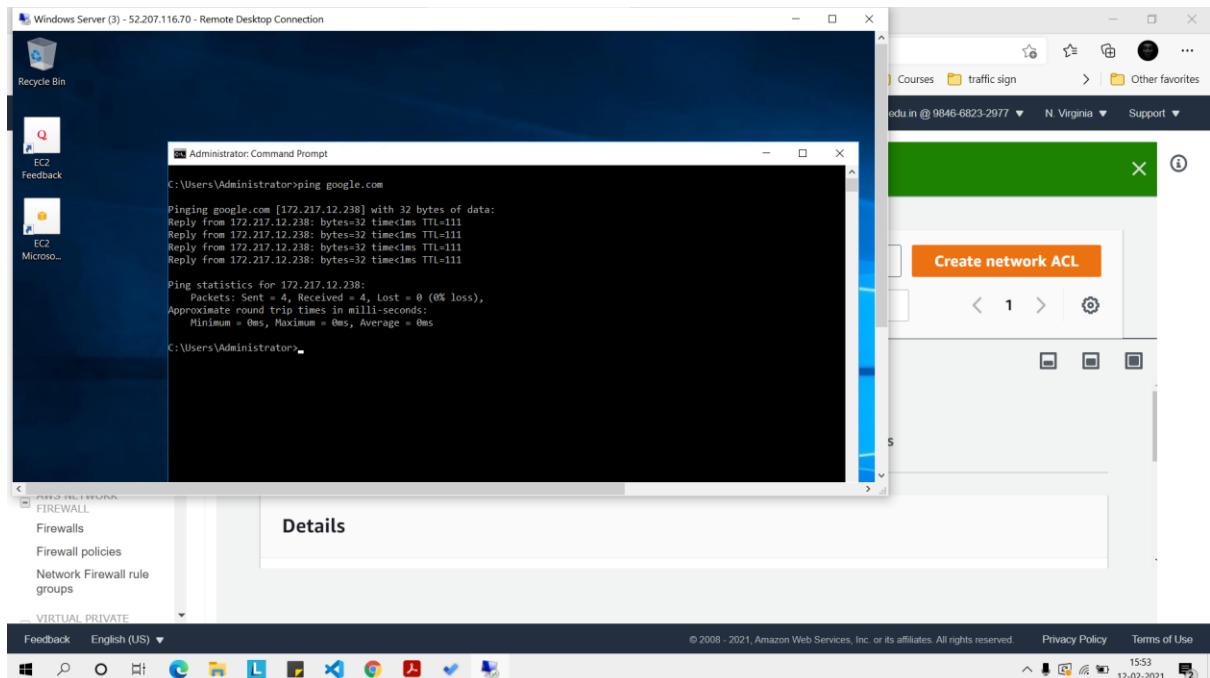
Windows Server (2) - 52.207.116.70 - Remote Desktop Connection

AMAZ-3MHEBK
Instance ID: i-0de2b2abcdb7b5
Public IP Address: 52.207.116.70
Private IP Address: 10.0.0.180
Instance Size: t2.micro
Availability Zone: us-east-1a
Architecture: AMD64
Total Memory: 1024 MB
Network Performance: Low to

Note: In inbound we just require RDP for us to connect to the Ec2 instance.

In outbound we require custom TCP for the instance to connect to servers in AWS.

Task-9: Check the internet connectivity using cmd or browser.



Part-2: Access AWS resources using VPC Endpoints

Task-1: Create VPC by creating 2 subnets in it (1 public and private).

		Subnet ID	Status	VPC	CIDR Range
<input type="checkbox"/>	-	subnet-4e1d8b35	Available	vpc-a827d6c3	172.31.16.0/24
<input type="checkbox"/>	Private Subnet	subnet-07453cade181ea7c4	Available	vpc-0c4eb5279d4e8a2b6	10.0.1.0/24
<input type="checkbox"/>	-	subnet-29074865	Available	vpc-a827d6c3	172.31.0.0/24
<input type="checkbox"/>	-	subnet-4e061826	Available	vpc-a827d6c3	172.31.32.0/24
<input type="checkbox"/>	Public Subnet	subnet-0e777add8230...	Available	vpc-0c4eb5279d4e8a2b6	10.0.0.0/24

Task-2: Attach IGW to the VPC and configure the Route Table.

Internet gateway ID	State	VPC ID	Owner
igw-01206cdccb4403cf6	Attached	vpc-0c4eb5279d4e8a2b6 VPC_EP	277391238495

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID
Private RT	rtb-0f121c9bd7467f600	-	-	No	vpc-0c4eb5279d4
Public RT	rtb-0f399356c8da4e466	-	-	No	vpc-0c4eb5279d4
	rtb-07192c00229aaa9ef	-	-	Yes	vpc-0c4eb5279d4
	rtb-ca2196a1	-	-	Yes	vpc-a827d6c3

Edit Routes and direct traffic via IGW.

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	igw-01206cdccb4403cf6	active	No

* Required Cancel **Save routes**



Edit Subnet associations

Route table rtb-0f399356c8da4e466 (Public RT)

Associated subnets: subnet-0e777add823092c5c

Subnet ID	IPv4 CIDR	IPv6 CIDR	Current Route Table
subnet-07453cade181ea7c4 Private Subnet	10.0.1.0/24	-	Main
subnet-0e777add823092c5c Public Subnet	10.0.0.0/24	-	Main

* Required Cancel Save

Task-3: Launch 1 EC2 Linux instance in each subnet.

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 Launch into Auto Scaling Group

Purchasing option: Request Spot instances

Network: vpc-0c4eb5279d4e8a2b6 | VPC_EP Create new VPC

Subnet: subnet-0e777add823092c5c | Public Subnet | ap-sou Create new subnet
251 IP Addresses available

Auto-assign Public IP: Enable

Placement group: Add instance to placement group

Capacity Reservation: Open

Domain Join directory: No directory Create new directory

IAM role: None Create new IAM role

Cancel Previous Review and Launch Next: Add Storage

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances	<input type="text" value="1"/>	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-0c4eb5279d4e8a2b6 VPC_EP <input type="button" value="Create new VPC"/>	
Subnet	subnet-07453cade181ea7c4 Private Subnet ap-so <input type="button" value="Create new subnet"/> 251 IP Addresses available	
Auto-assign Public IP	<input type="button" value="Use subnet setting (Disable)"/>	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	Open <input type="button" value="Create new capacity reservation"/>	
Domain Join directory	No directory <input type="button" value="Create new directory"/>	
IAM role	None <input type="button" value="Create new IAM role"/>	

Buttons: Cancel, Previous, Review and Launch (highlighted), Next: Add Storage



Instances | EC2 Management Console

Instances (2) Info Actions ▾ Launch instances ▾

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check
<input type="checkbox"/>	Public Server	i-0e47fe3d0c33aff93	Running <input type="button" value="Stop"/>	t2.micro	2/2 checks ...
<input type="checkbox"/>	Private Server	i-0764f86a6ff2914c1	Running <input type="button" value="Stop"/>	t2.micro	2/2 checks ...

Select an instance above

Left sidebar:

- New EC2 Experience
- EC2 Dashboard
- Events
- Tags
- Limits
- Instances
 - Instances (highlighted)
 - Instance Types
 - Launch Templates
 - Spot Requests
 - Savings Plans
 - Reserved Instances

Bottom:

Task-4: Create a VPC Endpoint and select the S3 Gateway service.

A screenshot of a web browser window titled 'Create Endpoint | VPC Manager'. The URL is <https://ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#CreateVpcEndpoint>. The page displays a search bar with 'search : gateway' and a table with three rows:

Service Name	Owner	Type
com.amazonaws.ap-south-1.dynamodb	amazon	Gateway
com.amazonaws.ap-south-1.s3	amazon	Gateway
com.amazonaws.ap-south-1.storagegateway	amazon	Interface

The 'com.amazonaws.ap-south-1.s3' row is selected. Below the table, there is a dropdown menu labeled 'VPC*' containing 'vpc-a827d6c3'.

Task-5: associate it with the private subnet.

A screenshot of the same 'Create Endpoint | VPC Manager' page. The 'Service Name' dropdown now shows 'vpc-0c4eb5279d4e8a2b6'. A note at the top states: 'Configure route tables A rule with destination pi-78a54011 (com.amazonaws.ap-south-1.s3) and a target with this endpoints' ID (e.g. vpce-12345678) will be added to the route tables you select below.' Below this, a note says: 'Subnets associated with selected route tables will be able to access this endpoint.' A route table named 'rtb-0f121c9bd7467f600' is selected. The table lists three route entries:

Route Table ID	Main	Associated With
rtb-0f121c9bd7467f600	No	subnet-07453cade181ea7c4 Private Subnet
rtb-0f399356c8da4e466	No	subnet-0e777add823092c5c Public Subnet
rtb-07192c00229aa9ef	Yes	0 subnets

Create Endpoint

Name	Endpoint ID	VPC ID	Service name	Endpoint type	Status	Creation time
EP_S3	vpce-0d014a0a08d0f3c79	vpc-0c4eb5279d4...	com.amazonaws.ap-south-1.s3	Gateway	available	February 17, 2021 at 9:30 PM

Endpoint: vpce-0d014a0a08d0f3c79

- Details
- Route Tables
- Policy
- Tags

Endpoint ID: vpce-0d014a0a08d0f3c79
Status: available
Creation time: February 17, 2021 at 9:33:32 PM UTC+5:30

VPC ID: vpc-0c4eb5279d4e8a2b6 | VPC_EP
Status message:
Service name: com.amazonaws.ap-south-1.s3

Task-6: Check the Private Route Table to make sure you see a route using the VPC Endpoint to S3.

Create route table

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID
Private RT	rtb-0f121c9bd7467f600	subnet-07453cade181ea7c4	-	No	vpc-0c4eb5279d4...
Public RT	rtb-0f399356c8da4e466	subnet-0e777add823092c5c	-	No	vpc-0c4eb5279d4...
	rtb-07192c00229aaa9ef	-	-	Yes	vpc-0c4eb5279d4...
	rtb-ca2196a1	-	-	Yes	vpc-a827d6c3

Private RT

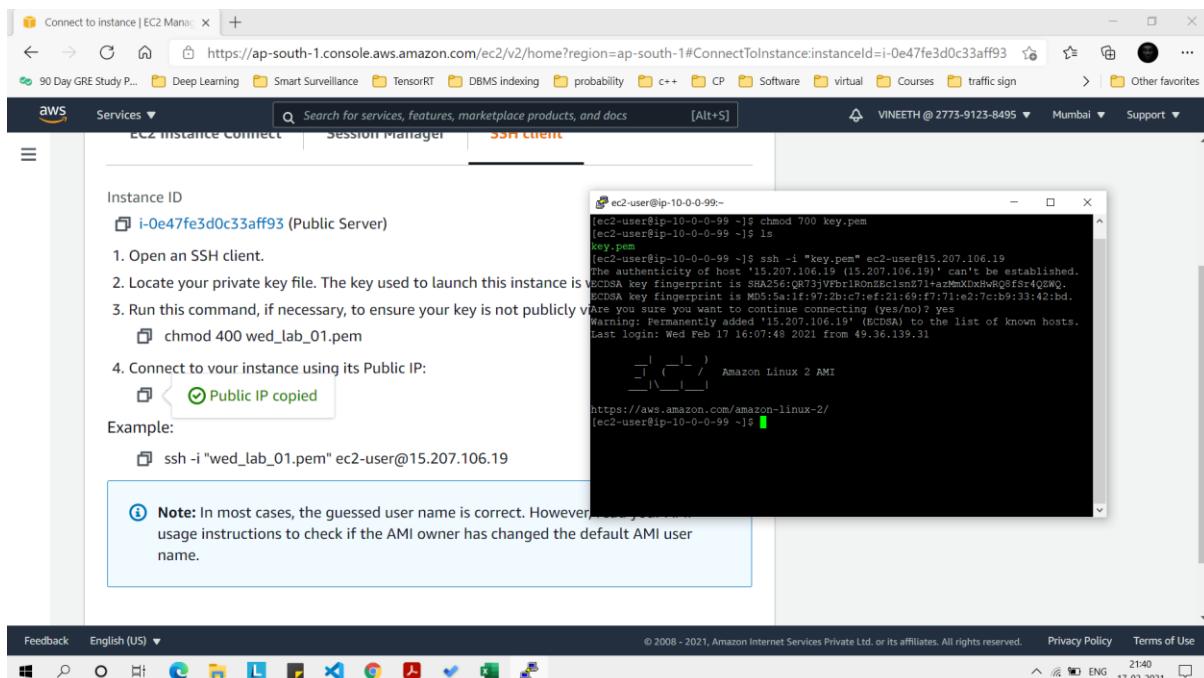
- Summary
- Routes
- Subnet Associations
- Edge Associations
- Route Propagation
- Tags

Edit routes

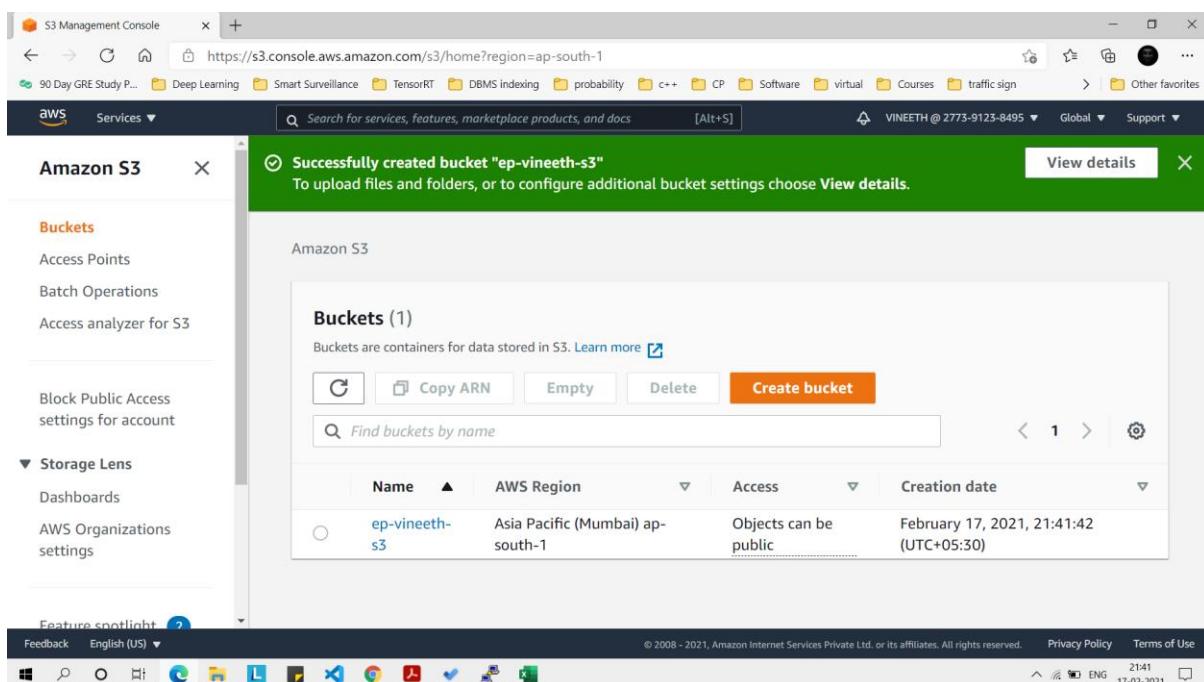
View: All routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
pl-78a54011 (com.amazonaws.ap-south-1.s3, 52.219.156.0/22, 52.219.160.0/23, 52.219.62.0/23, 3.5.212.0/23, 3.5.208.0/22, 52.219.64.0/22)	vpce-0d014a0a08d0f3c79	active	No

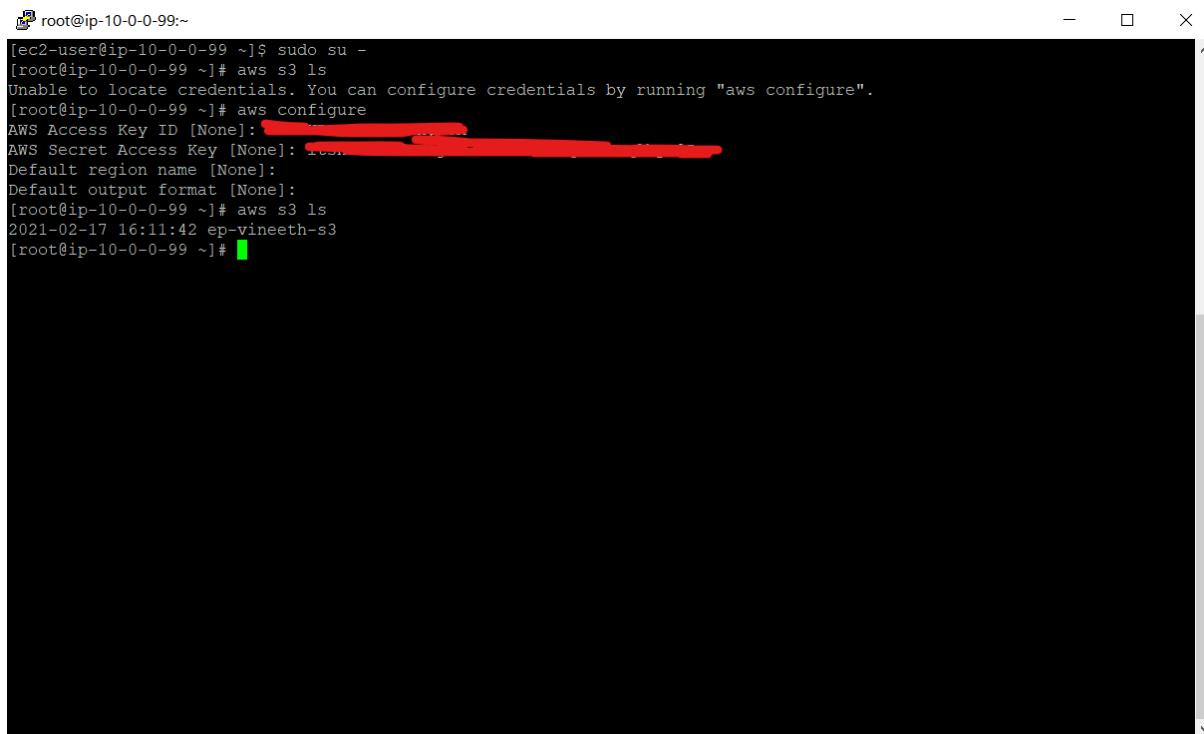
Task-7: Verify by doing SSH into the public instance.



Task-8: Create a S3 bucket.



Task-9: Check the availability of the AWS resources publicly and confirm the S3 buckets are shown in the current environment.

A screenshot of a terminal window titled 'root@ip-10-0-0-99:~'. The window shows a series of commands being run in a root shell. The commands include 'sudo su -', 'aws s3 ls', 'aws configure' (which prompts for AWS Access Key ID and AWS Secret Access Key), and 'aws s3 ls' again, which outputs the result '2021-02-17 16:11:42 ep-vineeth-s3'. The terminal has a dark background with white text and standard Linux-style syntax highlighting.

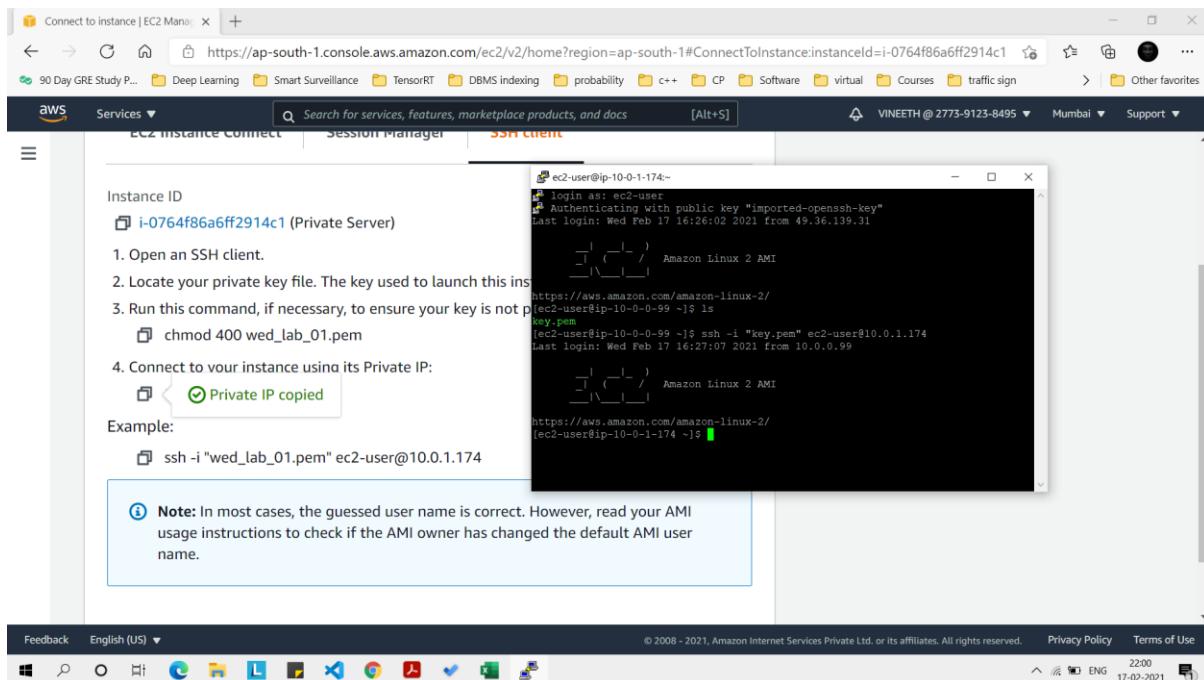
```
[ec2-user@ip-10-0-0-99 ~]# sudo su -
[root@ip-10-0-0-99 ~]# aws s3 ls
Unable to locate credentials. You can configure credentials by running "aws configure".
[root@ip-10-0-0-99 ~]# aws configure
AWS Access Key ID [None]: [REDACTED]
AWS Secret Access Key [None]: [REDACTED]
Default region name [None]:
Default output format [None]:
[root@ip-10-0-0-99 ~]# aws s3 ls
2021-02-17 16:11:42 ep-vineeth-s3
[root@ip-10-0-0-99 ~]#
```

Task-10: Check the availability of the AWS resources privately and confirm the S3 buckets are shown in the current environment.

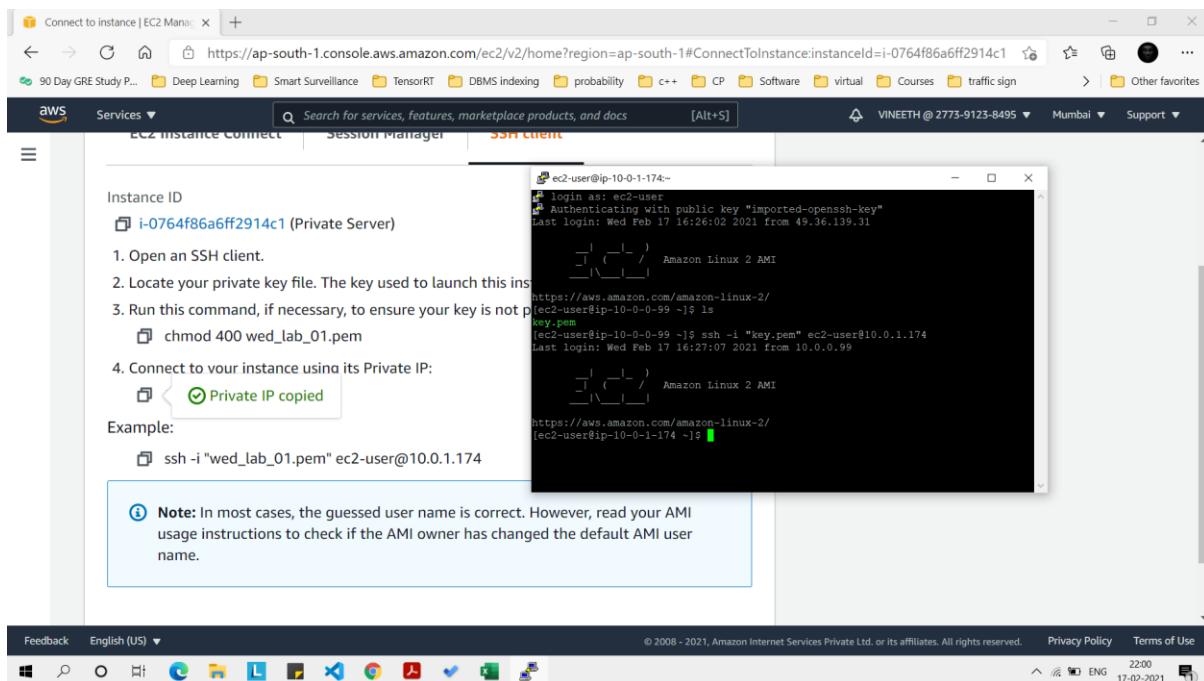
Access the private resource by SSH from the public server terminal.

Steps:

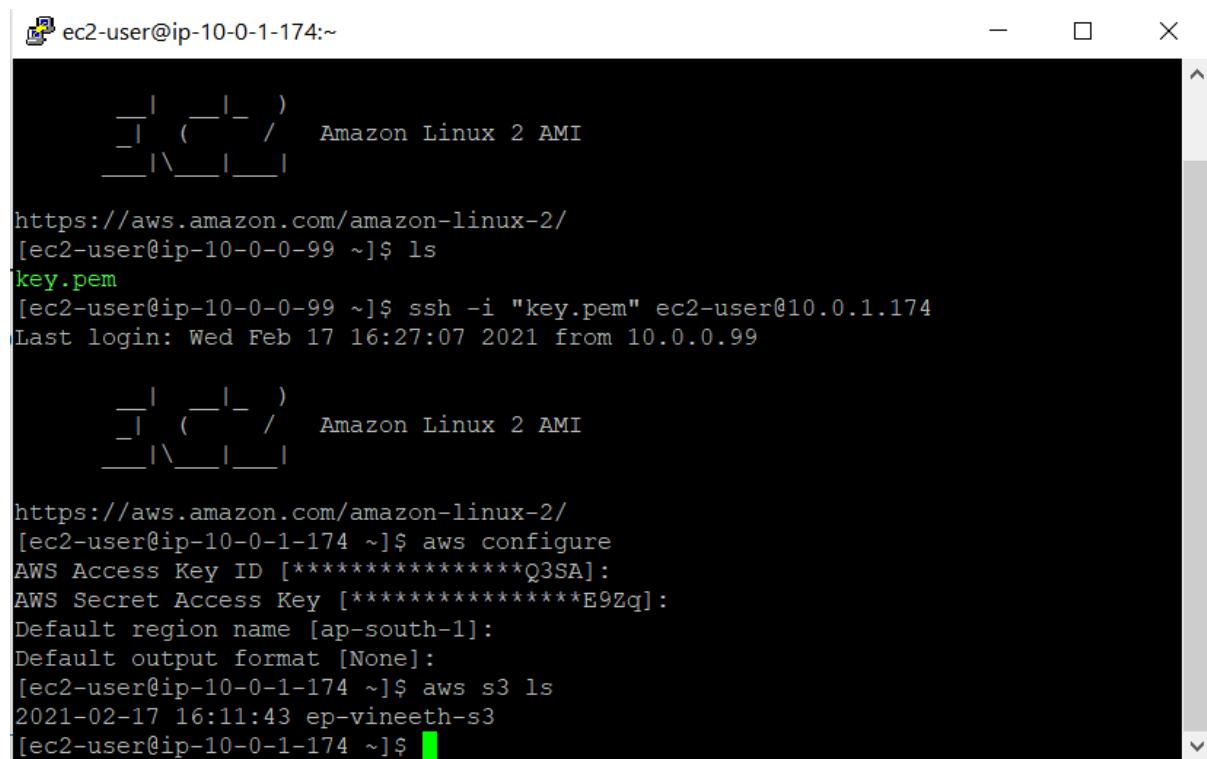
1. Putty into Public Server as private server cannot be directly accessed.
2. Remote login into private server via the public server using SSH.



3. Run the AWS configure command and set the default region.



Now try to access the S3 bucket via this private server.



```
ec2-user@ip-10-0-1-174:~  
https://aws.amazon.com/amazon-linux-2/  
[ec2-user@ip-10-0-0-99 ~]$ ls  
key.pem  
[ec2-user@ip-10-0-0-99 ~]$ ssh -i "key.pem" ec2-user@10.0.1.174  
Last login: Wed Feb 17 16:27:07 2021 from 10.0.0.99  
  
https://aws.amazon.com/amazon-linux-2/  
[ec2-user@ip-10-0-1-174 ~]$ aws configure  
AWS Access Key ID [*****Q3SA]:  
AWS Secret Access Key [*****E9Zq]:  
Default region name [ap-south-1]:  
Default output format [None]:  
[ec2-user@ip-10-0-1-174 ~]$ aws s3 ls  
2021-02-17 16:11:43 ep-vineeth-s3  
[ec2-user@ip-10-0-1-174 ~]$
```

Hence, we are able to successfully access this S3 bucket from the private server via the VPC Endpoint and without using NAT Gateway.