

In Part 1 we did the following things:

1. Created a VPC A
2. Created four subnets(two Public subnet and two Private subnets) in VPC A in two availability zones i.e us-west-1a and us-west-1b.
3. Created a NaCL and associated all the Subnets to the NaCL
4. Created inbound and outbound rule with Rule number 100 and to allow all traffic from internet

Part 2:

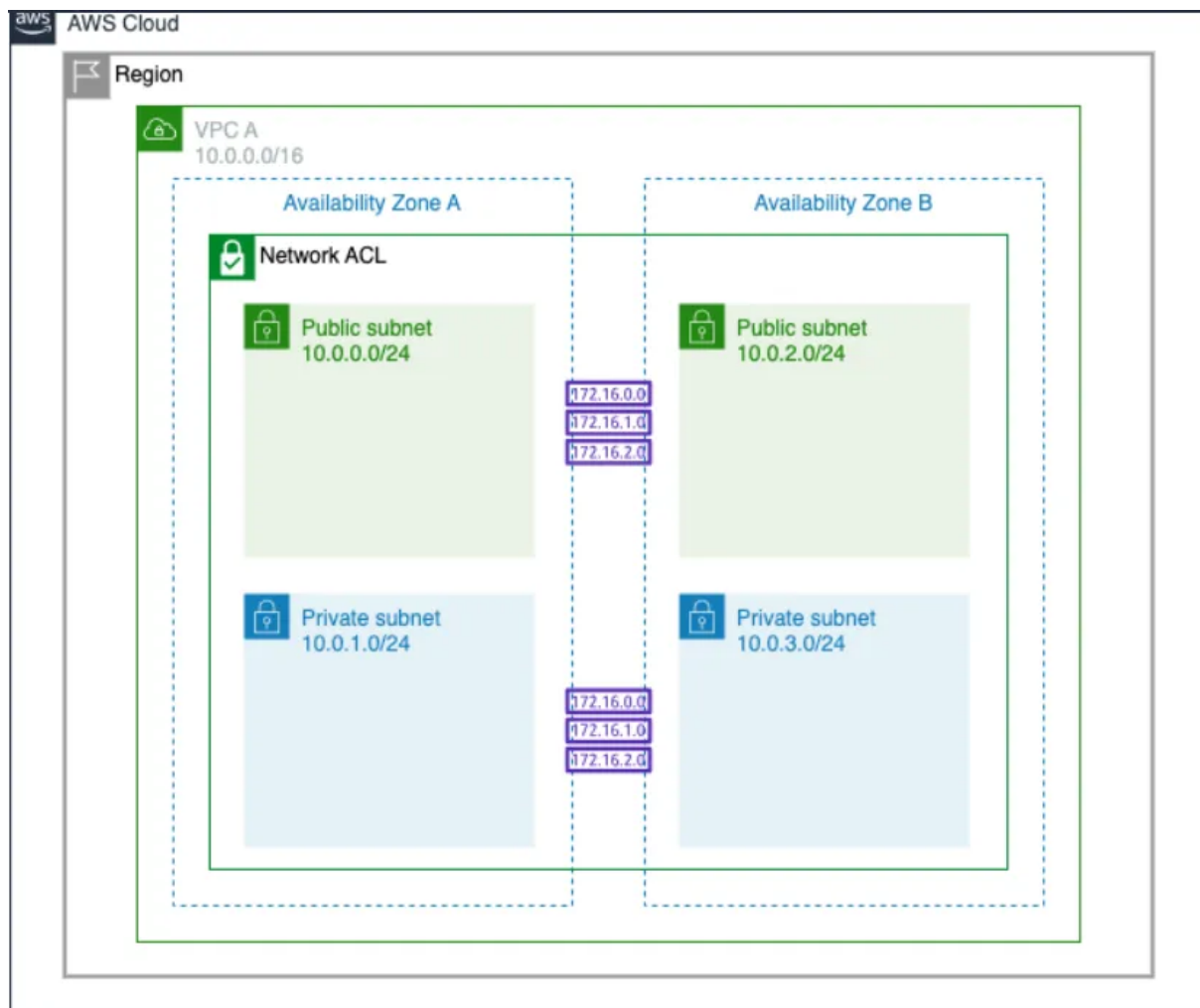
Route Tables:

There is an implicit router in the VPC you have created and route tables is used to control the network traffic.

A route table contains a set of rules, called *routes*, that determine where network traffic from your subnet or gateway is directed.

Each subnet in your VPC must be associated with a route table, which controls the routing for the subnet (subnet route table). You can

explicitly associate a subnet with a particular route table. Otherwise, the subnet is implicitly associated with the main route table. A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same subnet route table.



Create Route table for Subnets:

We will now create a new public route table for the public subnets with a route to the internet via the Internet Gateway.

1. Click on Create route table
2. Enter Name as VPC A Public Route Table

3. Select VPC A

4. 4. Create route table

[VPC](#) > [Route tables](#) > Create 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.

VPC
The VPC to use for this route table.

After the creation of route table we have to select the newly created route table and we can see there is only a local route, so we're going to enable internet access by adding a route to an Internet Gateway in a coming step.

<input checked="" type="checkbox"/>	VPC A Public Route Table	rtb-0701a38ce5bb3bb2b	-	-
-------------------------------------	--------------------------	-----------------------	---	---

Details

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (1)

Both

Edit routes

Destination

Target

Status

Propagated

10.0.0.0/16

local

Active

No

5. Select VPC A Public Subnet AZ1 and VPC A Public Subnet AZ2 and click Save association

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/4)

Filter subnet associations

<input type="checkbox"/>	Name ▾	Subnet ID ▾	IPv4 CIDR
<input type="checkbox"/>	VPC A Private Subnet AZ2	subnet-012c0447e69c5fbf2	10.0.3.0/24
<input checked="" type="checkbox"/>	VPC A Public Subnet AZ1	subnet-02db9bf794c4b9fea	10.0.0.0/24
<input type="checkbox"/>	VPC A Private Subnet AZ1	subnet-050b46f7ff48526cd	10.0.1.0/24
<input checked="" type="checkbox"/>	VPC A Public Subnet AZ2	subnet-0b7b6cb4287205...	10.0.2.0/24

6. The two public subnets will now be associated with the public route table under Explicit Subnet Associations within the Subnet associations tab.

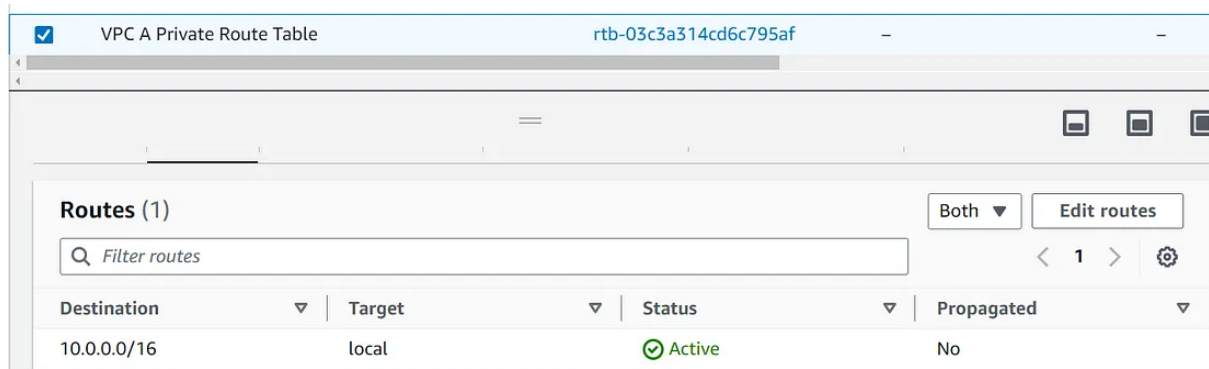
Create Route Table for Private Subnets:

1. Click on Create route table
2. Enter Name as VPC A Private Route Table
3. Select VPC A
4. Create route table

A new route table will be created with a local route. Now in order to enable outbound access to internet we will add a route to internet via NAT Gateway, so we have to associate the Private Subnets to the route table

5. In the Subnet Associations tab click on Edit subnet associations

6. Select the VPC A Private Subnet AZ1 and VPC A Private Subnet AZ2 and click Save associations



A new route table will be created with a local route. Now in order to enable outbound access to internet we will add a route to internet via NAT Gateway, so we have to associate the Private Subnets to the route table

5. In the Subnet Associations tab click on Edit subnet associations

6. Select the VPC A Private Subnet AZ1 and VPC A Private Subnet AZ2 and click Save associations

[VPC](#) > [Route tables](#) > [rtb-03c3a314cd6c795af](#) > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/4)

<input type="checkbox"/>	Name	Subnet ID	IPv4 CIDR	IPv6
<input checked="" type="checkbox"/>	VPC A Private Subnet AZ2	subnet-012c0447e69c5fbf2	10.0.3.0/24	–
<input type="checkbox"/>	VPC A Public Subnet AZ1	subnet-02db9bf794c4b9fea	10.0.0.0/24	–
<input checked="" type="checkbox"/>	VPC A Private Subnet AZ1	subnet-050b46f7ff48526cd	10.0.1.0/24	–
<input type="checkbox"/>	VPC A Public Subnet AZ2	subnet-0b7b6cb4287205...	10.0.2.0/24	–

7. Now click on Route tables and confirm that there are three route tables under VPC A: main/default, Public and Private.

<input type="checkbox"/>	–	rtb-07c2707cc44bf546f	–
<input type="checkbox"/>	VPC A Public Route Table	rtb-0701a38ce5bb3bb2b	2 subnets
<input type="checkbox"/>	VPC A Private Route Table	rtb-03c3a314cd6c795af	2 subnets

Internet Connectivity

Internet Gateway:

Internet Gateway is component of VPC that allows communication between your VPC and the internet. It supports IPv4 and IPv6 traffic.

IGw is highly available, horizontally scaled and redundant component of VPC.

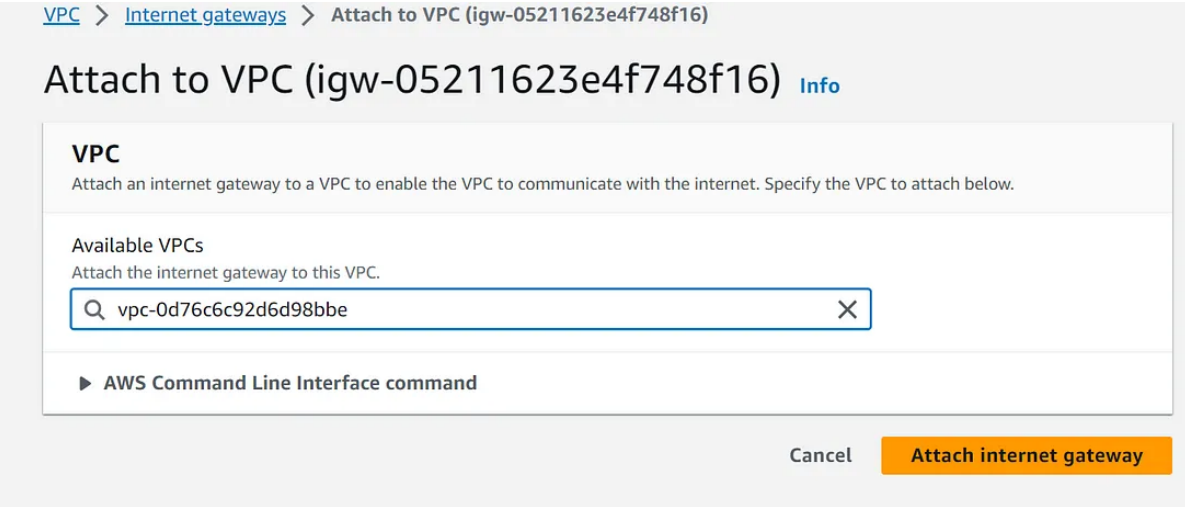
It provides inbound and outbound connectivity of resources in public subnets to the internet .

NAT Gateway:

NAT Gateway is a Network Address Translation Service, it provides access to the instances in private subnets to the services outside your VPC but external services cannot access the resources in

Deploy an Internet Gateway:

1. In the left panel select Internet Gateway and click on Create internet gateway
2. Give name as VPC A IGW and click on Create Internet Gateway
3. Click the newly created IGW and click on Attach to VPC:
4. Select VPC A and click on Attach internet gateway



The screenshot shows the AWS Management Console interface for attaching an Internet Gateway to a VPC. The breadcrumb navigation at the top reads: [VPC](#) > [Internet gateways](#) > [Attach to VPC \(igw-05211623e4f748f16\)](#). The main heading is **Attach to VPC (igw-05211623e4f748f16)** with an [Info](#) link. Below this, there is a section titled **VPC** with the instruction: "Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below." Underneath, the **Available VPCs** section says "Attach the internet gateway to this VPC." and contains a search input field with the text "vpc-0d76c6c92d6d98bbe" and a clear button (X). At the bottom of the main content area, there is a link: [▶ AWS Command Line Interface command](#). At the bottom right of the dialog, there are two buttons: **Cancel** and **Attach internet gateway** (which is highlighted in orange).

5. The Internet Gateway should attach successfully.

We now have an internet access for our VPC, but in order to use the newly created Internet Gateway, we need to update VPC routing tables

to point the default routes for our public subnets to this Internet Gateway.

[Update Route Table for Public Subnets](#)

1. In left hand panel of the VPC Dashboard click on [Route Tables](#) and select VPC A Public Route Table
2. Go to the Routes tab and edit routes
 - Click on Add route
 - Enter 0.0.0.0/0 in the Destination
 - Select Internet Gateway from the Target dropdown

Edit routes

Destination

Q 0.0.0.0/0 X

Target

Internet Gateway ▼

Q igw-05211623e4f748f16 X

Status

–

Propagated

No

Remove

3. Click Save changes and confirm that a new route has been added to the Routes tab

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (2)

Both ▾

Edit routes

Q Filter routes

< 1 >

⚙

Destination ▾	Target ▾	Status ▾	Propagated ▾
0.0.0.0/0	igw-05211623e4f748f16	✔ Active	No
10.0.0.0/16	local	✔ Active	No

Next we will add outbound connectivity from the private subnets by deploying a NAT Gateway in a public subnet for use by workloads that should not be directly exposed to the internet.

[Create NAT Gateway](#)

1. In the left hand panel of the VPC Dashboard click on [NAT Gateways](#) and click on Create NAT gateway
2. In the Create NAT gateway screen * Enter **VPC A NATGW** as the name * Choose **VPC A Public Subnet AZ1** * Click Allocate Elastic IP * Click Create NAT gateway

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

VPC A NATGW

The name can be up to 256 characters long.

Subnet

Select a subnet in which to create the NAT gateway.

subnet-02db9bf794c4b9fea (VPC A Public Subnet AZ1) ▼

Connectivity type

Select a connectivity type for the NAT gateway.

☒ Public

☐ Private

Elastic IP allocation ID [Info](#)

Assign an Elastic IP address to the NAT gateway.

eipalloc-04c474846f75883a6 ▼

Allocate Elastic IP

3. Upon creation the NAT Gateway details are displayed [Update Route Table for Private Subnets](#)

Now that we have a NAT Gateway in a public subnet we need to create a route to it from the private subnets and we will do that by adding an entry to the Route Table for the private subnets.

1. In the left hand panel of the VPC Dashboard click on [Route Tables](#)

2. Select **VPC A Private Route Table**, scroll down to the Routes tab and click on Edit routes

Edit routes

Destination

Target

Status

–

Propagated

No

Remove

Add route

3. Choose **VPC A NATGW** and click on Save changes

**** An *Elastic IP address* is a static, public IPv4 address designed for dynamic cloud computing. You can associate an Elastic IP address with**

any instance or network interface in any VPC in your account. With an Elastic IP address, you can mask the failure of an instance by rapidly remapping the address to another instance in your VPC.

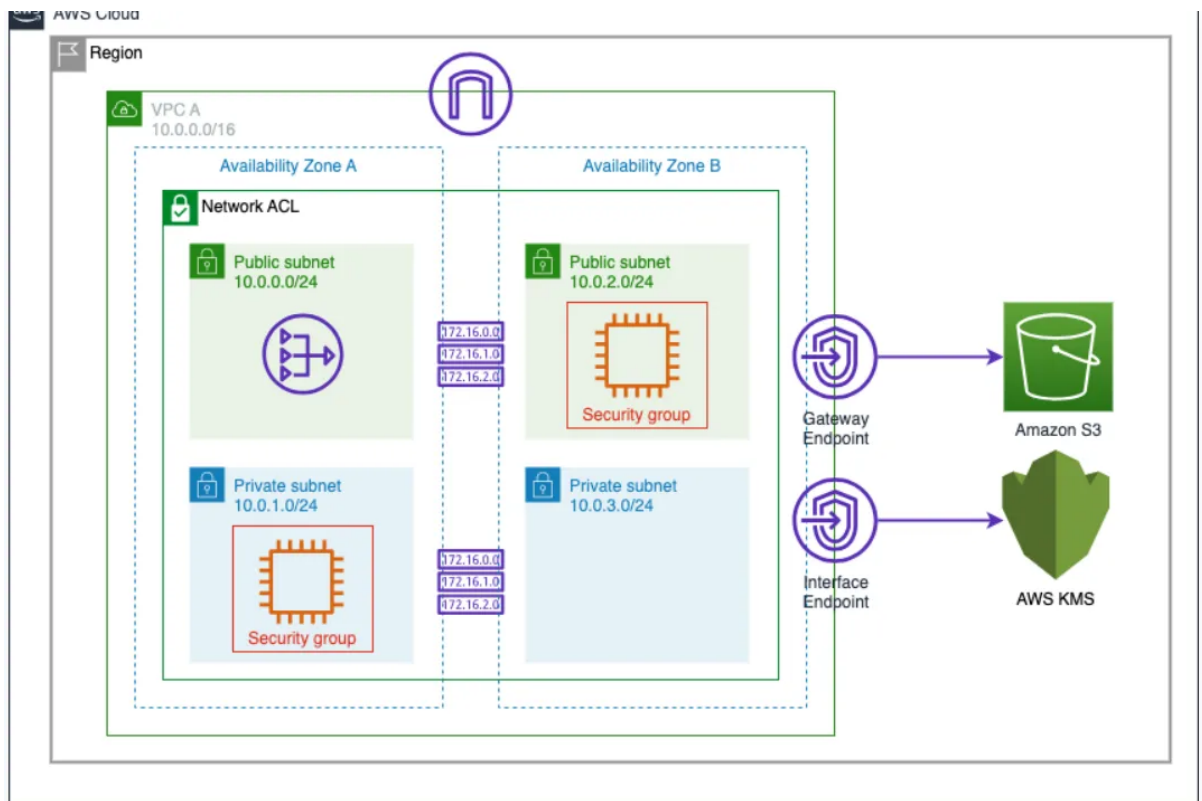
VPC Endpoints

VPC Endpoints allows customers to privately connect to AWS resources.

VPC Endpoints are powered by AWS Private Link .

VPC endpoints are virtual devices. They are horizontally scaled, redundant, and highly available Amazon VPC components that allow communication between instances in an Amazon VPC and services without imposing availability risks or bandwidth constraints on network traffic. There are two types of VPC endpoints:

1. Gateway endpoints: It supports only S3 and DynamoDB and reach these services via a gateway from VPC.
2. Interface endpoints: It is a collection of one or more elastic network interfaces with a private IP address that serves as an entry point for traffic destined to a supported service.



Create an Interface Endpoint for KMS

1. Navigate to [Endpoints](#) with the VPC console and click on
Create Endpoint to start creating a VPC Endpoint
2. In the Endpoint settings screen
 - Enter VPC A KMS Endpoint as the Name tag
 - Search for 'kms' under Services

Endpoint settings

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

VPC A KMS Endpoint

Service category

Select the service category

☒ **AWS services**
Services provided by Amazon

☐ **Private Service**

☐ **EC2 Instance Connect Endpoint**
An elastic network interface that allow you to connect to resources in a private subnet

☐ **Other**
Find se

3. From the results select the KMS service name without the '-fips' suffix

4. In the VPC section

- Select VPC A from the dropdown
- Expand the Additional settings section
- Ensure that Enable DNS name is checked

- Select the IPv4 radio button

Search

Service Name = com.amazonaws.us-east-1.kms X Clear filters

Service Name	Owner
VPC Select the VPC in which to create the endpoint	
VPC The VPC in which to create your endpoint. <input type="text" value="vpc-0d76c6c92d6d98bbe (VPC A)"/>	
Additional settings	
DNS name <input checked="" type="checkbox"/> Enable DNS name Info Associates a private hosted zone with the VPC that contains a record set that enables you to leverage Amazon' connectivity to the service while making requests to the service's default public endpoint DNS name. To use th attributes 'Enable DNS hostnames' and 'Enable DNS support' are enabled for your VPC.	
DNS record IP type <input checked="" type="radio"/> IPv4	

5. Select VPC A Private Subnet AZ1 and VPC A Private Subnet AZ2

from the subnets and check the IPv4 radio button.

Subnets (2/6) [Info](#)

<input checked="" type="checkbox"/>	Availability Zone	Subnet ID	Designate IP
<input checked="" type="checkbox"/>	us-east-1a (use1-az2)	subnet-02db... ▼	[
<input checked="" type="checkbox"/>	us-east-1b (use1-az4)	subnet-0b7b... ▼	[
<input type="checkbox"/>	us-east-1c (use1-az6)	i No subnet availabl e	

6. Select the default security group and leave the Policy as **Full Access**

7. Click on Create endpoint button to create the VPC Endpoint for KMS in VPC A.

[Create a Gateway Endpoint for S3](#)

1. Click 'Create Endpoint' to start creating another VPC Endpoint

Endpoint settings

Name tag - *optional*

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

VPC A S3 Endpoint

Service category

Select the service category

☒ **AWS services**
Services provided by Amazon

☐ **EC2 Instance Connect Endpoint**
An elastic network interface that allow you to connect to resources in a private subnet

2. Select the endpoint that has a “Type” listed as “Gateway” and in the drop down box for VPC

Services (1/242)			
<input type="text" value="Search"/>			
	Service Name	Owner	Type
<input type="radio"/>	com.amazonaws.us-east-1.rum-dataplane	amazon	Interface
<input type="radio"/>	com.amazonaws.us-east-1.runtime-me...	amazon	Interface
<input type="radio"/>	com.amazonaws.us-east-1.runtime-v2-lex	amazon	Interface
<input checked="" type="radio"/>	com.amazonaws.us-east-1.s3	amazon	Gateway
<input type="radio"/>	com.amazonaws.us-east-1.s3	amazon	Interface

3. Select **VPC A** as the VPC and check the checkbox for all the route tables

VPC
Select the VPC in which to create the endpoint

VPC
The VPC in which to create your endpoint.
vpc-0d76c6c92d6d98bbe (VPC A) ▼ C

Route tables (3/3) [Info](#)

<input checked="" type="checkbox"/>	Name ▼	Route Table ID ▼	Main
<input checked="" type="checkbox"/>	–	rtb-0504591a4a4093691	Yes
<input checked="" type="checkbox"/>	VPC A Public Route Table	rtb-0701a38ce5bb3bb2b (VPC A Public ...	No
<input checked="" type="checkbox"/>	VPC A Private Route Table	rtb-03c3a314cd6c795af (VPC A Private ...	No

4. Leave the Policy as **Full Access**

5. Click on Create endpoint button to create the VPC Endpoint for S3 attached to VPC A

✓ **Successfully created VPC endpoint**
vpce-0e9faaf3ea0d2dbe4

Endpoints (2) [Info](#)

🔍 Search

<input type="checkbox"/>	Name ▾	VPC endpoint ID ▾
<input type="checkbox"/>	VPC A KMS Endpoint	vpce-059e5c99a4af64463
<input type="checkbox"/>	VPC A S3 Endpoint	vpce-0e9faaf3ea0d2dbe4

We have now gone through the bread and butter of AWS networking and built a networking foundation of public and private subnets across two availability zones with internet access and private connectivity to AWS service endpoints.

Dear Friends, Thank you for reading all the way through. Catch you in the next part !!