



General Immersion Day

Lab 3

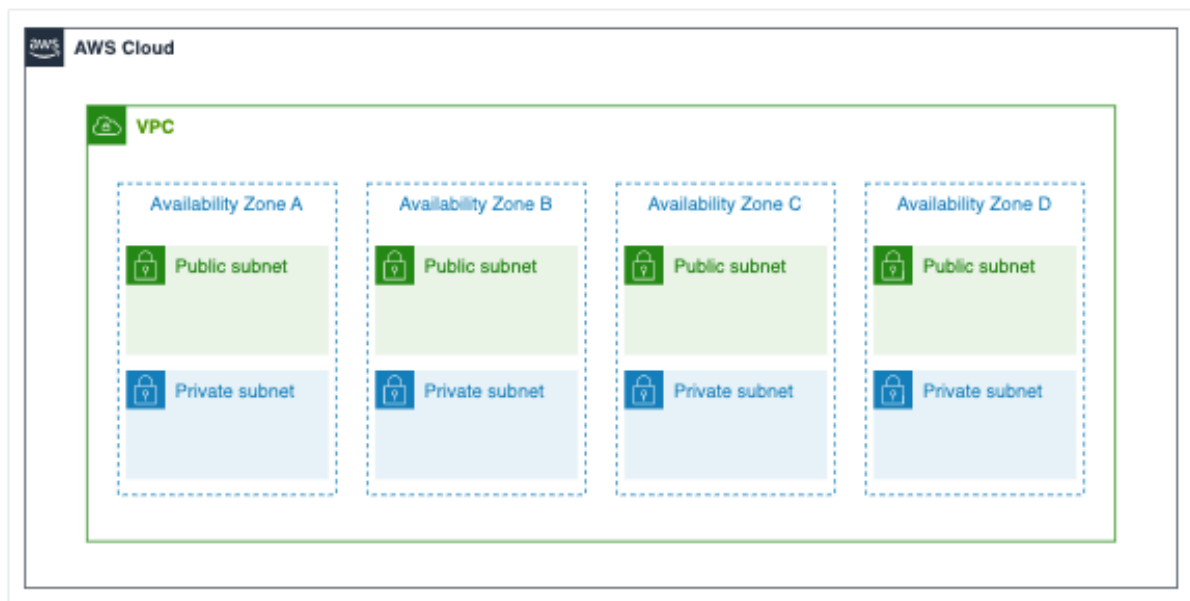
Network - VPC Hands on Lab

VPC Hands on Lab

Amazon VPC(Virtual Private Cloud) Overview

[Amazon Virtual Private Cloud\(Amazon VPC\)](#) enables you to launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

Amazon VPC lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can use both IPv4 and IPv6 in your VPC for secure and easy access to resources and applications.

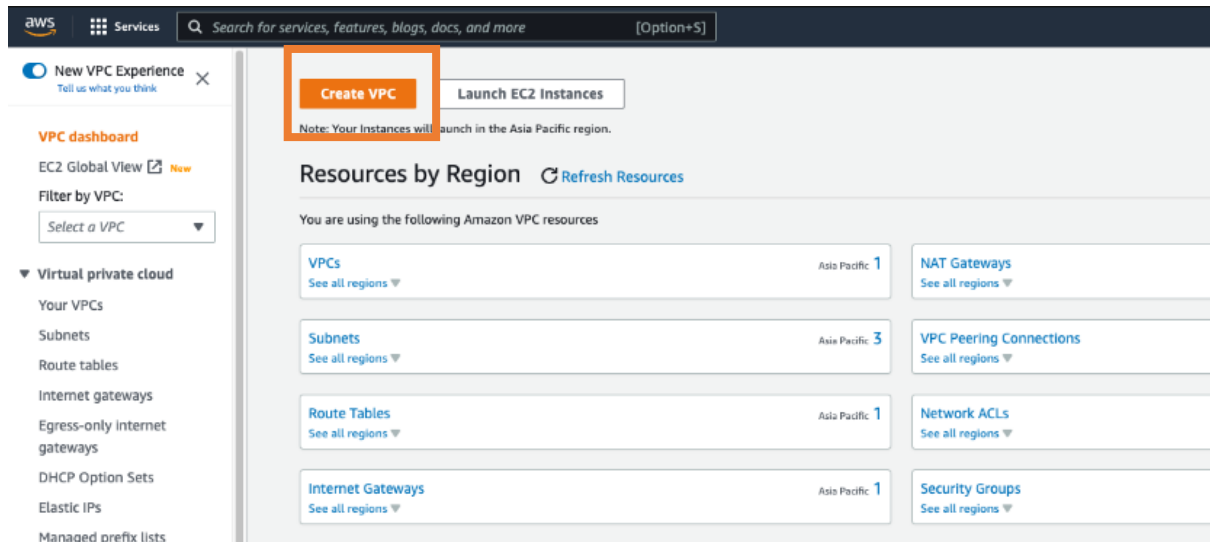


Configure your own network by going through the labs in the order below:

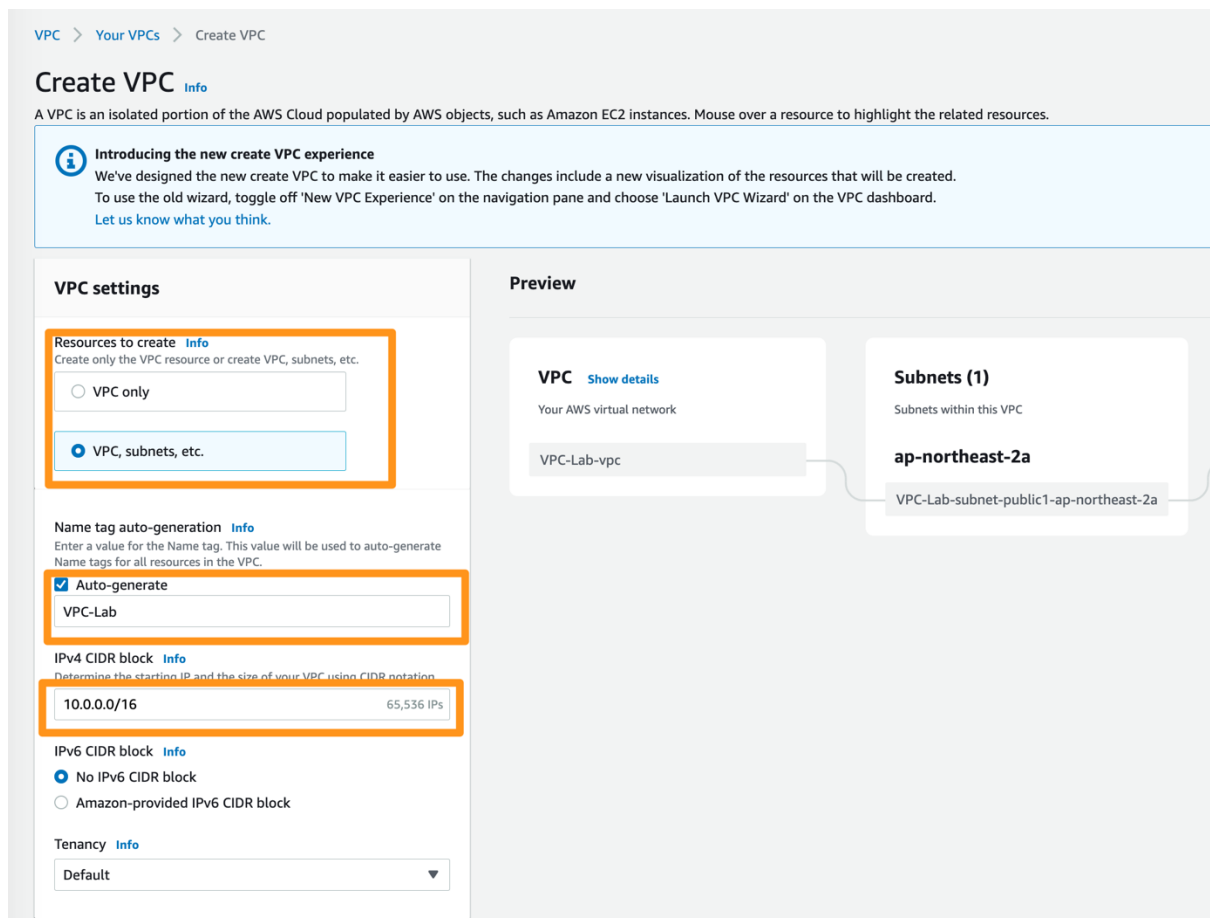
1. [Create a VPC](#)
2. [Create additional subnets](#)
3. [Edit the routing table](#)
4. [Create a Security Group](#)
5. [VPC Flow Logs \(Optional\)](#)
6. [Clean up resources](#)

3-1 Create a VPC

1. Log in to VPC Console .
2. Click **Create VPC** on the screen below to start the Launch VPC wizard. The Launch VPC wizard makes it easy to create a non-default VPC configuration.



3. Under VPC Settings, select **VPC, Subnet, etc..** For the name, type **VPC-Lab**. Set the CIDR block to the default value **10.0.0.0/16**.



- Choose 1 Availability Zone (AZ) and select **ap-southeast-1a**. The Availability Zone is a subset of the VPCs that you set up earlier. Select the number of public subnet as 1 and set the CIDR block to **10.0.10.0/24**. You do not create private subnet for this part so select 0. Then click **Create VPC** button at the bottom.

Number of Availability Zones (AZs) [Info](#)

Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1

2

3

► Customize AZs

Number of public subnets [Info](#)

The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0

1

Number of private subnets [Info](#)

The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0

1

2

► Customize subnets CIDR blocks

NAT gateways (\$) [Info](#)

Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

None

In 1 AZ

1 per AZ

VPC endpoints [Info](#)

Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

None

S3 Gateway

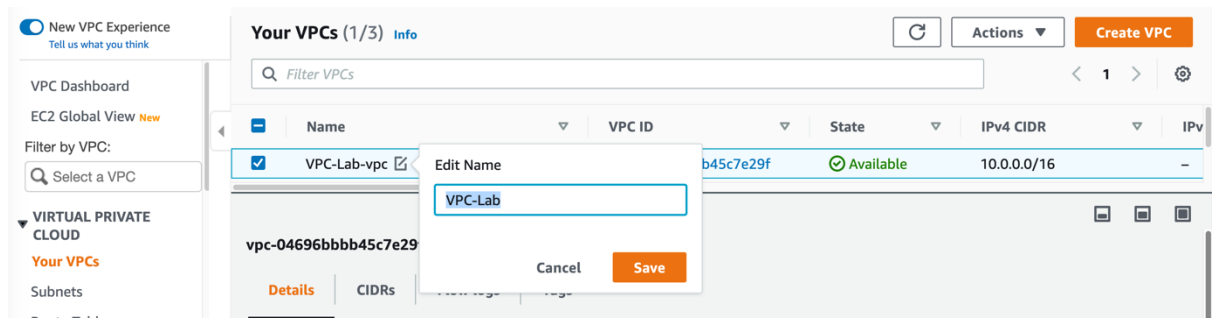
DNS options [Info](#)

☒ Enable DNS hostnames

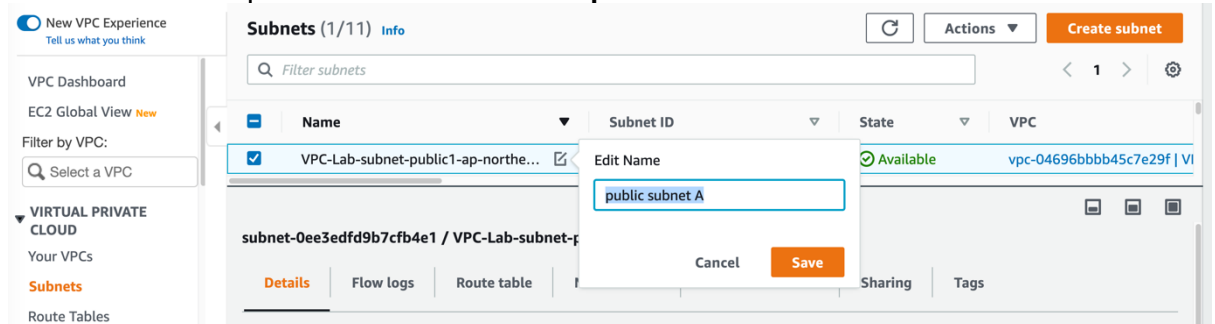
☒ Enable DNS resolution

Note: When entering a value for the VPC IPv4 CIDR block, it is important to allocate it so that the address does not overlap with networks that are likely to connect directly in the future. Also, allocate addresses large enough for future expansion.

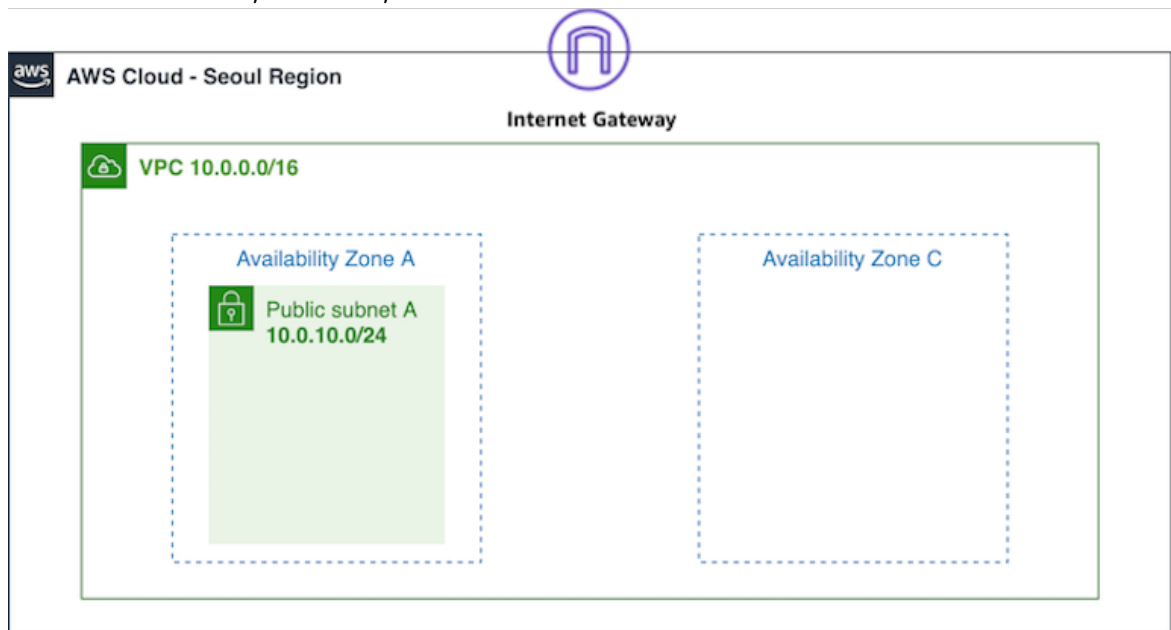
- After you create the VPC, you can see a VPC with the name **VPC-Lab-vpc**. Rename it as **VPC-Lab**



6. Go to Subnet tap and rename the subnet as **public subnet A**

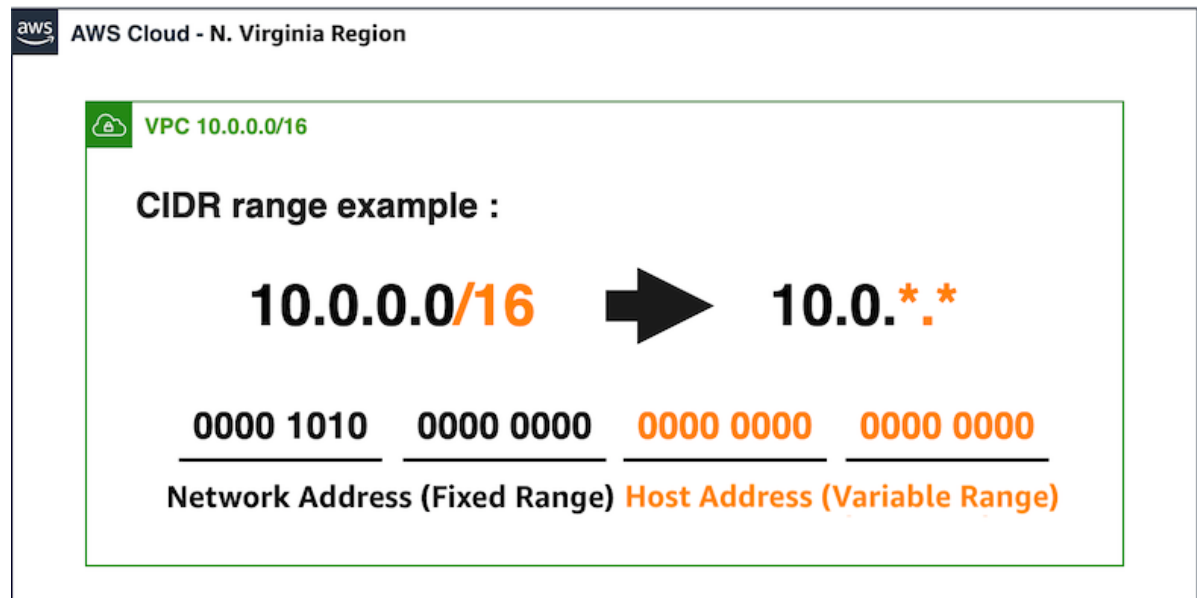


7. The architecture, as of now, is below.



Understanding CIDR address range

CIDR (Classless Inter-Domain Routing) is one of the ways to express the address and size of the network. The VPC you created above uses a range of IP addresses with 16 as the subnet value. The number of IPs that can be given to each resource is 65,536, which is 2 to the power of 16.



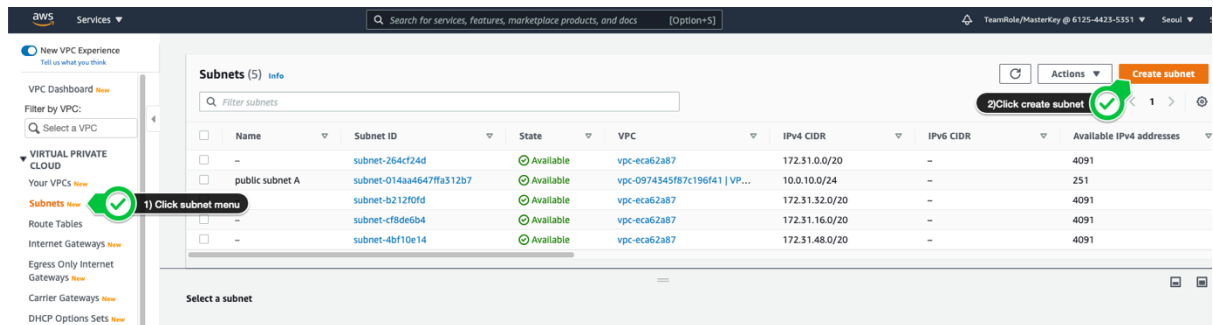
When specifying a VPC CIDR block, the allowed block size is /16 netmask (65,536 usable IP addresses) ~ /28 netmask (16 usable IP addresses). In each subnet CIDR block, the first 4 IP addresses and the last IP address are not available to users and cannot be assigned to instances. For example, in the subnet of the 10.0.0.0/24 CIDR block, the following 5 IP addresses are reserved.

Key	Value
10.0.0.0	Network address
10.0.0.1	Reserved for VPC routers from AWS
10.0.0.2	DNS server address
10.0.0.3	Reserved for future use from AWS
10.0.0.255	Network broadcast address

3-2 Creating Additional Subnets

To maintain high availability, it is important to deploy services across multiple Availability Zones. So, in this lab, you will create a subnet in an Availability Zone C, which is different from the Availability Zone A, where the subnet created earlier is located.

1. Click the **Subnet** menu on the left sidebar, then click the **Create Subnet** button.



2. For VPC ID, choose the VPC you just created.

VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.

Select a VPC

Q |

vpc-eca62a87
172.31.0.0/16 (default)

vpc-0974345f87c196f41 (VPC-Lab)
10.0.0.0/16

Select a VPC first to create new subnets.

Add new subnet

Cancel Create subnet

3. In the **Subnet settings** below, enter values as shown on the screen and click the **Create subnet** button.

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.

public subnet C

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 (Singapore) / ap-southeast-1c ▼

IPv4 CIDR block [Info](#)

10.0.20.0/24 X

▼ **Tags - optional**

Key

Q Name X

Value - optional

Q public subnet C X

Remove

Add new tag

You can add 49 more tags.

Remove

Add new subnet

key	value
Subnet name	public subnet C
Availability Zone	ap-southeast-1c
IPv4 CIDR block	10.0.20.0/24
Name	public subnet C

4. You can see that both **public subnet A** and **public subnet C** have been created.

Subnets (1/6) [info](#)

Filter subnets

< 1 >

⚙

<input checked="" type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses
<input checked="" type="checkbox"/>	public subnet C	subnet-0f9fa61bcf22173f4	Available	vpc-0974345f87c196f41 VP...	10.0.20.0/24	–	251
<input type="checkbox"/>	public subnet A	subnet-014aa4647ffa512b7	Available	vpc-0974345f87c196f41 VP...	10.0.10.0/24	–	251
<input type="checkbox"/>	–	subnet-264cf24d	Available	vpc-eca62a87	172.31.0.0/20	–	4091
<input type="checkbox"/>	–	subnet-b212f0fd	Available	vpc-eca62a87	172.31.32.0/20	–	4091
<input type="checkbox"/>	–	subnet-cf8de6b4	Available	vpc-eca62a87	172.31.16.0/20	–	4091
<input type="checkbox"/>	–	subnet-4bf10e14	Available	vpc-eca62a87	172.31.48.0/20	–	4091

Details

Flow logs

Route table

Network ACL

Sharing

Tags

Details

Subnet ID

subnet-0f9fa61bcf22173f4

Available IPv4 addresses

251

Network border group

ap-northeast-2

State

Available

IPv6 CIDR

–

Route table

rtb-0147aed7dd6f8bdf8

VPC

vpc-0974345f87c196f41 | VPC-Lab

Availability Zone

ap-northeast-2c

Network ACL

acl-05f2f240120dc9aa8

IPv4 CIDR

10.0.20.0/24

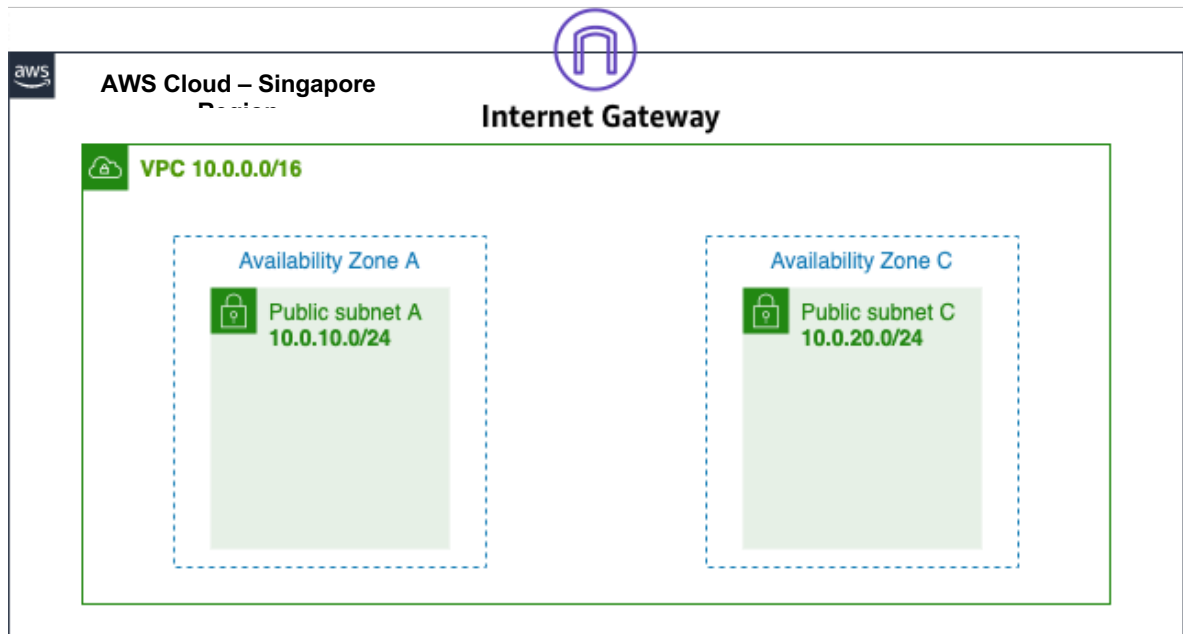
Availability Zone ID

apne2-az3

Default subnet

No

5. The architecture so far is as below.



3-3 Edit the routing table

Understanding VPC route table

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

- **Main route table** automatically comes with your VPC. It controls the routing for all subnets that are not explicitly associated with any other route table.
- **Custom route table** A route table that you create for your VPC.

Edit routing table connection

1. Click the **Actions** button in the **Subnet** menu and select **Edit routing table association**.

Name	State	VPC	IPv4 CIDR	IPv6 CIDR
public subnet C	Available	vpc-0974345f87c196f41 VP...	10.0.20.0/24	-
public subnet A	Available	vpc-0974345f87c196f41 VP...	10.0.10.0/24	-
-	Available	vpc-eca62a87	172.31.0.0/20	-
-	Available	vpc-eca62a87	172.31.32.0/20	-
-	Available	vpc-eca62a87	172.31.16.0/20	-
-	Available	vpc-eca62a87	172.31.48.0/20	-

2. Select a route table **other than** the main route table from the route table ID and save it. At this point, see if there is a route to the Internet in the selected routing table.

VPC > Subnets > subnet-0f9fa61bcf22173f4 > Edit route table association

Edit route table association

Subnet route table settings

Subnet ID
subnet-0f9fa61bcf22173f4

Route table ID
rtb-0c21eaa1ec6cd668e

rtb-0c21eaa1ec6cd668e
rtb-0147aed7dd6f8bdf8
Main route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-069c6c48857df4966

Cancel Save

3. After selecting **public subnet C**, you can see the routing information by clicking the hyperlink of the changed route table in the Details tab.

Subnets (1/6) info

Filter subnets

1) Select subnet C

	Name		State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses
<input checked="" type="checkbox"/>	public subnet C	subnet-0f9fa61bcf22173f4	Available	vpc-0974345f87c196f41 VP...	10.0.20.0/24	–	251
<input type="checkbox"/>	public subnet A	subnet-014aa4647ffa312b7	Available	vpc-0974345f87c196f41 VP...	10.0.10.0/24	–	251
<input type="checkbox"/>	–	subnet-264cf24d	Available	vpc-eca62a87	172.31.0.0/20	–	4091
<input type="checkbox"/>	–	subnet-b212f0fd	Available	vpc-eca62a87	172.31.32.0/20	–	4091
<input type="checkbox"/>	–	subnet-cf8de6b4	Available	vpc-eca62a87	172.31.16.0/20	–	4091
<input type="checkbox"/>	–	subnet-4bf10e14	Available	vpc-eca62a87	172.31.48.0/20	–	4091

Details

Flow logs

Route table

Network ACL

Sharing

Tags

2) Click Details tab

Subnet ID

subnet-0f9fa61bcf22173f4

Available IPv4 addresses

251

Network border group

ap-northeast-2

State

Available

IPv6 CIDR

–

Route table

rtb-0c21eaa1ec6cd68e

3) Check routing info

VPC

vpc-0974345f87c196f41 | VPC-Lab

Availability Zone

ap-northeast-2c

Network ACL

acl-05f2f240120dc9aa8

IPv4 CIDR

10.0.20.0/24

Availability Zone ID

apne2-az3

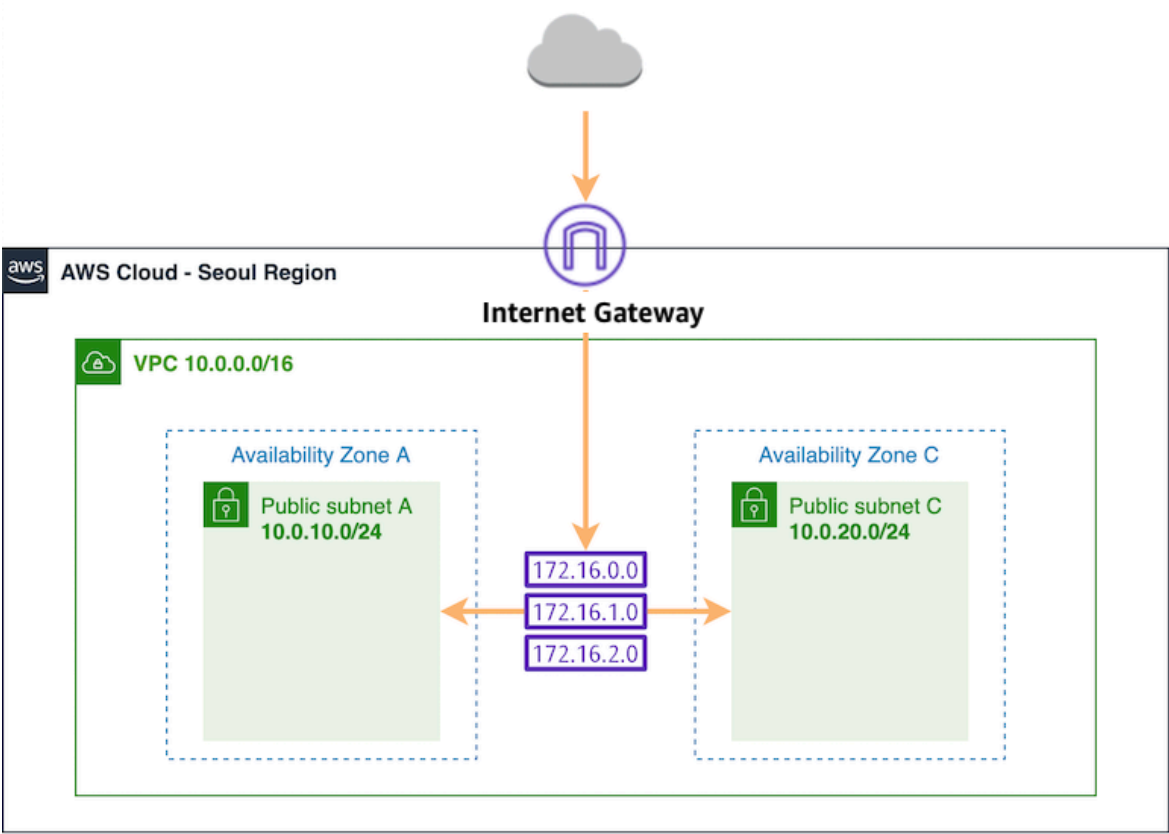
Default subnet

No

After clicking the routing table, what you can see from **Route** tab is as below. As a result, we can confirm that a route to the internet has also been created for public subnet C.

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-000

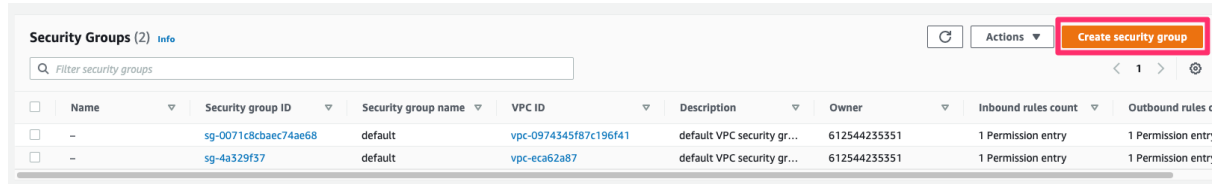
4. The architecture, so far, is as below.



3-4 Create a security group

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic.

1. Click the **Security Groups** menu on the left sidebar, then click the **Create security group** button.



2. Enter the Security group name and Description as shown on the below screen and select the VPC you created in this lab

Create security group

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:

Description:

VPC:

This security group has no inbound rules.

key	value
Security group name	webserver-sg
Description	security group for web servers
VPC	VPC-Lab

3. Add rules to the **Inbound rules** as shown below, and click the **Create security group** button at the bottom right.

Inbound rules

Type	Protocol	Port range	Source	Description - optional	
HTTP	TCP	80	Custom 54.239.119.4/32		Delete
SSH	TCP	22	Custom 54.239.119.4/32		Delete

Add rule

Type	Source
HTTP	Custom: [Input your private IP address followed by a /32] (You can find you local IP by searching What is my IP.)
SSH	Custom: [Input your private IP address followed by a /32] (You can find you local IP by searching What is my IP.)

4. Review that the inbound rule has been created as shown below

VPC > Security Groups > sg-05d8ac2f5b6602cad - webserver-sg

sg-05d8ac2f5b6602cad - webserver-sg Actions ▾

Details

Security group name webserver-sg	Security group ID sg-05d8ac2f5b6602cad	Description security group for web servers	VPC ID vpc-028f270dbb4e42231
Owner 233219696677	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	

Inbound rules | Outbound rules | Tags

You can now check network connectivity with Reachability Analyzer Run Reachability Analyzer ×

Inbound rules (2) Manage tags Edit inbound rules

Filter security group rules

<input type="checkbox"/>	Name ▾	Security group rule... ▾	IP version ▾	Type ▾	Protocol ▾	Port range ▾	Source ▾	Description
<input type="checkbox"/>	-	sgr-0952f89e79004a633	IPv4	HTTP	TCP	80	0.0.0.0/0	-
<input type="checkbox"/>	-	sgr-0c730b8845e8596ff	IPv4	SSH	TCP	22	0.0.0.0/0	-