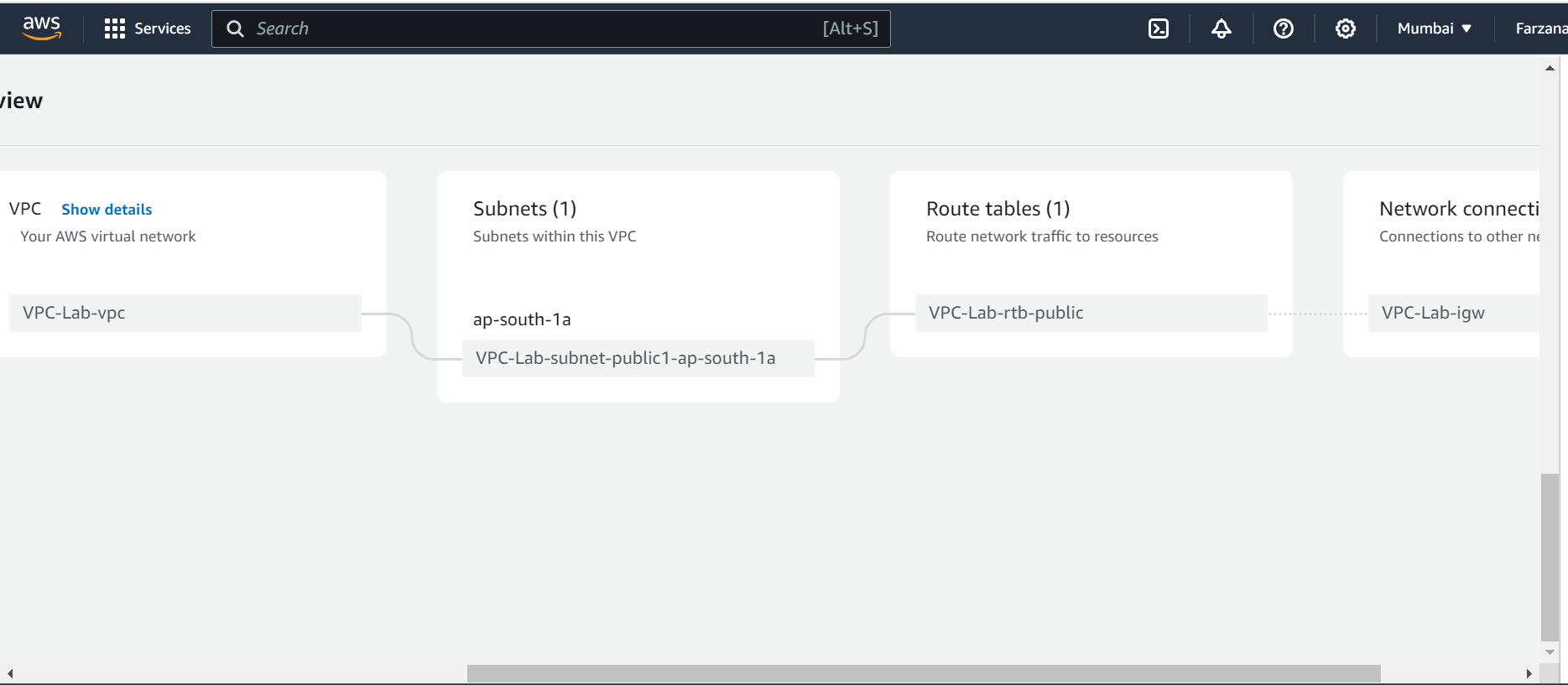
VPC Hands on Lab

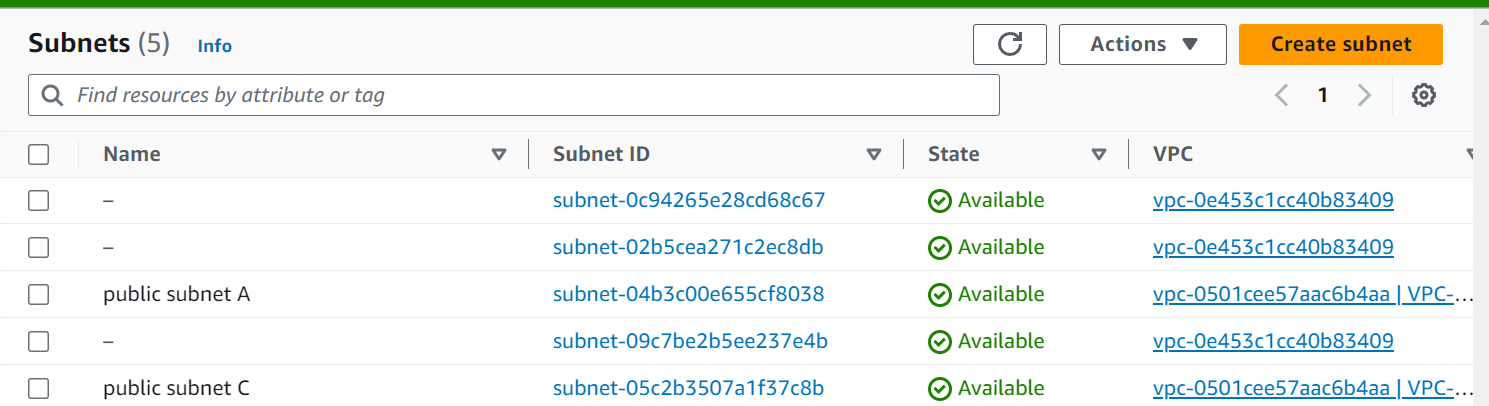
Create a VPC

1. Log in to VPC Console
2. Create VPC
3. Under VPC settings , select VPC and more, enter a name tag, set CIDR block to 10.0.0.0/16
4. choose 1 Availability Zone (AZ) then select **ap-northeast-2a**. Select the number of public subnet as 1, set the CIDR block to **10.0.10.0/24**.
5. After you create the VPC, you can see a VPC with the name **VPC-Lab-vpc**. Rename it as **VPC-Lab**
6. Go to Subnets tab on the left side bar and rename the subnet as **public subnet A**

****

Creating additional subnets

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.
3. In the **Subnet settings** below, enter values ​​as shown on the screen and click the **Create subnet** button.
4. You can see that both **public subnet A** and **public subnet C** have been created



# **Edit the routing 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**.
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.
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.

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**
3. Add rules to the **Inbound rules** as shown below, and click the **Create security group** button at the bottom right.
4. Review that the inbound rule has been created as shown below.

# **VPC Flow Logs**

Create VPC Flow logs

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to Amazon CloudWatch Logs or Amazon S3. After you create a flow log, you can retrieve and view its data in the chosen destination.

Flow logs can help you with a number of tasks, such as:

* Diagnosing overly restrictive security group rules
* Monitoring the traffic that is reaching your instance
* Determining the direction of the traffic to and from the network interfaces

Flow log data is collected outside of the path of your network traffic, and therefore does not affect network throughput or latency. You can create or delete flow logs without any risk of impact to network performance.

#### [Prerequisites:](https://catalog.workshops.aws/general-immersionday/en-US/basic-modules/20-vpc/vpc/5-vpc" \l "prerequisites:)

* **IAM Role** - This role will be used by flow logs to publish logs to CloudWatch.
* **Cloud Watch Log Group** - Flow logs will be published to this group.
* **EC2 Instance** - A test EC2 server with http configured to generate traffic.

Enable VPC Flow Logs

1. In the AWS Console search for VPC or select the **Services** menu and click on **VPC** under "Networking & Content Delivery".
2. In the VPC service page click the **Your VPCs** menu on the left sidebar, then select the **VPC-Lab**. In the bottom navigate to **Flow Logs** and click on **Create flow log**.
3. On the Create flow log page, fill in the following fields:

a. Under "Name - Optional" name it as [VPC-Lab-Flow-Log].

b. For **Maximum aggregation interval**, choose **1 minute**. (For this lab we are going with 1 Min to reduce initial wait time.)

c. For **Destination**, choose **Send to CloudWatch Logs**.

d. For **Destination log group**, choose **VPCFlowLogGroup**. (This was created as part of CloudFormation)

e. For **IAM role**, choose **RoleForVPCFlowLogs**. (This was also created as part of CloudFormation)

f. For **Log record format**, choose **AWS default format**.

g. Once details are filled as above click on **Create flow log** on the bottom of the screen.

