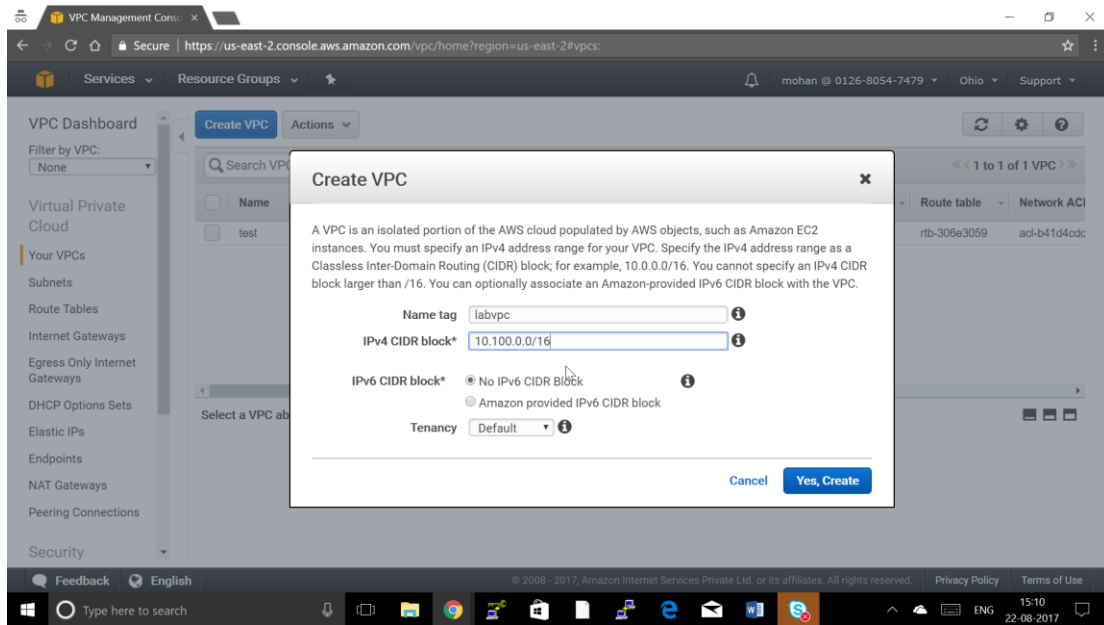


Give the Following

- VPC Name: labvpc
- VPC CIDR Block: 10.100.0.0/16
- Tenancy: Default
- And Press “Yes Create”



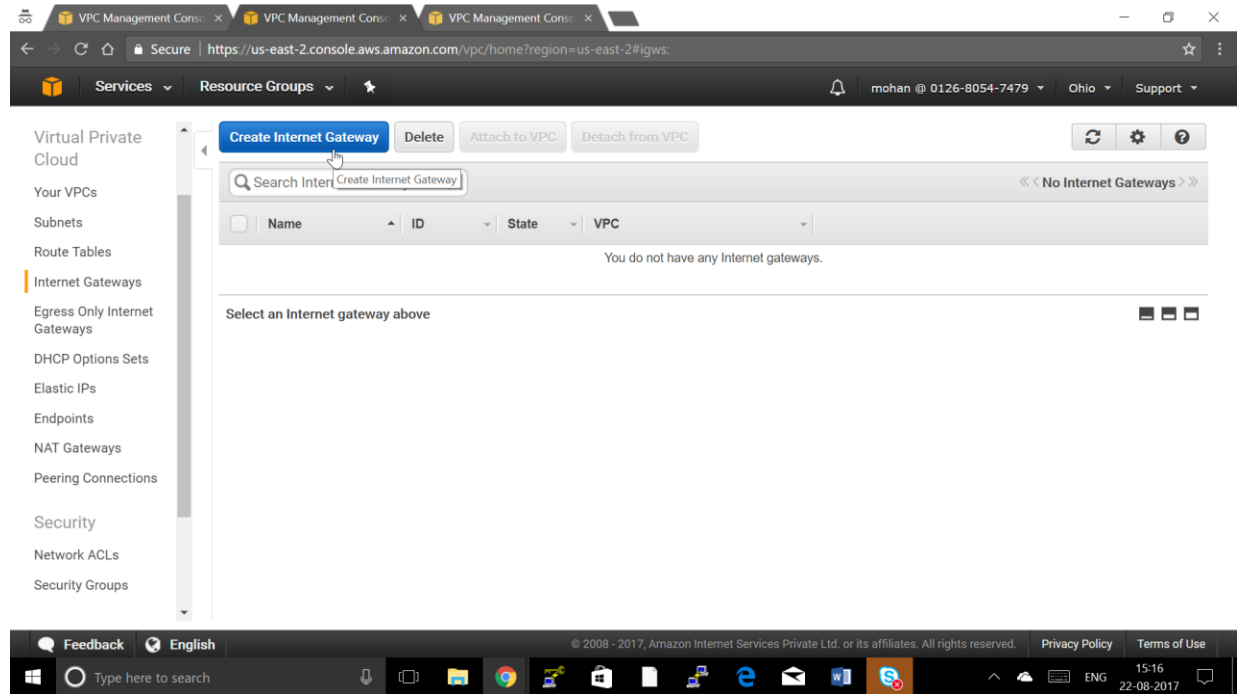
When you create a VPC the below are a Created by default

1. Default Route Table, by default used by all subnet
2. Default ACL , By Default used by all subnet
3. Default DHCP Options set , If it is the first VPC , Following VPC attached to the default DHCP Option Set.

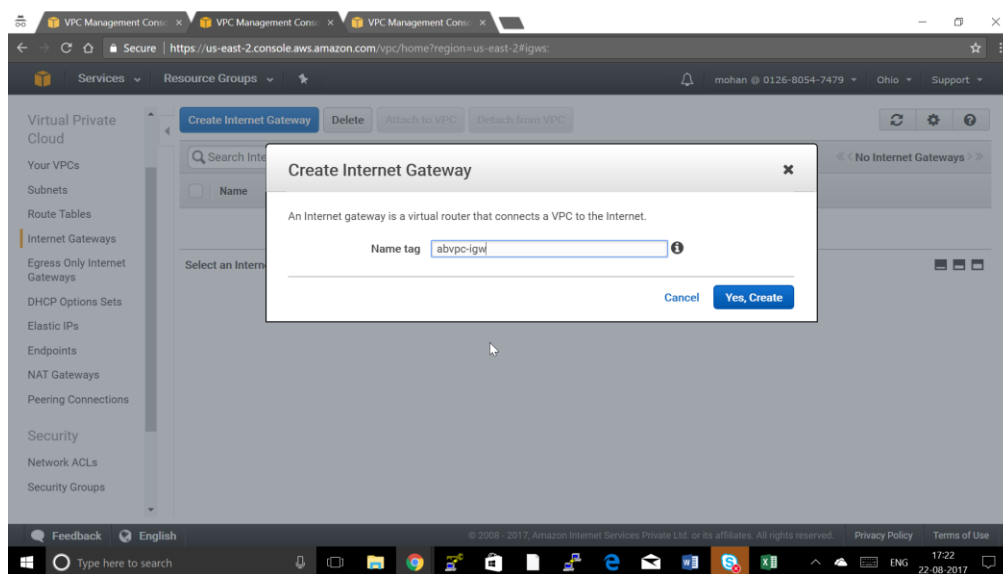
Note: All of these can be changed later

Step 2: Create Internet Gateway and Attach to VPC

a. Click on Internet Gateway and Click create internet Gateway



b. Give Internet Gateway name and click “Yes,Create”



c. Choose the Internet Gateway Created and choose “Attach to VPC”

The screenshot shows the AWS VPC Management Console interface. On the left sidebar, the 'Internet Gateways' link is highlighted. The main content area displays a table of Internet Gateways with one entry: 'abvpc-igw' with ID 'igw-5f781e36' and state 'detached'. Above the table, the 'Attach to VPC' button is highlighted with a mouse cursor. Below the table, the details for 'igw-5f781e36 | abvpc-igw' are shown, including the ID, state, and attached VPC ID.

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

NAT Gateways

Peering Connections

Security

Network ACLs

Security Groups

Create Internet Gateway Delete Attach to VPC Detach from VPC

Search Internet Gateways and X Attach to VPC

<< 1 to 1 of 1 Internet Gateway >>

Name	ID	State	VPC
abvpc-igw	igw-5f781e36	detached	

igw-5f781e36 | abvpc-igw

Summary Tags

ID: igw-5f781e36 | abvpc-igw Attached VPC ID:

State: detached Attachment state:

Feedback English

© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Type here to search

17:23 22-08-2017

d. Choose your VPC and click “Yes, Attach”

The screenshot shows the AWS VPC Management Console interface with the 'Attach to VPC' dialog box open. The dialog box prompts the user to attach an Internet gateway to a VPC. A dropdown menu for 'VPC' is open, showing three options: 'vpc-f2035e9b | labvpc', 'vpc-f2035e9b | labvpc', and 'vpc-f0b6f599 | test'. The 'Yes, Attach' button is highlighted with a mouse cursor.

Attach to VPC

Attach an Internet gateway to a VPC to enable communication with the Internet.

VPC vpc-f2035e9b | labvpc vpc-f2035e9b | labvpc vpc-f0b6f599 | test

Cancel Yes, Attach

State: detached Attachment state:

Feedback English

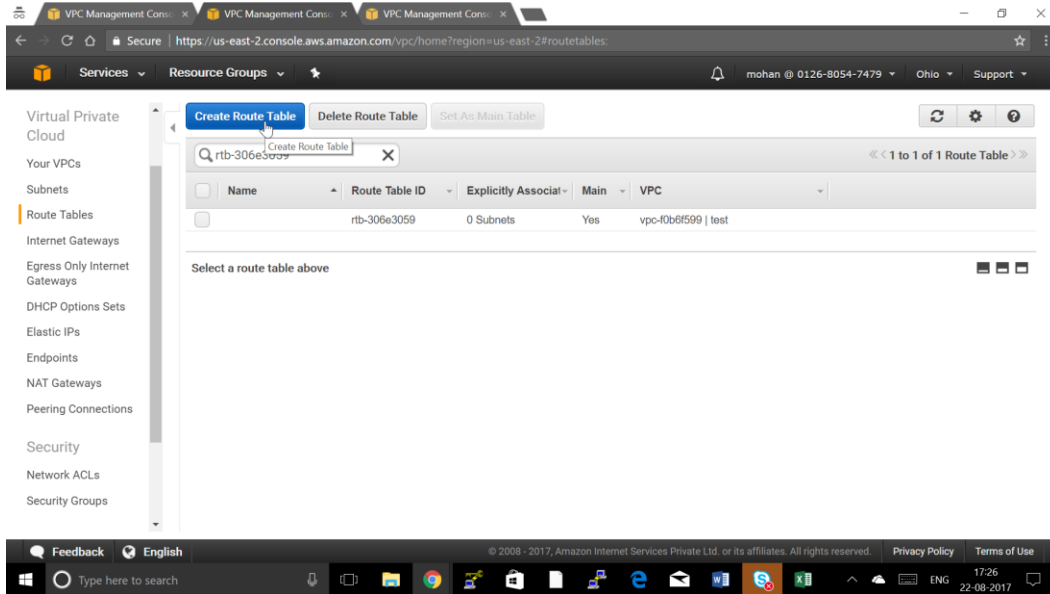
© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Type here to search

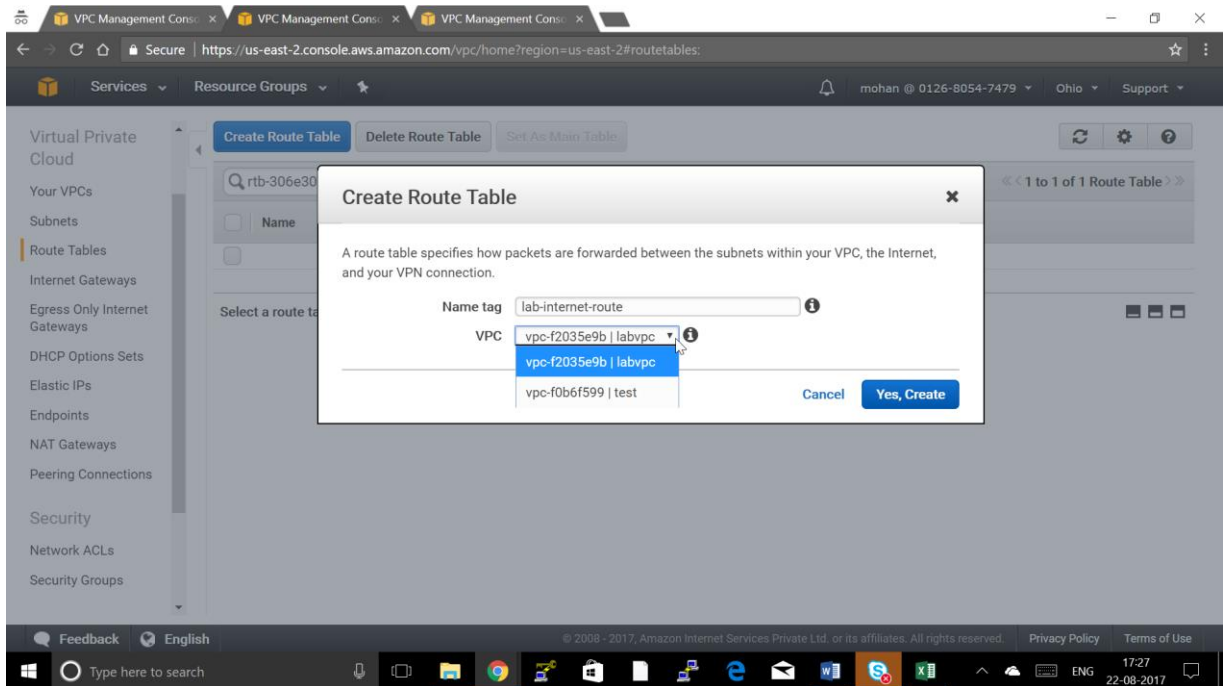
17:24 22-08-2017

Step 3: Creating a Route Table for Public Subnet to Route to Internet Gateway

a. Click on Route Tables and Click “Create Route Table”



b. Give Route Table Name and Choose your VPC and Click “Yes Create”



c. Click on Route table you created and click Routes Tab

The screenshot shows the AWS VPC console interface. The left sidebar contains navigation links for Virtual Private Cloud, Your VPCs, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, NAT Gateways, Peering Connections, Security, Network ACLs, and Security Groups. The main content area displays the 'Routes' tab for the selected route table 'rtb-306e3059'. The 'Routes' tab shows a table with columns: Destination, Target, Status, and Propagated. The table contains one entry: Destination '10.10.0.0/16', Target 'local', Status 'Active', and Propagated 'No'. The 'Edit' button is visible above the table. The top navigation bar shows 'Services', 'Resource Groups', and user information 'mohan @ 0126-8054-7479'.

Destination	Target	Status	Propagated
10.10.0.0/16	local	Active	No

d. Click Edit to Add the Internet Route and Click "Add Another Route"

The screenshot shows the AWS VPC console interface. The left sidebar contains navigation links for VPC Dashboard, Virtual Private Cloud, Your VPCs, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, NAT Gateways, Peering Connections, and Security. The main content area displays the 'Routes' tab for the selected route table 'rtb-10c2e879 | lab-internet-route'. The 'Routes' tab shows a table with columns: Destination, Target, Status, Propagated, and Remove. The table contains one entry: Destination '10.100.0.0/16', Target 'local', Status 'Active', and Propagated 'No'. The 'Add another route' button is visible below the table. The top navigation bar shows 'Services', 'Resource Groups', and user information 'mohan @ 0126-8054-7479'.

Destination	Target	Status	Propagated	Remove
10.100.0.0/16	local	Active	No	

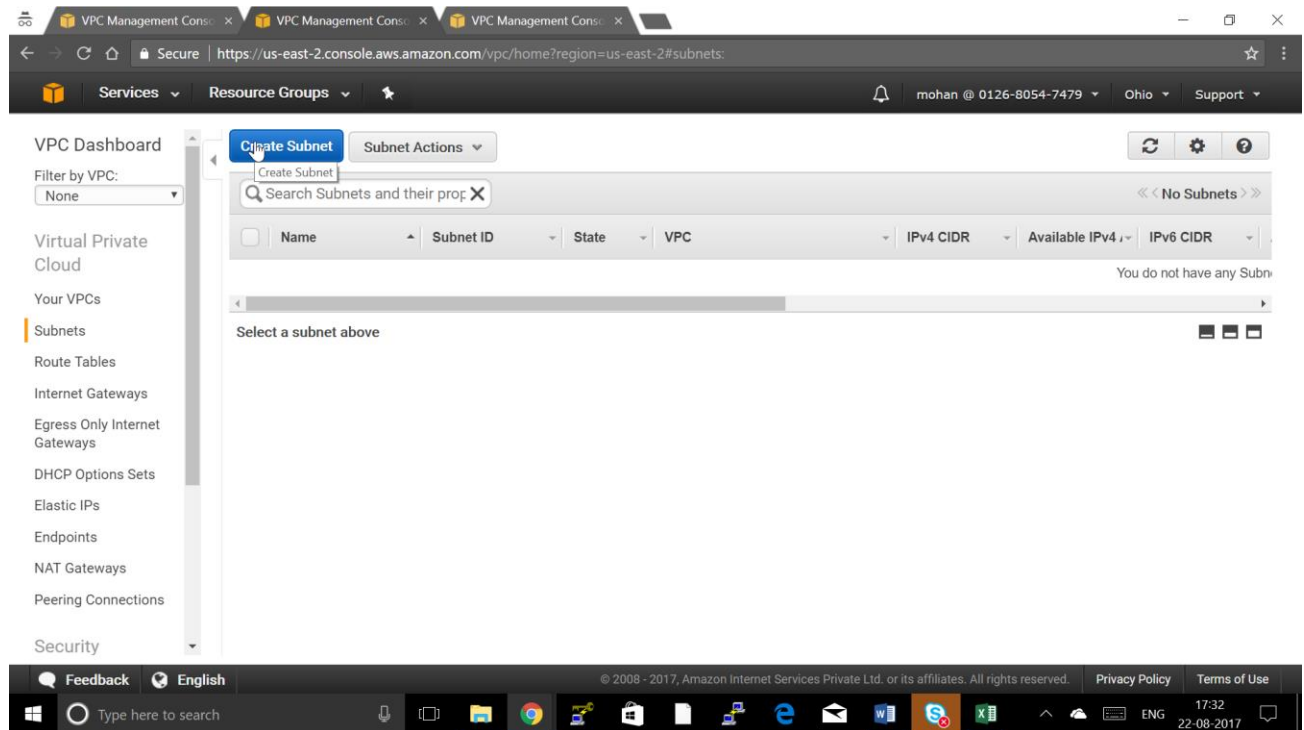
- e. Give Destination as 0.0.0.0/0 for Internet and Target and IGW you created and Click Save

The screenshot shows the AWS Management Console VPC Dashboard. The left sidebar contains navigation links for VPC Dashboard, Virtual Private Cloud, Your VPCs, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, NAT Gateways, Peering Connections, and Security. The main content area displays a list of route tables. The selected route table, 'lab-internet-route' (ID: rtb-10c2e879), is shown in detail. The 'Routes' tab is active, displaying a table of routes. The first route has a destination of 10.100.0.0/16 and a target of 'local', with a status of 'Active'. The second route has a destination of 0.0.0.0/0 and a target of 'igw-5f781e36', with a status of 'No'. A 'Save' button is visible at the top of the route configuration area.

Destination	Target	Status	Propagated	Remove
10.100.0.0/16	local	Active	No	
0.0.0.0/0	igw-5f781e36	No	No	+

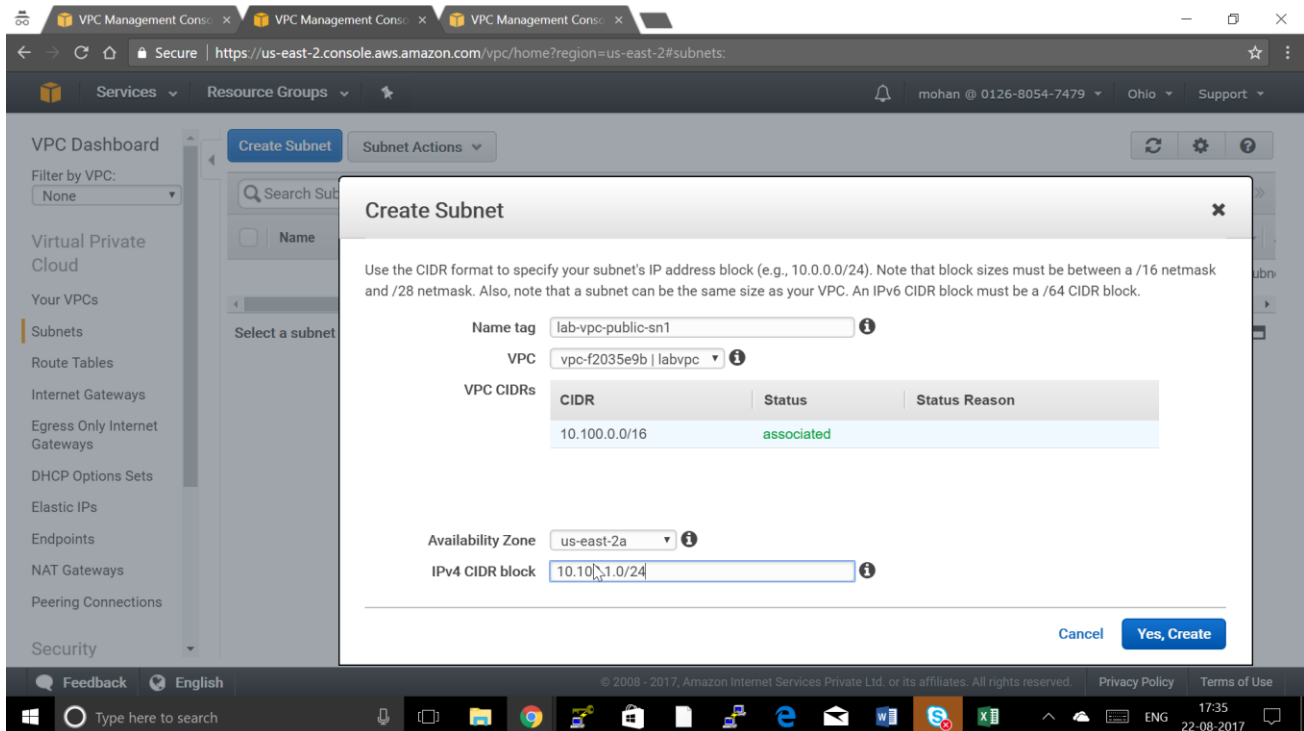
Step 4: Creating Public Subnet

a. Choose Subnet and say Create subnet

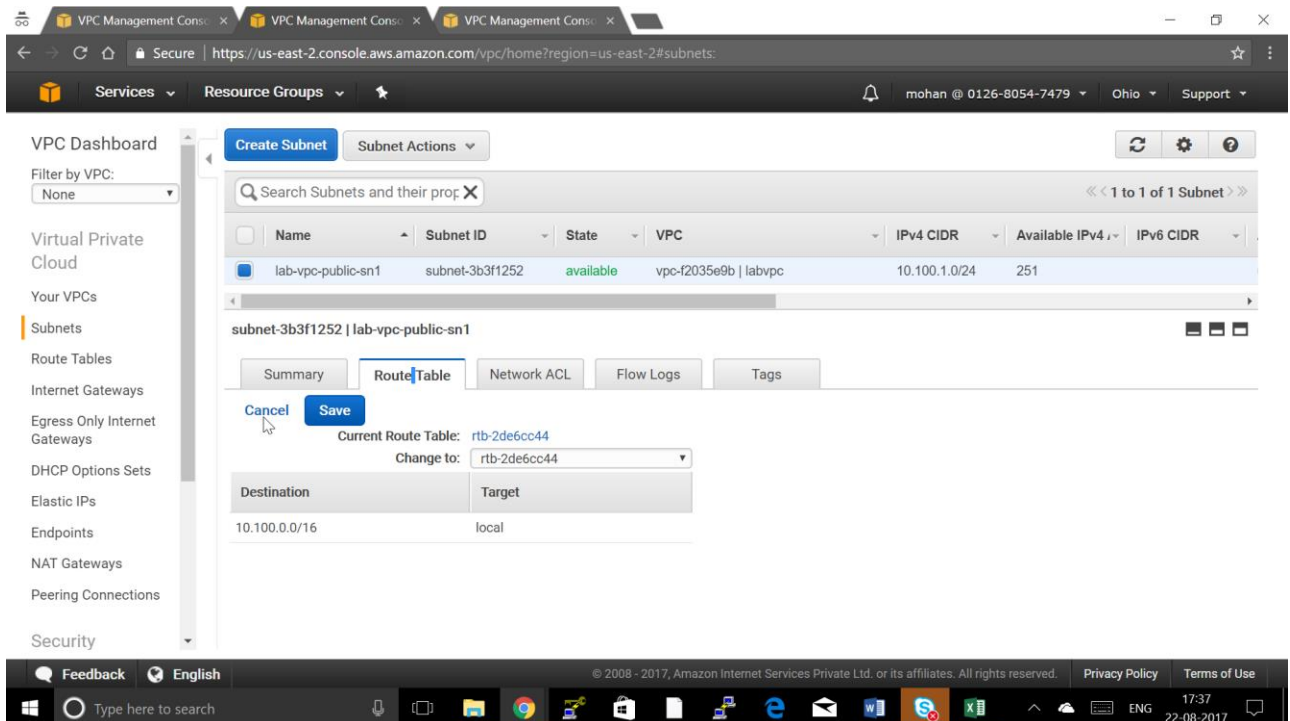


b. Give the following Details:

- Name Tag: lab-vpc-public-sn1 (Name of the Subnet)
- VPC: lab-vpc (Choose your VPC)
- Availability Zone : us-web-2a (Choose your Availability Zone)
- CIDR Block: 10.100.1.0/24 (CIDR block should be in the same range of VPC)
- Click “Yes Create” to Create Subnet



c. Choose Route Table tab and click Edit



d. Choose the Public Route Table created and Click Save

The screenshot shows the AWS VPC console interface. On the left, the 'Subnets' link is selected in the navigation pane. The main content area displays the details for subnet-3b3f1252 | lab-vpc-public-s1. The 'Route Table' tab is active, showing the current route table as 'rtb-2de6cc44'. A dropdown menu is open, showing 'Change to:' with the option 'rtb-10c2e879 | lab-internet-route' selected. Below this, a table lists destinations and their targets:

Destination	Target
10.100.0.0/16	rtb-2de6cc44
0.0.0.0/0	igw-5f781e36

The 'Save' button is highlighted in blue. The bottom of the screen shows the Windows taskbar with the time 17:37 on 22-08-2017.

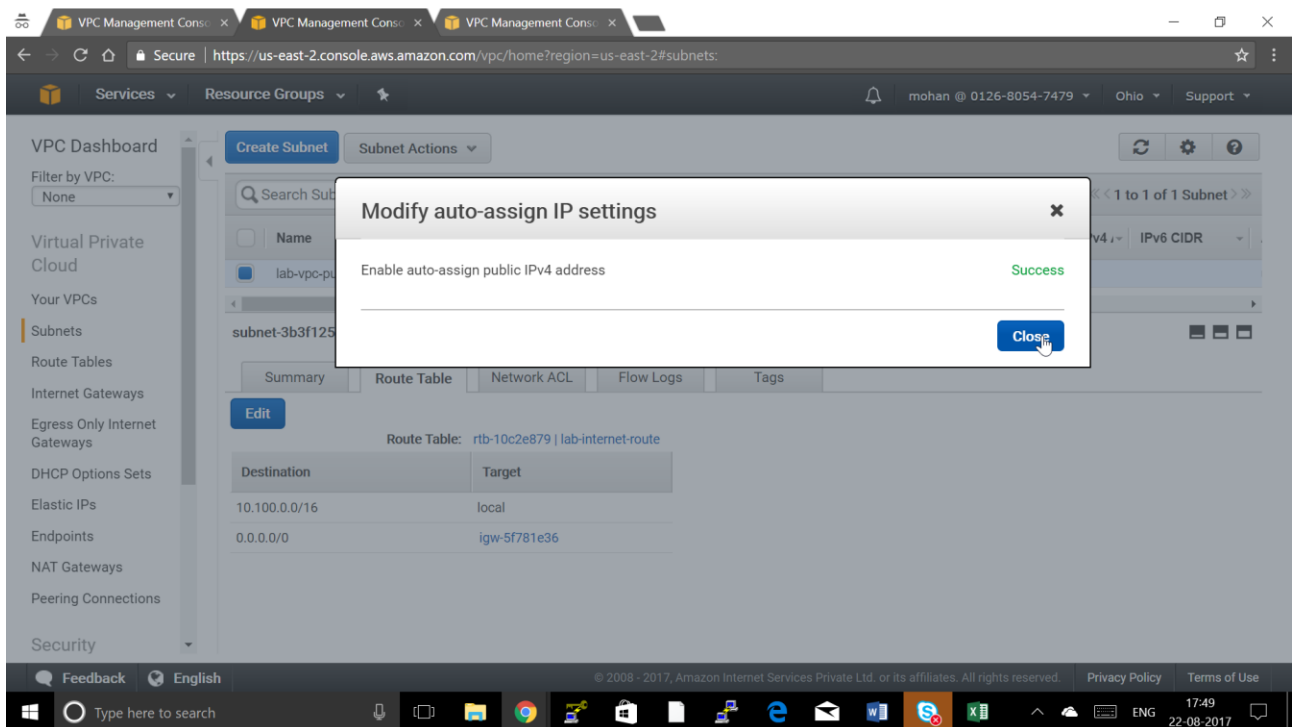
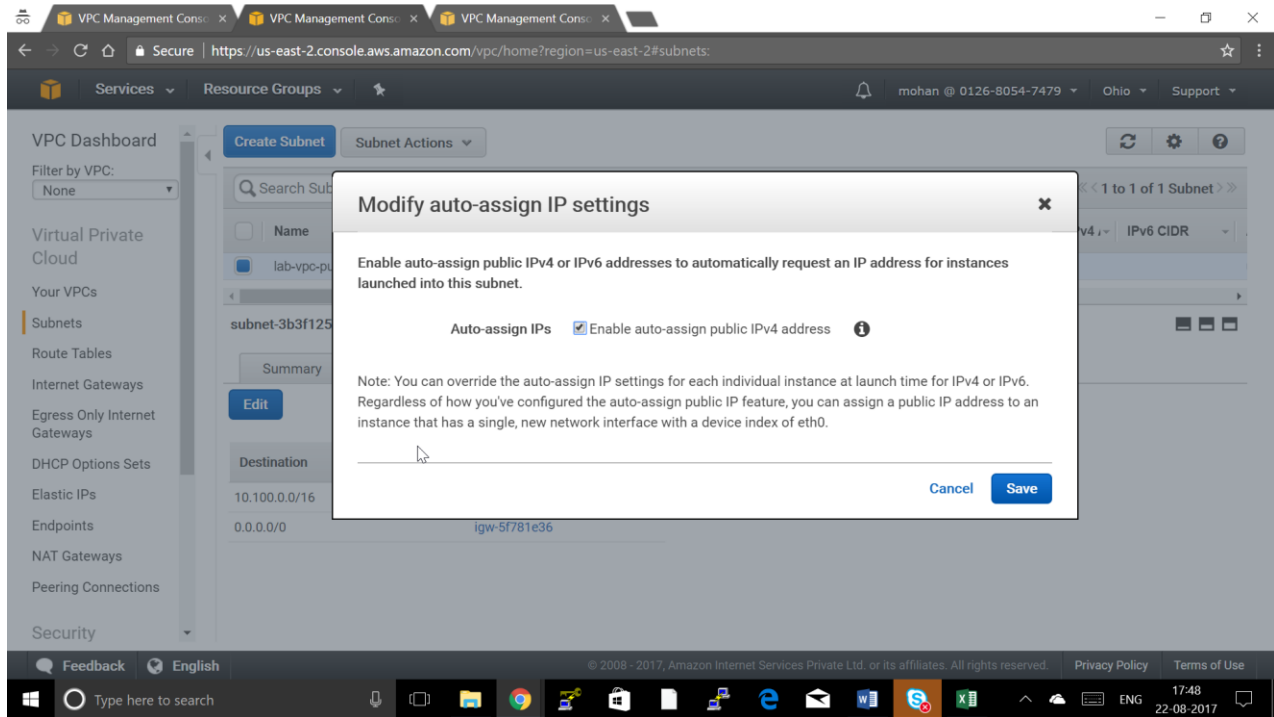
e. Choose Subnet and Click on Subnet Actions and Choose “Modify Auto Assign Public IP”

The screenshot shows the AWS VPC console interface. On the left, the 'Subnets' link is selected in the navigation pane. The main content area displays the details for subnet-3b3f1252 | lab-vpc-public-s1. The 'Subnet Actions' dropdown menu is open, showing options: 'Delete Subnet', 'Edit IPv6 CIDRs', 'Create Flow Log', and 'Modify auto-assign IP settings'. The 'Modify auto-assign IP settings' option is highlighted. Below the dropdown, the 'Route Table' tab is active, showing the route table as 'rtb-10c2e879 | lab-internet-route'. A table lists destinations and their targets:

Destination	Target
10.100.0.0/16	local
0.0.0.0/0	igw-5f781e36

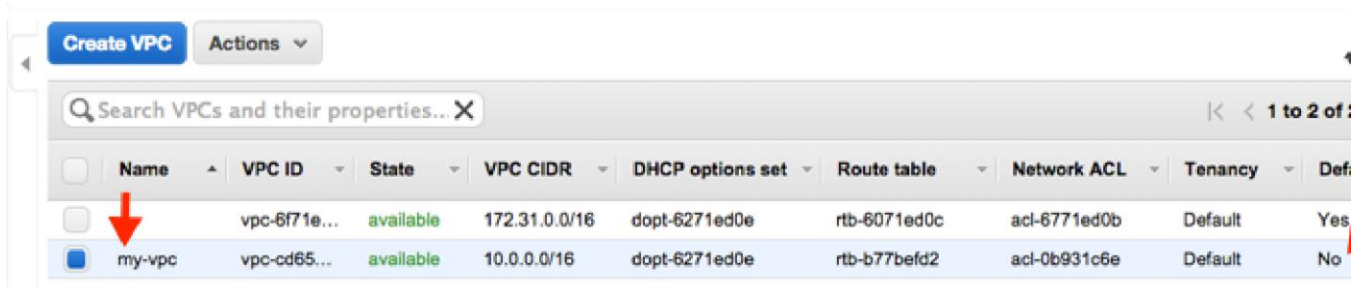
The bottom of the screen shows the Windows taskbar with the time 17:39 on 22-08-2017.

f. Choose “Enable auto-assign public IPv4 address” and Save



Step 5: Repeat the Previous Step to Create one more Subnet but in a Different Availability Zone and different Name

Step 6: Viewing Information About Your VPC



The screenshot shows the AWS VPC console interface. At the top, there is a 'Create VPC' button and an 'Actions' dropdown menu. Below this is a search bar labeled 'Search VPCs and their properties...'. A table lists VPCs with columns: Name, VPC ID, State, VPC CIDR, DHCP options set, Route table, Network ACL, Tenancy, and Default. Two VPCs are listed: one with ID 'vpc-6f71e...' and another named 'my-vpc' with ID 'vpc-cd65...'. A red arrow points to the 'my-vpc' row.

<input type="checkbox"/>	Name	VPC ID	State	VPC CIDR	DHCP options set	Route table	Network ACL	Tenancy	Default
<input type="checkbox"/>		vpc-6f71e...	available	172.31.0.0/16	dopt-6271ed0e	rtb-6071ed0c	acl-6771ed0b	Default	Yes
<input checked="" type="checkbox"/>	my-vpc	vpc-cd65...	available	10.0.0.0/16	dopt-6271ed0e	rtb-b77befd2	acl-0b931c6e	Default	No

After you've created the VPC, you can view information about the subnet, the Internet gateway, and the route tables. The VPC that you created has two route tables — a main route table that all VPCs have by default, and a custom route table that was created by the wizard. The custom route table is associated with your subnet, which means that the routes in that table determine how the traffic for the subnet flows. If you add a new subnet to your VPC, it uses the main route table by default.

To view information about your VPC

1. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. In the navigation pane, choose **Your VPCs**. Take note of the name and the ID of the VPC that you created (look in the **Name** and **VPC ID** columns). You will use this information to identify the components that are associated with your VPC.
3. In the navigation pane, choose **Subnets**. The console displays the subnet that was created when you created your VPC. You can identify the subnet by its name in **Name** column, or you can use the VPC information that you obtained in the previous step and look in the **VPC** column.
4. In the navigation pane, choose **Internet Gateways**. You can find the Internet gateway that's attached to your VPC by looking at the **VPC** column, which displays the ID and the name (if applicable) of the VPC.
5. In the navigation pane, choose **Route Tables**. There are two route tables associated with the VPC. Select the custom route table (the **Main** column displays **No**), and then choose the **Routes** tab to display the route information in the details pane:

- The first row in the table is the local route, which enables instances within the VPC to communicate. This route is present in every route table by default, and you can't remove it.
 - The second row shows the route that the Amazon VPC wizard added to enable traffic destined for an IP address outside the VPC (0.0.0.0/0) to flow from the subnet to the Internet gateway.
6. Select the main route table. The main route table has a local route, but no other routes.

Step 7: Creating Your WebServerSG Security Group

You can create your security group using the Amazon VPC console.

To create the WebServerSG security group and add rules

1. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. In the navigation pane, choose **Security Groups**.
3. Choose **Create Security Group**.
4. In the **Group name** field, enter `WebServerSG` as the name of the security group, and provide a description. You can optionally use the **Name tag** field to create a tag for the security group with a key of `Name` and a value that you specify.
5. Select the ID of your VPC from the **VPC** menu, and then choose **Yes, Create**.
6. Select the `WebServerSG` security group that you just created (you can view its name in the **Group Name** column).
7. On the **Inbound Rules** tab, choose **Edit** and add rules for inbound traffic as follows, and then choose **Save** when you're done:
 - a. Select **HTTP** from the **Type** list, and enter `0.0.0.0/0` in the **Source** field.
 - b. Choose **Add another rule**, then select **HTTPS** from the **Type** list, and enter `0.0.0.0/0` in the **Source** field.

- c. Choose **Add another rule**. If you're launching a Linux instance, select **SSH** from the **Type** list, or if you're launching a Windows instance, select **RDP** from the **Type** list. Enter your network's public IP address range in the **Source** field. If you don't know this address range, you can use `0.0.0.0/0` for this exercise.

Caution

If you use `0.0.0.0/0`, you enable all IP addresses to access your instance using SSH or RDP. This is acceptable for the short exercise, but it's unsafe for production environments. In production, you'll authorize only a specific IP address or range of addresses to access your instance.

Type	Protocol	Port Range	Source	Remove
HTTP (80)	TCP (6)	80	0.0.0.0/0	
HTTPS (443)	TCP (6)	443	0.0.0.0/0	
SSH (22)	TCP (6)	22	192.0.2.0/24	
RDP (3389)	TCP (6)	3389	192.0.2.0/24	

[Add another rule](#)

Step 8: To launch an EC2 instance into a VPC

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. In the navigation bar, on the top-right, ensure that you select the same region in which you created your VPC and security group.
3. From the dashboard, choose **Launch Instance**.
4. On the first page of the wizard, choose the AMI that you want to use. For this exercise, we recommend that you choose an Amazon Linux AMI or a Windows AMI.
5. On the **Choose an Instance Type** page, you can select the hardware configuration and size of the instance to launch. By default, the wizard selects the

first available instance type based on the AMI you selected. You can leave the default selection, and then choose **Next: Configure Instance Details**.

6. On the **Configure Instance Details** page, select the VPC that you created from the **Network** list, and the subnet from the **Subnet1** list.

7. Go to Advanced Setting Give the below in User Data

```
#!/bin/bash
```

```
yum -y install httpd
```

```
systemctl start httpd
```

```
systemctl enable httpd
```

```
echo "This is A Web Server" > /var/www/html/index.html
```

8. Leave the rest of the default settings, and go through the next pages of the wizard until you get to the **Tag Instance** page.

9. On the **Tag Instance** page, you can tag your instance with a `Name` tag; for example `Name=MyWebServer`. This helps you to identify your instance in the Amazon EC2 console after you've launched it. Choose **Next: Configure Security Group** when you are done.

10. On the **Configure Security Group** page, the wizard automatically defines the launch-wizard-x security group to allow you to connect to your instance. Instead, choose the **Select an existing security group** option, select the **WebServerSG** group that you created previously, and then choose **Review and Launch**.

11. On the **Review Instance Launch** page, check the details of your instance, and then choose **Launch**.

12. In the **Select an existing key pair or create a new key pair** dialog box, you can choose an existing key pair, or create a new one. If you create a new key pair, ensure that you download the file and store it in a secure location. You'll need the contents of the private key to connect to your instance after it's launched.

To launch your instance, select the acknowledgment check box, and then choose **Launch Instances**.

13. On the confirmation page, choose **View Instances** to view your instance on the **Instances** page. Select your instance, and view its details in the **Description** tab. The **Private IPs** field displays the private IP address that's assigned to your instance from the range of IP addresses in your subnet.

14. A Linux Server with httpd installed and deploy a index.html

Step 9 : Repeat the Previos step to create the instance in Next Subnet

Step 10: Create Load Balancer

a. From the navigation bar, select a region for your load balancers. Be sure to select the same region that you selected for your EC2 instances. 2. In the navigation pane, under LOAD BALANCING, click Load Balancers. 3. Click Create Load Balancer. 4. In Load Balancer name, enter a name for your load balancer.

The name of your load balancer must be unique within your set of load balancers for the region, can have a maximum of 32 characters, and can contain only alphanumeric characters and hyphens.

b. From Create LB inside, select the same network that you selected for your instances 6. Leave the default listener configuration.

c. Click Next: Assign Security Groups.

d. Assign Security Groups to Your Load Balancer in a VPC

- On the Assign Security Groups page, select Create a new security group.
- Enter a name and description for your security group, or leave the default name and description. This new security group contains a rule that allows traffic to the port that you configured your load balancer to use.

e. Configure Security Settings Click Next

f. Configure Health Checks for Your EC2 Instances

g. On the Configure Health Check page, do the following:

- Leave Ping Protocol set to its default value, HTTP.
- Leave Ping Port set to its default value, 80.

- In the Ping Path field, replace the default value with a single forward slash ("/"). This tells Elastic Load Balancing to send health check queries to the default home page for your web server, such as index.html or default.html.
- Leave the other fields set to their default values.

h. Click Next: Add EC2 Instances.

i. Register EC2 Instances with Your Load Balancer

j. On the Add EC2 Instances page, select the instances to register with your load balancer.

k. Click Next: Add Tags.

l. Tag Your Load Balancer

- On the Add Tags page, specify a key and a value for the tag.
- To add another tag, click Create Tag and specify a key and a value for the tag. ☐ After you are finished adding tags, click Review and Create.

m. Create and Verify Your Load Balancer

n. On the Review page, check your settings. If you need to make changes, click the corresponding link to edit the settings.

o. Click Create to create your load balancer.

p. After you are notified that your load balancer was created, click Close.

q. Select your new load balancer.

r. In the bottom pane, on the Description tab, check the Status row. If it indicates that some of your instances are not in service, it's probably because they are still in the registration process.

Step 11: Validate the Configuration

After you've verified that at least one of your EC2 instances is InService, you can test your load balancer. Copy the string from the DNS Name field and paste it into the address field of an Internet-connected web browser. (For example, my-load-balancer-1234567890.us-

west2.elb.amazonaws.com.) If your] load balancer is working, you see the default page of your HTTP server