

AWS VPC Creation SOP



Table of Contents

1. AWS VPC Creation.....	3
1.1 Description.....	3
1.2 Architecture Diagram	3
1.3 Lab Steps	4
1.4 Troubleshooting.....	17

1. AWS VPC Creation

1.1 Description

The VPC template is the foundation for everything you build on AWS with the Startup Kit. It creates a VPC with the following network resources:

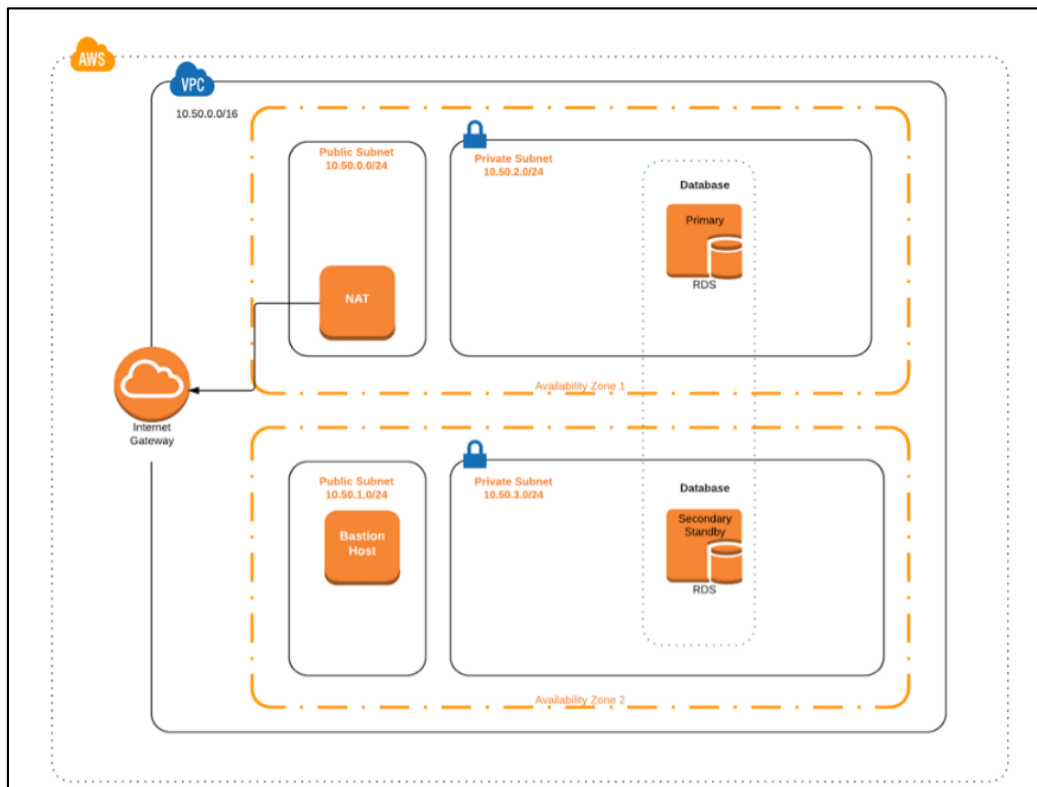
- Two public subnets, which have routes to a public Internet gateway.
- Two private subnets, which do NOT have routes to the public Internet gateway.
- A NAT Gateway to allow instances in private subnets to communicate with the public Internet, for example, to pull down patches and upgrades, and access AWS services that have public endpoints (though some AWS services may be accessed entirely privately).
- Two route tables, one for public subnets and the other for private subnets.
- Security groups for an app, load balancer, database, and bastion host.

The bastion host template creates a bastion host that provides SSH access to resources you place in private subnets for greater security. Resources placed in private subnets could include application instances, database instances, analytics clusters, and other resources you do not want to be discoverable via the public Internet. For example, along with enabling proper authentication and authorization controls, placing database instances in private subnets can help avoid security problems risked by exposing databases to the public Internet.

After you have created your VPC and bastion host, you can optionally create a relational database using the database template. Either a MySQL or PostgreSQL database is created in the Amazon Relational Database Service (Amazon RDS), which automates much of the heavy lifting of database setup and maintenance. Following best practices, the database is created in your VPC's private subnets and is concealed from the public Internet.

1.2 Architecture Diagram

The diagram below displays a visual representation of the underlying application architecture:



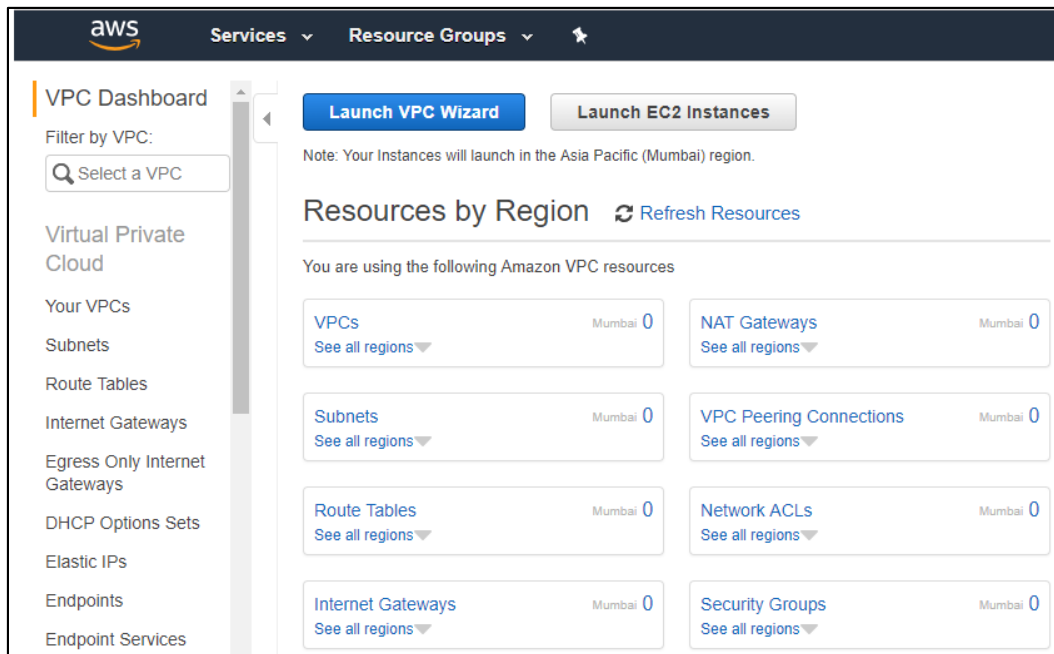
1.3 Lab Steps

Follow the steps outlined below to achieve the objectives of this lab exercise:

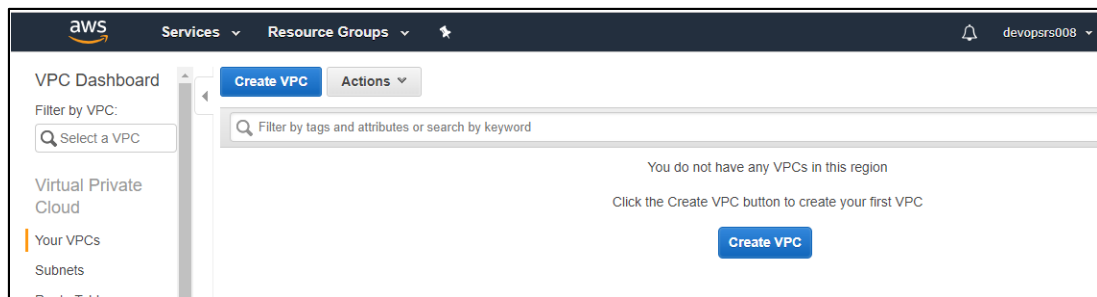
Prerequisites:

- Sign in to the AWS Management Console.
- An Amazon EC2 key pair, if you do not have one.

1. Create a VPC:



a. Click **Your VPCs** menu:



b. Click **Create VPC**.

Create VPC

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You must specify an IPv4 address range for your VPC. Specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally associate an Amazon-provided IPv6 CIDR block with the VPC.

Name tag

IPv4 CIDR block*

IPv6 CIDR block ☒ No IPv6 CIDR Block ☐ Amazon provided IPv6 CIDR block

Tenancy

* Required

Cancel **Create**

c. Mention the tag and IPv4 address, and click **Create** button:

Create VPC

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You must specify an IPv4 address range for your VPC. Specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally associate an Amazon-provided IPv6 CIDR block with the VPC.

Name tag

IPv4 CIDR block*

IPv6 CIDR block ☒ No IPv6 CIDR Block ☐ Amazon provided IPv6 CIDR block

Tenancy

* Required

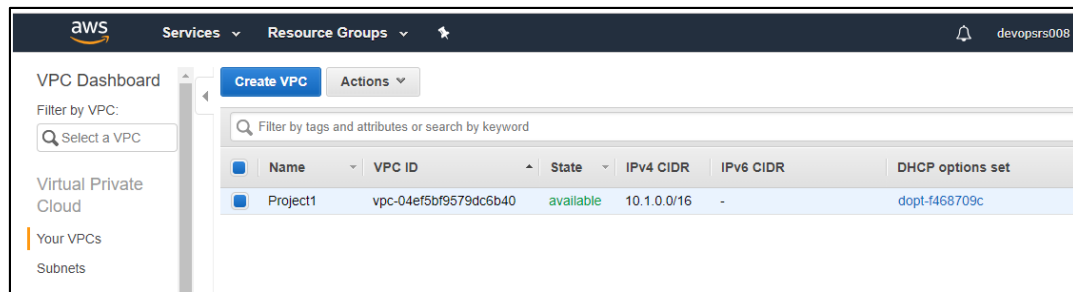
Cancel **Create**

Create VPC

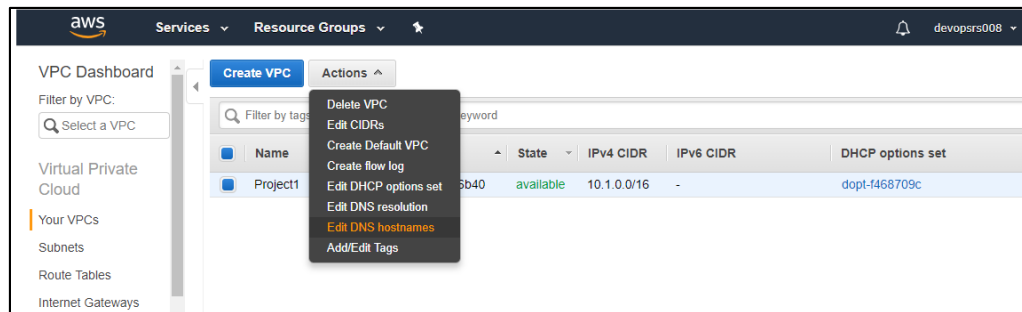
✓ The following VPC was created:

VPC ID [vpc-04ef5bf9579dc6b40](#)

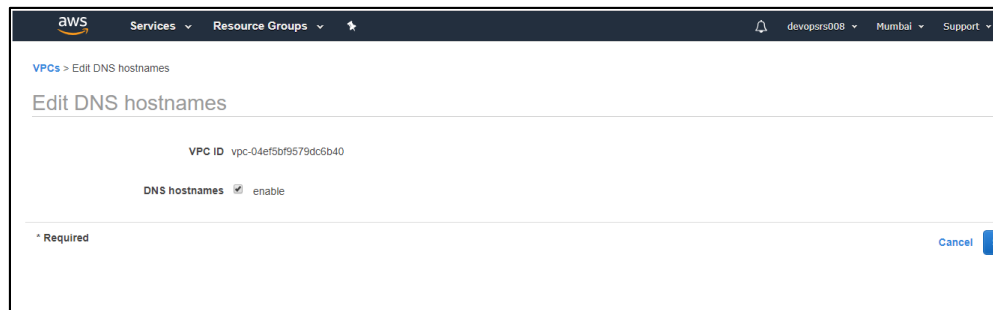
Close



d. Enable the DNS host names:

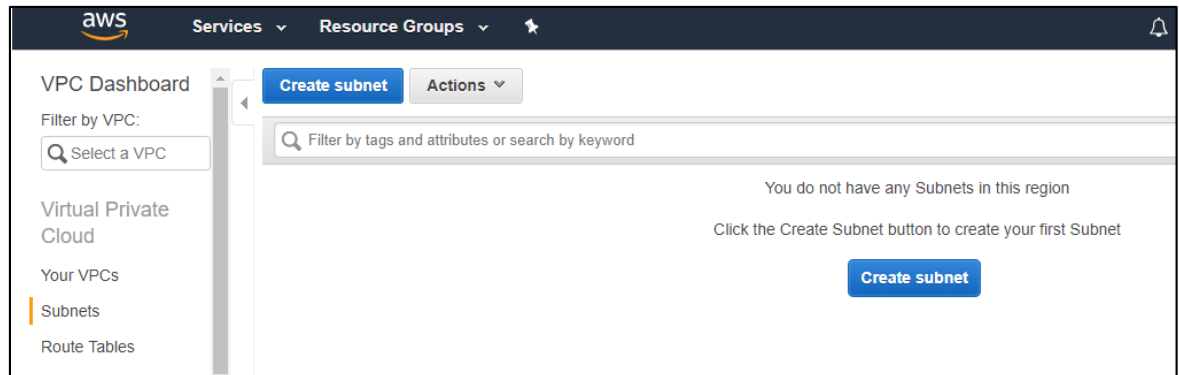


e. Click **Save** button:

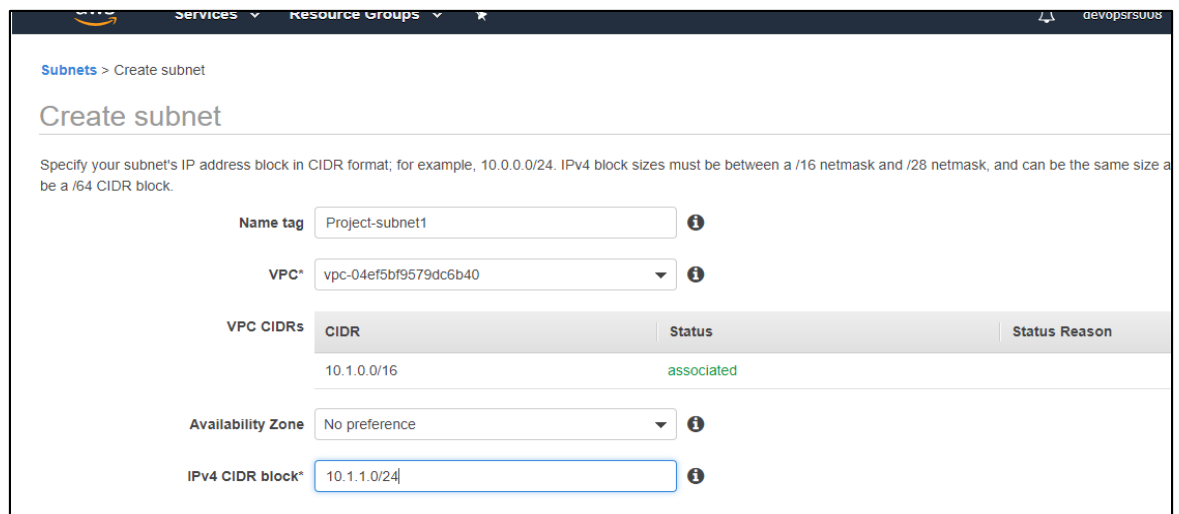


2. Subnet creation:

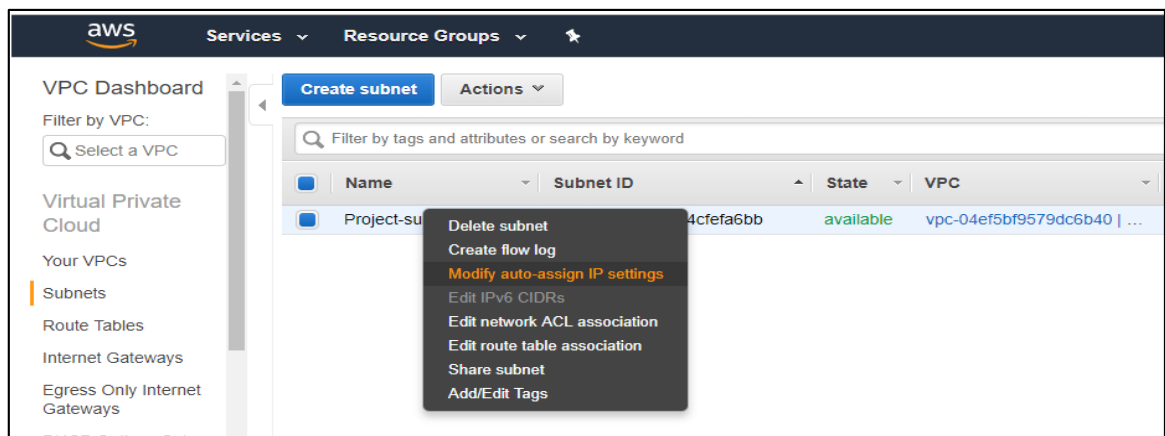
- a. Click the **subnets** menu.

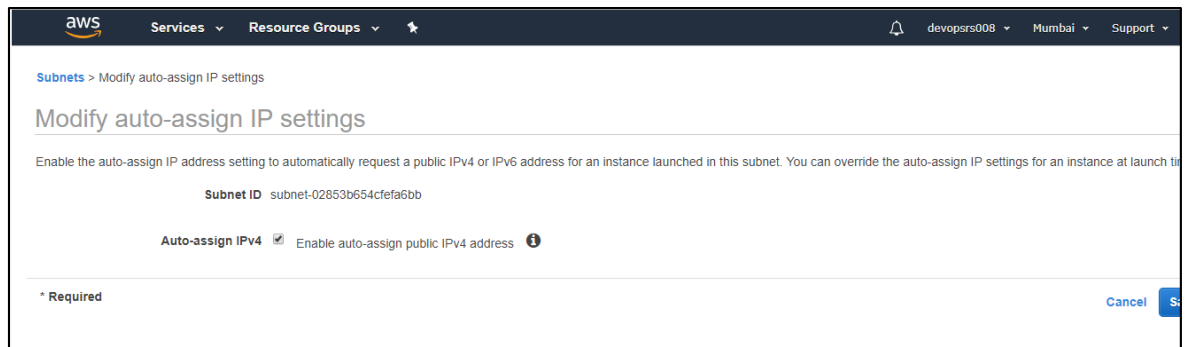


Once you created VPC, you can create subnet which means you have to define your servers within the availability zones.

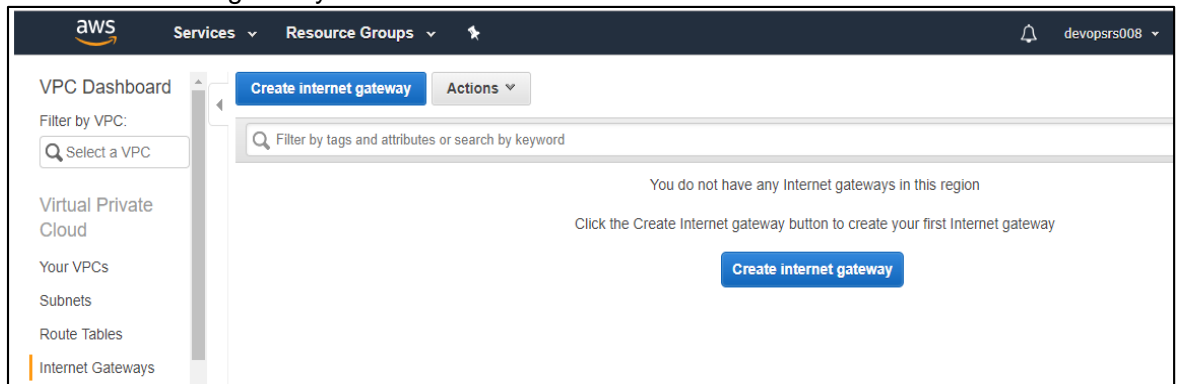


- b. Assign the auto IP address to subnet:

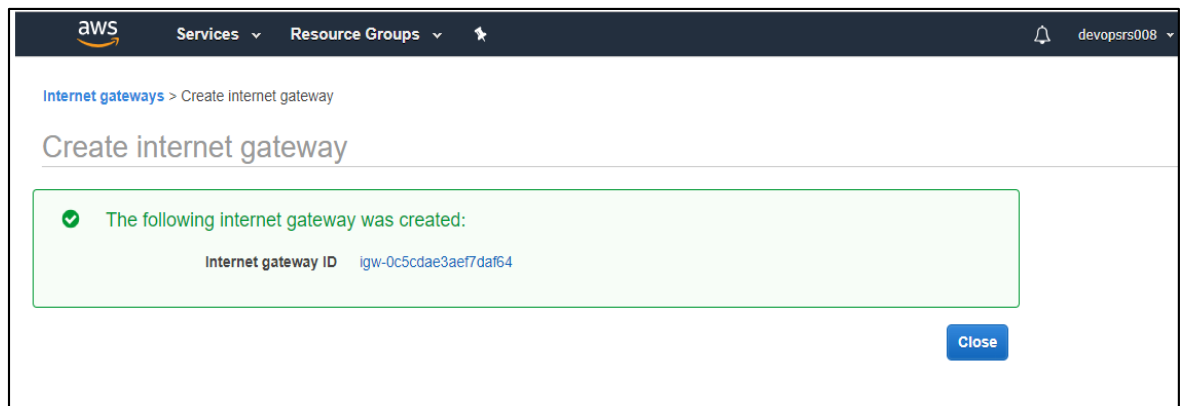




- c. Create an internet gateway to access the server from outside:



- d. Click the **internet gateway** button and provide the name:



- e. Once the Internet gateway is created, attach it in VPC.

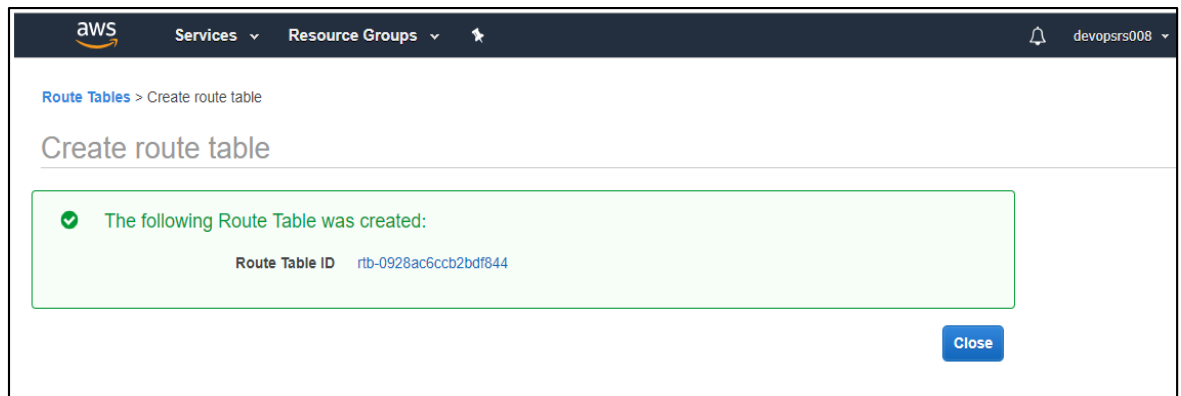
The screenshot shows the AWS VPC console. In the top navigation bar, 'Services' and 'Resource Groups' are visible. The left sidebar shows the 'VPC Dashboard' with options like 'Virtual Private Cloud', 'Your VPCs', 'Subnets', and 'Route Tables'. The main content area displays a table of Internet gateways. A dropdown menu is open for the selected gateway, showing options: 'Delete internet gateway', 'Attach to VPC', 'Detach from VPC', and 'Add/Edit Tags'. Below this, the 'Attach to VPC' page is shown, with a 'VPC*' dropdown menu open, displaying a list of VPCs with columns 'VPC ID' and 'Name'. The 'Attach' button is visible at the bottom right.

3. Route Table creation:

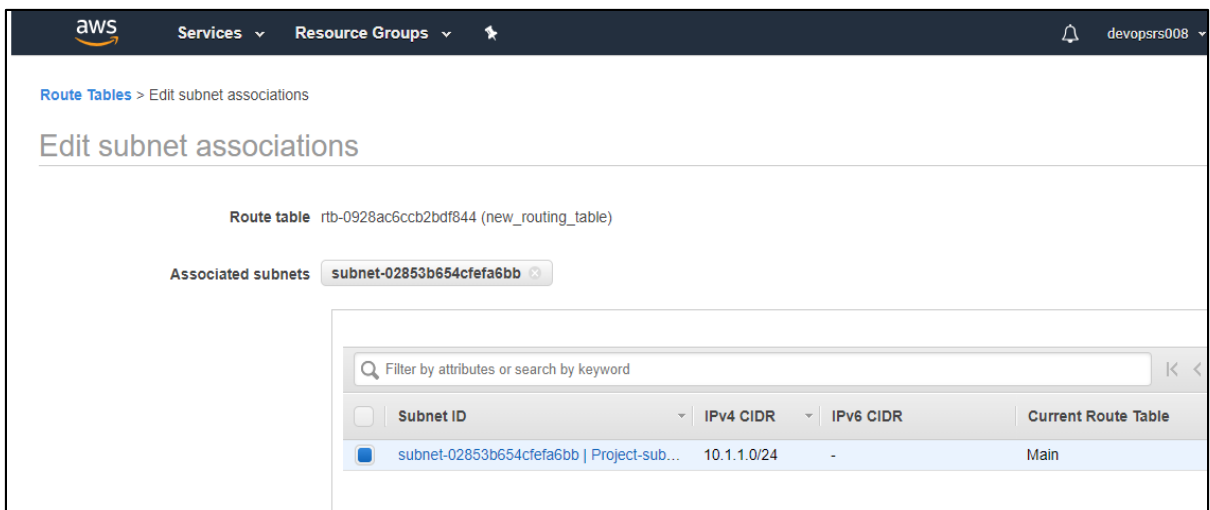
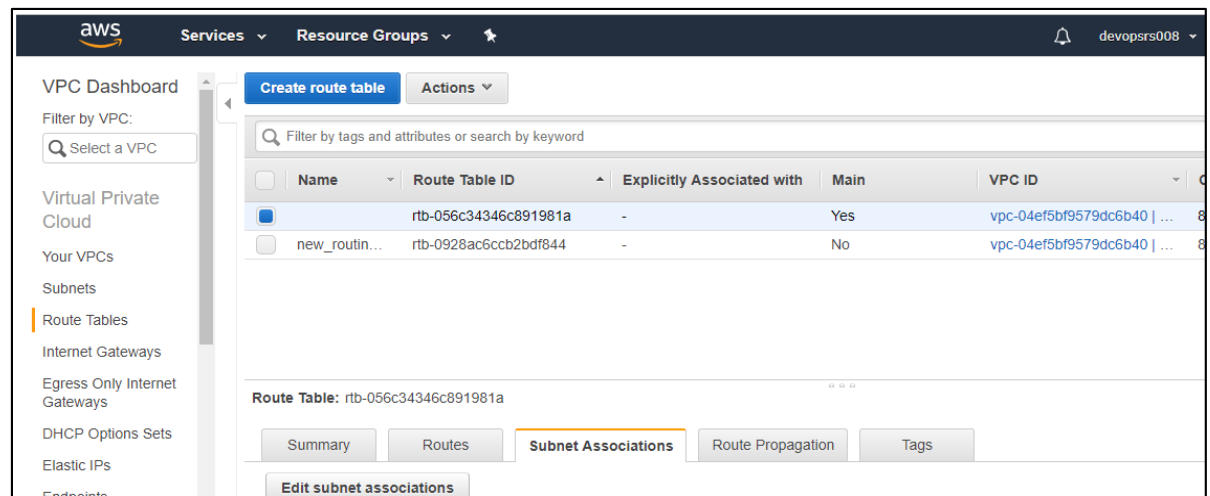
The screenshot shows the AWS VPC console. The left sidebar shows the 'VPC Dashboard' with options like 'Virtual Private Cloud', 'Your VPCs', 'Subnets', and 'Route Tables'. The main content area displays a table of Route Tables. The 'Create route table' button is visible at the top. Below the table, the 'Create route table' page is shown, with a 'Name tag' input field and a 'VPC*' dropdown menu. The 'Create' button is visible at the bottom right.

- a. Click the **Create route table** button:

The screenshot shows the AWS VPC console. The left sidebar shows the 'VPC Dashboard' with options like 'Virtual Private Cloud', 'Your VPCs', 'Subnets', and 'Route Tables'. The main content area displays the 'Create route table' page. The 'Name tag' input field is filled with 'new_routing_table'. The 'VPC*' dropdown menu is open, showing a list of VPCs with columns 'VPC ID' and 'Name'. The 'Create' button is visible at the bottom right.



4. Subnet association:
 - a. Select the routing table and select the subnet associations tab.



b. Check the routes tab:

The screenshot shows the AWS VPC Dashboard. On the left, the 'Route Tables' link is selected in the navigation menu. The main area displays a list of route tables. The table has columns: Name, Route Table ID, Explicitly Associated with, Main, and VPC ID. One route table is selected, and the 'Routes' tab is active. Below the tabs, there is a table with columns: Destination, Target, Status, and Propagated. The table shows a single route with Destination '10.1.0.0/16', Target 'local', Status 'active', and Propagated 'No'.

Name	Route Table ID	Explicitly Associated with	Main	VPC ID
new_routin...	rtb-0928ac6ccb2bdf844	subnet-02853b654cfe6a6bb	No	vpc-04ef5bf9579dc6b40 ...

Destination	Target	Status	Propagated
10.1.0.0/16	local	active	No

We have to redirect the traffic to different routing procedure: Within subnets we will use local routing table. For instance, if we want to browse something in the VM then it should not go and hit the local routing table so we are creating a new routing to hit the internet gateway.

c. Click the edit routes button:

The screenshot shows the 'Edit routes' page in the AWS VPC Dashboard. The page has a header 'Route Tables > Edit routes' and a title 'Edit routes'. Below the title, there is a table with columns: Destination, Target, Status, and Propagated. The table shows a single route with Destination '10.1.0.0/16', Target 'local', Status 'active', and Propagated 'No'. Below the table, there is an 'Add route' button. At the bottom, there is a '* Required' label and a 'Save routes' button.

Destination	Target	Status	Propagated
10.1.0.0/16	local	active	No

* Required

Cancel Save routes

Route Tables > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.1.0.0/16	local	active	No
0.0.0.0/0	igw-	No	No

Add route

* Required

Cancel Save routes

Route Tables > Edit routes

Edit routes

✓ Routes successfully edited

Close

New routing is created and find the below screen.

VPC Dashboard

Filter by VPC: Select a VPC

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

Create route table Actions

Filter by tags and attributes or search by keyword

Name	Route Table ID	Explicitly Associated with	Main	VPC ID	Owner
	rtb-056c34346c891981a	-	Yes	vpc-04ef5bf9579dc6b40 ...	825676162749
new_routin...	rtb-0928ac6ccb2bdf844	subnet-02853b654cfefa6bb	No	vpc-04ef5bf9579dc6b40 ...	825676162749

Route Table: rtb-0928ac6ccb2bdf844

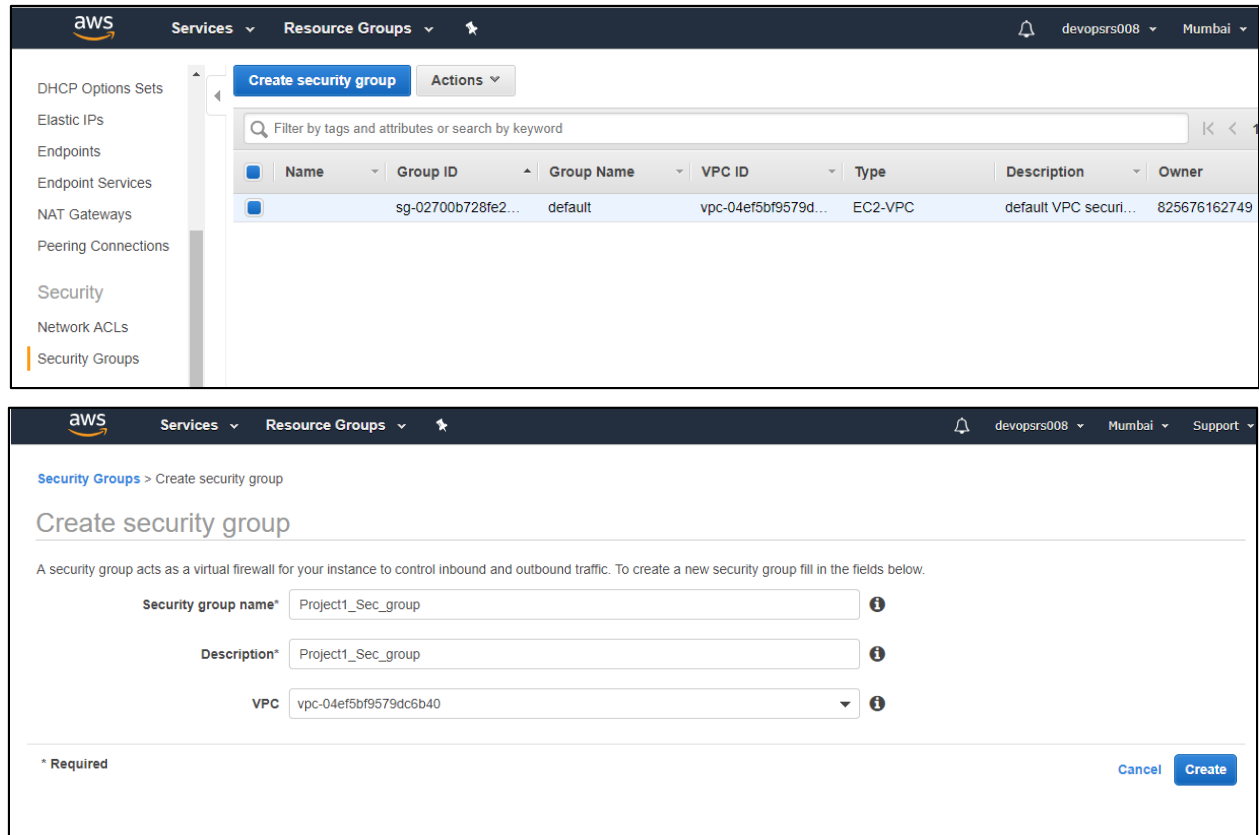
Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.1.0.0/16	local	active	No
0.0.0.0/0	igw-0c5cdae3aef7daf64	active	No

5. Create a security group:



The screenshot shows the AWS Management Console interface for creating a security group. The left sidebar lists various services, with 'Security Groups' highlighted. The main content area shows a table of existing security groups and a form to create a new one.

Name	Group ID	Group Name	VPC ID	Type	Description	Owner
sg-02700b728fe2...	default	vpc-04ef5bf9579d...	EC2-VPC	default VPC securi...	825676162749	

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 fill in the fields below.

Security group name*

Description*

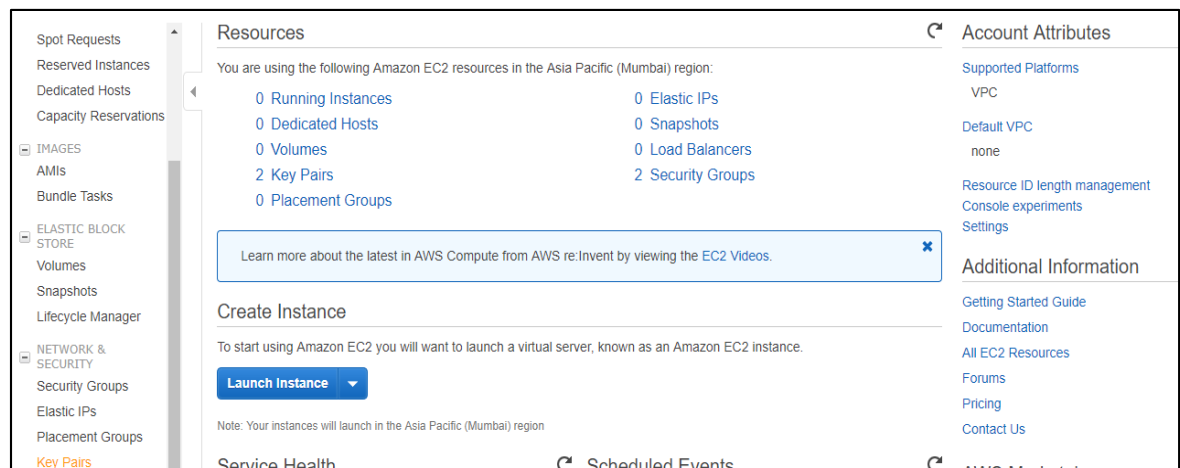
VPC

* Required

[Cancel](#) [Create](#)

6. Create key-pairs:

a. Select the key Pairs under Network security group.



The screenshot shows the AWS Management Console interface for the 'Resources' page. The left sidebar lists various services, with 'Key Pairs' highlighted. The main content area shows a list of resources and a 'Create Instance' button.

Resources

You are using the following Amazon EC2 resources in the Asia Pacific (Mumbai) region:

0 Running Instances	0 Elastic IPs
0 Dedicated Hosts	0 Snapshots
0 Volumes	0 Load Balancers
2 Key Pairs	2 Security Groups
0 Placement Groups	

[Learn more about the latest in AWS Compute from AWS re:Invent by viewing the EC2 Videos.](#)

Create Instance

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

[Launch Instance](#)

Note: Your instances will launch in the Asia Pacific (Mumbai) region

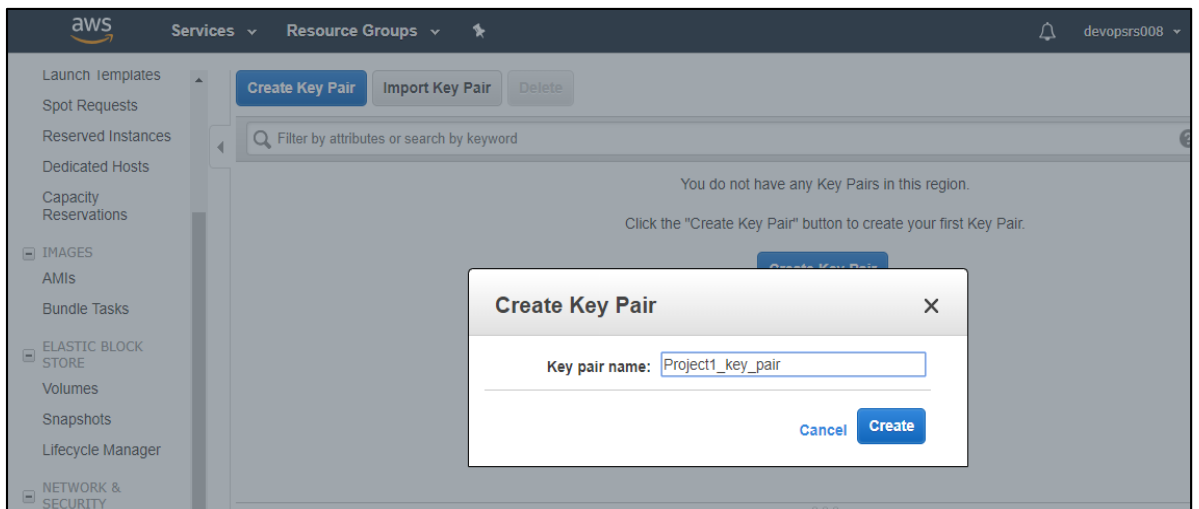
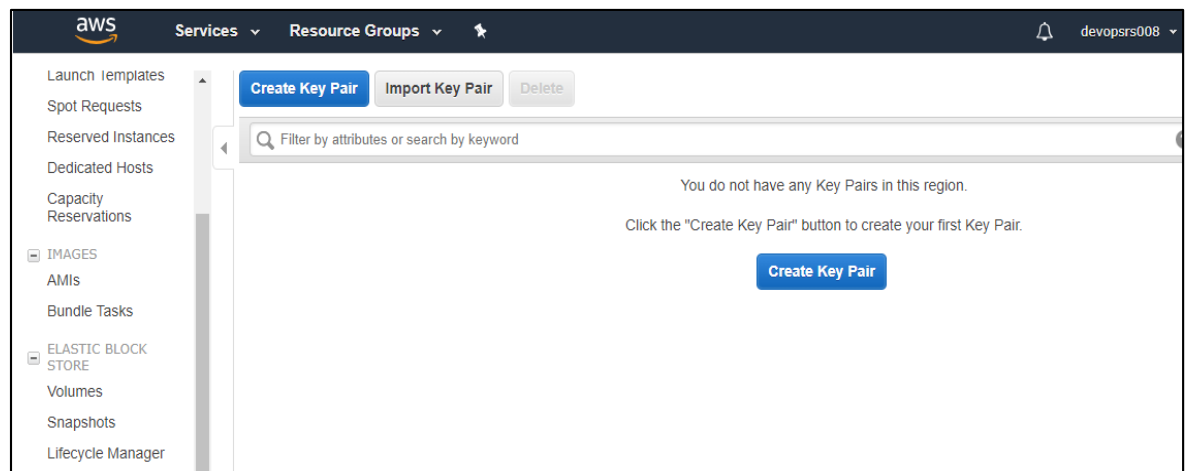
Service Health [Scheduled Events](#)

Account Attributes

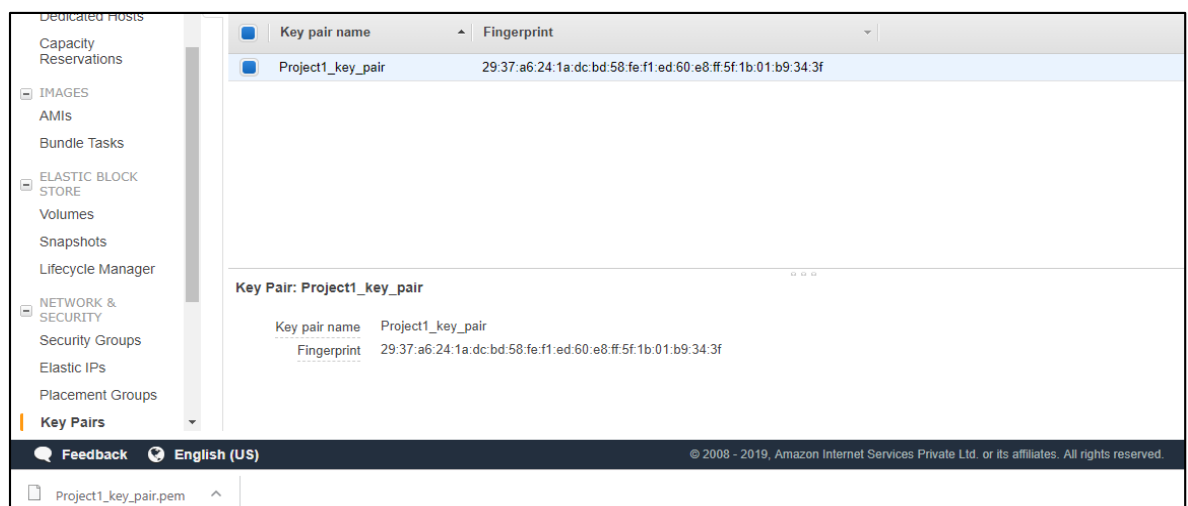
- Supported Platforms
 - VPC
- Default VPC
 - none
- Resource ID length management
 - Console experiments
 - Settings

Additional Information

- Getting Started Guide
- Documentation
- All EC2 Resources
- Forums
- Pricing
- Contact Us



Note: PEM file will be downloaded in our download directory:



- Public and private key would be created.
- Private key comes to us.

7. Create a new VM:

a. Select the VPC and subnet from the dropdown.

aws Services Resource Groups devopsrs008

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

Monitoring (i) ☐ Enable CloudWatch detailed monitoring
Additional charges apply.

Tenancy (i) Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.

T2/T3 Unlimited (i) ☐ Enable
Additional charges may apply

▼ **Network interfaces** (i)

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses
eth0	New network interface ▼	subnet-02853b66 ▼	10.1.1.100	Add IP

Add Device

b. Select the Tag if you want:

aws Services Resource Groups devopsrs008 Mumbai

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key	Value	Instances	Volume
name	Project1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ENV	Prod	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add another tag (Up to 50 tags maximum)

- c. Select the newly created security group from the dropdown:

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 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.

Assign a security group: ☐ Create a new security group
☒ Select an existing security group

Security Group ID	Name	Description
sg-02700b728fe24898a	default	default VPC security group
sg-0f4fde94b5489f029	Project1_Sec_group	Project1_Sec_group

- d. Select the security as mentioned in the below screenshot and click the review and launch.

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 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.

Assign a security group: ☐ Create a new security group
☒ Select an existing security group

Security Group ID	Name	Description
sg-02700b728fe24898a	default	default VPC security group
sg-0f4fde94b5489f029	Project1_Sec_group	Project1_Sec_group

- e. Select the recently created key pair as mentioned in the below screenshot:

Step 7: Review Instance Launch

Please review your instance launch details. You can launch your instance now or save the configuration for later.

AMI Details

Amazon Linux 2 AMI (HVM), S...

Free tier eligible

Amazon Linux 2 comes with five years of software packages through extras.

Root Device Type: ebs Virtualization type: x86_64

Instance Type

Instance Type	ECUs
t2.micro	Variable

Security Groups

Security Group ID

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair

Select a key pair

Project1_key_pair

☒ I acknowledge that I have access to the selected private key file (Project1_key_pair.pem), and that without this file, I won't be able to log into my instance.

Cancel Launch Instances

1.4 Troubleshooting

S. No	Problem	Solution
1	VPC is not working as expected.	Use the following command to check the VPC status. <pre>show vpc</pre>
2	The VPC peer ports or membership ports do not have identical configurations.	Use the following command to determine where the configuration mismatch occurs. <pre>show vpc consistency-parameters interface</pre>