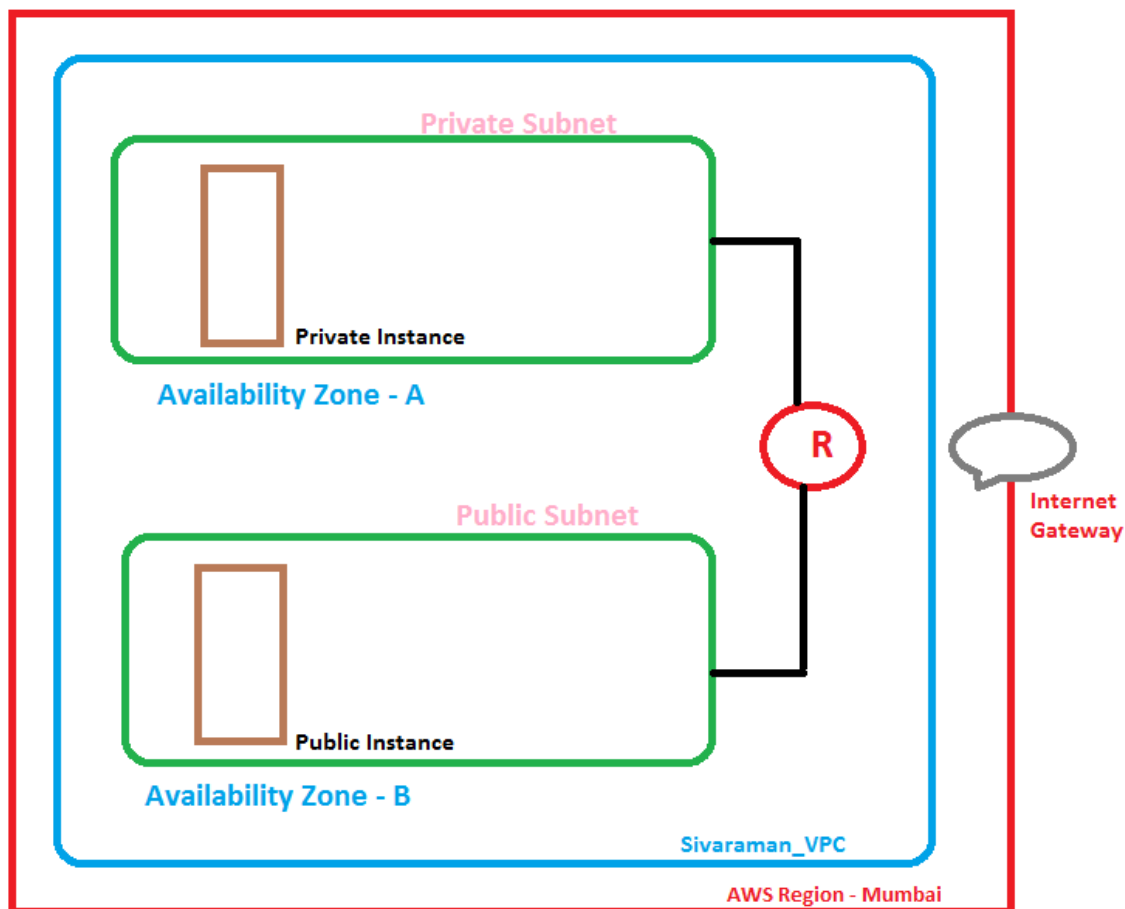


Lab: Need to access public network from Public subnet and access Public subnet from Public network.

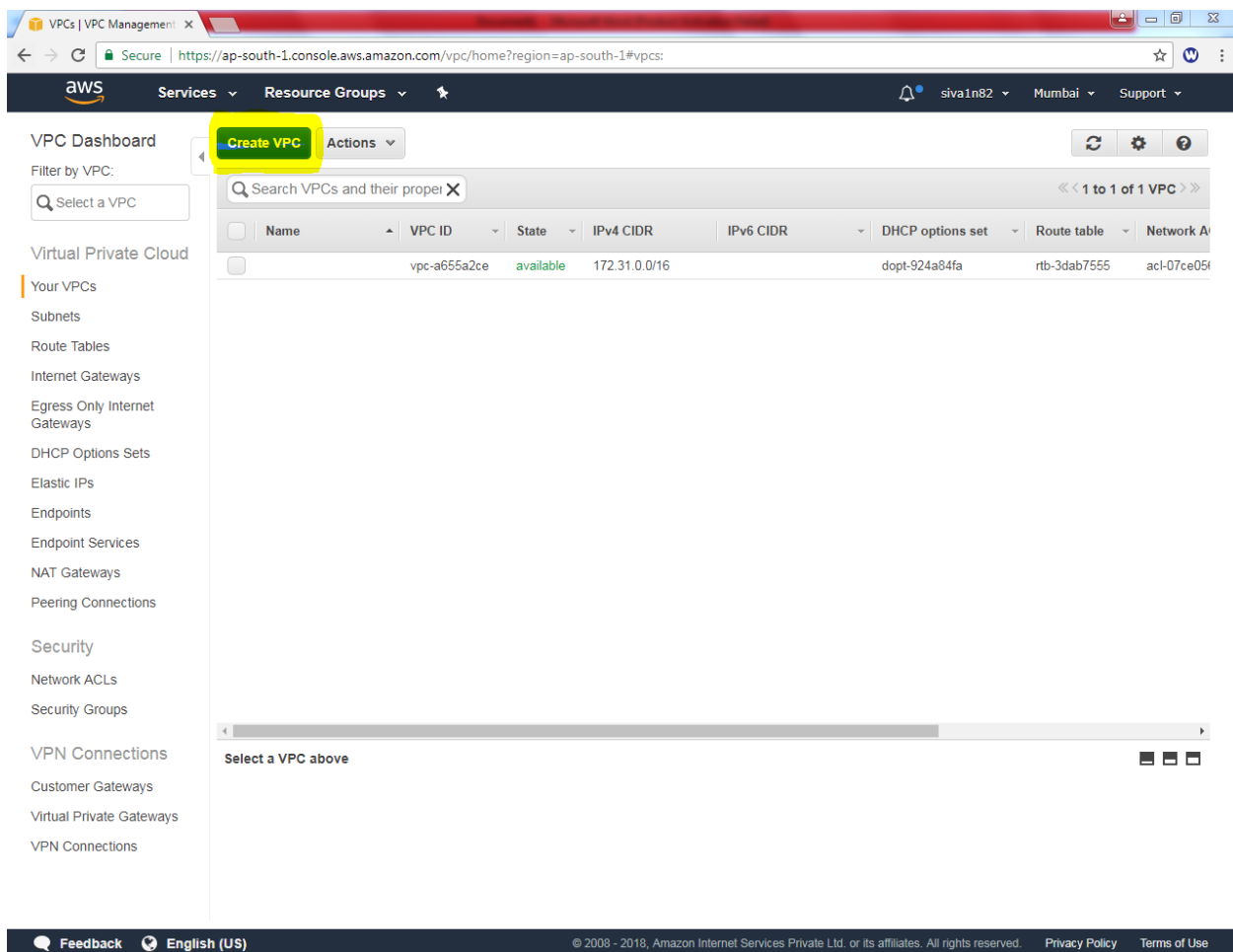
Scenario:



In Mumbai Region, We have required to create a VPC as “Sivaraman VPC”. In Sivaraman VPC, we need to create two subnets i.e. Private Subnet and Public Subnet. In public subnet we need to create an instance and private subnet also we need to create an instance. By default both availability zone will be communicate by using a router. Now we need to design VPC, Subnet and Subnet routing table and instances for the above scenario.

Please login to the aws console, <https://aws.amazon.com> by using your login credentials.

- While logged on to the AWS portal, please go to **Networking & Content Delivery**
Then select **“VPC”**



The screenshot shows the AWS VPC Management console. The 'Create VPC' button is highlighted with a yellow box. The console displays a table of existing VPCs. Below the table, there is a section for selecting a VPC.

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set	Route table	Network A
	vpc-a655a2ce	available	172.31.0.0/16		dopt-924a84fa	rtb-3dab7555	acl-07ce05f

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* ⓘ

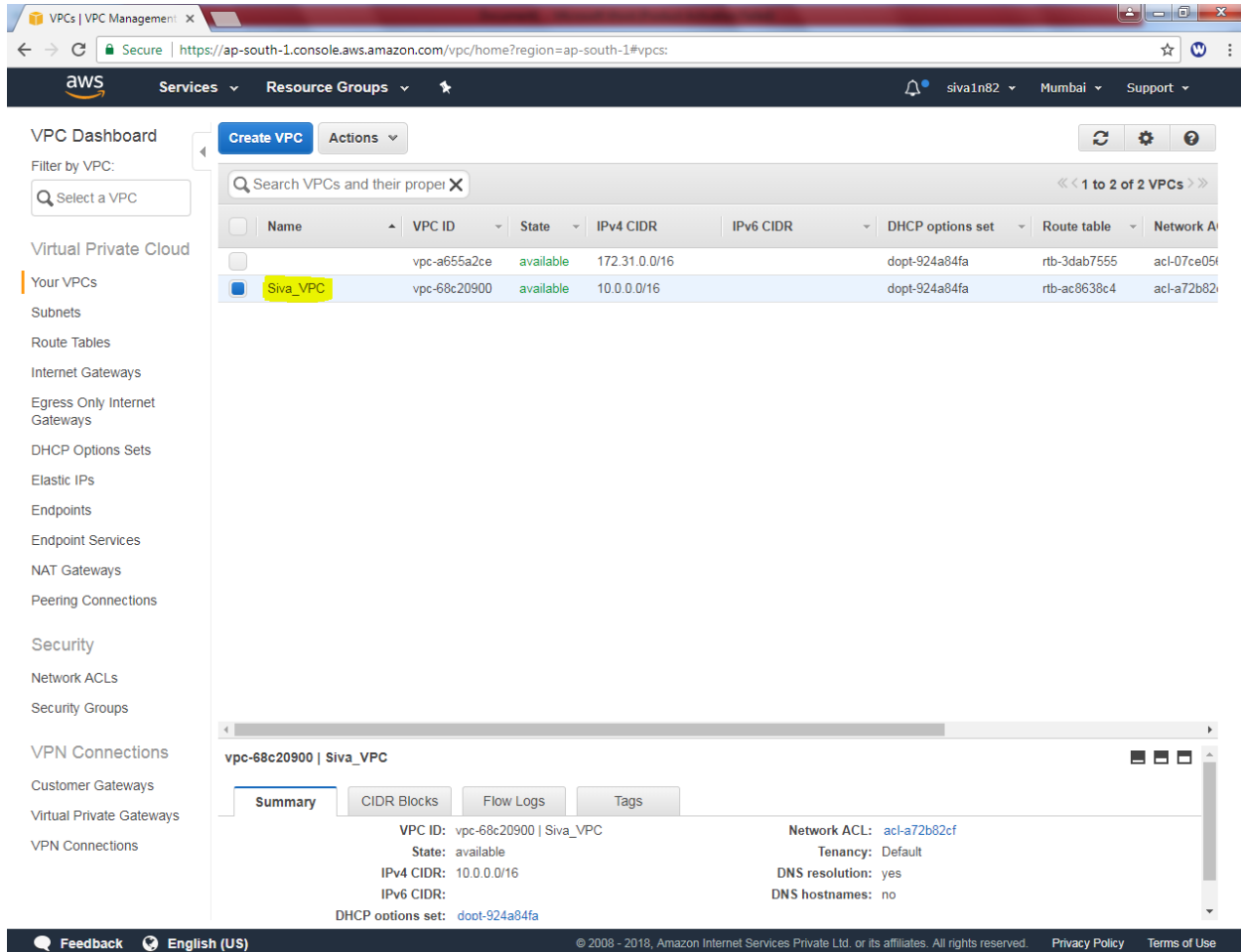
IPv6 CIDR block* ☒ No IPv6 CIDR Block ⓘ ☐ Amazon provided IPv6 CIDR block

Tenancy ⓘ

[Cancel](#) [Yes, Create](#)

While creating VPC, in Name Tag “Siva_VPC” and IPV4 CIDR block “10.0.0.0/16”. Then click “Yes create” button.

Now you can able to view the Siva VPC in VPC option.



The screenshot shows the AWS Management Console VPC Dashboard. The left sidebar contains navigation links for VPCs, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, Endpoint Services, NAT Gateways, Peering Connections, Security, Network ACLs, Security Groups, VPN Connections, Customer Gateways, Virtual Private Gateways, and VPN Connections. The main content area displays a table of VPCs. The 'Siva_VPC' is highlighted in yellow. Below the table, the details for 'vpc-68c20900 | Siva_VPC' are shown, including the Summary tab with VPC ID, State, IPv4 CIDR, IPv6 CIDR, DHCP options set, Network ACL, Tenancy, DNS resolution, and DNS hostnames.

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set	Route table	Network ACL
vpc-a655a2ce	vpc-a655a2ce	available	172.31.0.0/16		dopt-924a84fa	rtb-3dab7555	acl-07ce05f
Siva_VPC	vpc-68c20900	available	10.0.0.0/16		dopt-924a84fa	rtb-ac8638c4	acl-a72b82cf

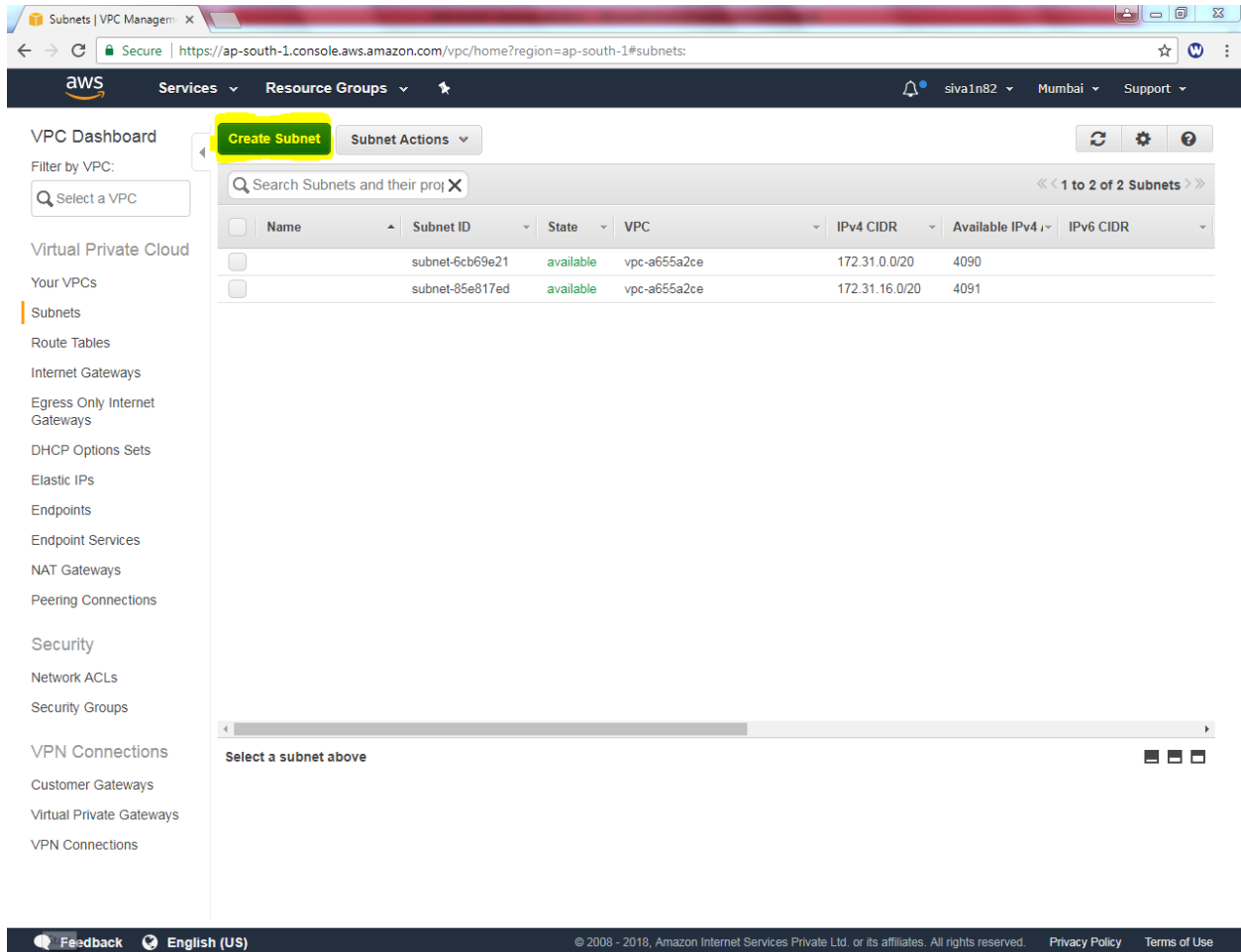
vpc-68c20900 | Siva_VPC

Summary | CIDR Blocks | Flow Logs | Tags

VPC ID: vpc-68c20900 | Siva_VPC
 State: available
 IPv4 CIDR: 10.0.0.0/16
 IPv6 CIDR:
 DHCP options set: dopt-924a84fa
 Network ACL: acl-a72b82cf
 Tenancy: Default
 DNS resolution: yes
 DNS hostnames: no

Then we need to create subnet for VPC, i.e. Public Subnet and Private Subnet.

In Under VPC dashboard, “Subnets” option is there



The screenshot shows the AWS VPC Subnets dashboard. The 'Create Subnet' button is highlighted in yellow. The dashboard displays a table of subnets with the following data:

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR
	subnet-6cb69e21	available	vpc-a655a2ce	172.31.0.0/20	4090	
	subnet-85e817ed	available	vpc-a655a2ce	172.31.16.0/20	4091	

Select “Create Subnet”

In Name Tag **"Siva_Public_Network"** , VPC Select **"Siva_VPC"**, Availability Zone select **"1B"** and IPV4 CIDR BLOCK **10.0.2.0/24**.

Create Subnet

Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag

VPC

VPC CIDRs	CIDR	Status	Status Reason
	10.0.0.0/16	associated	

Availability Zone

IPv4 CIDR block

[Cancel](#) [Yes, Create](#)

Then click **"Yes, Create"**.

In Name Tag **"Siva_Private_Network"** , VPC Select **"Siva_VPC"**, Availability Zone select **"1A"** and IPV4 CIDR BLOCK **10.0.1.0/24**.

Create Subnet ✕

Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag

VPC

VPC CIDRs	CIDR	Status	Status Reason
	10.0.0.0/16	associated	

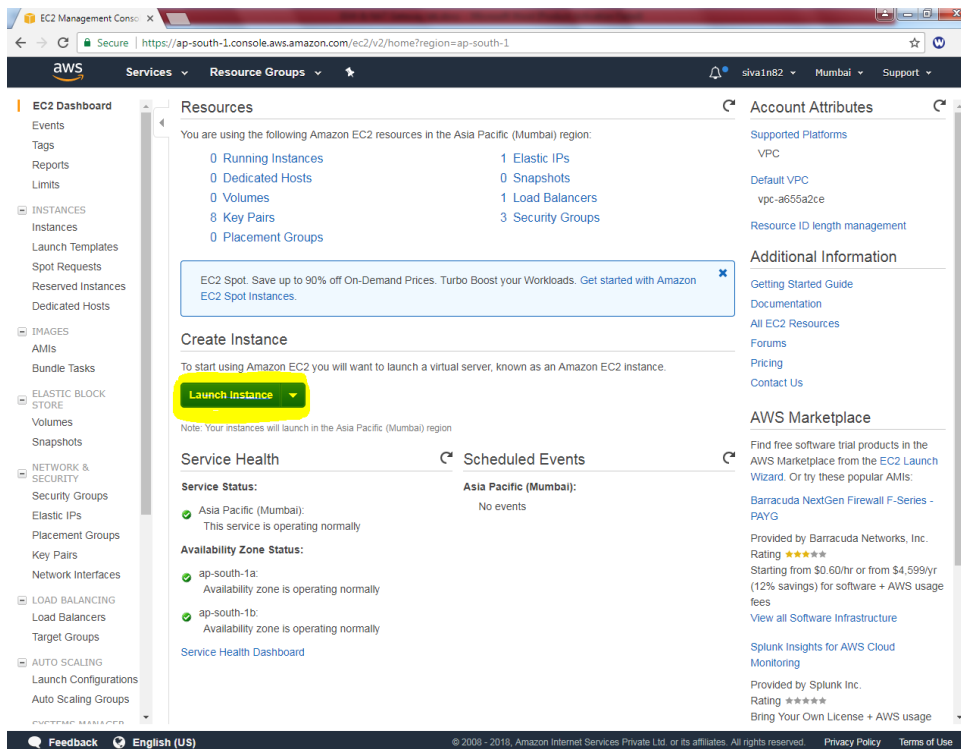
Availability Zone

IPv4 CIDR block

Cancel
Yes, Create

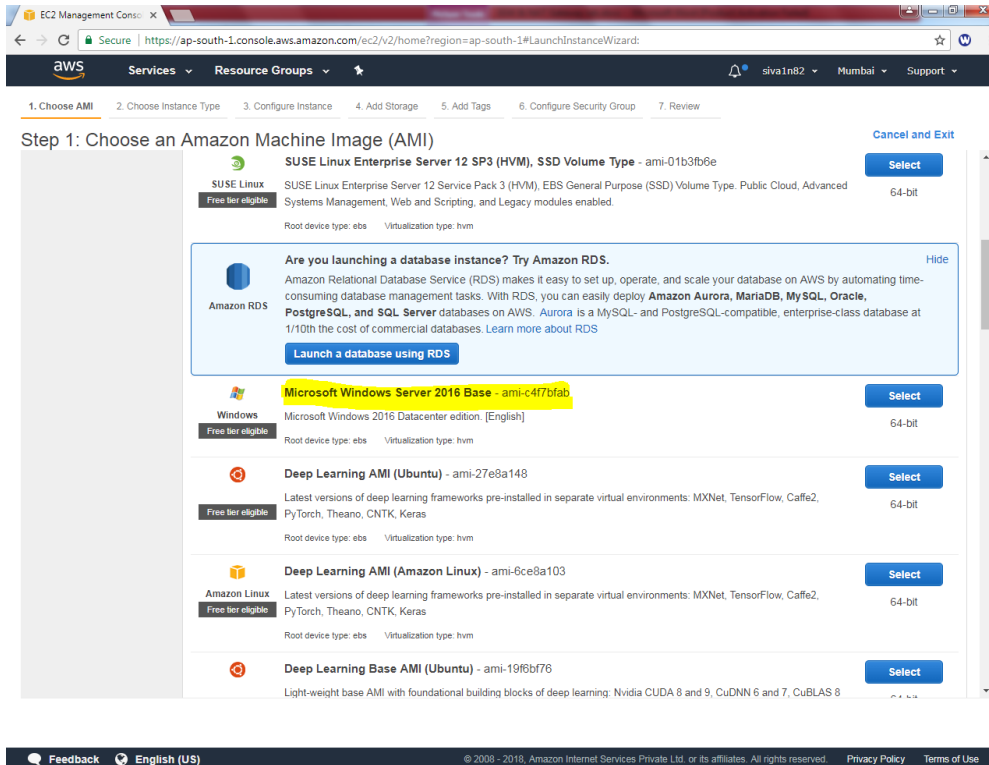
Then click **“Yes, Create”**.

Now we need to create an instance, on public network. Click **Launch Instance**



The screenshot shows the AWS Management Console interface. On the left is a navigation menu with categories like EC2 Dashboard, INSTANCES, IMAGES, ELASTIC BLOCK STORE, NETWORK & SECURITY, LOAD BALANCING, and AUTO SCALING. The main content area is titled 'Resources' and lists various EC2 resources. Below this, the 'Create Instance' section is visible, where the 'Launch Instance' button is highlighted with a yellow box. To the right of the main content, there are sections for 'Account Attributes' and 'AWS Marketplace'.

Select “AMI”



EC2 Management Console: X

Secure | <https://ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard>

Services Resource Groups

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

Step 1: Choose an Amazon Machine Image (AMI) Cancel and Exit

SUSE Linux
Free tier eligible
SUSE Linux Enterprise Server 12 SP3 (HVM), SSD Volume Type - ami-01b3fb6e
SUSE Linux Enterprise Server 12 Service Pack 3 (HVM), EBS General Purpose (SSD) Volume Type, Public Cloud, Advanced Systems Management, Web and Scripting, and Legacy modules enabled.
Root device type: ebs Virtualization type: hvm
64-bit
Select

Amazon RDS
Are you launching a database instance? Try Amazon RDS.
Amazon Relational Database Service (RDS) makes it easy to set up, operate, and scale your database on AWS by automating time-consuming database management tasks. With RDS, you can easily deploy **Amazon Aurora**, **MariaDB**, **MySQL**, **Oracle**, **PostgreSQL**, and **SQL Server** databases on AWS. **Aurora** is a MySQL- and PostgreSQL-compatible, enterprise-class database at 1/10th the cost of commercial databases. [Learn more about RDS](#)
Launch a database using RDS

Windows
Free tier eligible
Microsoft Windows Server 2016 Base - ami-c4f7bfab
Microsoft Windows 2016 Datacenter edition, [English]
Root device type: ebs Virtualization type: hvm
64-bit
Select

Deep Learning AMI (Ubuntu) - ami-27e8a148
Free tier eligible
Latest versions of deep learning frameworks pre-installed in separate virtual environments: MXNet, TensorFlow, Caffe2, PyTorch, Theano, CNTK, Keras
Root device type: ebs Virtualization type: hvm
64-bit
Select

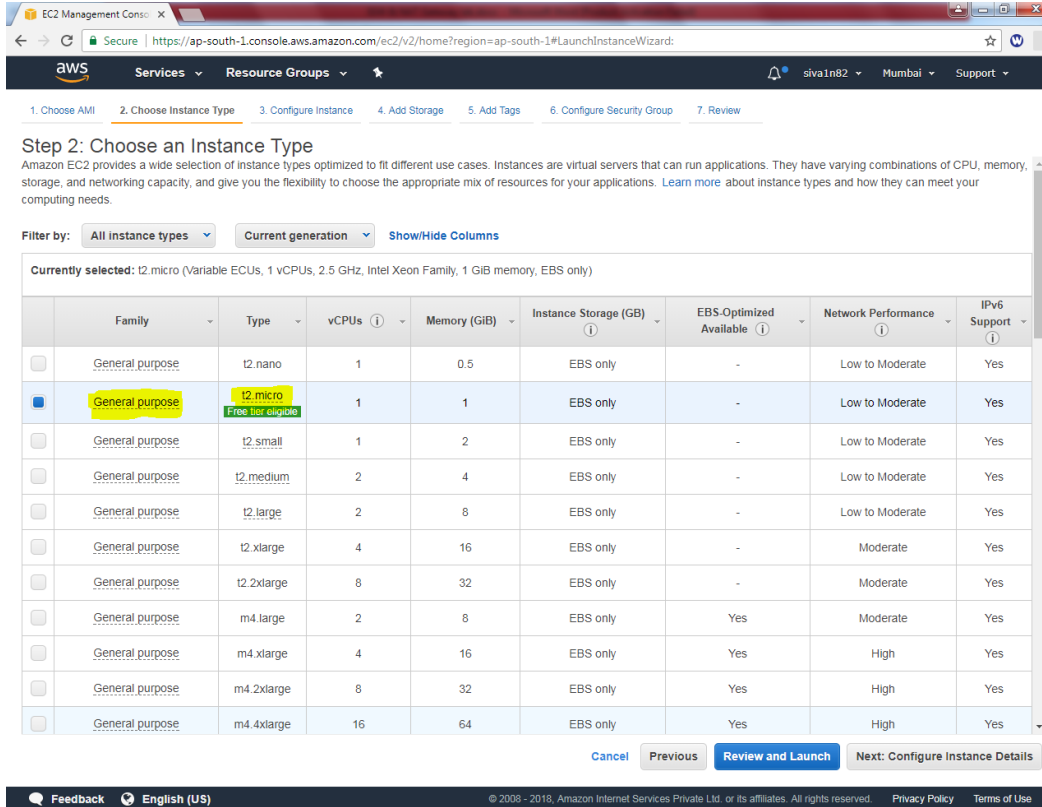
Deep Learning AMI (Amazon Linux) - ami-6ce8a103
Free tier eligible
Latest versions of deep learning frameworks pre-installed in separate virtual environments: MXNet, TensorFlow, Caffe2, PyTorch, Theano, CNTK, Keras
Root device type: ebs Virtualization type: hvm
64-bit
Select

Deep Learning Base AMI (Ubuntu) - ami-19f8bf76
Light-weight base AMI with foundational building blocks of deep learning: Nvidia CUDA 8 and 9, CuDNN 6 and 7, CuBLAS 8
Select

Feedback English (US)

© 2008 - 2016, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Select “General Purpose – t2 micro” then click “Next”



EC2 Management Console

Secure | <https://ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard>

Services Resource Groups

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

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance types Current generation Show/Hide Columns

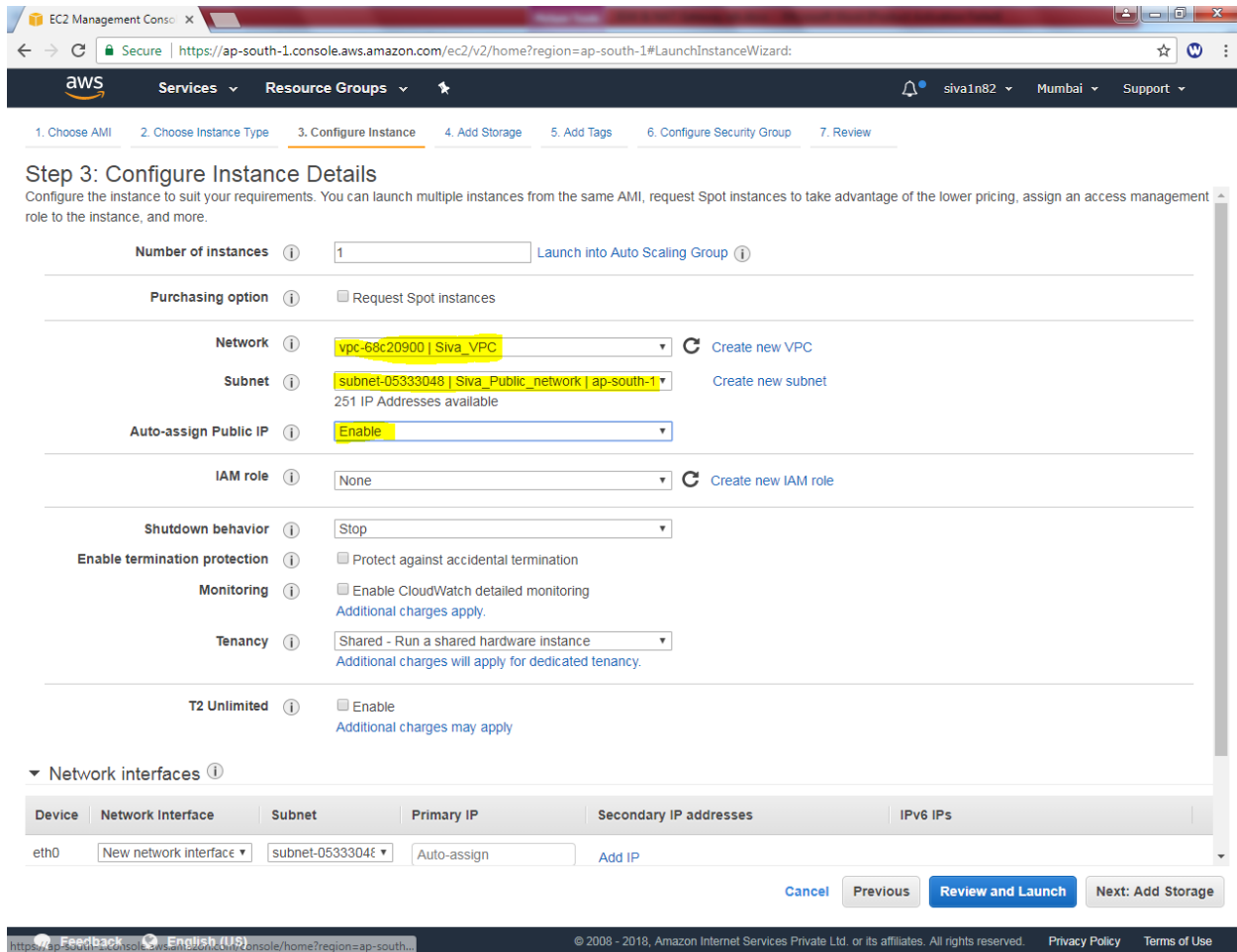
Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	m4.large	2	8	EBS only	Yes	Moderate	Yes
<input type="checkbox"/>	General purpose	m4.xlarge	4	16	EBS only	Yes	High	Yes
<input type="checkbox"/>	General purpose	m4.2xlarge	8	32	EBS only	Yes	High	Yes
<input type="checkbox"/>	General purpose	m4.4xlarge	16	64	EBS only	Yes	High	Yes

Cancel Previous **Review and Launch** Next: Configure Instance Details

Feedback English (US) © 2009 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

In Network, select **“Siva_VPC”**, in subnet select **“Siva_Public_network”** and in Auto assign Public IP **“Enable”**.



EC2 Management Console

Secure | <https://ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard>

Services | Resource Groups | siva1n82 | Mumbai | Support

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

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances ⓘ 1 [Launch into Auto Scaling Group](#) ⓘ

Purchasing option ⓘ ☐ Request Spot instances

Network ⓘ vpc-68c20900 | Siva_VPC [Create new VPC](#)

Subnet ⓘ subnet-05333048 | Siva_Public_network | ap-south-1 [Create new subnet](#)
251 IP Addresses available

Auto-assign Public IP ⓘ Enable

IAM role ⓘ None [Create new IAM role](#)

Shutdown behavior ⓘ Stop

Enable termination protection ⓘ ☐ Protect against accidental termination

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

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

T2 Unlimited ⓘ ☐ Enable
[Additional charges may apply](#)

▼ **Network interfaces** ⓘ

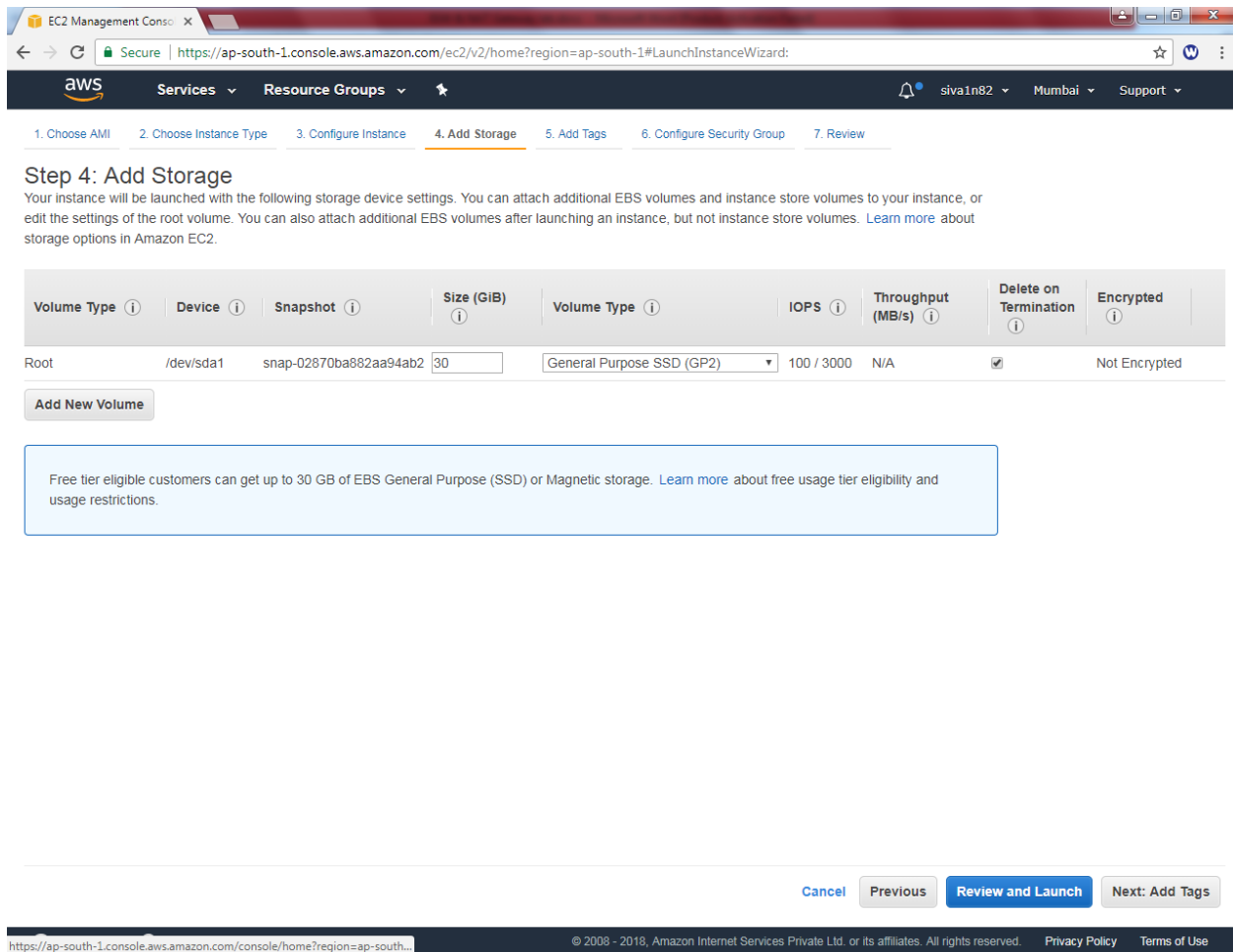
Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface ▼	subnet-05333048 ▼	Auto-assign	Add IP	

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

[Feedback](#) [English \(US\)](#) | © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

Then click **“Next”**

Leave this setting by default.



The screenshot shows the AWS Management Console interface for the 'Step 4: Add Storage' wizard. The breadcrumb trail at the top indicates the steps: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage (current step), 5. Add Tags, 6. Configure Security Group, and 7. Review. The main heading is 'Step 4: Add Storage'. Below it, a paragraph explains that the instance will be launched with the following storage device settings and that additional EBS volumes can be attached after launching. A table lists the storage settings for the root volume. The table has columns for Volume Type, Device, Snapshot, Size (GiB), Volume Type, IOPS, Throughput (MB/s), Delete on Termination, and Encrypted. The root volume is shown with a size of 30 GiB, General Purpose SSD (GP2) volume type, 100 / 3000 IOPS, N/A throughput, and is not encrypted. Below the table is an 'Add New Volume' button. A blue box contains a note about free tier eligibility. At the bottom, there are navigation buttons: Cancel, Previous, Review and Launch (highlighted), and Next: Add Tags. The footer shows the URL and copyright information.

EC2 Management Console

Secure | <https://ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard>

Services Resource Groups

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

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ	Volume Type ⓘ	IOPS ⓘ	Throughput (MB/s) ⓘ	Delete on Termination ⓘ	Encrypted ⓘ
Root	/dev/sda1	snap-02870ba882aa94ab2	30	General Purpose SSD (GP2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

[Add New Volume](#)

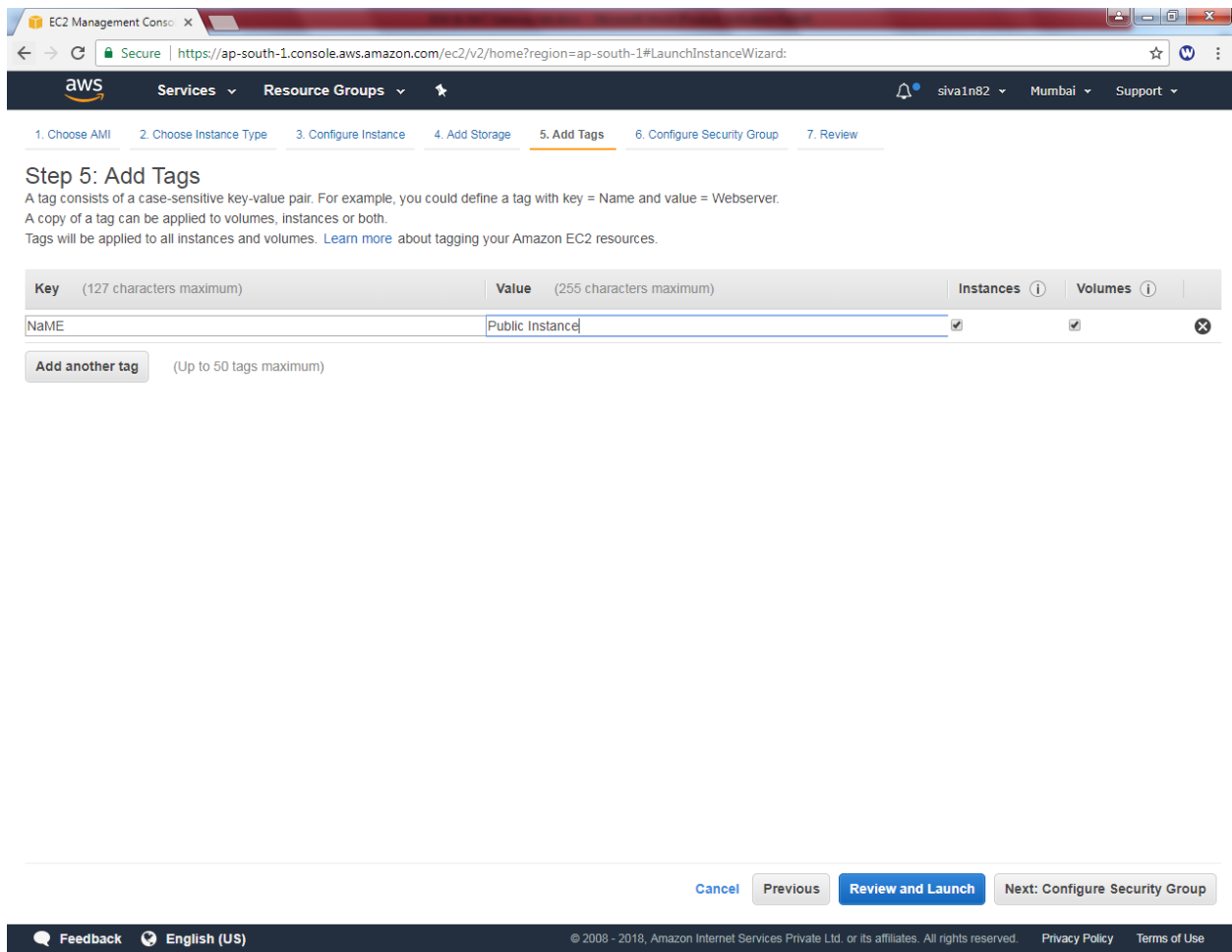
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Tags](#)

<https://ap-south-1.console.aws.amazon.com/console/home?region=ap-south-1> © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

Then Click “Next”.

In Key “name” and in value “Public Instance”.



EC2 Management Console

Secure | <https://ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard:>

aws Services Resource Groups

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 (127 characters maximum)	Value (255 characters maximum)	Instances ⓘ	Volumes ⓘ
Name	Public Instance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[Add another tag](#) (Up to 50 tags maximum)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security Group](#)

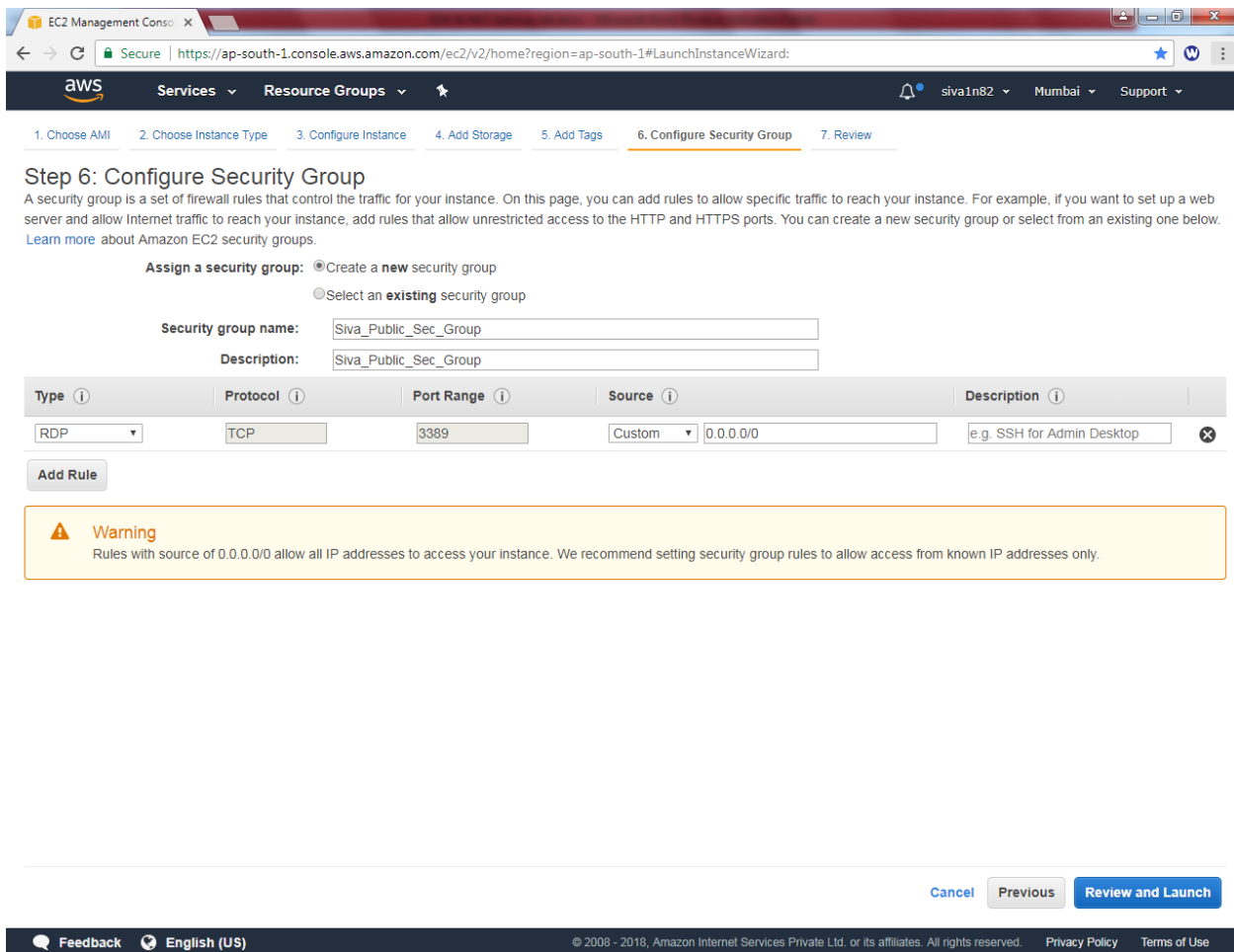
[Feedback](#) [English \(US\)](#) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

Then click “Next”.

In Assign a Security group click “Create a new security Group”

Security Group name: Siva_Public_Sec_Group

Description: Siva_Public_Sec_Group



EC2 Management Console

Secure | <https://ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard>

Services Resource Groups

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

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 set up a web server and 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 below. [Learn more](#) about Amazon EC2 security groups.

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

Security group name:

Description:

Type	Protocol	Port Range	Source	Description
RDP	TCP	3389	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

Add Rule

Warning

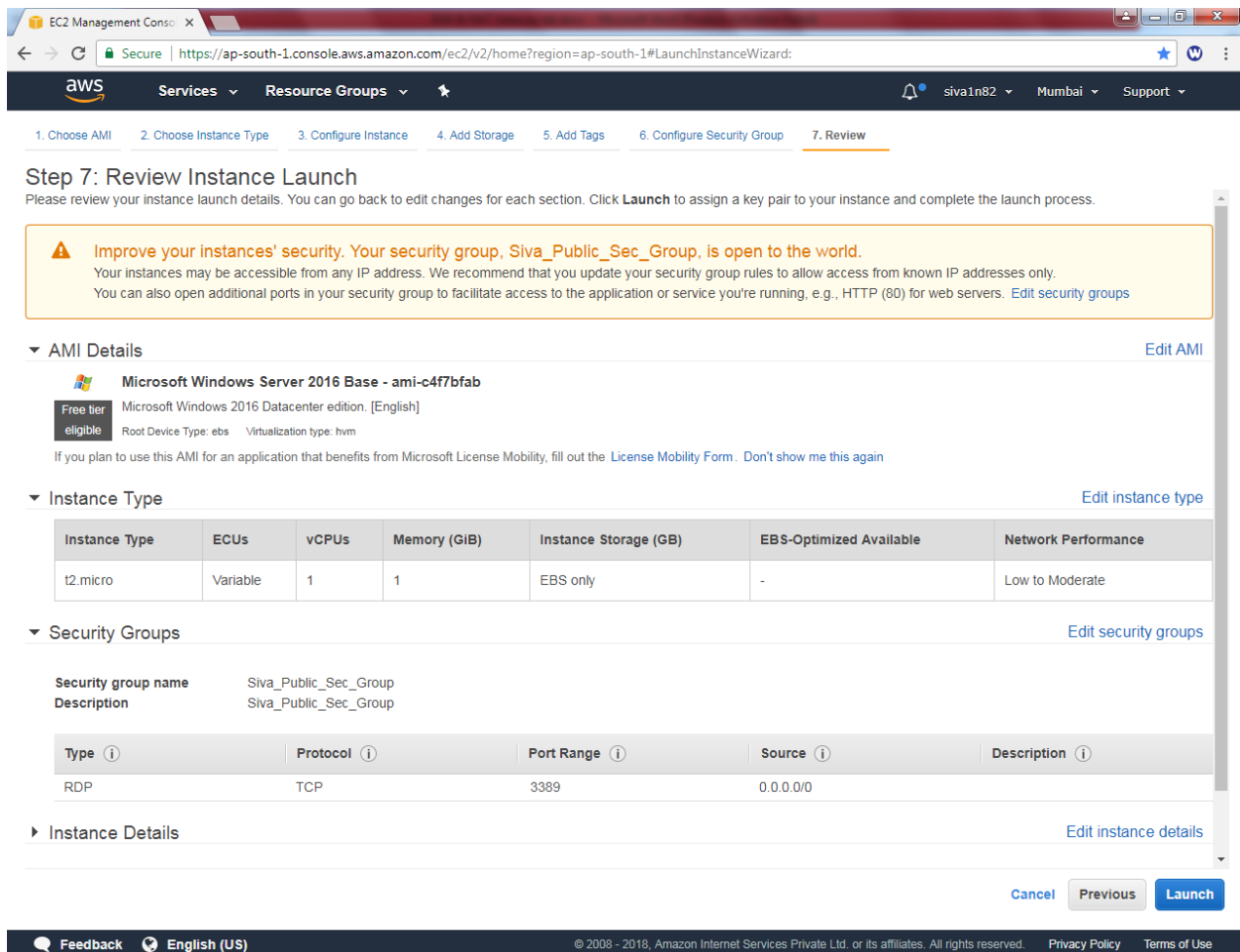
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Cancel Previous **Review and Launch**

Feedback English (US) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Click Review and Launch.

Leave the settings default.



EC2 Management Console

Secure | <https://ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard>

Services | Resource Groups | siva1n82 | Mumbai | Support

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


Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

⚠ Improve your instances' security. Your security group, Siva_Public_Sec_Group, is open to the world.

Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

▼ AMI Details [Edit AMI](#)

 **Microsoft Windows Server 2016 Base - ami-c4f7bfab**

Free tier eligible Microsoft Windows 2016 Datacenter edition. [English]
Root Device Type: ebs Virtualization type: hvm

If you plan to use this AMI for an application that benefits from Microsoft License Mobility, fill out the [License Mobility Form](#). [Don't show me this again](#)

▼ Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

▼ Security Groups [Edit security groups](#)

Security group name: Siva_Public_Sec_Group
Description: Siva_Public_Sec_Group

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ	Description ⓘ
RDP	TCP	3389	0.0.0.0/0	

► Instance Details [Edit instance details](#)

[Cancel](#) [Previous](#) [Launch](#)

Feedback | English (US) | © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. | [Privacy Policy](#) | [Terms of Use](#)

Click Launch.

While click launch, need to select the Choose an existing key pair and select the key pair as “siva_vpc” and Select the option I acknowledge.

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

siva_vpc

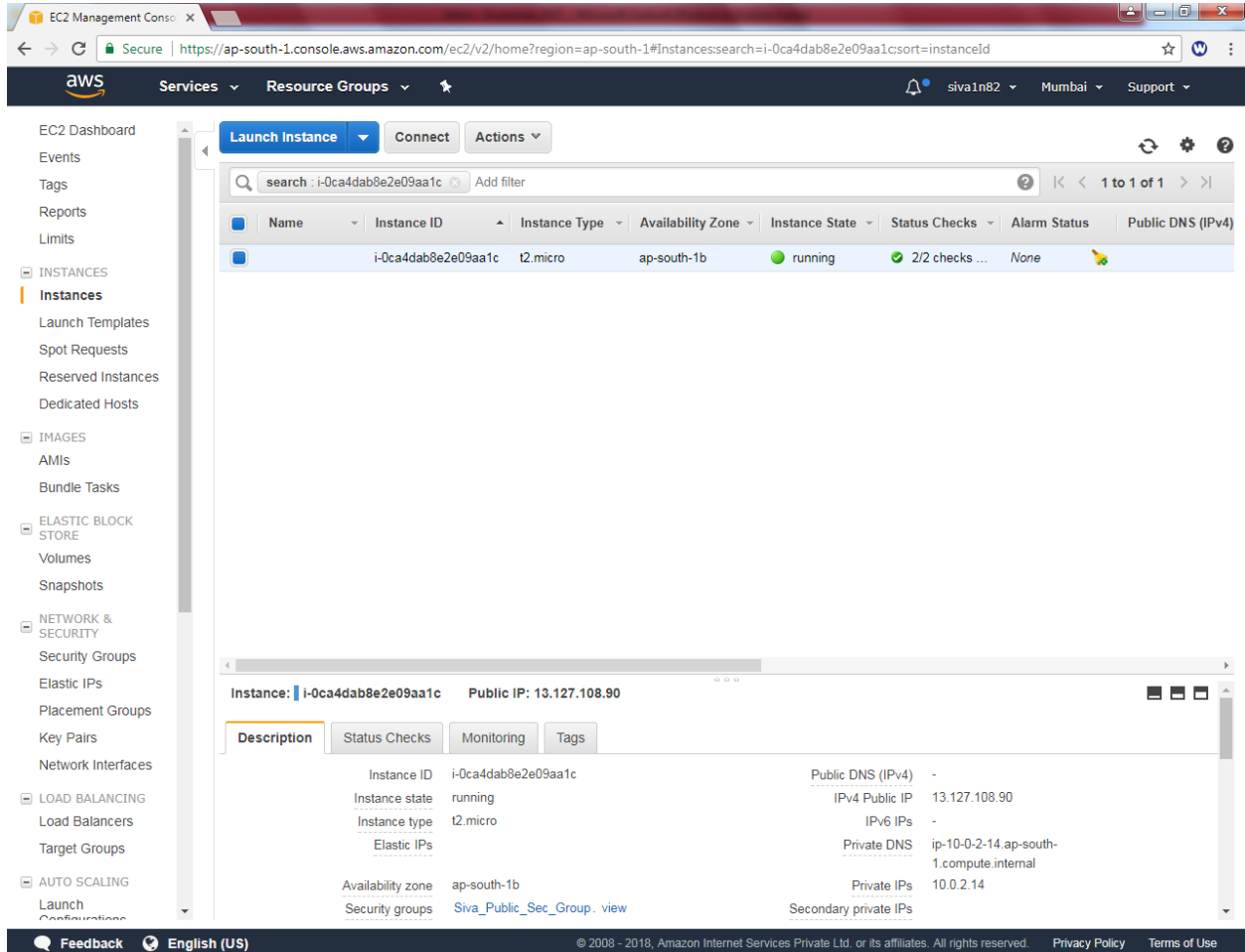
☒ I acknowledge that I have access to the selected private key file (siva_vpc.pem), and that without this file, I won't be able to log into my instance.

Cancel

Launch Instances

Then click launch instance.

Now, public instance is ready and we have got public IP also.

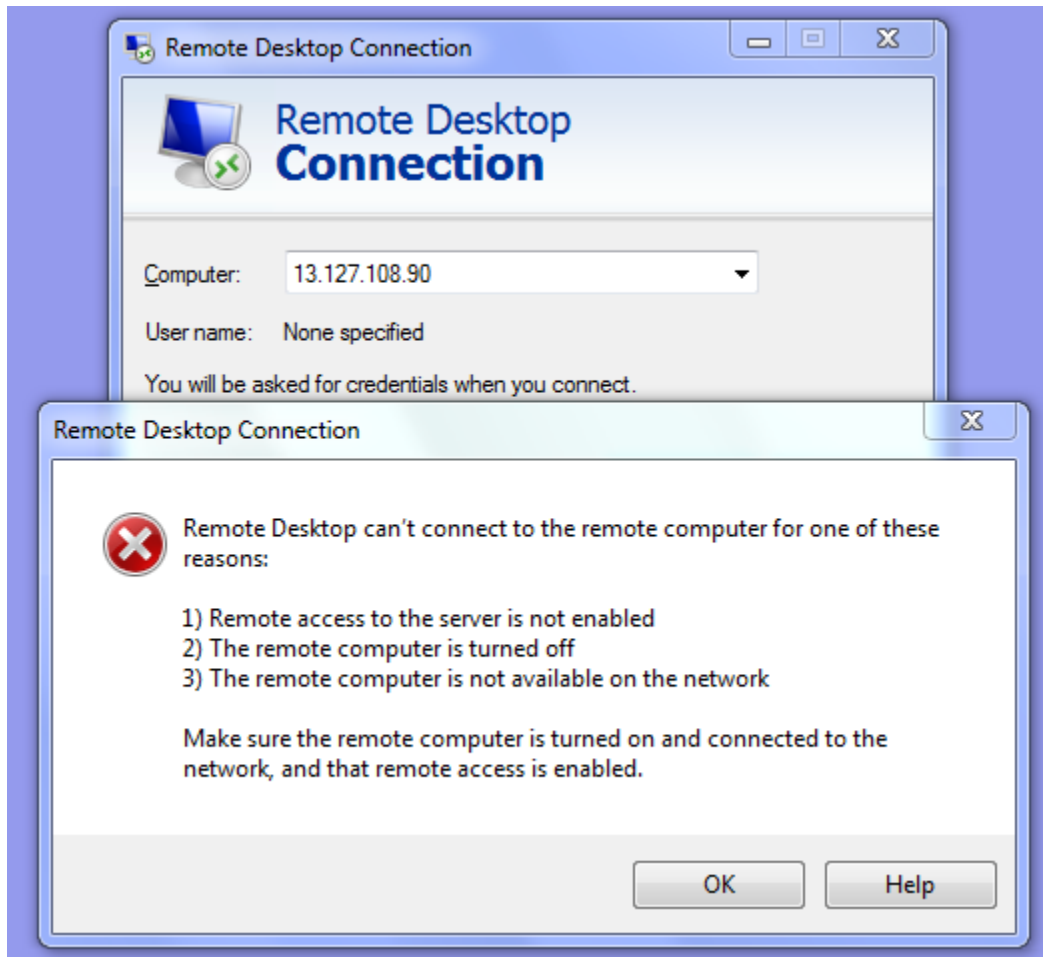


The screenshot displays the AWS Management Console interface. The left-hand navigation pane shows various services, with 'INSTANCES' selected. The main content area shows a list of EC2 instances. One instance, with ID 'i-0ca4dab8e2e09aa1c', is shown in a 'running' state. Below the list, the details for this instance are displayed, including its public IP address: 13.127.108.90.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
	i-0ca4dab8e2e09aa1c	t2.micro	ap-south-1b	running	2/2 checks ...	None	

Instance: i-0ca4dab8e2e09aa1c		Public IP: 13.127.108.90
Description	Instance ID	i-0ca4dab8e2e09aa1c
	Instance state	running
	Instance type	t2.micro
	Elastic IPs	
	Availability zone	ap-south-1b
	Security groups	Siva_Public_Sec_Group. view
	Public DNS (IPv4)	-
	IPv4 Public IP	13.127.108.90
	IPv6 IPs	-
	Private DNS	ip-10-0-2-14.ap-south-1.compute.internal
	Private IPs	10.0.2.14
	Secondary private IPs	

Now we can try to RDP for 13.127.108.90 IP.

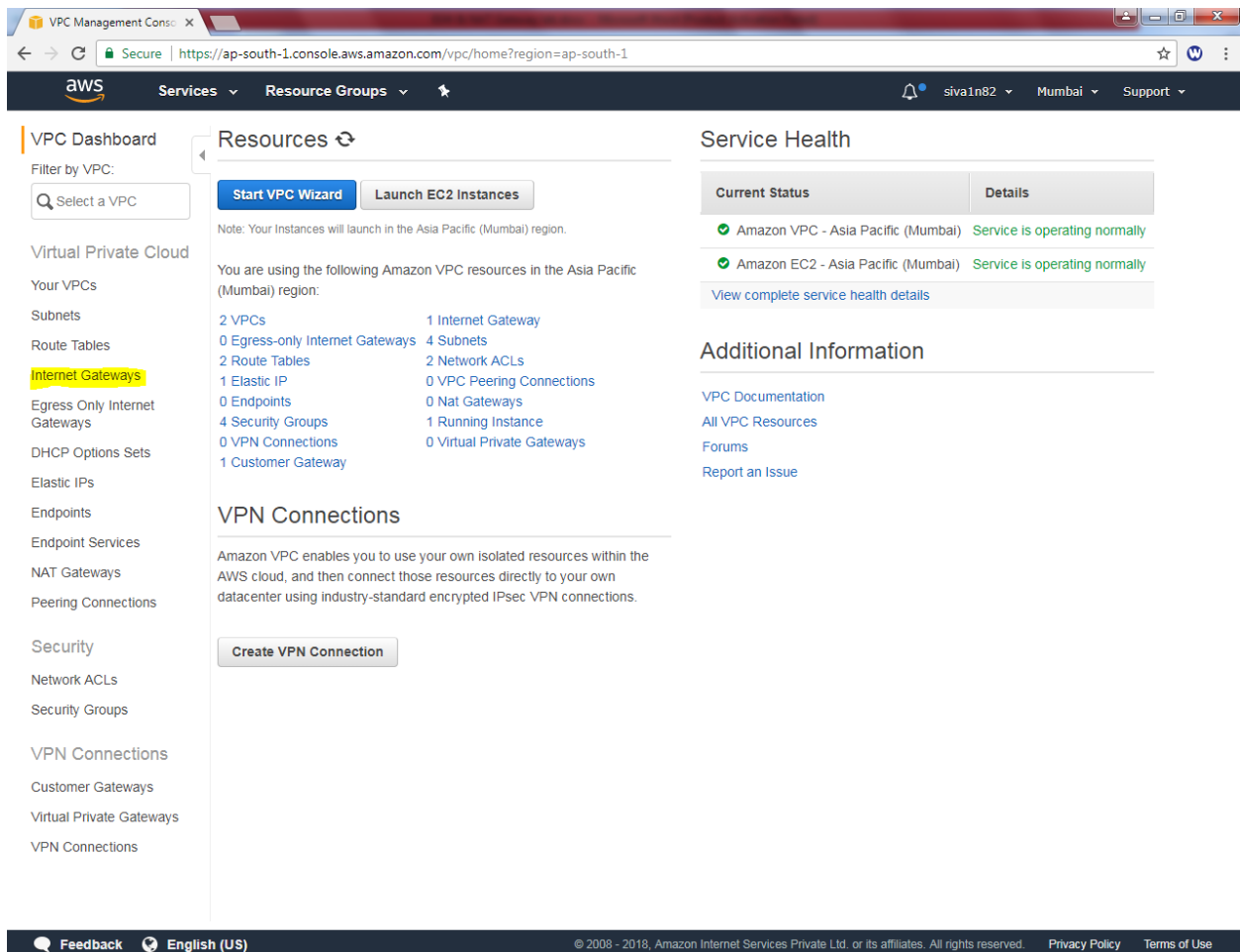


While try to connect 13.127.108.90 IP, we are getting an above error message.

What could be the reason of unable to connect RDP?

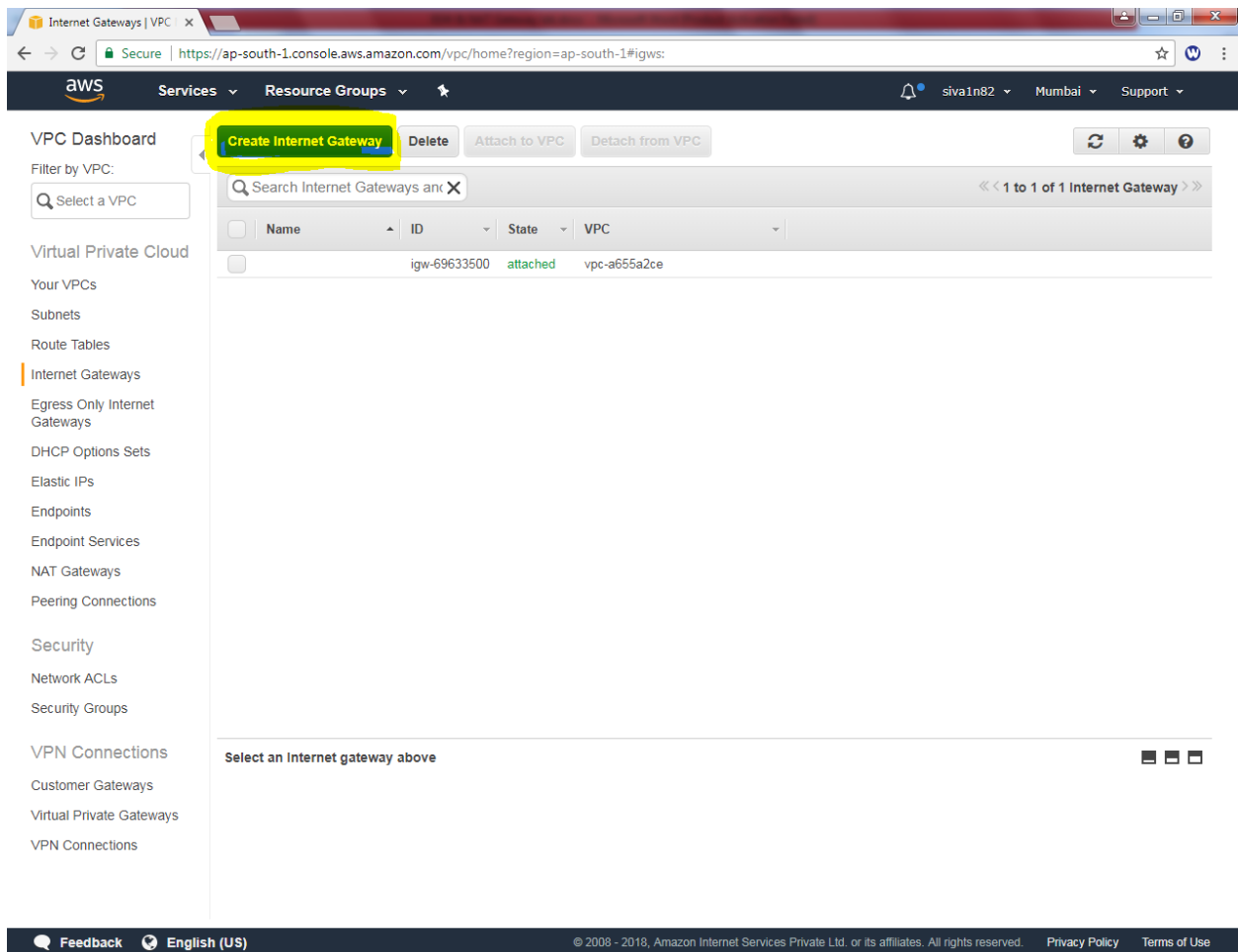
We have required Internet gateway to connect outside network from Public Subnet. Hence we need to create an internet gateway.

Goto VPC Dashboard, we can able to see an **Internet Gateways** option.



The screenshot shows the AWS VPC Management Console interface. The left sidebar contains a navigation menu with the following items: Virtual Private Cloud, Your VPCs, Subnets, Route Tables, **Internet Gateways** (highlighted in yellow), Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, Endpoint Services, NAT Gateways, Peering Connections, Security, Network ACLs, Security Groups, VPN Connections, Customer Gateways, Virtual Private Gateways, and VPN Connections. The main content area displays the 'Resources' section for the selected VPC, showing a list of resources: 2 VPCs, 0 Egress-only Internet Gateways, 2 Route Tables, 1 Elastic IP, 0 Endpoints, 4 Security Groups, 0 VPN Connections, 1 Customer Gateway, 1 Internet Gateway, 4 Subnets, 2 Network ACLs, 0 VPC Peering Connections, 0 Nat Gateways, 1 Running Instance, and 0 Virtual Private Gateways. The 'Service Health' section on the right indicates that both Amazon VPC and Amazon EC2 services are operating normally. The 'Additional Information' section provides links to VPC Documentation, All VPC Resources, Forums, and Report an Issue. The footer contains a Feedback link, English (US) language selection, and copyright information for Amazon Internet Services Private Ltd.

Click the Internet Gateways in VPC Dashboard,



The screenshot shows the AWS VPC Dashboard for the region 'ap-south-1'. The 'Create Internet Gateway' button is highlighted with a yellow box. The dashboard includes a sidebar with navigation links for VPCs, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, Endpoint Services, NAT Gateways, Peering Connections, Security, Network ACLs, Security Groups, VPN Connections, Customer Gateways, Virtual Private Gateways, and VPN Connections. The main content area displays a table of Internet Gateways with columns for Name, ID, State, and VPC. A single gateway is listed with ID 'igw-69633500', State 'attached', and VPC 'vpc-a655a2ce'. The bottom of the dashboard features a footer with 'Feedback', 'English (US)', and copyright information.

Click “create Internet Gateway”.

In Name Tag, Type “Siva IGW”.

Create Internet Gateway

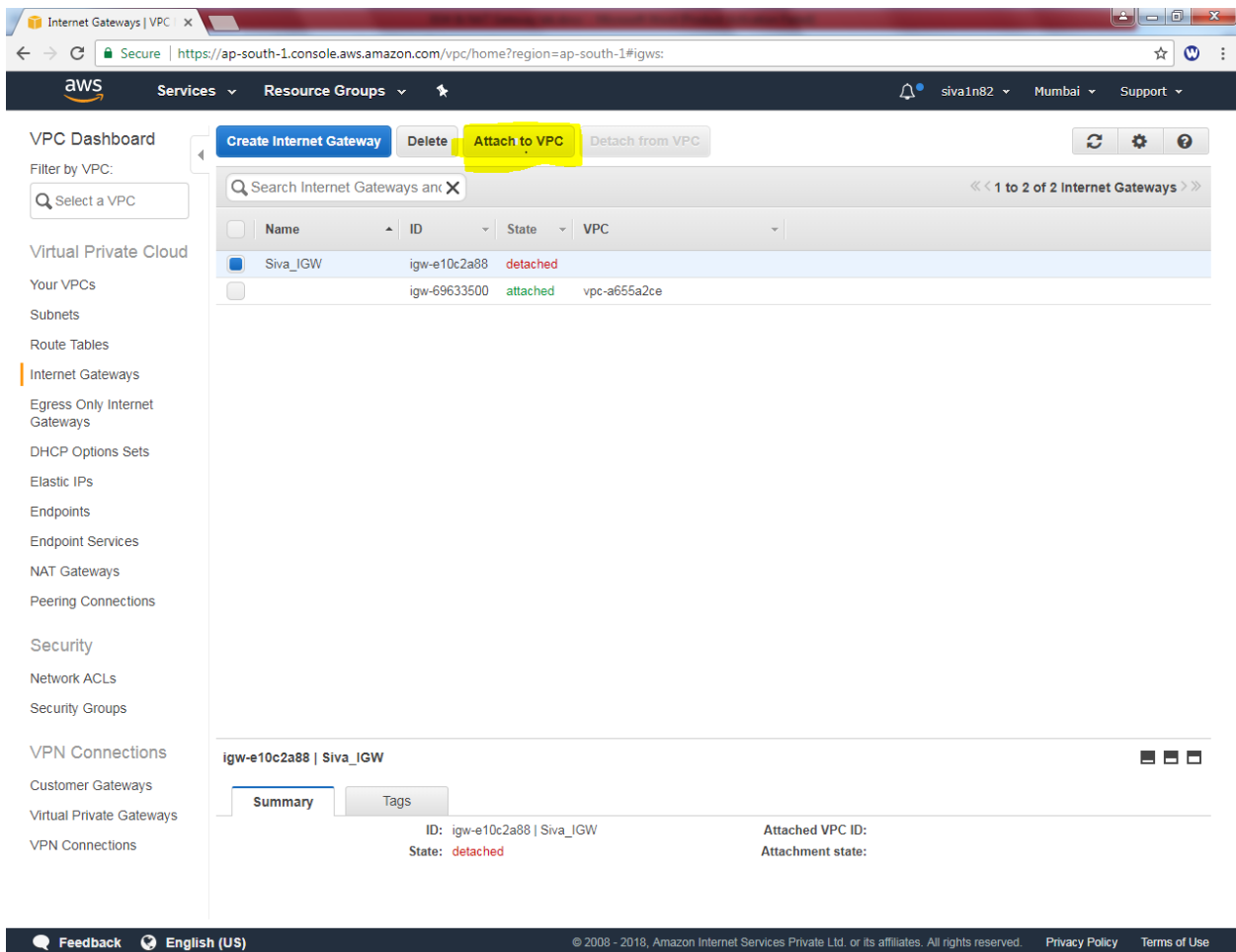
An Internet gateway is a virtual router that connects a VPC to the Internet.

Name tag

[Cancel](#) [Yes, Create](#)

Then click “Yes, Create”.

We can able to see “Siva IGW” option. But it is detached mode.



Internet Gateways | VPC

Secure | <https://ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#igws>

aws Services Resource Groups

siva1n82 Mumbai Support

VPC Dashboard

Filter by 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

Security

Network ACLs

Security Groups

VPN Connections

Customer Gateways

Virtual Private Gateways

VPN Connections

Create Internet Gateway Delete Attach to VPC Detach from VPC

Search Internet Gateways and

<< 1 to 2 of 2 Internet Gateways >>

<input type="checkbox"/>	Name	ID	State	VPC
<input checked="" type="checkbox"/>	Siva_IGW	igw-e10c2a88	detached	
<input type="checkbox"/>		igw-69633500	attached	vpc-a655a2ce

igw-e10c2a88 | Siva_IGW

Summary Tags

ID: igw-e10c2a88 | Siva_IGW

State: detached

Attached VPC ID:

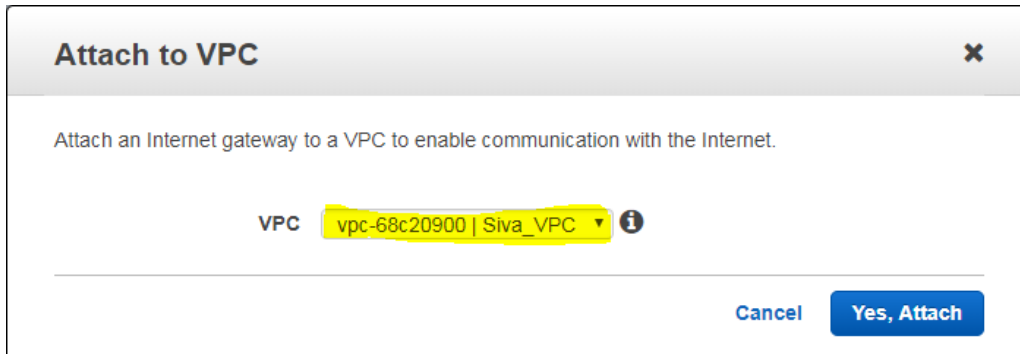
Attachment state:

Feedback English (US)

© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

We need to attach VPC into that i.e. Siva_VPC.

In Attach to VPC, Siva_VPC is selected,



Attach to VPC [X]

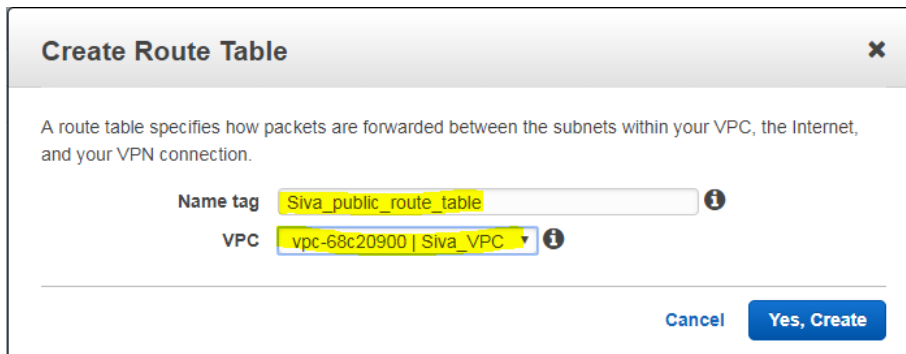
Attach an Internet gateway to a VPC to enable communication with the Internet.

VPC vpc-68c20900 | Siva_VPC ⓘ

Cancel Yes, Attach

Click Yes, Attach button.

We need to create route table for Public subnet. In Name tag “Siva_Public_route_table”. Then select VPC as “Siva VPC”.



Create Route Table [X]

A route table specifies how packets are forwarded between the subnets within your VPC, the Internet, and your VPN connection.

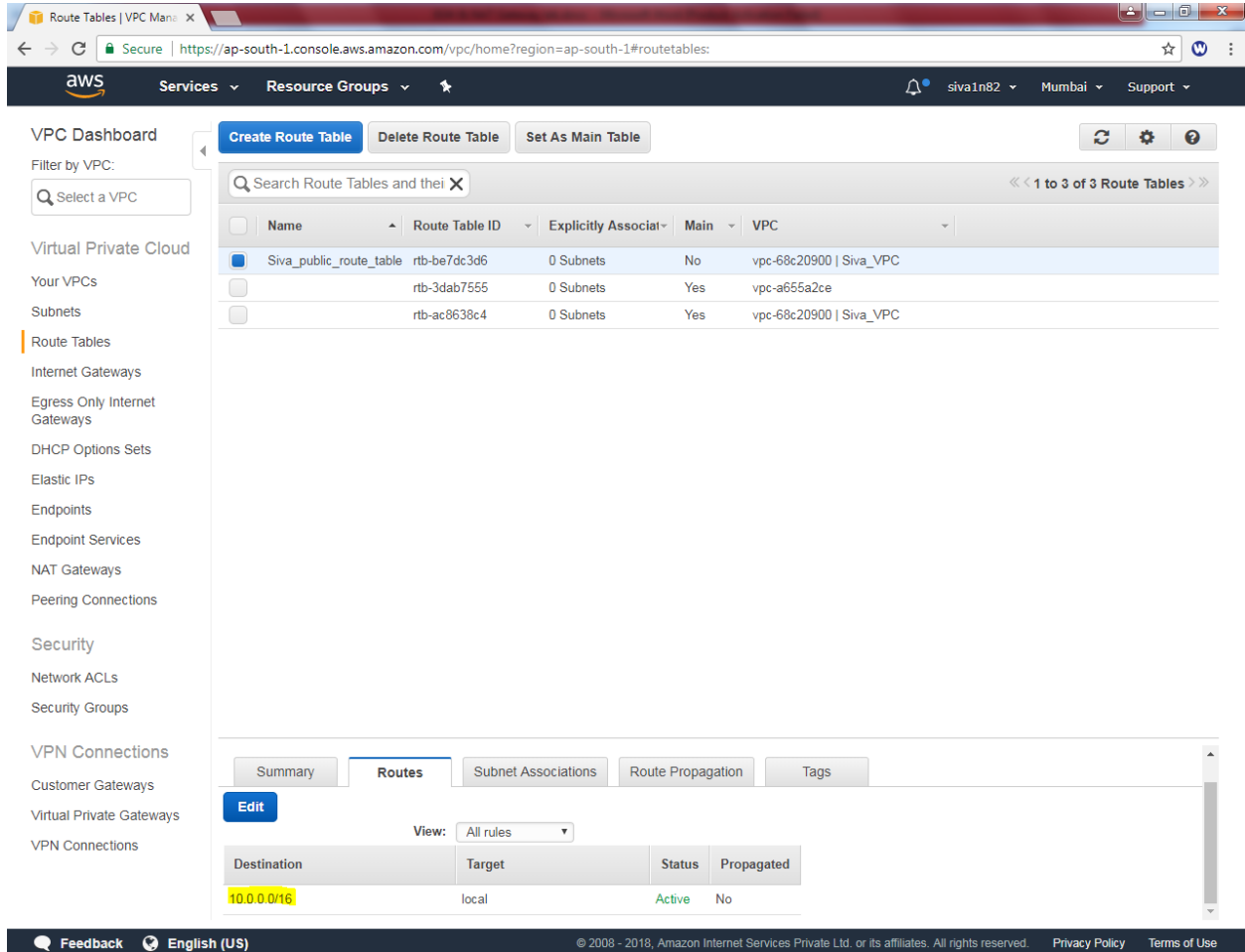
Name tag Siva_public_route_table ⓘ

VPC vpc-68c20900 | Siva_VPC ⓘ

Cancel Yes, Create

Click “yes, create”.

By default, 10.0.0.0/16 subnet route only available.



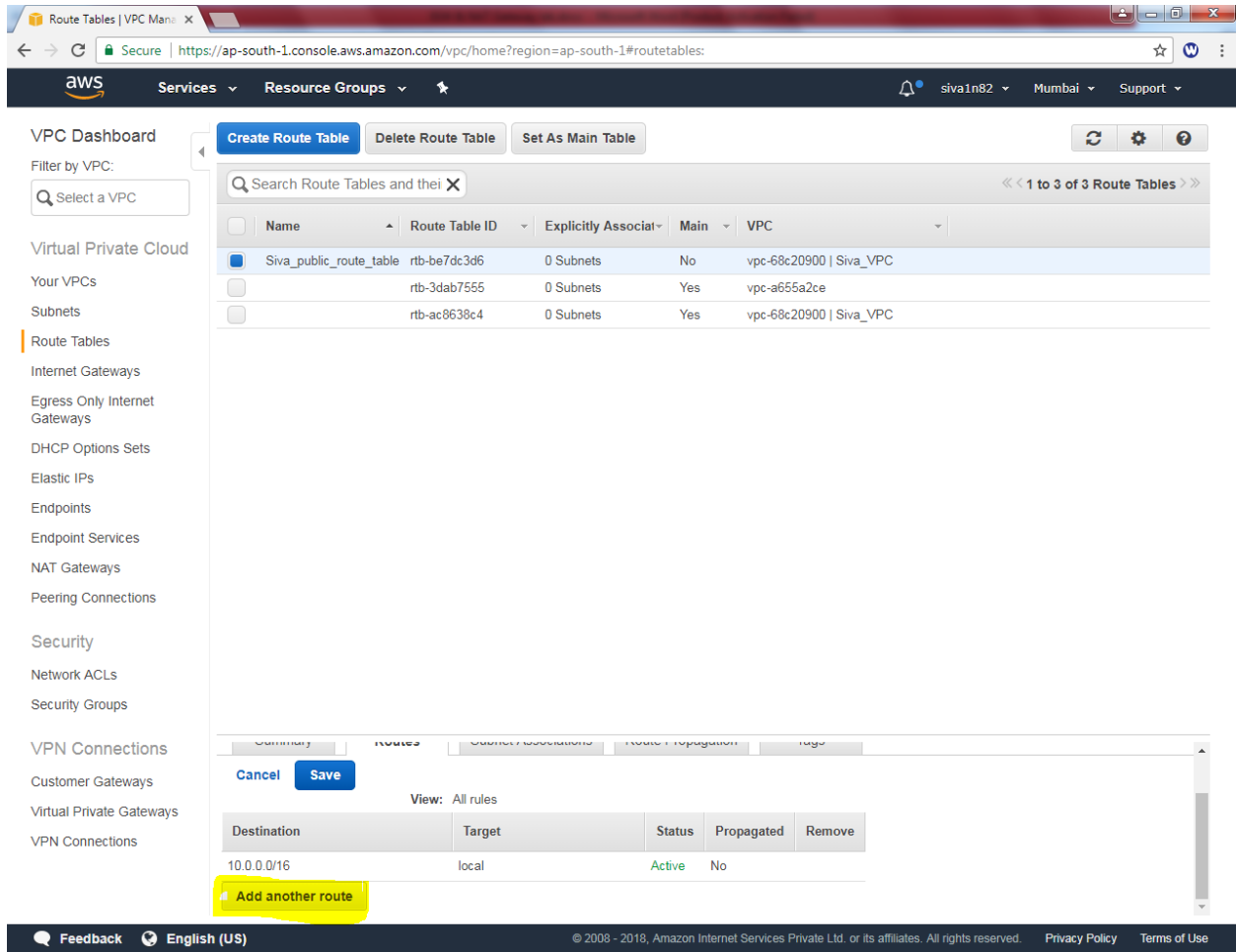
The screenshot shows the AWS Management Console interface for Route Tables. The left sidebar contains navigation links for VPC Dashboard, Virtual Private Cloud, and various network services. The main content area displays a list of route tables. Below the list, the 'Routes' tab is active, showing a table of routes.

Name	Route Table ID	Explicitly Associat	Main	VPC
Siva_public_route_table	rtb-be7dc3d6	0 Subnets	No	vpc-68c20900 Siva_VPC
	rtb-3dab7555	0 Subnets	Yes	vpc-a655a2ce
	rtb-ac8638c4	0 Subnets	Yes	vpc-68c20900 Siva_VPC

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

Click Edit option in route table.

Then click “add another route”.

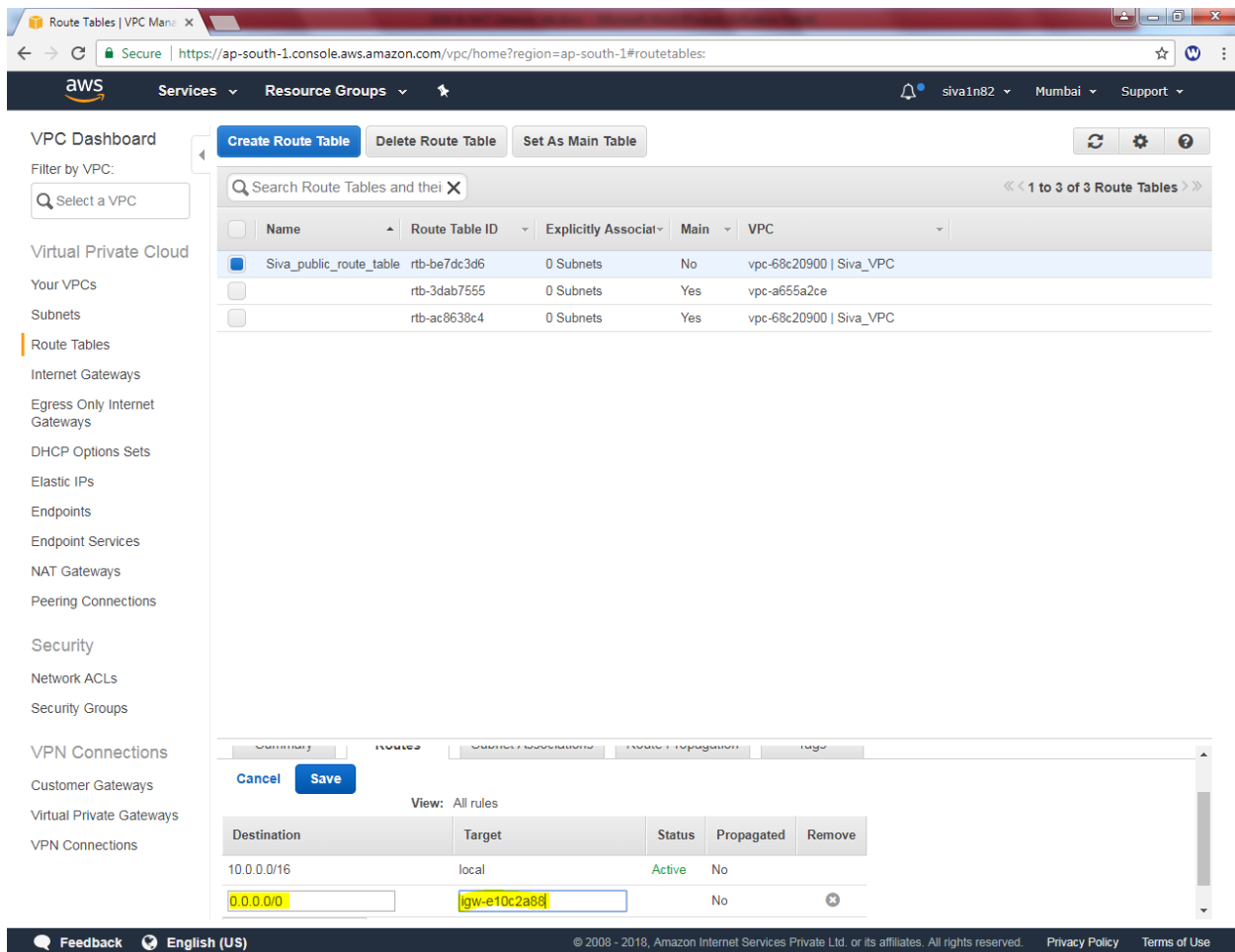


The screenshot shows the AWS Management Console interface for Route Tables. The left sidebar contains navigation links for VPC Dashboard, Virtual Private Cloud, and various network services. The main content area displays a list of Route Tables. Below the list, a modal window is open for editing a route table, showing a table with columns for Destination, Target, Status, Propagated, and Remove. The 'Add another route' button is highlighted in yellow.

Name	Route Table ID	Explicitly Associat	Main	VPC
Siva_public_route_table	rtb-be7dc3d6	0 Subnets	No	vpc-68c20900 Siva_VPC
	rtb-3dab7555	0 Subnets	Yes	vpc-a655a2ce
	rtb-ac8638c4	0 Subnets	Yes	vpc-68c20900 Siva_VPC

Destination	Target	Status	Propagated	Remove
10.0.0.0/16	local	Active	No	

In Public route table, add default route 0.0.0.0/0 with next hop address as igw (internet gateway).

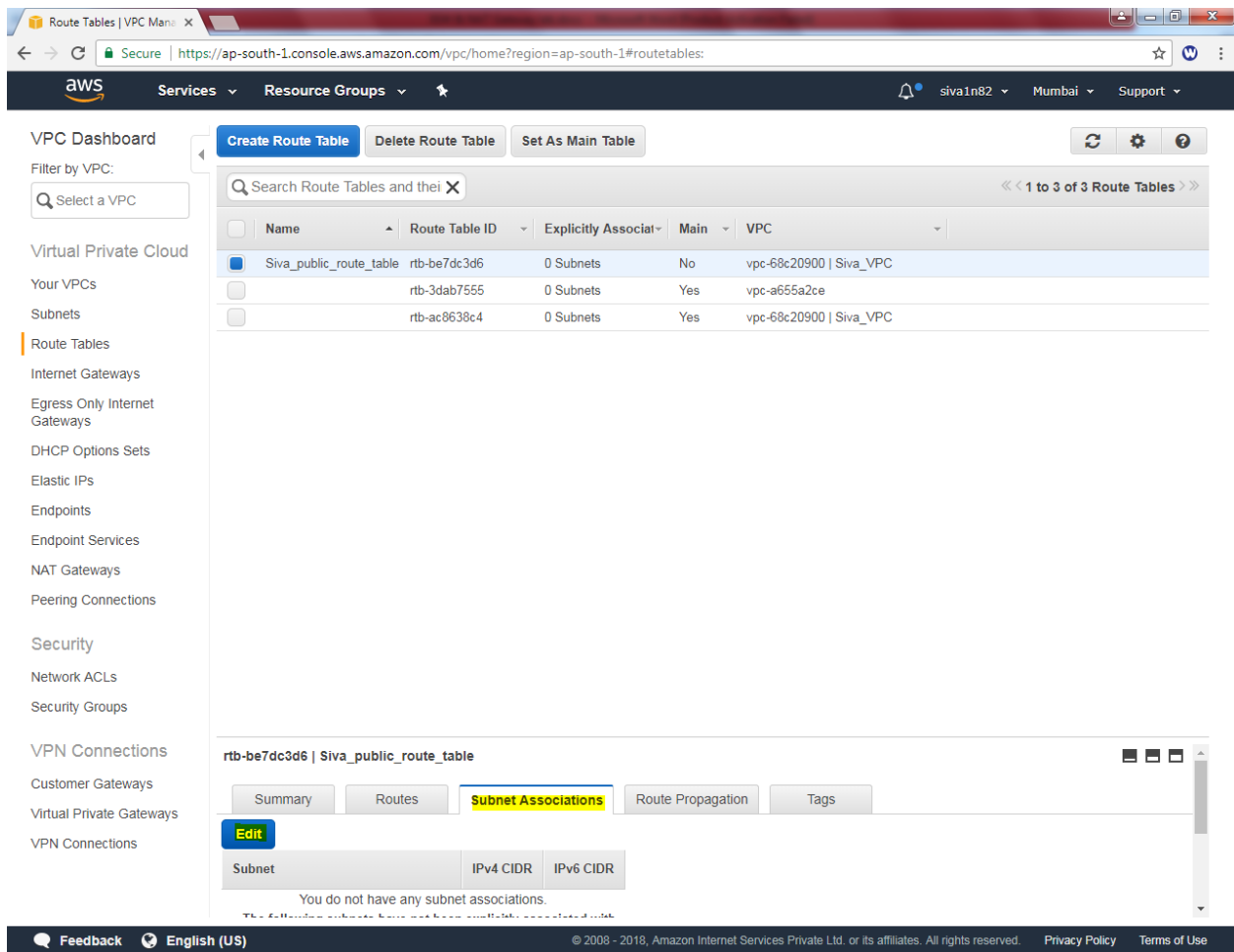


The screenshot shows the AWS Management Console for Route Tables. The 'Routes' tab is selected, showing a table of routes. A new route is being added with the destination '0.0.0.0/0' and the target 'igw-e10c2a88'. The 'Save' button is highlighted.

Destination	Target	Status	Propagated	Remove
10.0.0.0/16	local	Active	No	
0.0.0.0/0	igw-e10c2a88	No		

Then Click “Save”.

In Subnet associations, click edit option.



The screenshot shows the AWS Management Console interface for the VPC Dashboard. The left sidebar contains a navigation menu with options like VPC Dashboard, Your VPCs, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, Endpoint Services, NAT Gateways, Peering Connections, Security, Network ACLs, Security Groups, VPN Connections, Customer Gateways, Virtual Private Gateways, and VPN Connections. The main content area displays a list of Route Tables. The 'Siva_public_route_table' is selected, and the 'Subnet Associations' tab is active. Below the tabs, there is a table with columns for Subnet, IPv4 CIDR, and IPv6 CIDR. The message 'You do not have any subnet associations.' is displayed.

Name	Route Table ID	Explicitly Associat	Main	VPC
Siva_public_route_table	rtb-be7dc3d6	0 Subnets	No	vpc-68c20900 Siva_VPC
	rtb-3dab7555	0 Subnets	Yes	vpc-a655a2ce
	rtb-ac8638c4	0 Subnets	Yes	vpc-68c20900 Siva_VPC

rtb-be7dc3d6 | Siva_public_route_table

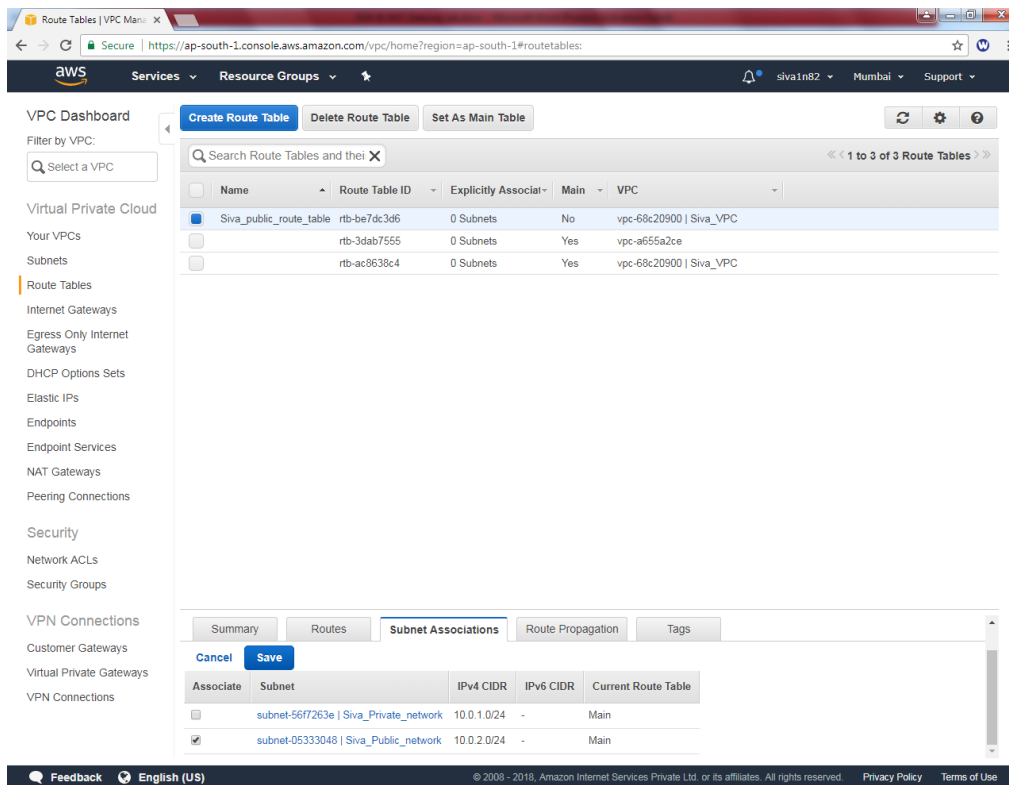
Summary Routes **Subnet Associations** Route Propagation Tags

Edit

Subnet	IPv4 CIDR	IPv6 CIDR
You do not have any subnet associations.		

© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

In Edit option, select “Siva_Public_network”.

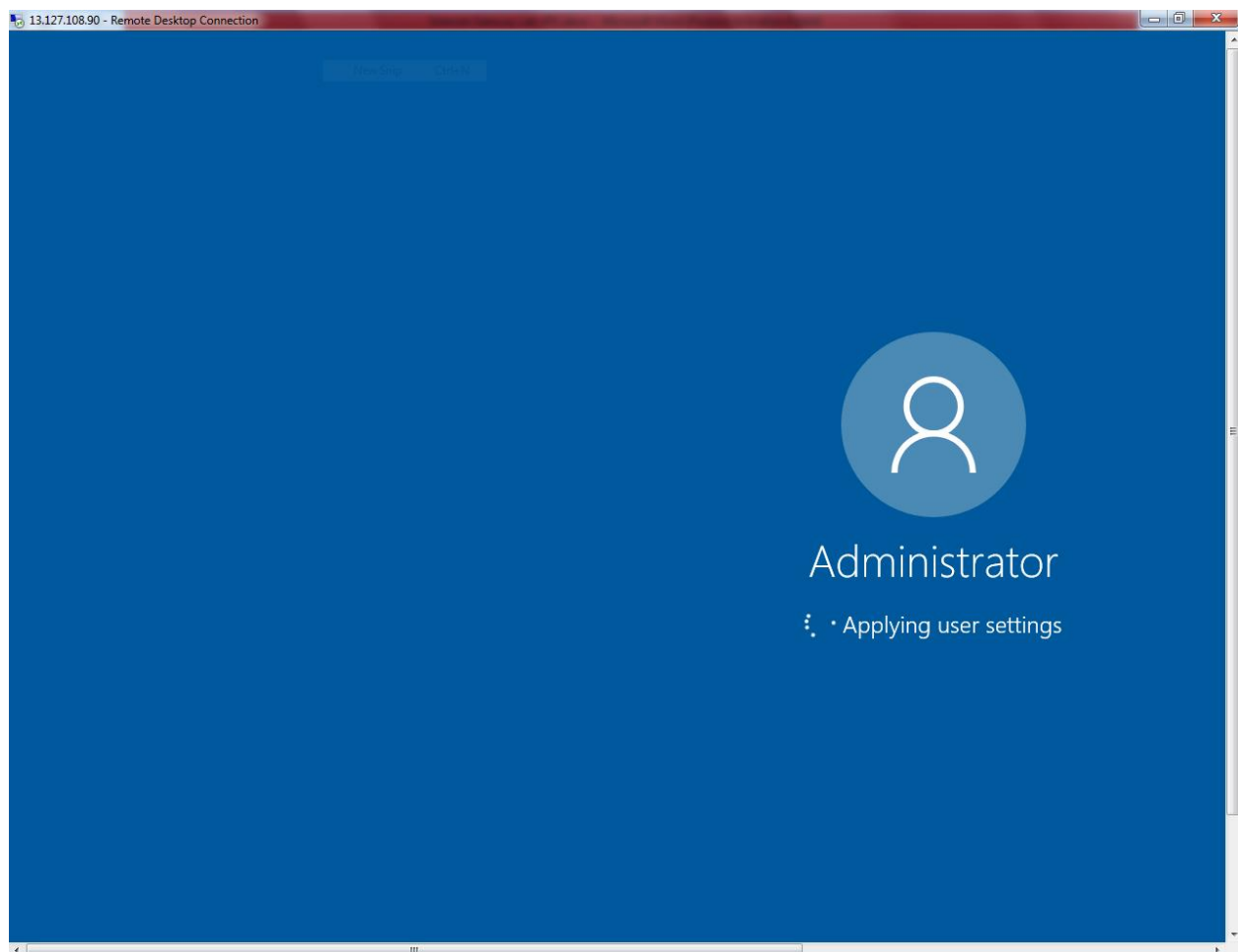
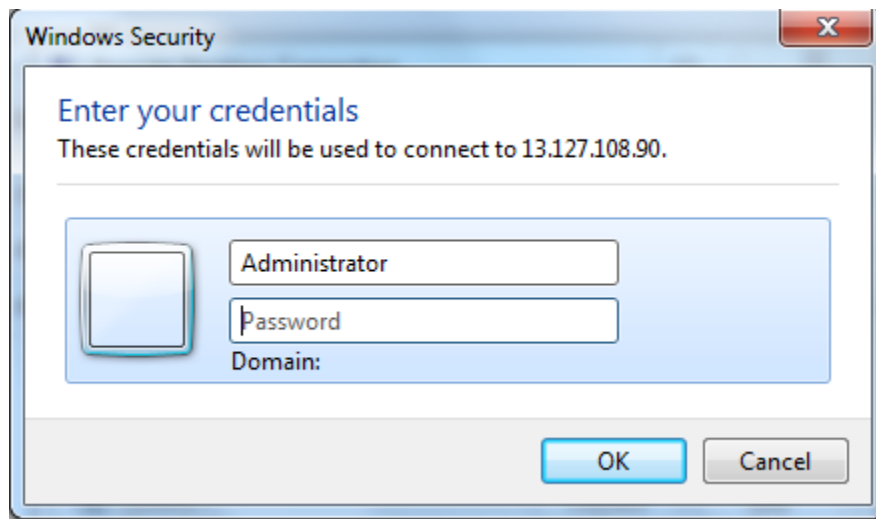


The screenshot shows the AWS Management Console interface for editing a route table. The left sidebar contains navigation links for VPC Dashboard, Virtual Private Cloud, and various network services. The main content area displays a table of route tables. The 'Siva_public_route_table' is selected, and the 'Subnet Associations' tab is active. The table shows two subnets: 'subnet-56f7263e | Siva_Private_network' and 'subnet-05333048 | Siva_Public_network'. The 'Siva_Public_network' is checked for association.

Associate	Subnet	IPv4 CIDR	IPv6 CIDR	Current Route Table
<input type="checkbox"/>	subnet-56f7263e Siva_Private_network	10.0.1.0/24	-	Main
<input checked="" type="checkbox"/>	subnet-05333048 Siva_Public_network	10.0.2.0/24	-	Main

Then click save.

Now you Can try to connect internet, it will work.



You have successfully logged into the public server (windows server 2016).