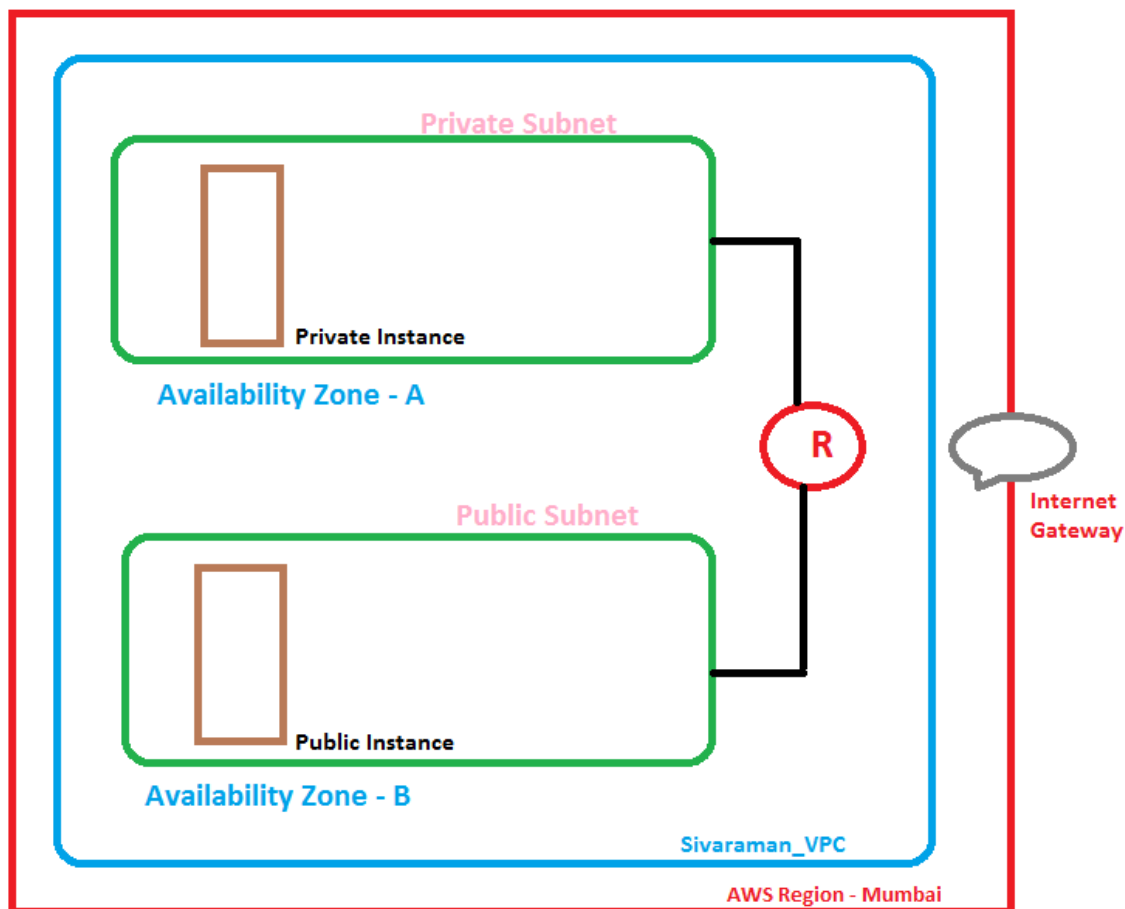


Lab: Need to access public network from Public subnet and access Public subnet from Public network.

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 Dashboard in the 'ap-south-1' region. The 'Create VPC' 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 existing VPCs with columns for Name, VPC ID, State, IPv4 CIDR, IPv6 CIDR, DHCP options set, Route table, and Network ACL. A single VPC is listed with ID 'vpc-a655a2ce' and state 'available'. The bottom of the page features a footer with 'Feedback', 'English (US)', and copyright information.

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set	Route table	Network ACL
	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 displays the AWS VPC Dashboard in the 'ap-south-1' region. The left sidebar shows the navigation menu with 'Your VPCs' selected. The main content area shows a table of VPCs. The 'Siva\_VPC' (vpc-68c20900) is highlighted. Below the table, the details for 'vpc-68c20900 | Siva\_VPC' are shown, including its state (available), IPv4 CIDR (10.0.0.0/16), DHCP options set (doot-924a84fa), and Network ACL (acl-a72b82cf).

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set	Route table	Network ACL
Siva_VPC	vpc-68c20900	available	10.0.0.0/16		doot-924a84fa	rtb-ac8638c4	acl-a72b82cf

**vpc-68c20900 | Siva\_VPC**

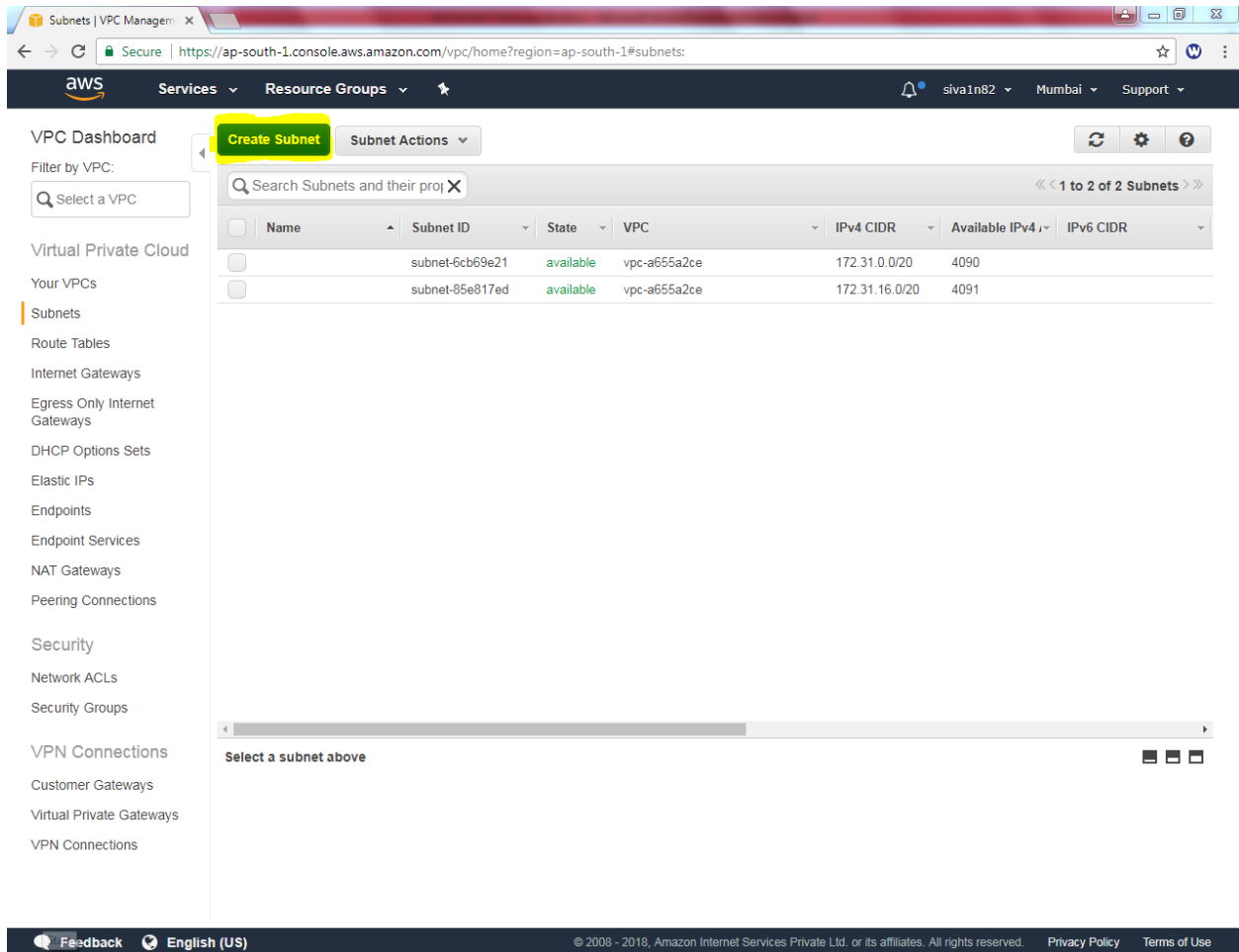
**Summary** | CIDR Blocks | Flow Logs | Tags

VPC ID: vpc-68c20900 | Siva\_VPC  
State: available  
IPv4 CIDR: 10.0.0.0/16  
IPv6 CIDR:   
DHCP options set: doot-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 displays the AWS VPC Subnets dashboard. The left sidebar contains a navigation menu with options like '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', and 'VPN Connections'. The 'Subnets' option is highlighted. The main content area shows a 'VPC Dashboard' with a 'Create Subnet' button highlighted in yellow. Below this is a search bar and a table of subnets. The table has columns: Name, Subnet ID, State, VPC, IPv4 CIDR, Available IPv4, and IPv6 CIDR. Two subnets are listed: subnet-6cb69e21 and subnet-85e817ed, both in 'available' state. The bottom of the dashboard shows a 'Select a subnet above' prompt and a footer with 'Feedback', 'English (US)', and copyright information.

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

Siva\_Public\_network

VPC

vpc-68c20900 | Siva\_VPC

VPC CIDRs

CIDR	Status	Status Reason
10.0.0.0/16	associated	

Availability Zone

ap-south-1b

IPv4 CIDR block

10.0.2.0/24

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

Siva\_Private\_network

VPC

vpc-68c20900 | Siva\_VPC

VPC CIDRs

CIDR	Status	Status Reason
10.0.0.0/16	associated	

Availability Zone

ap-south-1a

IPv4 CIDR block

10.0.1.0/24

Cancel

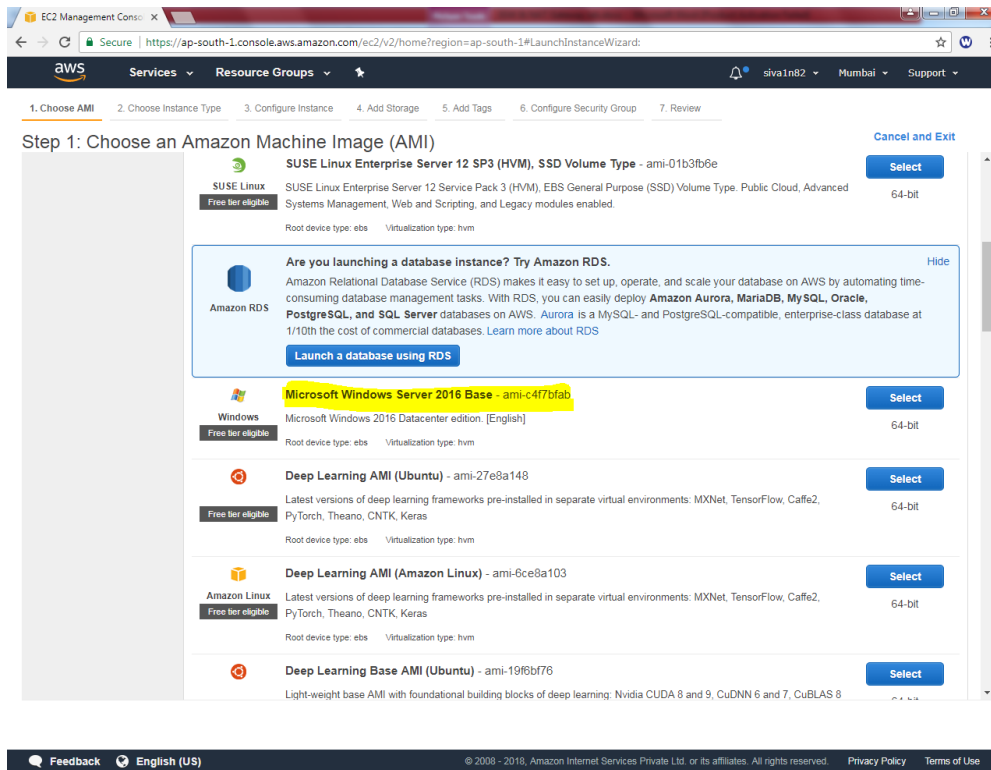
Yes, Create

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

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

The screenshot displays the AWS Management Console for the EC2 service in the Asia Pacific (Mumbai) region. The left-hand navigation pane lists various EC2-related services, with 'INSTANCES' currently selected. The main content area is divided into several sections: 'Resources' (showing counts for Running Instances, Elastic IPs, Snapshots, etc.), 'Create Instance' (with a prominent yellow 'Launch Instance' button), 'Service Health' (indicating normal status for the region and availability zones), and 'Scheduled Events' (showing no events). On the right, there are panels for 'Account Attributes' and 'Additional Information'.

Select **“AMI”**



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



EC2 Management Console

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 Free tier eligible	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

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 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  Launch into Auto Scaling Group

Purchasing option ☐ Request Spot instances

Network  Create new VPC

Subnet  Create new subnet  
251 IP Addresses available

Auto-assign Public IP

IAM role  Create new IAM role

Shutdown behavior

Enable termination protection ☐ Protect against accidental termination

Monitoring ☐ Enable CloudWatch detailed monitoring  
Additional charges apply.

Tenancy  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 'Add Storage' step of the EC2 instance launch wizard. The breadcrumb navigation at the top includes: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage (highlighted), 5. Add Tags, 6. Configure Security Group, and 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.

At the bottom right, there are navigation buttons: [Cancel](#), [Previous](#), [Review and Launch](#) (highlighted), and [Next: Add Tags](#).

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

Then Click “Next”.

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

EC2 Management Console

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>

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 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.**

**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 for the EC2 service. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and user information 'siva1n82' in 'Mumbai'. The left sidebar lists various EC2-related services like INSTANCES, IMAGES, ELASTIC BLOCK STORE, NETWORK & SECURITY, LOAD BALANCING, and AUTO SCALING. The main content area shows a list of instances with a search filter 'i-0ca4dab8e2e09aa1c'. A table lists the instance details:

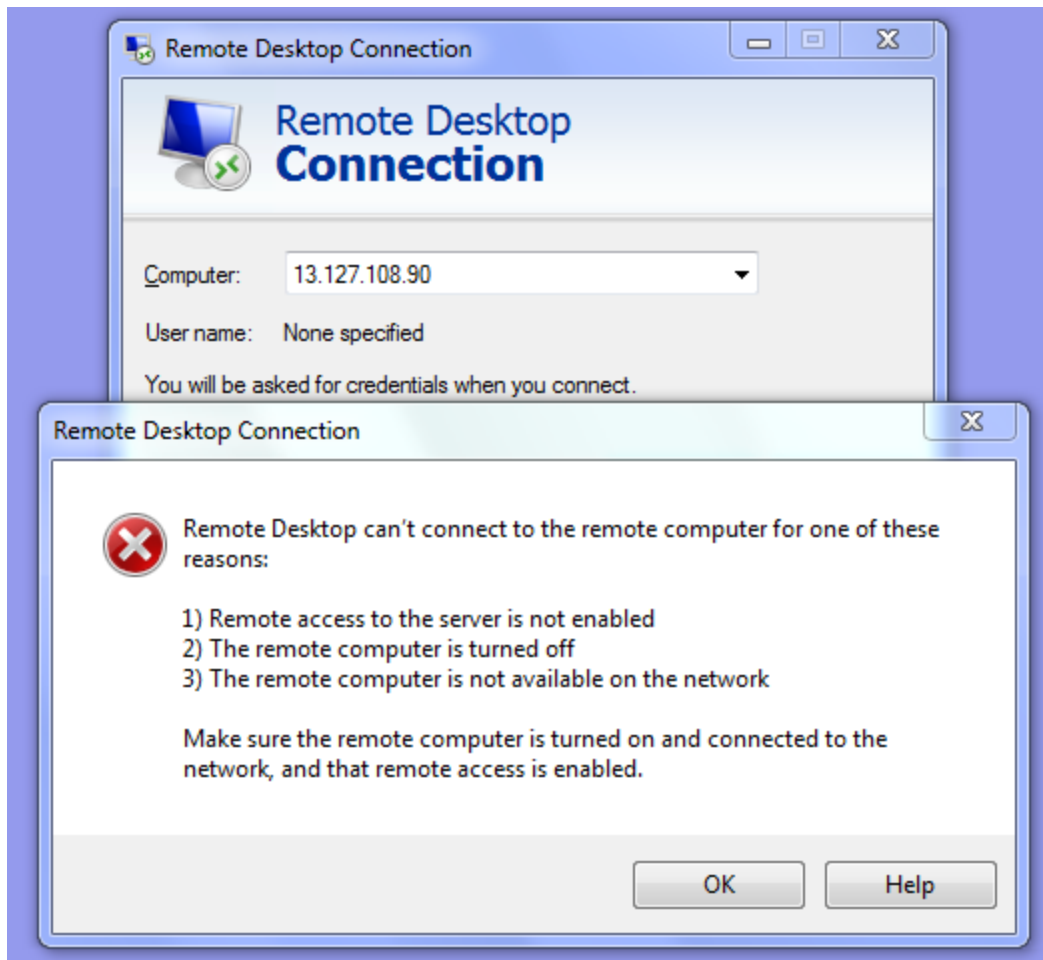
Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
	i-0ca4dab8e2e09aa1c	t2.micro	ap-south-1b	running	2/2 checks ...	None	

Below the table, the details for the selected instance 'i-0ca4dab8e2e09aa1c' are shown, including its Public IP: 13.127.108.90. The 'Description' tab is active, displaying the following information:

Property	Value
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.

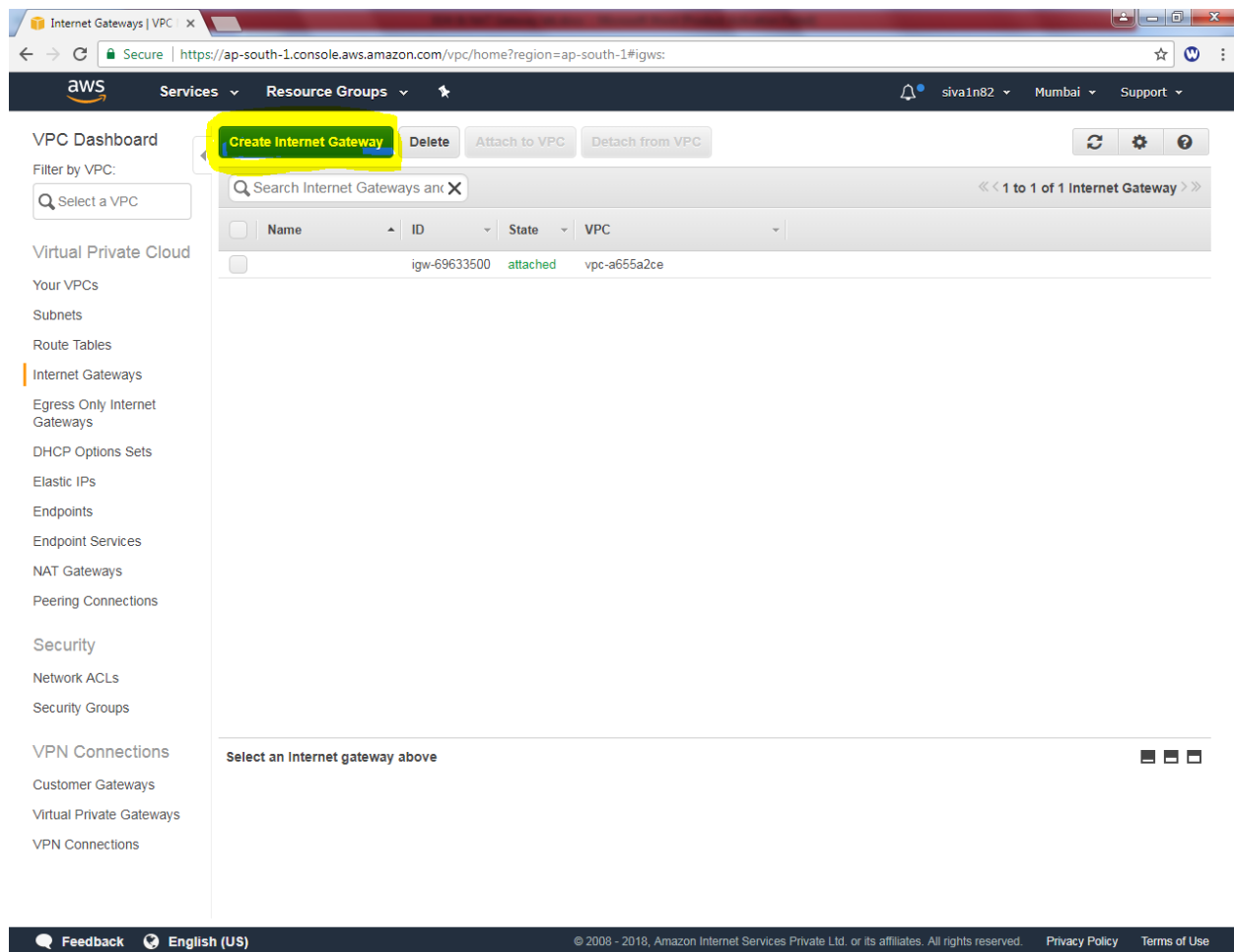
What could be the reason of unable to connect RDP?

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.

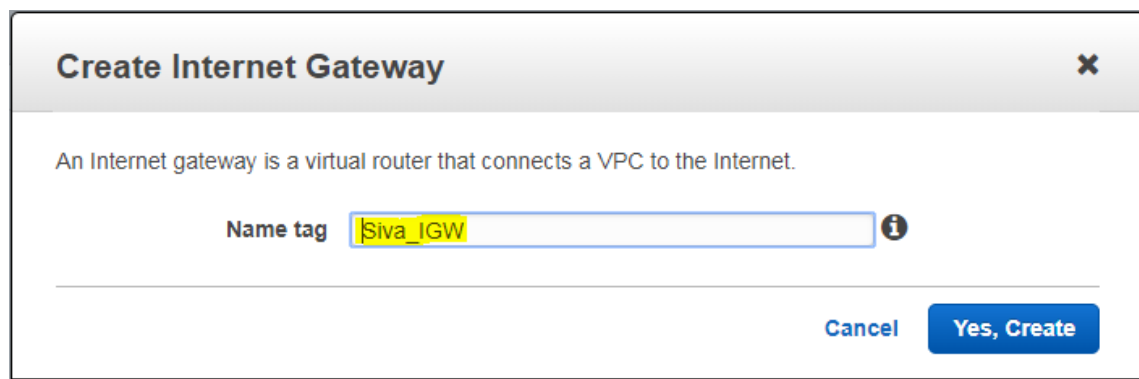
The screenshot displays the AWS VPC Management Console interface. The left sidebar contains a navigation menu with the following items: Virtual Private Cloud, Your VPCs, Subnets, Route Tables, **Internet Gateways** (highlighted in yellow), Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, 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 is titled 'Resources' and shows a list of resources in the Asia Pacific (Mumbai) region: 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 are operating normally. The 'Additional Information' section provides links to VPC Documentation, All VPC Resources, Forums, and Report an Issue. The footer includes a Feedback button, English (US) language selection, and copyright information for Amazon Internet Services Private Ltd.

Click the Internet Gateways in VPC Dashboard,



Click “create Internet Gateway”.

In Name Tag, Type “Siva IGW”.



Then click “Yes, Create”.

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

The screenshot shows the AWS VPC Dashboard for the region 'ap-south-1'. The left sidebar contains navigation links for VPC Dashboard, Virtual Private Cloud, 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. Two gateways are listed: 'Siva\_IGW' (ID: igw-e10c2a88, State: detached) and 'igw-69633500' (ID: igw-69633500, State: attached, VPC: vpc-a655a2ce). The 'Attach to VPC' button is highlighted in yellow. Below the table, the details for 'igw-e10c2a88 | Siva\_IGW' are shown, indicating it is detached from VPC vpc-a655a2ce.

Name	ID	State	VPC
Siva_IGW	igw-e10c2a88	detached	
igw-69633500	igw-69633500	attached	vpc-a655a2ce

igw-e10c2a88 | Siva\_IGW

Summary Tags

ID: igw-e10c2a88 | Siva\_IGW  
State: detached

Attached VPC ID:  
Attachment state:

We need to attach VPC into that i.e. Siva\_VPC.

In Attach to VPC, Siva\_VPC is selected,

The screenshot shows the 'Attach to VPC' dialog box. The title is 'Attach to VPC'. The instruction says 'Attach an Internet gateway to a VPC to enable communication with the Internet.' The 'VPC' dropdown is set to 'vpc-68c20900 | Siva\_VPC'. The 'Yes, Attach' button is highlighted in blue.

Attach to VPC

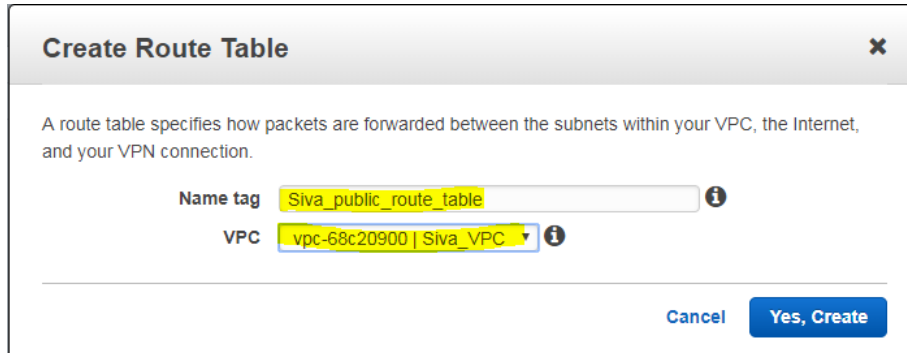
Attach an Internet gateway to a VPC to enable communication with the Internet.

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** ✕

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

Name tag  ⓘ

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. The 'Edit' button is visible next to the route table.

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”.

Route Tables | VPC Manager

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

aws Services Resource Groups

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

Security

Network ACLs

Security Groups

VPN Connections

Customer Gateways

Virtual Private Gateways

VPN Connections

Create Route Table Delete Route Table Set As Main Table

Search Route Tables and their

<< 1 to 3 of 3 Route Tables >>

<input type="checkbox"/>	Name	Route Table ID	Explicitly Associated	Main	VPC
<input checked="" type="checkbox"/>	Siva_public_route_table	rtb-be7dc3d6	0 Subnets	No	vpc-68c20900   Siva_VPC
<input type="checkbox"/>		rtb-3dab7555	0 Subnets	Yes	vpc-a655a2ce
<input type="checkbox"/>		rtb-ac8638c4	0 Subnets	Yes	vpc-68c20900   Siva_VPC

Cancel Save

View: All rules

Destination	Target	Status	Propagated	Remove
10.0.0.0/16	local	Active	No	

Add another route

Feedback English (US)

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

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 interface for the 'Route Tables' section. The left sidebar contains a navigation menu with options like 'Virtual Private Cloud', 'Route Tables', 'Internet Gateways', etc. The main content area displays a list of route tables. The 'Siva\_public\_route\_table' is selected, and a modal window is open to add a new route. The 'Destination' field is set to '0.0.0.0/0' and the 'Target' field is set to 'igw-e10c2a88'. The 'Status' is 'Active' and 'Propagated' is 'No'. The 'Save' button is highlighted.

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	
0.0.0.0/0	igw-e10c2a88	No	No	*

Then Click "Save".

In Subnet associations, click edit option.



The screenshot displays the AWS VPC console interface. On the left, the navigation pane shows various VPC resources, with 'Route Tables' highlighted. The main content area shows a list of route tables. The 'Siva\_public\_route\_table' (rtb-be7dc3d6) is selected. Below the list, the 'Subnet Associations' tab is active, showing a table with columns for Subnet, IPv4 CIDR, and IPv6 CIDR. The message 'You do not have any subnet associations.' is displayed at the bottom of the table.

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

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

In Edit option, select “Siva\_Public\_network”.

The screenshot shows the AWS Management Console interface for the 'Route Tables' section. The left sidebar contains a navigation menu with options like 'VPC Dashboard', 'Virtual Private Cloud', 'Route Tables', 'Internet Gateways', etc. The main content area displays a table of route tables. Below the table, the 'Subnet Associations' tab is active, showing a list of subnets with their associated IPv4 and IPv6 CIDR blocks and the current route table. The 'Associate' checkbox is checked for the subnet 'subnet-05333048 | Siva\_Public\_network'.

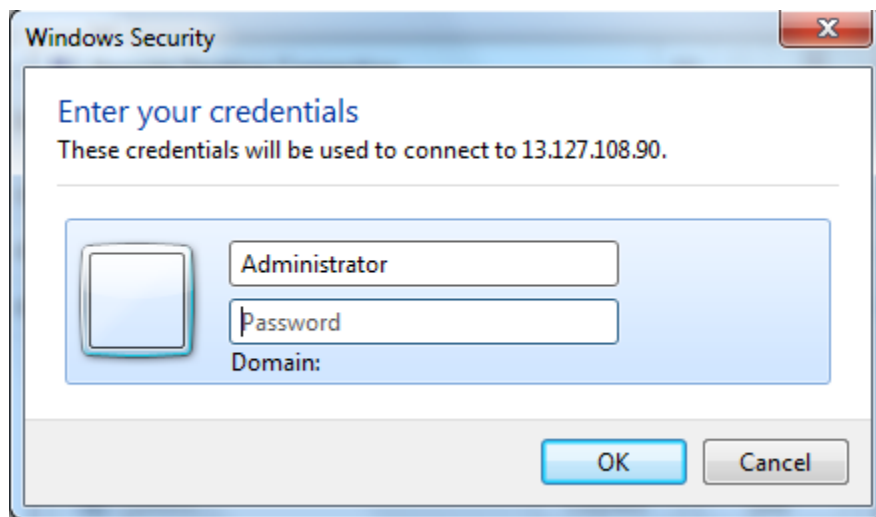
Name	Route Table ID	Explicitly Associat	Main	VPC
Siva_public_route_table	rtb-be7dc3d6	0 Subnets	No	vpc-68c20900   Siva_VPC
	rtb-3dab7555	0 Subnets	Yes	vpc-a655a2ce
	rtb-ac9638c4	0 Subnets	Yes	vpc-68c20900   Siva_VPC

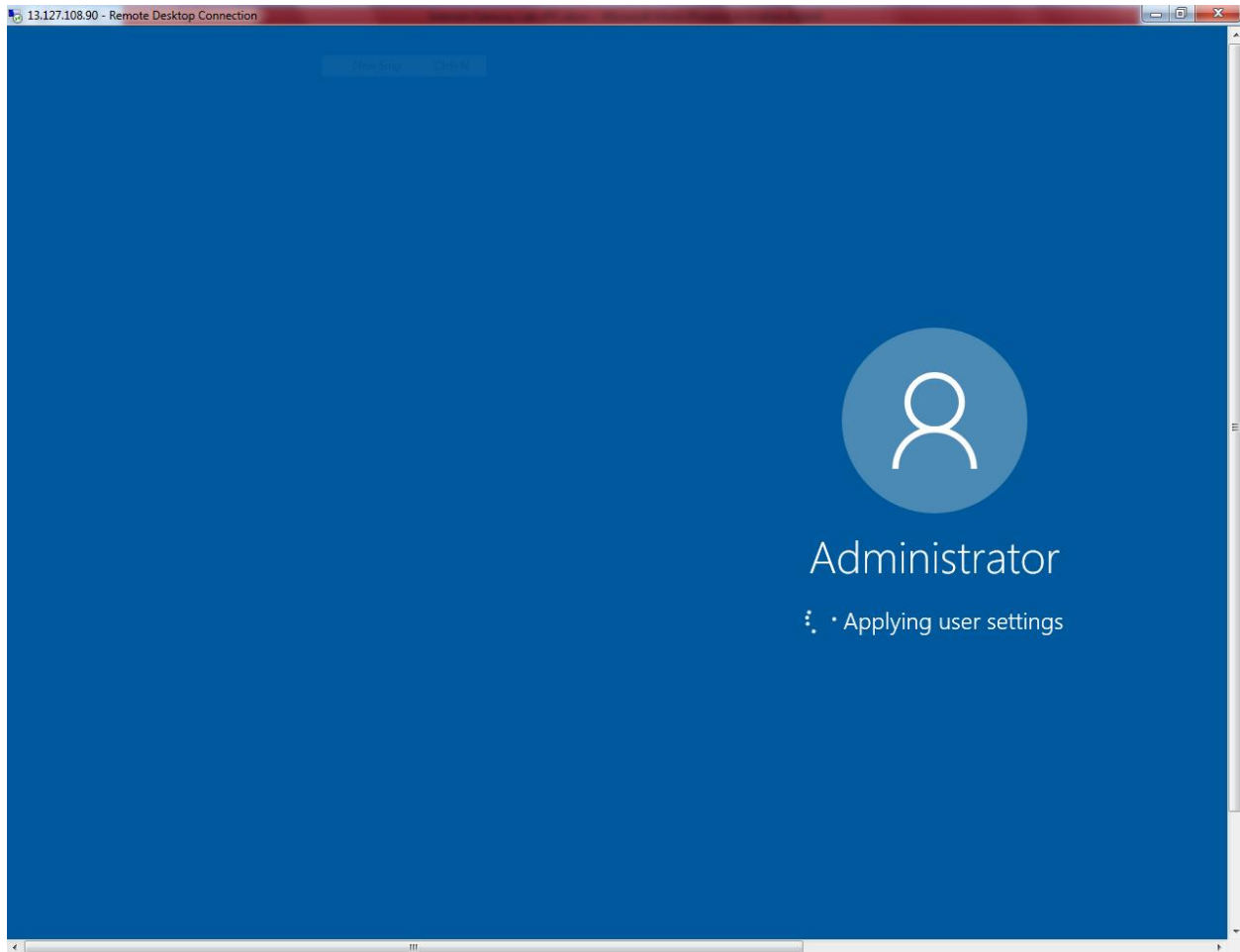
  

Associate	Subnet	IPv4 CIDR	IPv6 CIDR	Current Route Table
<input type="checkbox"/>	subnet-56f7263e   Siva_Private_network	10.0.1.0/24	-	Main
<input checked="" type="checkbox"/>	subnet-05333048   Siva_Public_network	10.0.2.0/24	-	Main

Then click save.

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





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