

Amazon Virtual Private Cloud (VPC)

What is VPC?

- Amazon VPC enables you to provision a logically isolated section of the Amazon web services (AWS) cloud where you can launch AWS resources (EC2, DB etc) in a virtual network that you define.
- This virtual network closely resembles a traditional network that you'd operate in your own datacenter.

Why it is used?

- You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can use both IPv4 and IPv6 in your VPC for secure and easy access to resources and applications.

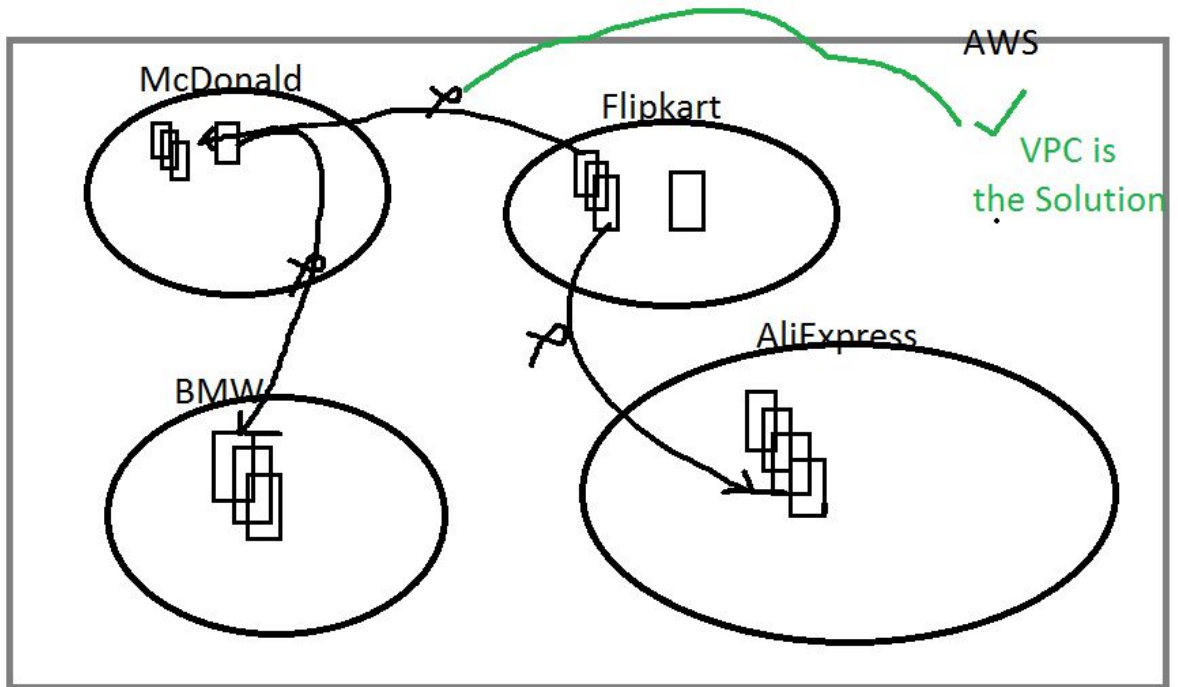
(This is like creating a Data center within our organization with the benefits of using the scalable infrastructure of AWS)

How ?

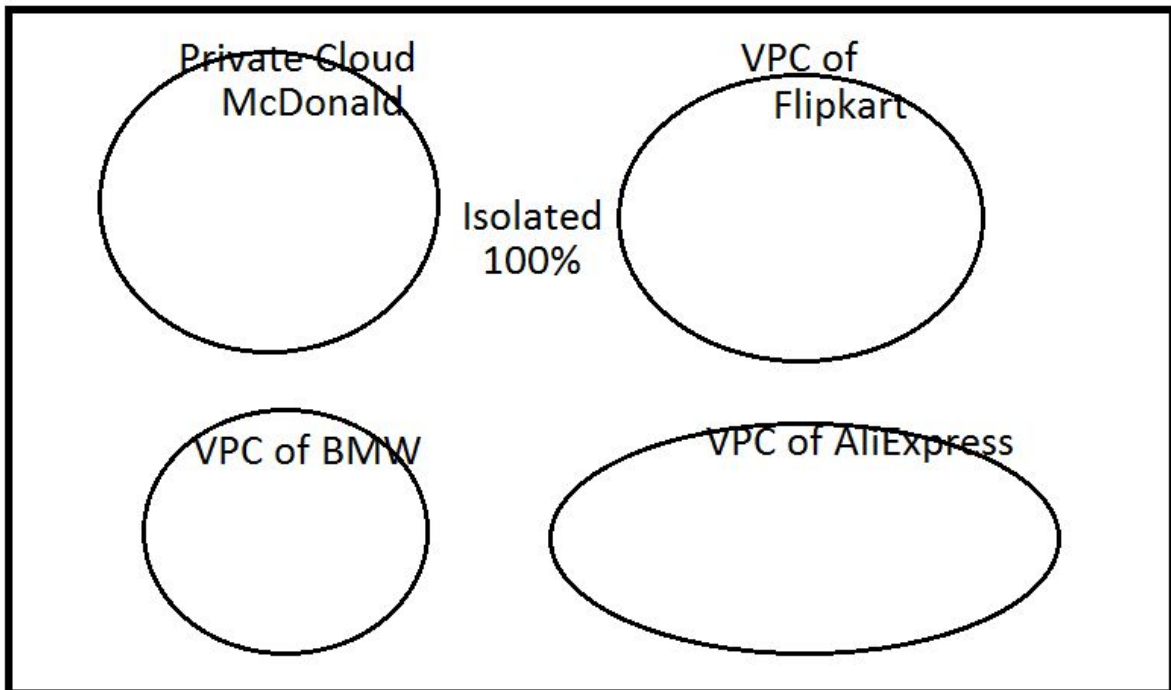
With few clicks if you know the basic concept of networking

Purpose

- Logically isolate network for AWS resources
- Logically secure yourself from other tenants
- Provides security
- Isolation



There was a possibility that other tenants can compromise the security of your network hence AWS given a solution of Virtual Private Cloud. without VPC you can't use EC2 services



Key Concepts

VPC : A Virtual Private Cloud is a sub cloud inside the AWS public cloud. Sub-cloud means it is inside an isolated logical network.

→ Other servers can't see instances that are inside a VPC. you can launch your AWS resources, such as Amazon EC2 instances, into your VPC. You can configure your VPC, you can select its IP address range , create subnets, and configure route tables, network gateway and security settings.while doing Lab, we can use default VPC as amazon is providing that.

NOTE: By default, instances communicate between different subnets if it is in same VPC

Subnet :

- A subnet is a range of IP addresses in your VPC.
- You can launch AWS resources into the subnet that you select.
- Use a public subnet for resources that must be connected to the internet and a private subnet for resources that won't be connected to the internet.
- A subnet is a sub-network inside a VPC. An example of a subnet inside a VPC (10.123.X.Y) is 10.123.1.A/24. This means any instance that belongs to this subnet will have an IP 10.123.1.A where **A** can be anything between 2 and 254. These are also known as CIDR notations. (CIDR- Classless Inter-Domain Routing)
- CIDR is a method of assigning your IP address and defining your IP routings.
- A instance always belongs to a subnets. You cannot have an instance inside a VPC that does not belong to any subnets, while spawning instances inside AWS VPC , one must specify which subnet the instance should belong to.

Security Group :

- Act as a firewall for associated amazon EC2 instances, controlling both inbound and outbound traffic at the instance level.

Network Access Control List (ACLs)

- Act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level.

Internet Gateway

- Internet gateway allows communications between instances in your VPC and the internet.
- It is horizontally scaled, redundant, and highly available VPC component
- It therefore imposes no availability risks or bandwidth constraints on your network traffic.
- It always connected to VPC

NAT Device:

- NAT device is to enable instances in a private subnet to connect to the internet

- For example, in the case of software updates or other AWS services, but prevent the internet from initiating connections with the instances.

Route Tables

- A route table contains a set of rules, called as **routes**, that are used to determine where traffic is directed

→ Each subnet in your VPC must be associated with a route table; the table controls the routing for the subnet. A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same route table.

- Network traffic of any instance inside a subnet is dictated by a routing table.

An example of routing table is :

CIDR	--	target
10.123.X.Y/16		local
0.0.0.0/0		igw

Above example shows that any traffic destined for 10.123.X.Y IP (where X and Y can be anything from 2 to 254) will be sent directly. The rest of the traffic will be directed to igw

Network Access Control List

- It is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets.
- You might setup network ACL with rules similar to your security groups in order to add an additional layer of security to your VPC.
- Apart from routing tables, each subnet also assigned a network ACL. Network ACLs specify what type of traffic is allowed inside the subnet. By default, it might have the following rules

Rule number	port	protocol	source	action
100	ALL	ALL	0.0.0.0/0	allow

This means that all traffic is allowed within this network. You can think of Network ACL as subnet-wide security groups. They are effective while isolating subnets from each other, reducing the collision of domains etc.

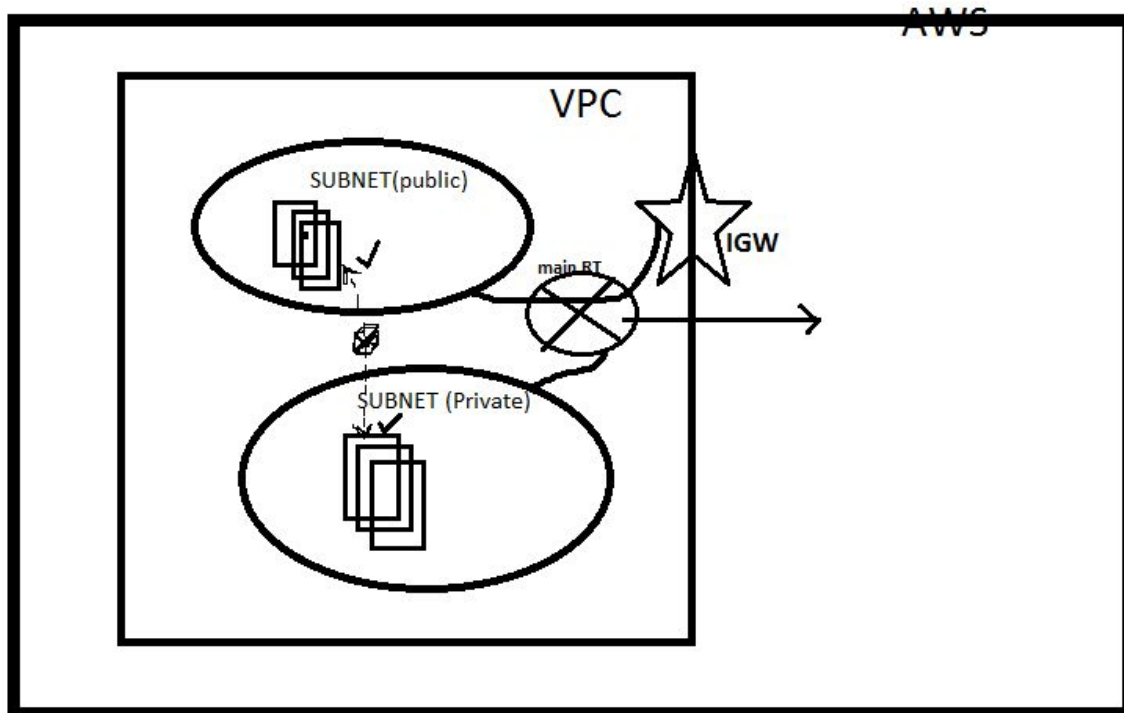
LAB

Requirement:

Some servers are publicly accessible

Some servers are on private subnet (Not reachable over internet) like Databases

WEB (PUBLIC) → DATABASE (PRIVATE)



Login to management console and then check for VPC service in Networking

You will see 1 Default VPC , 1 route table , 1 security group , 1 network ACL, 1 IGW , 6 subnets
(based on North Virginia Region)

You will see 1 default VPC, 1 Route Table, 1 Security group , 1 network ACL, 1 IGW, 2 subnets
(based on mumbai region)

VPC Dashboard

Filter by VPC:

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Resources ↻

Start VPC Wizard

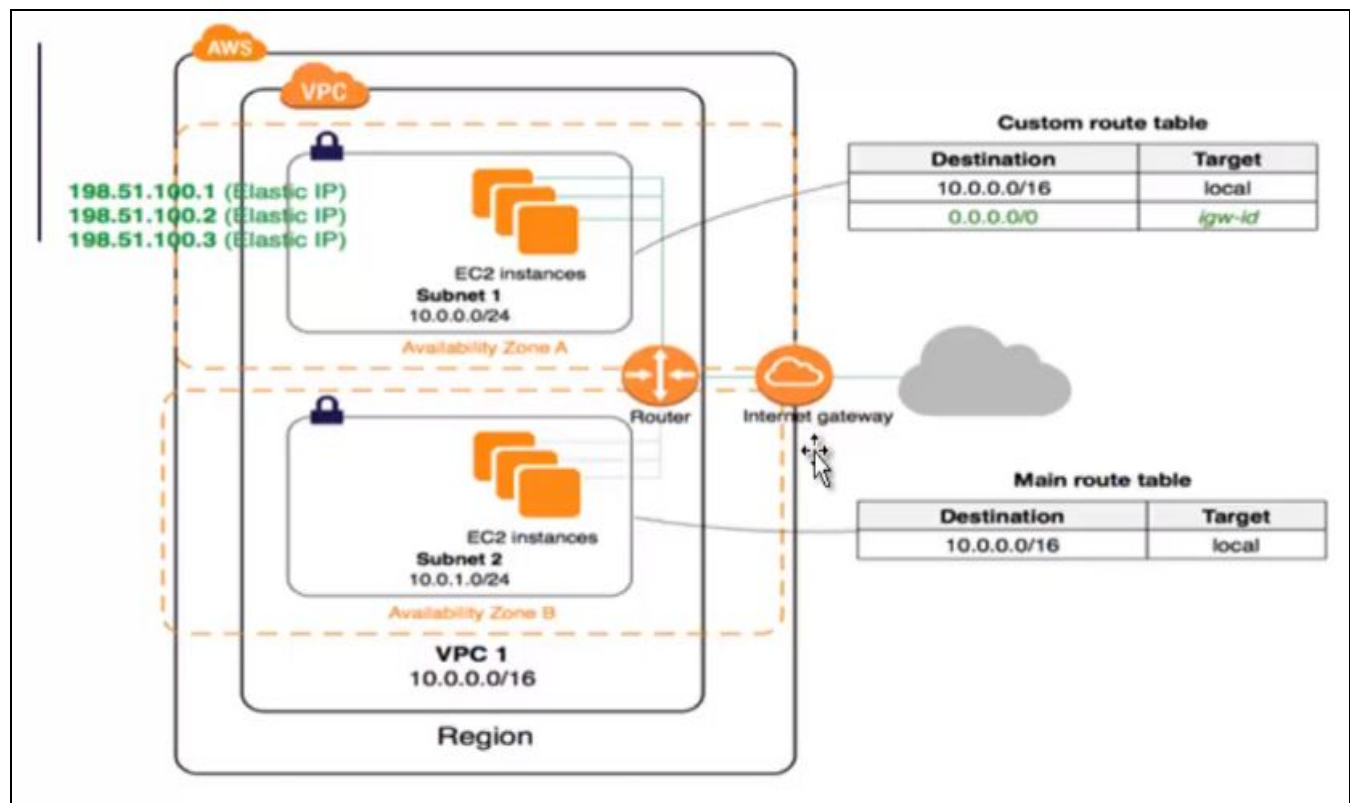
Launch EC2 Instances

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

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

1 VPC
0 Egress-only Internet Gateways
1 Route Table
0 Elastic IPs
0 Endpoints
1 Security Group
0 VPN Connections
0 Customer Gateways

1 Internet Gateway
2 Subnets
1 Network ACL
0 VPC Peering Connections
0 Nat Gateways
0 Running Instances
0 Virtual Private Gateways



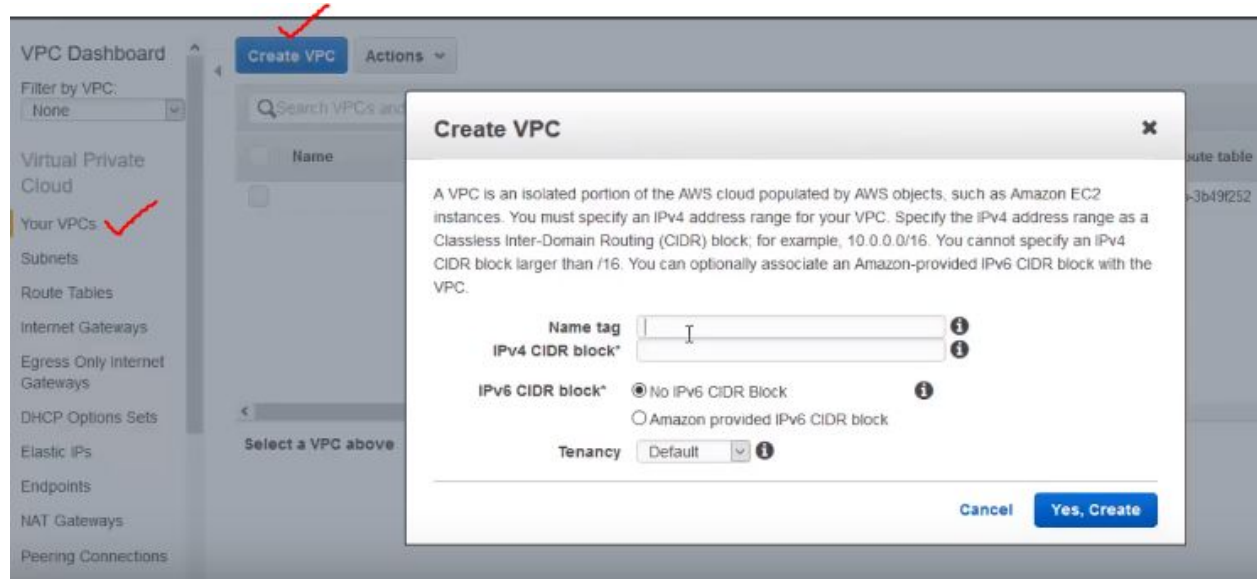
This is the architecture which we are going to implement in our AWS.

So we implement 1 VPC in a region and with 2 subnets we can give any IP range in these subnets based on our need. We make one subnet for private and other for public.

Public subnet will route out to internet but we have to place a IGW

Go to your VPC tab

Click on create VPC



Fill out the fields

Name Tag : MyVPC

IPv4 CIDR block: 10.0.0.0/16 you cannot mention as 10.0.0.0/8

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

MyVPC

IPv4 CIDR block*

IPv6 CIDR block*

Tenancy

Cancel

Yes, Create

The range of IPv4 addresses for your VPC in CIDR block format, for example, 10.0.0.0/24. Block sizes must be between a /16 netmask and /28 netmask.

As a part of VPC , **main route table** and Network ACL and Security Group also got created. But subnet and IGW will not be created.

VPC Dashboard

Filter by VPC:

None

Virtual Private Cloud

Your VPCs

Subnets

Route Tables ✓

Internet Gateways

Egress Only Internet Gateways

Create Route Table

Delete Route Table

Set As Main Table

Search Route Tables and their

	Name	Route Table ID	Explicitly Associat-	Main	VPC
		rtb-3b49f252	0 Subnets	Yes	vpc-76e85a1f
		rtb-7f3c0416	0 Subnets	Yes ✓	vpc-e1557288 MyVPC ✓

Since subnet is not created so we will create now.

Go to subnet tab and click on create subnet

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: 10.0.1.0-AP S 1A ⓘ

VPC: vpc-e1557288 | MyVPC ⓘ

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 ⓘ

The CIDR format to specify the range of IP addresses (e.g., 10.0.0.0/24) in a subnet. The range of IP addresses in the subnet must be a subset of the IP address in the VPC. Block sizes must be between a /16 netmask and /28 netmask. The size of the subnet can equal the size of the VPC.

Cancel Yes, Create

Verify

VPC Dashboard

Filter by VPC: None

Virtual Private Cloud

Your VPCs

Subnets ✓

Route Tables

Internet Gateways

Egress Only Internet Gateways

Subnet Actions

Search Subnets and their properties

<< 1 to 3 of 3 Subnets >>

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone
10.0.1.0-AP S 1A ✓	subnet-e209258b	available	vpc-e1557288 MyVPC ✓	10.0.1.0/24 ✓	4089		ap-south-1a
	subnet-e919a580	available	vpc-76e85a1f	172.31.16.0/20	4089		ap-south-1a
	subnet-0539c448	available	vpc-76e85a1f	172.31.0.0/20	4091		ap-south-1b

Create one more subnet in another AZ

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

10.0.2.0-AP S 1B

VPC

vpc-e1557288 | MyVPC

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

Verify :

VPC Dashboard

Create Subnet

Subnet Actions

Filter by VPC:

None

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

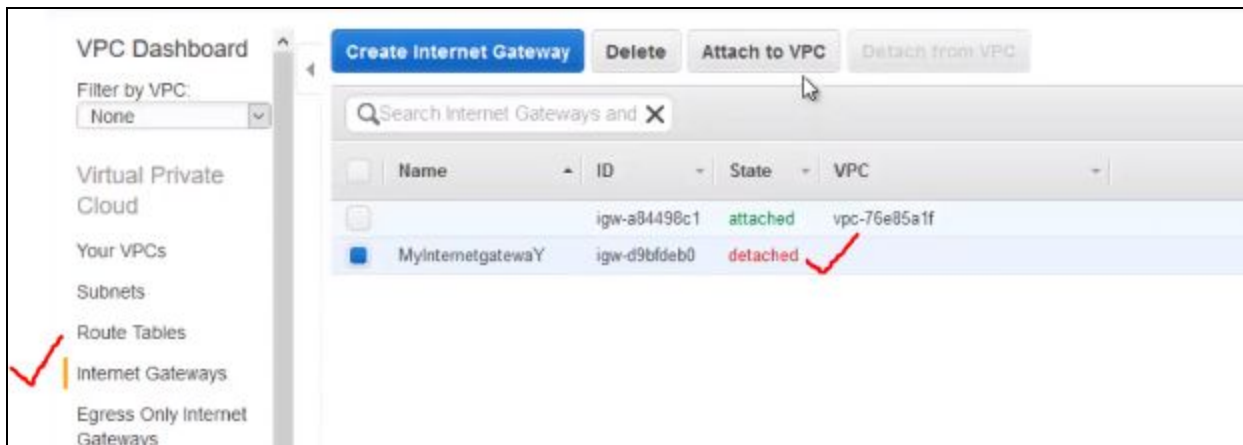
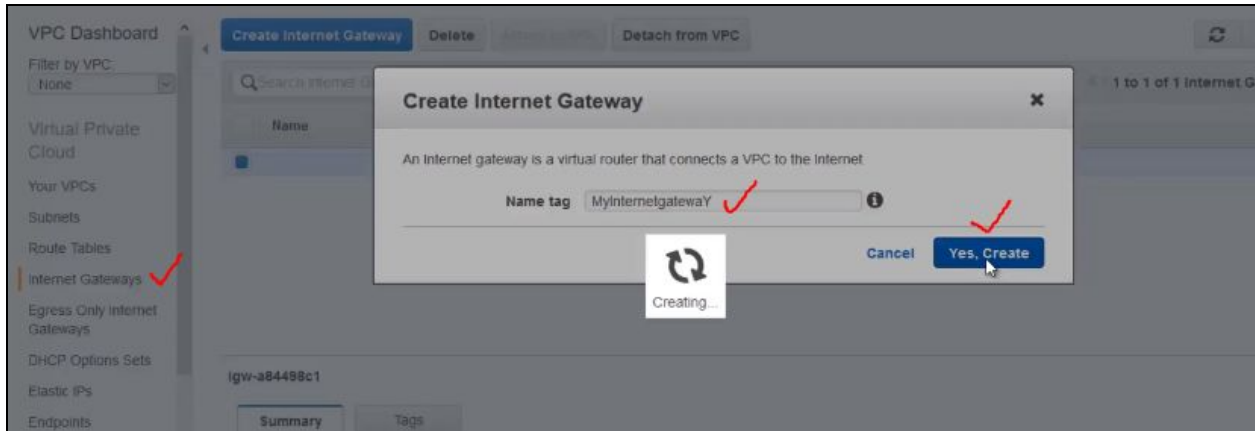
Search Subnets and their prop

1 to 4 of 4 Subnets

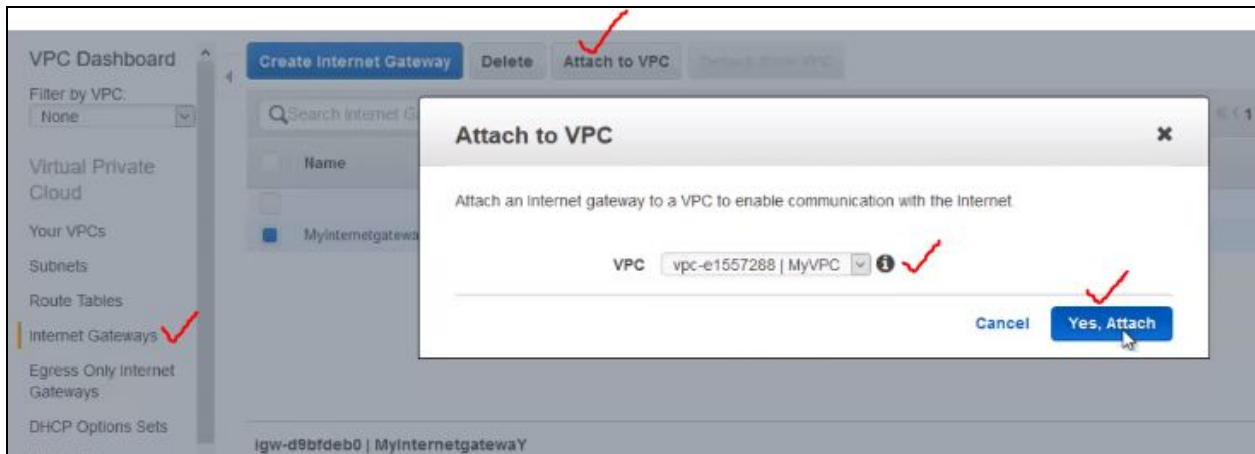
	Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability
<input type="checkbox"/>		subnet-e919a580	available	vpc-76e85a1f	172.31.16.0/20	4089		ap-south-1a
<input type="checkbox"/>	10.0.1.0-AP S 1A	subnet-e209258b	available	vpc-e1557288 MyVPC	10.0.1.0/24	251		ap-south-1a
<input checked="" type="checkbox"/>	10.0.2.0-AP S 1B	subnet-e886e3a5	available	vpc-e1557288 MyVPC	10.0.2.0/24	251		ap-south-1b
<input type="checkbox"/>		subnet-0539c448	available	vpc-76e85a1f	172.31.0.0/20	4091		ap-south-1b

Now I want to make sure 1A subnet should be public subnet. We can make it by defining IGW

Create a IGW



Now attach that IGW to VPC



Note: One VPC , it can only be attached to single IGW.
Route Table

We have to make sure that there is a route out to internet so that instances launched into the public subnet , it should have access from internet

Don't change the main route table of MyVPC

VPC Dashboard

Filter by VPC: None

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

Create Route Table Delete Route Table Set As Main Table

Search Route Tables and their X

Name	Route Table ID	Explicitly Associat-	Main	VPC
	rtb-3b49f252	0 Subnets	Yes	vpc-76e85a1f
	rtb-7f3c0416	0 Subnets	Yes ✓	vpc-e1557288 MyVPC ✓

Summary Routes Subnet Associations Route Propagation Tags

Edit

View: All rules

Destination	Target	Status	Propagated
10.0.0.0/16 ✓	local ✓	Active	No

Create a new Route table

VPC Dashboard

Filter by VPC: None

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

Create Route Table Delete Route Table Set As Main Table

Search Route Tables and their X

Create Route Table

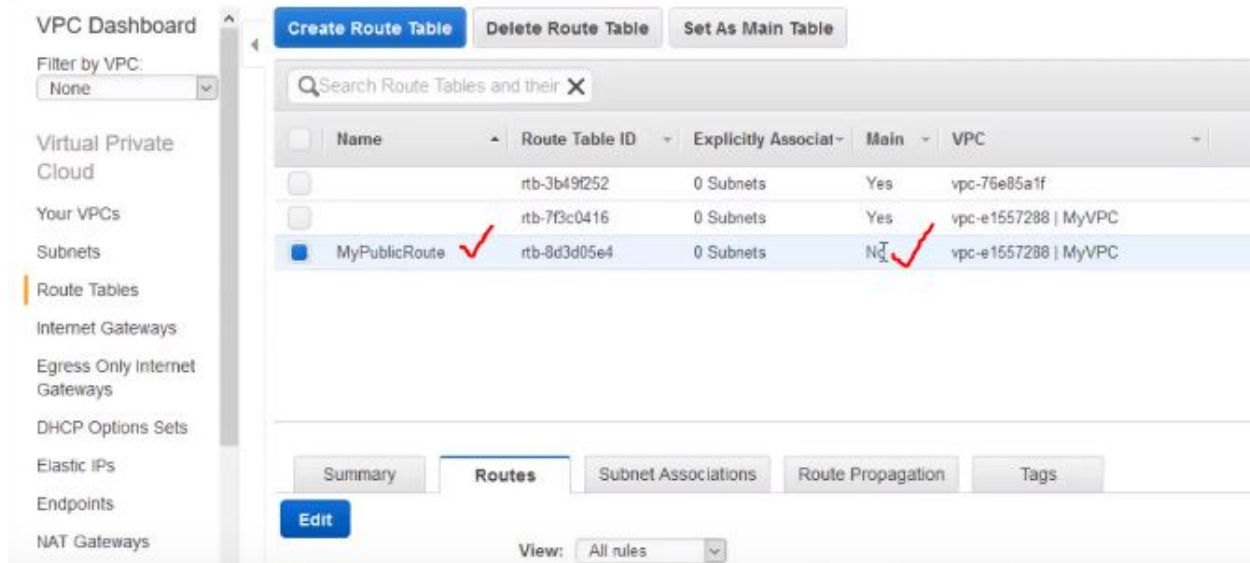
A route table specifies how packets are forwarded between the subnets within your VPC, the Internet, and your VPN connection.

Name tag MyPublicRoute

VPC vpc-e1557288 | MyVPC

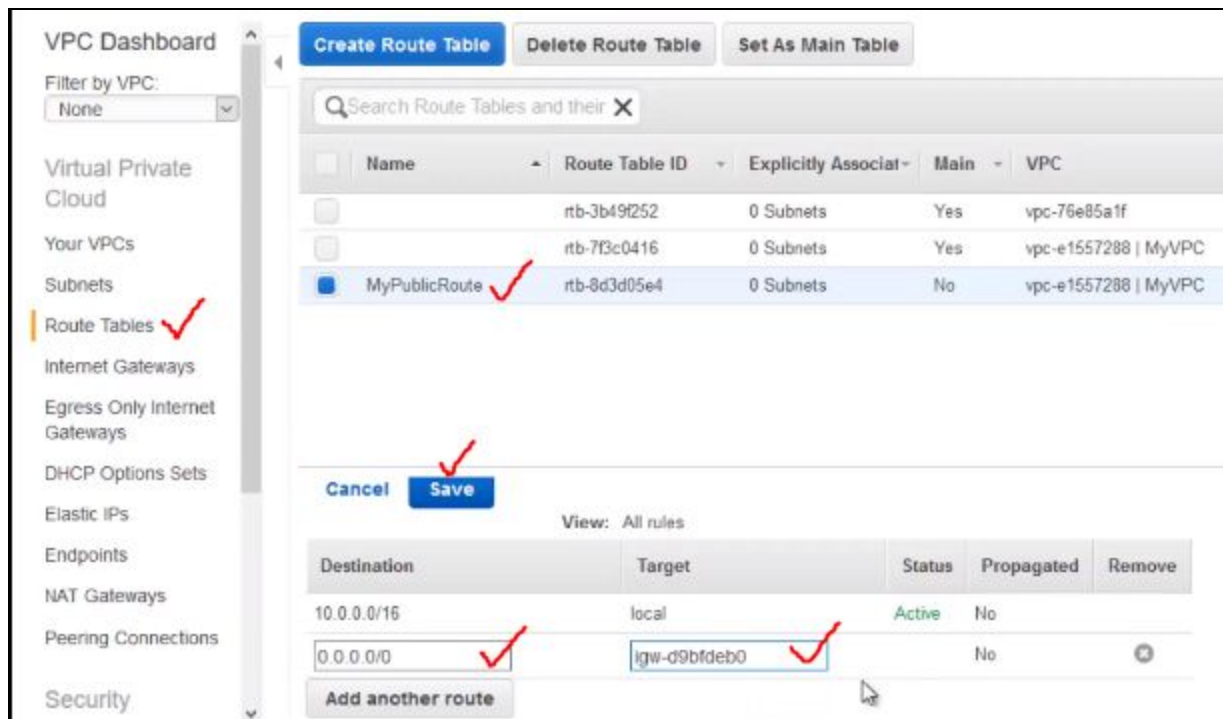
Cancel Yes, create ✓

Verify



NOW CREATE A ROUTE OUT TO INTERNET SO THAT THE TARGET IS IGW FOR THIS PARTICULAR PUBLIC SUBNET

In Route Tab , click on Edit



Now we define route
But still we did not associate to publicly created subnet.

Click on Subnet Association

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

NAT Gateways

Peering Connections

Name	Route Table ID	Explicitly Associated	Main	VPC
	rtb-3b49f252	0 Subnets	Yes	vpc-76e85a1f
	rtb-7f3c0416	0 Subnets	Yes	vpc-e1557288 MyVPC
MyPublicRoute	rtb-8d3d05e4	0 Subnets	No	vpc-e1557288 MyVPC

rtb-8d3d05e4 | MyPublicRoute

Summary Routes **Subnet Associations** Route Propagation Tags

Edit

Subnet	IPv4 CIDR	IPv6 CIDR
--------	-----------	-----------

You do not have any subnet associations.

VPC Dashboard

Filter by VPC: None

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

Create Route Table Delete Route Table Set As Main Table

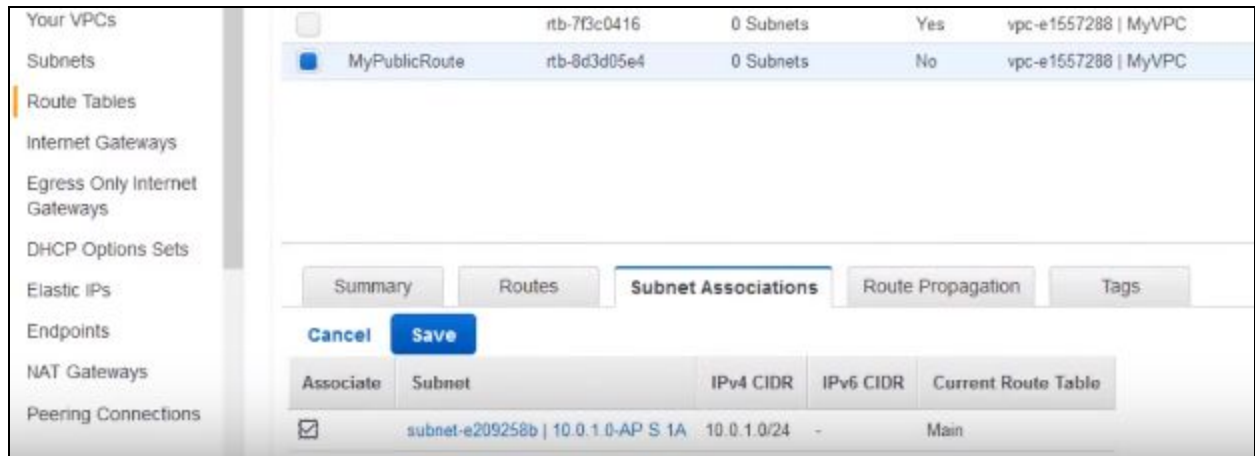
Search Route Tables and their

Name	Route Table ID	Explicitly Associated	Main	VPC
	rtb-3b49f252	0 Subnets	Yes	vpc-76e85a1f
	rtb-7f3c0416	0 Subnets	Yes	vpc-e1557288 MyVPC
MyPublicRoute	rtb-8d3d05e4	0 Subnets	No	vpc-e1557288 MyVPC

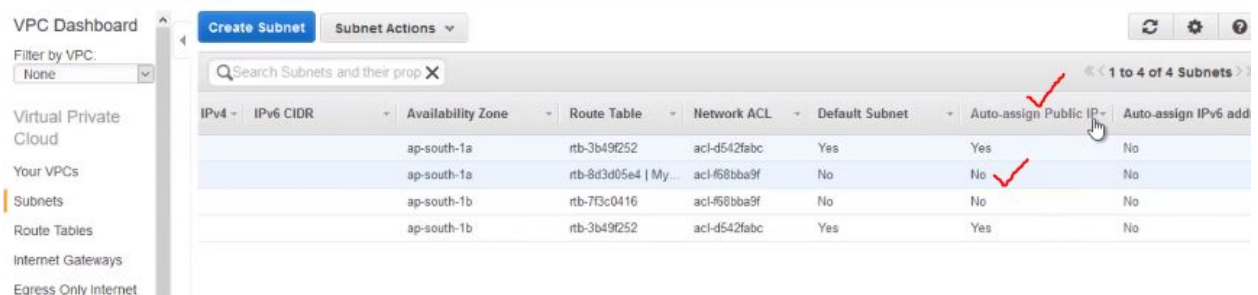
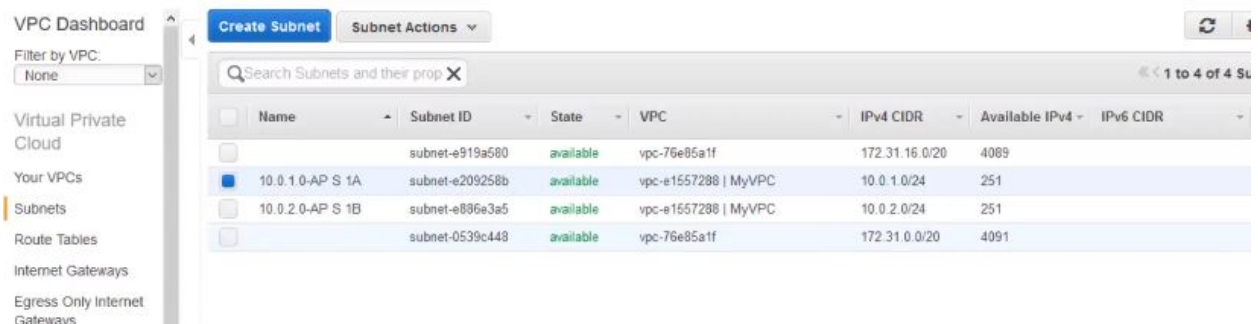
You do not have any subnet associations.

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Subnet	IPv4 CIDR	IPv6 CIDR
subnet-e209258b 10.0.1.0-AP S 1A	10.0.1.0/24	-
subnet-e886e3a5 10.0.2.0-AP S 1B	10.0.2.0/24	-



Click on Edit , select 1A and Save it



We can change that option

VPC Dashboard

Filter by VPC:

None

Virtual Private
Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Create Subnet

Subnet Actions

Search Subnets

Delete Subnet

Edit IPv6 CIDRs

Create Flow Log

Modify auto-assign IP settings

IPv4	IPv6 CIDR	Route Table	Network ACL	Default Subnet	Auto-assign Public IP
		rtb-3b49f252	acl-d542fab0	Yes	Yes
		rtb-8d3d05e4 My...	acl-f68bba9f	No	No
ap-south-1b		rtb-7f3c0416	acl-f68bba9f	No	No
ap-south-1b		rtb-3b49f252	acl-d542fab0	Yes	Yes

Create Subnet

Subnet Actions

Search Subnets

IPv4

IPv6 CIDR

Modify auto-assign IP settings

Enable auto-assign public IPv4 or IPv6 addresses to automatically request an IP address for instances launched into this subnet.

Auto-assign IPs



Enable auto-assign public IPv4 address

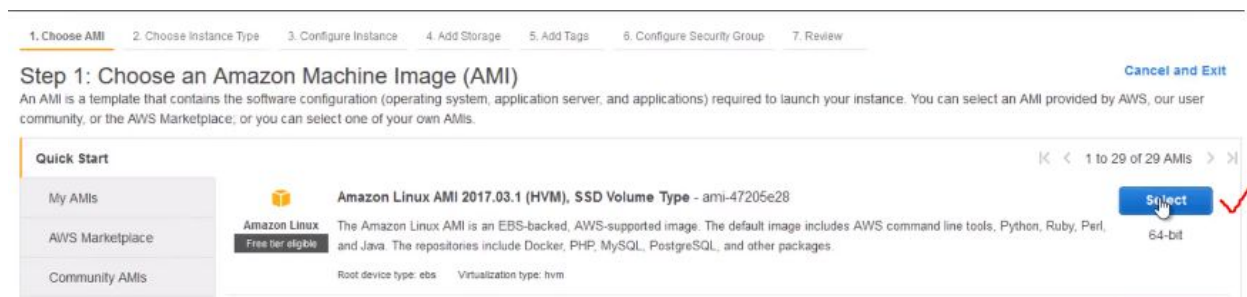
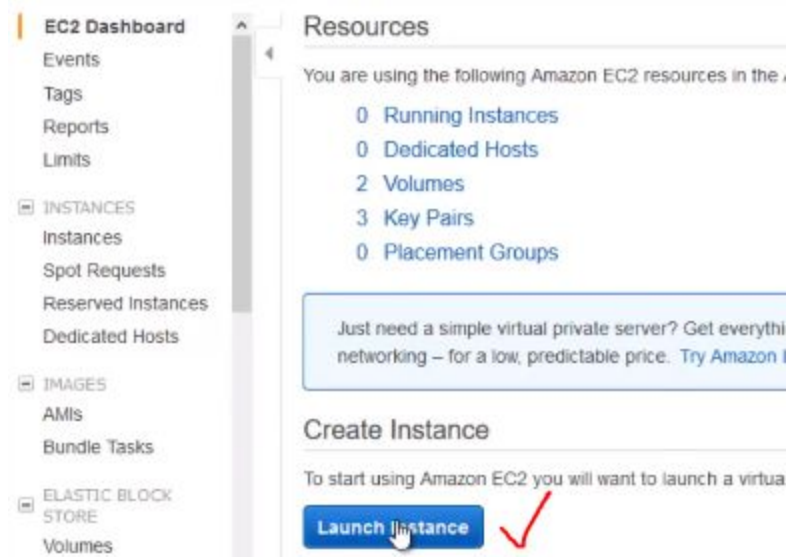
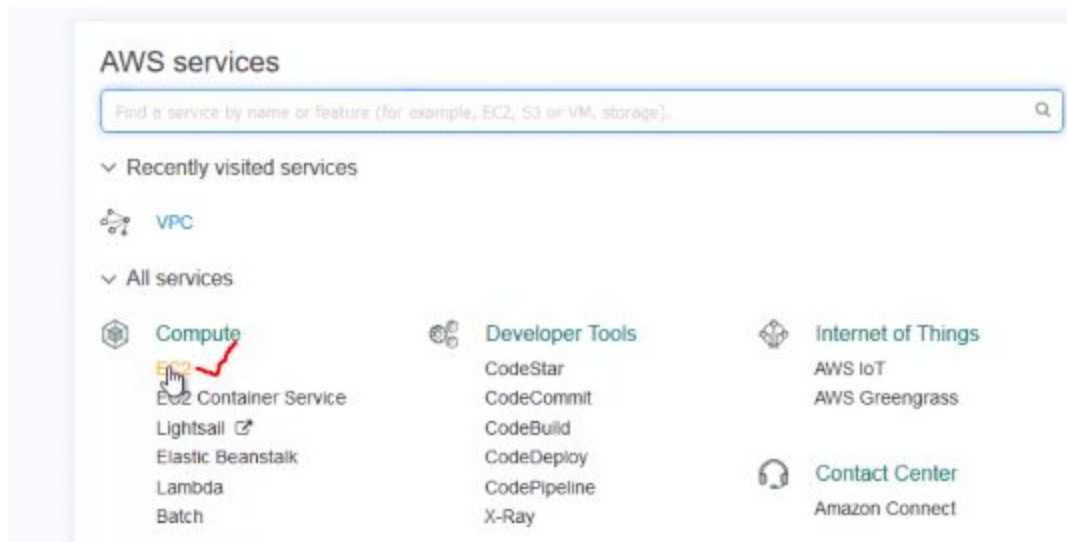


Note: You can override the auto-assign IP settings for each individual instance at launch time for IPv4 or IPv6. Regardless of how you've configured the auto-assign public IP feature, you can assign a public IP address to an instance that has a single, new network interface with a device index of eth0.

Cancel

Save

NOW Launch EC2 Instances



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

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

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 manager instance, and more.

Number of instances Launch into Auto Scaling Group

Purchasing option ☐ Request Spot instances

Network Create new VPC

Subnet Create new subnet

Auto-assign Public IP

IAM role Create new IAM role

Shutdown behavior

Enable termination protection ☐ Protect against accidental termination

Select MyVPC and public subnet

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

Additional charges will apply for dedicated tenancy.

Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-e209258t	Auto-assign	Add IP	

Add Device

Advanced Details

User data

☒ As text
☐ As file
☐ Input is already base64 encoded

```
#!bin/bash
yum install httpd -y
yum update -y
service httpd start
chkconfig httpd on
```

Cancel
Previous
Review and Launch
Next: Add Storage

Advanced Details

User data

☒ As text
☐ As file
☐ Input is already base64 encoded

```
yum install httpd -y
yum update -y
service httpd start
chkconfig httpd on
echo "<html><h1>Hello World!</h1></html>" > /var/www/html/index.html
```

Cancel
Previous
Review and Launch
Next: Add Storage

Add storage

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/xvda	snap-0a5aef08335a8992c8	8	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.

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	Webserver	<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](#)

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: WebSec ✓
Description: WebSec ✓

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ
SSH ✓	TCP	22	Custom 0.0.0.0/0
HTTP ✓	TCP	80	Custom 0.0.0.0, ::/0

[Add Rule](#)

Warning

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

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.

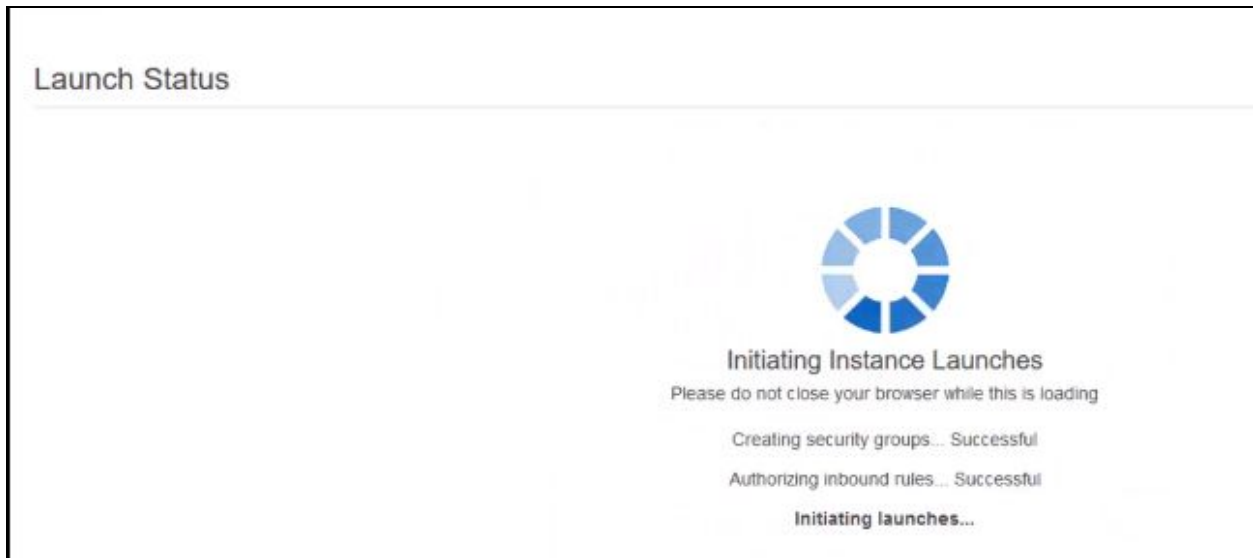
Note: The selected key pair will be added to the set of keys authorized for this instance. [Learn more](#) about [removing existing key pairs from a public AMI](#).

Create a new key pair ✓
Key pair name: WebSec ✓

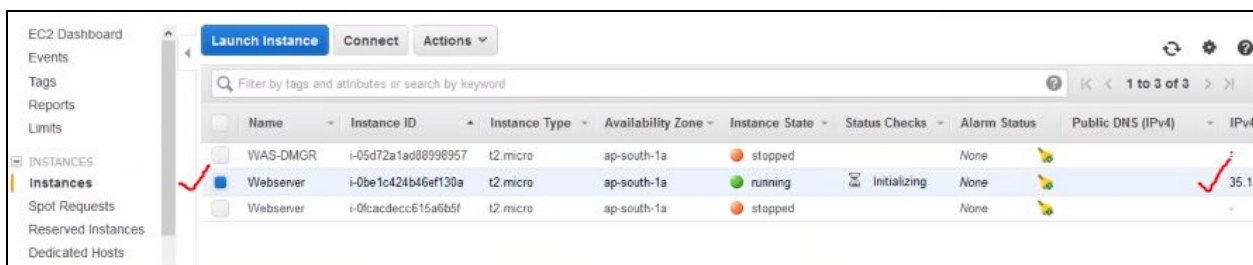
[Download Key Pair](#) ✓



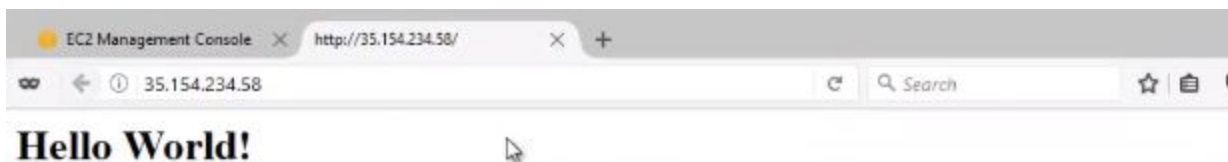
You have to download the **private key file** (*.pem file) before you can continue. Store it in a **secure and accessible location**. You will not be able to download the file again after it's created.



Now check EC2 is ready



Now try to open in browser



You will get the response as it is under public subnet

I.e from the internet, you can access ec2 instance which we place in public subnet

Launch EC2 Instance private subnet

Eg: DB instances normally inside private subnet

Select the private subnet in configuration

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

Auto-assign Public IP

IAM role Create new IAM role

Shutdown behavior

Enable termination protection ☐ Protect against accidental termination

Cancel Previous Review and Launch Next: Add Storage

In security Group, we are locking down to only public subnet

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
SSH	TCP	22	Custom 10.0.1.0/24
MYSQL/Aurora	TCP	3306	Custom 10.0.1.0/24
All ICMP - IPv4	ICMP	0 - 65535	Custom 10.0.1.0/24
All ICMP - IPv6	IPv6 ICMP	All	Custom 10.0.1.0/24

Add Rule

Cancel Previous Review and Launch

Verify

Tags
Reports
Limits

INSTANCES

Instances

Spot Requests
Reserved Instances
Dedicated Hosts

IMAGES

AMIs
Bundle Tasks

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public IP
WAS-DMGR	i-05d72a1ad88998957	t2.micro	ap-south-1a	stopped		None	
Webserver	i-0be1c424b46ef130a	t2.micro	ap-south-1a	running	2/2 checks ...	None	
MyDB	i-05d98c205bfc466b	t2.micro	ap-south-1b	running	Initializing	None	
Webserver	i-0fcacdecc615a6b5f	t2.micro	ap-south-1a	stopped		None	

EC2 Dashboard
Events
Tags
Reports
Limits

INSTANCES

Instances

Spot Requests
Reserved Instances
Dedicated Hosts

IMAGES

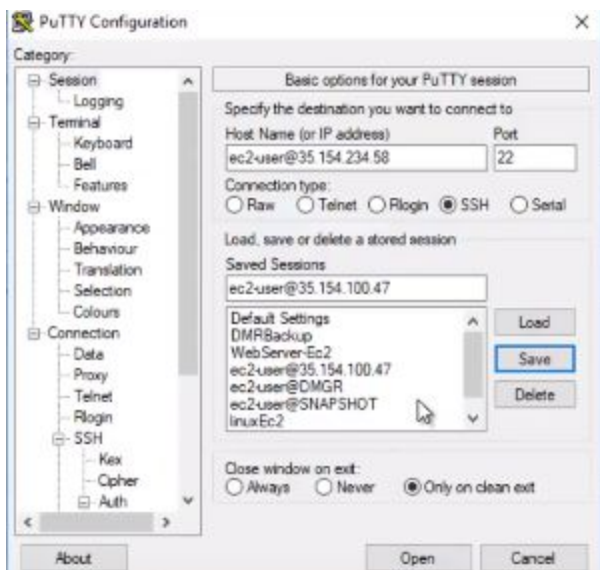
Launch Instance
Connect
Actions

Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP
t2.micro	ap-south-1a	stopped		None		
t2.micro	ap-south-1a	running	2/2 checks ...	None		35.154.234.58
t2.micro	ap-south-1b	running	Initializing	None		
t2.micro	ap-south-1a	stopped		None		

Db instance will not have any public IP address. As we did not give any public ip address enable.

We can access instances in private subnet from instances in public subnet

So first login to EC2 in public



Now try to hit the DB instance ip address

Webserver	i-0be1c424d46e1130a	t2.micro	ap-south-1a	running	2/2 checks ...	None
MyDB	i-0f5d98c205bfc466b	t2.micro	ap-south-1b	running	2/2 checks ...	None
Webserver	i-0fcacdecc615a6b5f	t2.micro	ap-south-1a	stopped		None

Elastic IPs		Private DNS	ip-10-0-2-46 ap-south-1 compute internal
Availability zone	ap-south-1b	Private IPs	10.0.2.46
Security groups	DBSec - view inbound rules	Secondary private IPs	
Scheduled events	No scheduled events	VPC ID	vpc-e1557288
AMI ID	amzn-ami-hvm-2017.03.1.20170523-x86_64	Subnet ID	subnet-e885e3a5

```

root@ip-10-0-1-185:/home/ec2-user
[root@ip-10-0-1-185 ec2-user]# ping 10.0.2.46
PING 10.0.2.46 (10.0.2.46) 56(84) bytes of data.
64 bytes from 10.0.2.46: icmp_seq=1 ttl=255 time=0.858 ms
64 bytes from 10.0.2.46: icmp_seq=2 ttl=255 time=0.924 ms
64 bytes from 10.0.2.46: icmp_seq=3 ttl=255 time=0.947 ms

```

Done, we are able to see the communication happen from public EC2 to private EC2 Application to DB

It happen because of Security group of DB instance (for troubleshooting purpose)

EC2 Dashboard	Create Security Group	Actions	
Events	Filter by tags and attributes or search by keyword		
Tags			1 to 10 of 10
Reports			
Limits			
INSTANCES			
Instances			
Spot Requests			
Reserved Instances			
Dedicated Hosts			
IMAGES			
AMIs			
Bundle Tasks			
ELASTIC BLOCK STORE			
Volumes			
Snapshots			
NETWORK & SECURITY			
Security Groups			
Elastic IPs			

Name	Group ID	Group Name	VPC ID	Description
<input checked="" type="checkbox"/>	sg-01228469	DBSec	vpc-e1557288	SecDB
<input type="checkbox"/>	sg-0e248266	WebSec	vpc-e1557288	WebSec
<input type="checkbox"/>	sg-1358a67b	rds-launch-wizard-1	vpc-76e85a1f	Created from the RDS Management Console
<input type="checkbox"/>	sg-1b8fe372	default	vpc-76e85a1f	default VPC security group
<input type="checkbox"/>	sg-403ac728	rds-launch-wizard	vpc-76e85a1f	Created from the RDS Management Console
<input type="checkbox"/>	sg-4588e42c	WAS-SG	vpc-76e85a1f	WAS Sec Group
<input type="checkbox"/>	sg-57ed873e	DemoSecGroup	vpc-76e85a1f	DEMO
<input type="checkbox"/>	sg-aa5b6dc2	default	vpc-e1557288	default VPC security group
<input type="checkbox"/>	sg-dbc6c1b2	Route53MumbaiSG	vpc-76e85a1f	launch-wizard-1 created 2017-04-26T11:33:49.995+05:30

SSH	TCP	22	10.0.1.0/24
Custom ICMP Rule - IPv6	All	N/A	10.0.1.0/24
MYSQL/Aurora	TCP	3306	10.0.1.0/24
All ICMP - IPv4	All	N/A	10.0.1.0/24

NAT Instances

- If you want to go from private servers to internet then you need to do translation from priv to pub
- Suppose for patching in private servers, you need to have access to internet
- You can use NAT instance in a public subnet in your VPC to enable instances in the private subnet to initiate outbound IPv4 traffic to the internet or other AWS services, but prevent the instances from receiving inbound traffic initiated by someone on the internet.
- So outbound traffic allowed - for patching or may be GIT repository connection from DB engine is the best use case for NAT instance

NAT Gateway

- Its a service offering from AWS and no need to maintain patching NAT instance, scaling up and on this things are not our headache
- We have to place the NAT gateway on public subnet

LAB:

Create a NAT gateway

Select a subnet (must be public subnet)

Create Elastic IP address

This completes the NAT gateway creation

Now goto RouteTable

Create a new private RT

---->privatenam

---->vpc name selected

Now Edit RT

Already main table line is there , add new line(to tell where to get internet)

0.0.0.0/0 ngw

Because of this it will go to the internet

Ngw already know which subnet it has to take internet

Subnet willask routetable to go internet

So very imp now is make sure in subnet association , add private subnet

Now priv subnet will get internet

Now you will be able to ping internet google