

day -4 AWS -- VPC and Dynamo DB

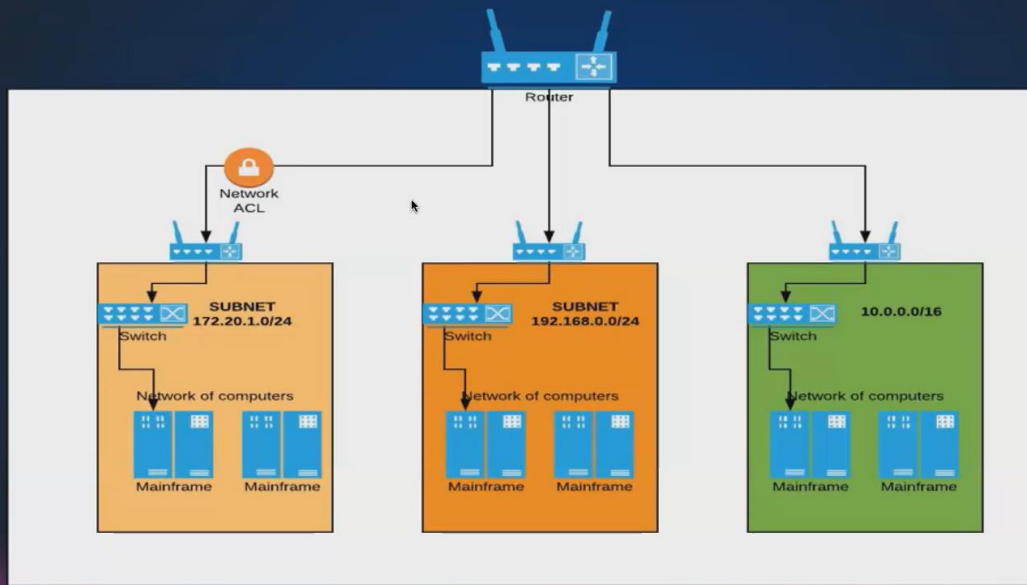
VPC:

- Vpc is a virtual private cloud
- We just logged into our aws console and we straight away. We created the resources. We launched S3 bucket. We launched ebs, we launched Ec 2 .
- What your aws will do. It will launch your resources in the default Vpc. Only if you see your Ec2 or anything, if you go and check the Vpc. It would have created in the default.

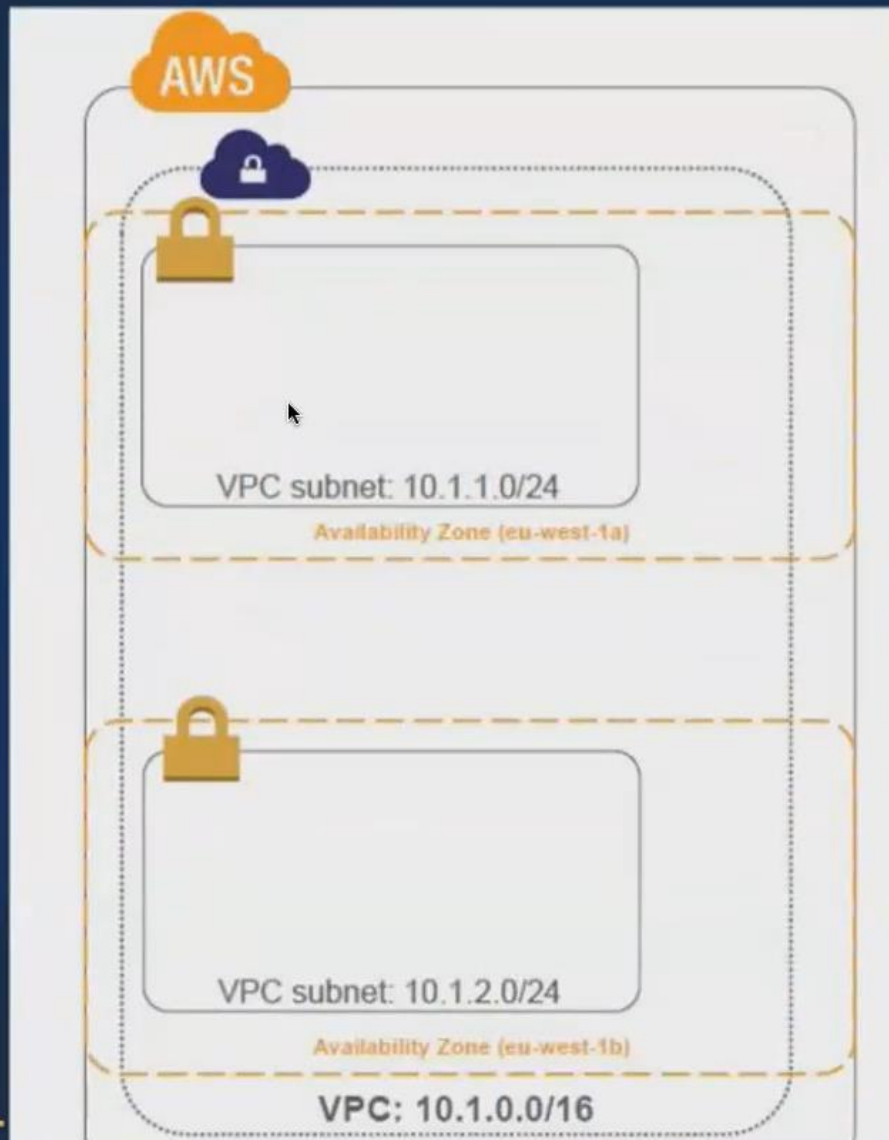
Why we are going for vpc?

- you have 2 applications, 2 different organizations. They create their Ec 2 machine. They wanted to launch their Ec2 machine in the same availability zone.
- So their privacy has been reduced. So you're sharing your application. If one application is hacked, another application will also be hacked. So in order to avoid all those things, to ensure security, every organization start by creating before launching any resource, they start by creating a Vpc.
- vpc is like a logical separation. Okay, so it is an isolated within your public cloud. You have a Aws cloud which is public
- You're creating a logical isolation for your resources. You create your isolator a small part in your aws, cloud, and launch all your aws resources within that area.
- you can define your own Vpc IP address. You can create your own subnets.
- Network divided into subnets. Each subnets have own Ip,Switches and all .

Corporate Datacenter



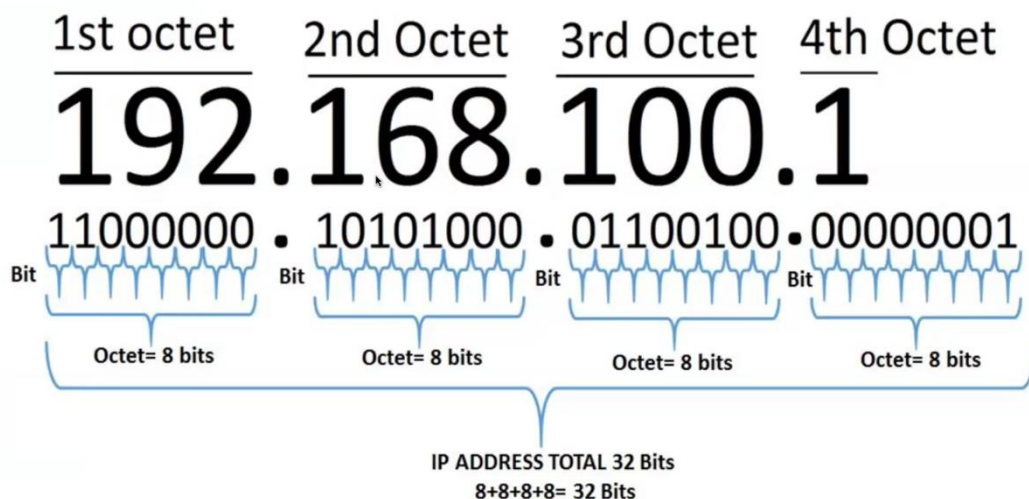
VPC Network



Virtual Private Cloud (VPC)

- VPC is a logical data center within an AWS Region.
- virtual private cloud is an on-demand configurable pool of shared computing resources allocated within a public cloud environment.
- Control over network environment, select IP address range, subnets and configure route tables and gateways.

IPv4 Address



Public and Private IP Division

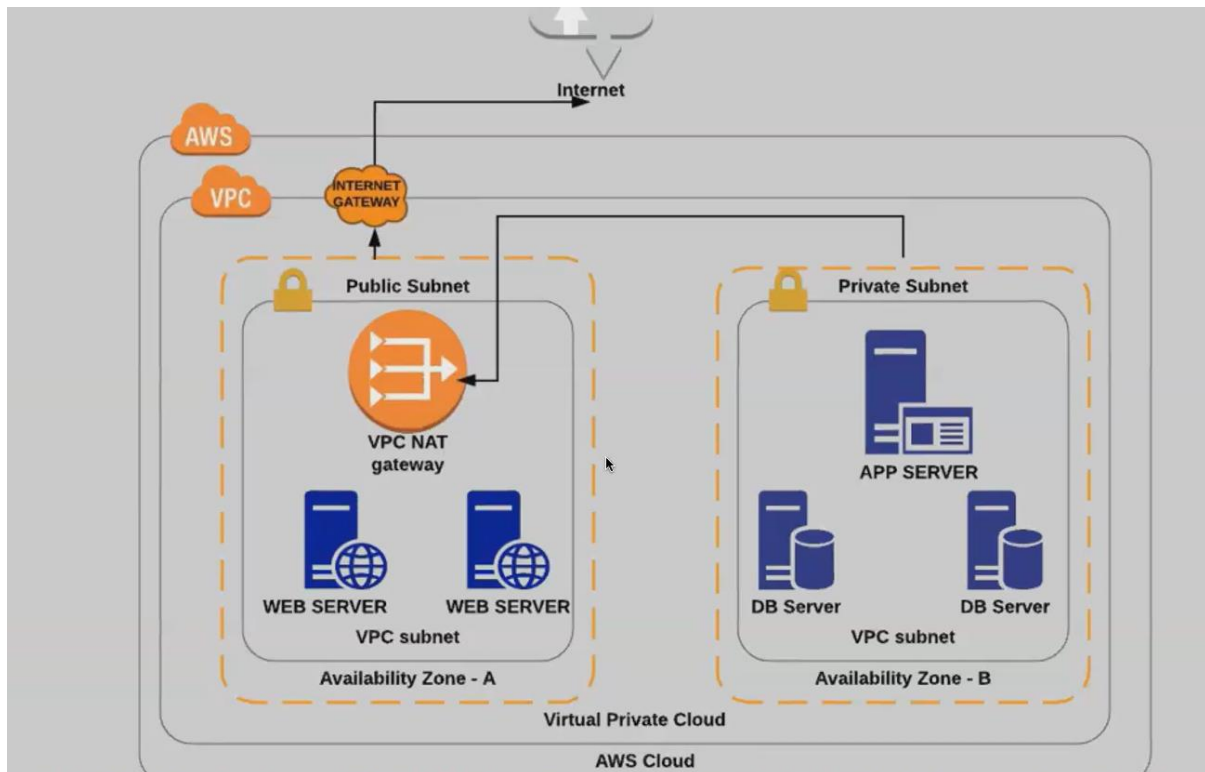
- Public IP => Internet
 - E:g 54.86.23.90
- Private IP => For local network design
 - E:g 192.168.1.10

Private IP Ranges

- Class A 10.0.0.0 - 10.255.255.255
- Class B 172.16.0.0 - 172.31.255.255
- Class C 192.168.0.0 - 192.168.255.255

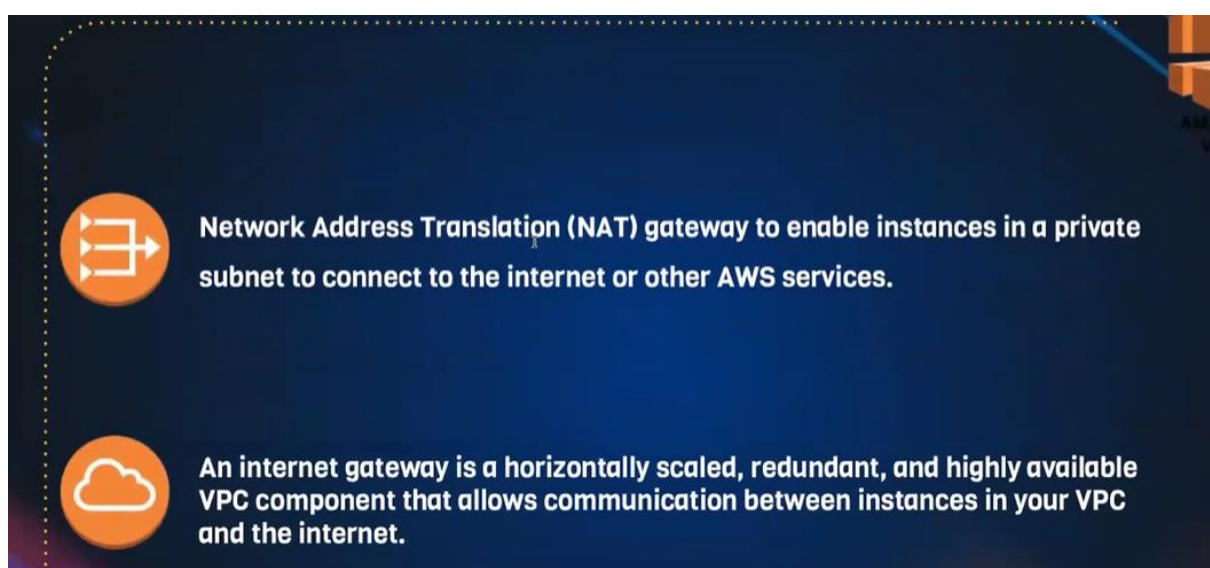
Aws will decide by default. It will assign the IP address for your ec2.

when you're creating your own Vpc. You can decide the IP address, range, and how many IP address.

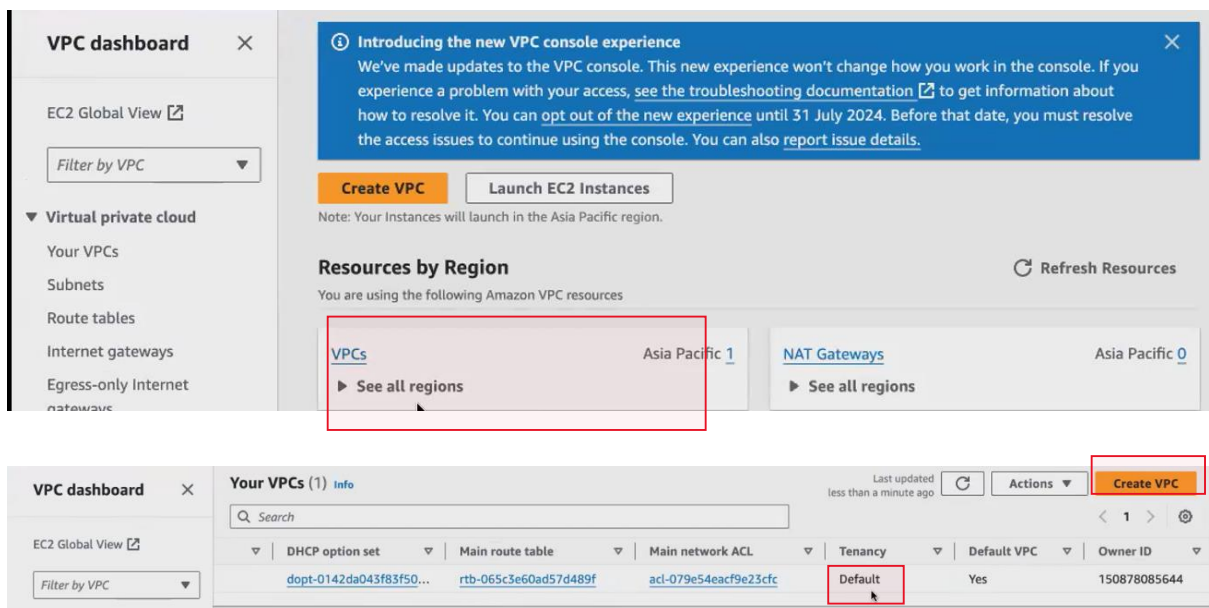
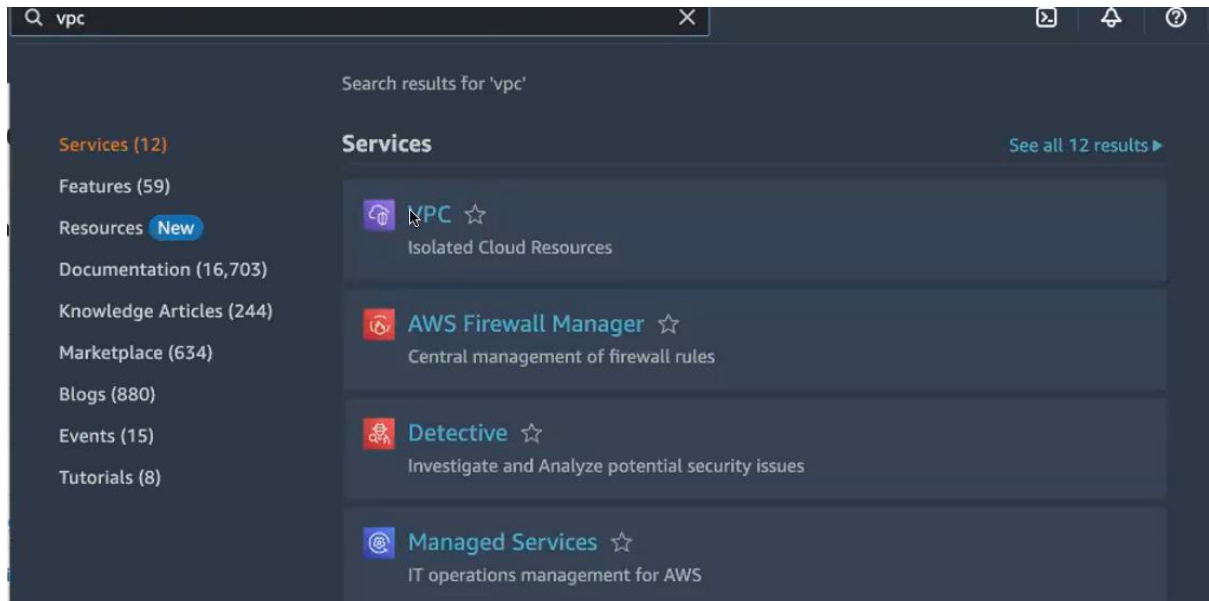


- **Aws cloud within the Aws, we launch the Vpc within Vpc, you launch subnets, you can launch multiple subnets. So you can launch either a public subnet or a private subnet.**
- **If you're launching a public subnet, public subnet can connect with the Internet.**
- **Public subnet means the resources that we are launching inside the public subnet can talk to the Internet how they can talk.**
- **They can talk with the help of Internet gateway. So you have to launch a component called Internet Gateway.**
- **So with the help of Internet gateway, the resources that we have placed inside the public subnet.**
- **certain resources you want to restrict from the outside world. So those resources you place it inside private subnet. for example: web application**
- **in web application. You have a front end. You have an application layer, and you have a database layer. Obviously, front end has to communicate with the outside world. Okay, where in your application layer, where you write all your logic, your database layer.**

- everything has to be kept private, so you cannot. You cannot allow outside world to access your applications. Logic for the database. So we place our database server and the application server inside the private subnet, so that no anyone through the Internet cannot access your resources, that if we are placing it inside the private subnet.
- if you want to connect. So here you only have the outbound traffic, which means, if my database wants to do a update or do a patchwork in that case, it has to connect with the Internet. So during that time only your in private subnet can connect with the Internet that do not directly it has to connect with an At gateway and via Nat Gateway. You will be connecting to the Internet gateway. Nat Gateway means network address translation.
- So this Nat gateway. What it will do. It will hide your resources. That is your database Ec2. It will not expose the IP address of your database to machine. Instead, it will it will mask the IP address, and it will connect with the Internet, so that just to protect us for the security reason.
- if you're using a Nat gateway, your address will be translated, it will assign a elastic IP address, a different IP address will be assigned, and it will be communicating to the Internet.
- 2 types of gateways:
 - 1. Nat gateway
 - 2. Internet gateway



How to create VPC:



This is default vpc. But we create vpc

VPC settings

Resources to create [Info](#)
Create only the VPC resource or the VPC and other networking resources.

☐ VPC only
 ☒ VPC and more

Name tag auto-generation [Info](#)
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

☒ Auto-generate

IPv4 CIDR block [Info](#)
Determine the starting IP and the size of your VPC using CIDR notation.

CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)

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

Tenancy [Info](#)

Preview

VPC [Show details](#)

Your AWS virtual network

myvpc-vpc

Subnets (4)

Subnets within this VPC

ap-south-1a

- myvpc-subnet-public1-ap-south-1a
- myvpc-subnet-private1-ap-south-1a

ap-south-1b

- myvpc-subnet-public2-ap-south-1b
- myvpc-subnet-private2-ap-south-

Route t

Route netv

myvpc-r

myvpc-r

myvpc-r

10.0.0./16 – 65,536 ip add created

Myvpc -name of my vpc

Name tag auto-generation [Info](#)
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

☒ Auto-generate

IPv4 CIDR block [Info](#)
Determine the starting IP and the size of your VPC using CIDR notation.

CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)

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

Tenancy [Info](#)

Number of Availability Zones (AZs) [Info](#)
Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

myvpc-vpc

ap-south-1a

- myvpc-subnet-public1-ap-south-1a
- myvpc-subnet-private1-ap-south-1a

ap-south-1b

- myvpc-subnet-public2-ap-south-1b
- myvpc-subnet-private2-ap-south-

AZ 2 means 2 public and 2 private n/w created

AZ 3 means 3 public and 3 private n/w created

Number of Availability Zones (AZs) [Info](#)

Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1	2	3
---	---	---

► **Customize AZs**

Number of public subnets [Info](#)

The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0	2
---	---

Number of private subnets [Info](#)

The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0	2	4
---	---	---

► **Customize subnets CIDR blocks**

NAT gateways (\$) [Info](#)

Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

None	In 1 AZ	1 per AZ
------	---------	----------

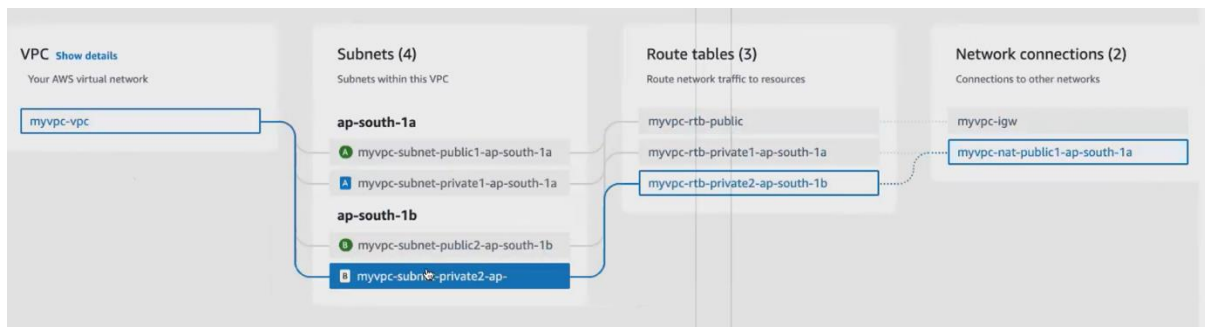
VPC endpoints [Info](#)

Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can

Nat gateway chargeable so select as 1 AZ

Vpc endpoint give none.

This is my vpc network architecture



Click create VPC all resources install one by one manually. Elastic ip is optional. Nat is enough

Details

- ✓ Create VPC: [vpc-00c1ee31a5757bbb5](#)
- ✓ Enable DNS hostnames
- ✓ Enable DNS resolution
- ✓ Verifying VPC creation: [vpc-00c1ee31a5757bbb5](#)
- ✓ Create subnet: [subnet-0ab228611b4e262a4](#)
- ✓ Create subnet: [subnet-0d7c6d5a9d81e5539](#)
- ✓ Create subnet: [subnet-0b0b58924bca6fa05](#)
- ✓ Create subnet: [subnet-0adb629a6523f9c73](#)
- ✓ Create internet gateway: [igw-0cd1456543a91d4c2](#)
- ✓ Attach internet gateway to the VPC
- ✓ Create route table: [rtb-0571508c07bbdcd72](#)
- ✓ Create route
- ✓ Associate route table
- ✓ Associate route table
- ✓ Allocate elastic IP: [eipalloc-073109dcc8fe9f7a0](#)
- ✓ Create NAT gateway: [nat-0c277b68c23639280](#)
- ✓ Wait for NAT Gateways to activate
- ✓ Create route table: [rtb-0669cca582cc16988](#)
- ✓ Create route
- ✓ Associate route table
- ✓ Create route table: [rtb-040921e43e2ec994d](#)
- ✓ Create route
- ✓ Associate route table
- ✓ Verifying route table creation

[View VPC](#)

VPC dashboard ×

EC2 Global View [↗](#)

Filter by VPC ▼

▼ Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only Internet gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

NAT gateways

Peering connections

▼ Security

Network ACLs

Security groups

VPC > Your VPCs > vpc-00c1ee31a5757bbb5

vpc-00c1ee31a5757bbb5 / myvpc-vpc Actions ▼

Details [Info](#)

VPC ID vpc-00c1ee31a5757bbb5	State Available	DNS hostnames Enabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-0142da043f83f50d0	Main route table rtb-0f96e5bae539ddd05	Main network ACL acl-0741114d17d25b0a2
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool -	IPv6 CIDR (Network border group) -
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups -	Owner ID 150878085644	

[Resource map](#) | [CIDRs](#) | [Flow logs](#) | [Tags](#) | [Integrations](#)

Resource map [Info](#)

VPC [Show details](#)
Your AWS virtual network

Subnets (4)
Subnets within this VPC

Route tables (4)
Route network traffic to resources

VPC dashboard ×

EC2 Global View [↗](#)

Filter by VPC ▼

▼ Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only Internet gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

NAT gateways

Peering connections

▼ Security

Network ACLs

Security groups

VPC > Subnets > subnet-0ea5f39b1147349a5

subnet-0ea5f39b1147349a5 Actions ▼

Details

Subnet ID subnet-0ea5f39b1147349a5	Subnet ARN arn:aws:ec2:ap-south-1:150878085644:subnet/subnet-0ea5f39b1147349a5	State Available	IPv4 CIDR 172.31.0.0/20
Available IPv4 addresses 4091	IPv6 CIDR -	Availability Zone ap-south-1b	Availability Zone ID aps1-az3
Network border group ap-south-1	VPC vpc-0a2846da1af1ddf8b	Route table rtb-065c3e60ad57d489f	Network ACL acl-079e54eac9e23cfc
Default subnet Yes	Auto-assign public IPv4 address Yes	Auto-assign IPv6 address No	Auto-assign customer-owned IPv4 address No
Customer-owned IPv4 pool -	Outpost ID -	IPv4 CIDR reservations -	IPv6 CIDR reservations -
IPv6-only No	Hostnamed type IP name	Resource name DNS A record Disabled	Resource name DNS AAAA record Disabled
DNS64 Disabled	Owner 150878085644		

Create route table to associate our public subnet to internet gateway

- now you have all the components separate. So you have your public subnet ,Internet gateway, private subnet, Nat Gateway. So we will be connecting all these things via Route Table.

VPC dashboard ×

EC2 Global View [↗](#)

Filter by VPC ▼

▼ Virtual private cloud

Your VPCs

Subnets

Route tables

Route tables (1) [Info](#)

Last updated 14 minutes ago ↻ Actions ▼ Create route table

Find resources by attribute or tag

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
<input type="checkbox"/>	-	rtb-065c3e60ad57d489f	-	-	Yes	vpc-0a2846da1af1ddf8b

Create route table [Info](#)

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

Route table settings

Name - *optional*

Create a tag with a key of 'Name' and a value that you specify.

VPC

The VPC to use for this route table.

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Value - *optional*

You can add 49 more tags.

Myvpc-vpc name my vpc

Now r.t created

How-to associate with public subnet

VPC dashboard ×

EC2 Global View

Filter by VPC ▾

▼ Virtual private cloud

- Your VPCs
- Subnets
- Route tables**
- Internet gateways
- Egress-only Internet gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- Endpoints
- Endpoint services
- NAT gateways
- Peering connections

Route table rtb-01ba69c6631e9dbaf | myvpc-rt was created successfully.

VPC > Route tables > rtb-01ba69c6631e9dbaf

rtb-01ba69c6631e9dbaf / myvpc-rt Actions ▾

Details **Info**

Route table ID rtb-01ba69c6631e9dbaf	Main No	Explicit subnet associations -	Edge associations -
VPC vpc-00c1ee31a5757bbb5 myvpc-vpc	Owner ID 150878085644		

Routes **Subnet associations** Edge associations Route propagation Tags

Explicit subnet associations (0) Edit subnet associations

Find subnet association

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
No subnet associations You do not have any subnet associations.			

VPC > Route tables > rtb-01ba69c6631e9dbaf > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/4)

Filter subnet associations

	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input checked="" type="checkbox"/>	myvpc-subnet-public1-ap-south-1a	subnet-0ab228611b4e262a4	10.0.0.0/20	-	rtb-0571508c07bbcd72
<input type="checkbox"/>	myvpc-subnet-private1-ap-south-1a	subnet-0b0b58924bca6fa05	10.0.128.0/20	-	rtb-0669cca582cc16988
<input type="checkbox"/>	myvpc-subnet-private2-ap-south-1b	subnet-0adb629a6523f9c73	10.0.144.0/20	-	rtb-040921e43e2ec994c
<input checked="" type="checkbox"/>	myvpc-subnet-public2-ap-south-1b	subnet-0d7c6d5a9d81e5539	10.0.16.0/20	-	rtb-0571508c07bbcd72

Selected subnets

subnet-0ab228611b4e262a4 / myvpc-subnet-public1-ap-south-1a × subnet-0d7c6d5a9d81e5539 / myvpc-subnet-public2-ap-south-1b ×

Cancel Save associations

we'll be creating a NAT gateway. So when you create a NAT gateway elastic IP will be created. So your eip means elastic IP address will be created. So whenever you're connecting your private, the resources with your Nat Gateway.

it will communicate will only expose the elastic IP address rather than exposing the private Ec2. Our private ip add now shown .only elastic IP address will show

VPC dashboard ×

EC2 Global View

Filter by VPC ▾

▼ Virtual private cloud

- Your VPCs
- Subnets
- Route tables
- Internet gateways
- Egress-only Internet gateways
- DHCP option sets
- Elastic IPs**

Elastic IP addresses (1) Actions ▾ Allocate Elastic IP address

Find resources by attribute or tag

	Allocated IPv4 addr...	Type	Allocation ID	Reverse DNS record	Associated inst
	13.233.59.185	Public IP	eipalloc-073109dcc8fe9f7a0	-	-

Elastic load balancer:

- aws elastic load balancer needs. So which distributes the traffic to your resources. So, for example, you're hosting application. You're hosting a web-based application in your Ec2. Mission.
- So you have some 10 Ec2 running which is hosting your application. You have a e-commerce website. And this e-commerce website is hosted in those 10 Ec2. You have user requests coming in to access the application.
- your client request will be coming in to access the application. So if, for some reason, if the traffic is high, so you have all of a sudden your application demand grows. So your user size also grows. So what happened? Your app your request? All the request goes to your Ec2 .so your aws will not know to how to route the traffic among all your Ec2 your aws will not know, aws randomly sends the traffic to any one of your Ec. 2
- you have 10 Ec2 running, so you have set the load for all the Ec2. So one Ec2 will be capable of handling only this much amount of load. It can only handle 500 requests per second.
- if the client who have you? You, you have some 100 requests, or you have some 1,000 requests hitting the same ec2 per second.
- So what will happen? Your Ec2 will go down it. It is not capable enough. It is not build enough to handle that much amount of load or that much amount of request. In that case, what we do, we build a load balancer in front of your Ec2. So you have a load balancer, and behind the load balancer, you create your service. You create your Ec2 servers, and inside the Ec2 servers, you host your application.
- you in front of all these servers you have your load, balancer. So when the clients sends the request, it will hit your load, balancer.so your load balancer, will get the request from your client, and it will distribute equally among all your Ec2
- so it will distribute the traffic. It will break down the traffic, and it will distribute it equally among all your Ec2. So instead of one machine receiving all 1,000 requests, every machine will receive 100 requests.
- So what will happen. Your machine can also respond quickly.

- We go for elastic load balancer. Elastic load Balancer means it can scale up and scale down.
- based on the applications requirement. Your aws can scale the traffic, and it can scale down the traffic also.

ELASTIC LOAD BALANCER

- Elastic Load Balancing distributes incoming application or network traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses, in multiple Availability Zones.
- Elastic Load Balancing supports three types of load balancers:
 - Application Load Balancer
 - Network Load Balancer
 - Classic Load Balancer
 - Gateway Load Balancer

before launching the load balancer, will launch some 2 Ec2.

[Add additional tags](#)

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Recents

Quick Start

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

SUSE Li

SUS

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type

Free tier eligible

ami-05e00961530ae1b55 (64-bit (x86)) / ami-072b1c33a2439c226 (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Canonical. Ubuntu. 22.04 LTS. amd64 iamvm image build on 2024-04-11

▼ Summary

Number of instances

[Info](#)

When launching more than 1 instance, consider EC2 Auto Scaling

Software Image (AMI)

Canonical, Ubuntu, 22.04 LTS, ...[read more](#)

ami-05e00961530ae1b55

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is

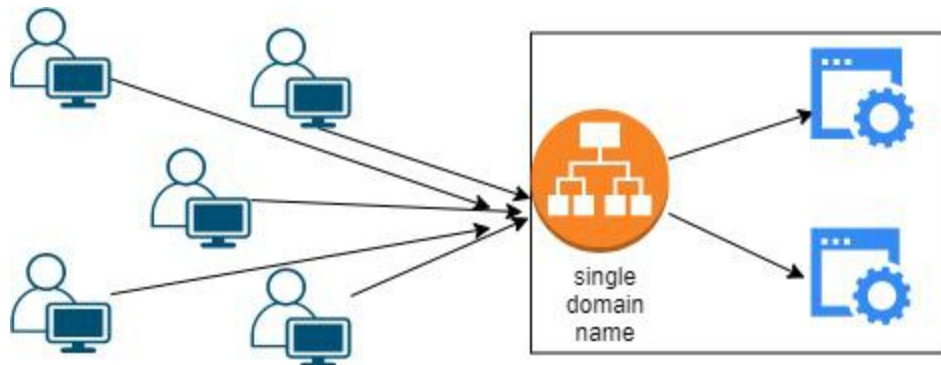
Cancel

Launch instance

https://docs.google.com/document/d/1abBZAHj0Mq5RFIb8v3lwO_fOXqgCWpquEF3-GjuK2S4/edit

Elastic load balancer

Elastic load balancer is a service provided by Amazon in which the incoming traffic is efficiently automatically distributed across a group of backend servers in a manner that increases speed and performance.



Application Load Balancer - HTTP and HTTPS traffic routing

This load balancer works at the Application layer of the OSI Model

Network Load Balancer - This type of load balancer works at the transport layer(TCP/SSL) of the OSI model.

Gateway Load Balancer - It's capable of handling millions of requests per second.

Launch ec2

Userdata amazon linux ec2

```
#!/bin/bash
sudo yum update -y
sudo amazon-linux-extras install nginx1 -y
sudo systemctl enable nginx
sudo systemctl start nginx
```

Ubuntu

```
#!/bin/bash
sudo apt update -y
sudo apt install nginx -y
sudo systemctl enable nginx
sudo systemctl start nginx
```

```
echo "<h1>Hello World from $(hostname -f)</h1>" >
/var/www/html/index.html
```

Or

```
#!/bin/bash
sudo apt update
sudo apt install apache2 wget unzip -y
wget https://www.tooplate.com/zip-
templates/2132_clean_work.zip
unzip 2132_clean_work.zip
sudo cp -r 2132_clean_work/* /var/www/html/
sudo systemctl restart apache2
```

Or

```
#!/bin/bash

# Installing Dependencies
echo "#####"
echo "Installing packages."
echo "#####"
sudo apt-get update > /dev/null
sudo apt-get install wget unzip apache2 -y > /dev/null
echo
```

```
# Start & Enable Service
echo "#####"
echo "Start & Enable Apache2 Service"
echo "#####"
sudo systemctl start apache2
sudo systemctl enable apache2
echo
```

```
# Creating Temp Directory
echo "#####"
echo "Starting Artifact Deployment"
echo "#####"
mkdir -p /tmp/webfiles
cd /tmp/webfiles
echo
```

```
wget https://www.tooplate.com/zip-templates/2098_health.zip >
/dev/null
unzip 2098_health.zip > /dev/null
sudo cp -r 2098_health/* /var/www/html/
echo
```

```
# Bounce Service
echo "#####"
echo "Restarting Apache2 service"
```

```
echo "#####"  
systemctl restart apache2  
echo
```

```
# Clean Up  
echo "#####"  
echo "Removing Temporary Files"  
echo "#####"  
rm -rf /tmp/webfiles  
echo
```

```
sudo systemctl status apache2  
ls /var/www/html/
```

```
=====
```

```
CentOs / Amazon Linux  
#!/bin/bash  
# Use this for your user data (script from top to bottom)  
# install httpd (Linux 2 version)  
yum update -y  
yum install -y httpd  
systemctl start httpd  
systemctl enable httpd  
echo "<h1>Hello World from $(hostname -f)</h1>" >  
/var/www/html/index.html
```

```
#!/bin/bash  
#install httpd  
sudo yum update -y  
sudo yum install -y httpd  
systemctl start httpd  
systemctl enable httpd  
echo "<h1>Hello World from $(hostname -f)</h1>" >  
/var/www/html/index.html
```

Steps to configure an Application load balancer in AWS:

Step 1: Launch the two instances on the AWS management console named Instance A and Instance B. Go to services and select load balancer

New EC2 Experience
Tell us what you think

Launch Instance Connect Actions

EC2 Dashboard New

Events New

Tags

Reports

Limits

INSTANCES

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts New

Scheduled Instances

Capacity Reservations

IMAGES

Security Group Name: default Add filter

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6
instanceA	i-015104070505078ef	t2.micro	us-east-1e	running	2/2 checks ...	None	ec2-100-27-3-177.com...	100.27.3.177	-
instanceB	i-0de23b37012599b...	t2.micro	us-east-1e	running	2/2 checks ...	None	ec2-52-91-122-21.com...	52.91.122.21	-

Select an instance above

Step 2: Click on create load balancer.

New EC2 Experience
Tell us what you think

Create Load Balancer Actions

Filter by tags and attributes or search by keyword

Name	DNS name	State	VPC ID	Availability Zones	Type	Create
You do not have any load balancers in this region.						

Select a load balancer

AMIs

Bundle Tasks

ELASTIC BLOCK STORE

Volumes

Snapshots

Lifecycle Manager

NETWORK & SECURITY

Security Groups New

Elastic IPs New

Placement Groups New

Key Pairs New

Network Interfaces

LOAD BALANCING

Load Balancers

Step 3: Select Application Load Balancer and click on create.

Select load balancer type

Elastic Load Balancing supports three types of load balancers: Application Load Balancers, Network Load Balancers (new), and Classic Load Balancers. Choose the load balancer type that meets your needs. [Learn more about which load balancer is right for you](#)

Application Load Balancer

HTTP
HTTPS

Create

Choose an Application Load Balancer when you need a flexible feature set for your web applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.

[Learn more >](#)

Network Load Balancer

TCP
TLS
UDP

Create

Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your application. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.

[Learn more >](#)

Classic Load Balancer

PREVIOUS GENERATION
for HTTP, HTTPS, and TCP

Create

Choose a Classic Load Balancer when you have an existing application running in the EC2-Classical network.

[Learn more >](#)

Step 4: Here you are required to configure the load balancer. Write the name of the load balancer. Choose the scheme as internet facing.

1. Configure Load Balancer 2. Configure Security Settings 3. Configure Security Groups 4. Configure Routing 5. Register Targets 6. Review

Step 1: Configure Load Balancer

Basic Configuration

To configure your load balancer, provide a name, select a scheme, specify one or more listeners, and select a network. The default configuration is an Internet-facing load balancer in the selected network with a listener that receives HTTP traffic on port 80.

Name ⓘ

Scheme ⓘ ☒ internet-facing
☐ internal

IP address type ⓘ

Listeners

A listener is a process that checks for connection requests, using the protocol and port that you configured.

Load Balancer Protocol	Load Balancer Port
<input type="text" value="HTTP"/>	<input type="text" value="80"/>
<input type="button" value="Add listener"/>	

[Cancel](#) [Next: Configure Security Settings](#)

Step 5: Add at least 2 availability zones. Select us-east-1a and us-east-1b

1. Configure Load Balancer 2. Configure Security Settings 3. Configure Security Groups 4. Configure Routing 5. Register Targets 6. Review

Step 1: Configure Load Balancer

Availability Zones

Specify the Availability Zones to enable for your load balancer. The load balancer routes traffic to the targets in these Availability Zones only. You can specify only one subnet per Availability Zone. You must specify subnets from at least two Availability Zones to increase the availability of your load balancer.

VPC ⓘ

Availability Zones

☒ us-east-1a IPv4 address ⓘ Assigned by AWS

☒ us-east-1b IPv4 address ⓘ Assigned by AWS

☐ us-east-1c

☐ us-east-1d

☐ us-east-1e


☐ us-east-1f

[Cancel](#) [Next: Configure Security Settings](#)

Step 6: We don't need to do anything here. Click on Next: Configure Security Groups

1. Configure Load Balancer 2. Configure Security Settings 3. Configure Security Groups 4. Configure Routing 5. Register Targets 6. Review

Step 2: Configure Security Settings

 **Improve your load balancer's security. Your load balancer is not using any secure listener.**
If your traffic to the load balancer needs to be secure, use the HTTPS protocol for your front-end connection. You can go back to the first step to add/configure secure listeners under [Basic Configuration](#) section. You can also continue with current settings.

[Cancel](#) [Previous](#) [Next: Configure Security Groups](#)

Step 7: Select the default security group. Click on Next: Configure Routing

1. Configure Load Balancer2. Configure Security Settings3. Configure Security Groups4. Configure Routing5. Register Targets6. Review

Step 3: Configure Security Groups

A security group is a set of firewall rules that control the traffic to your load balancer. On this page, you can add rules to allow specific traffic to reach your load balancer. First, decide whether to create a new security group or select an existing one.

Assign a security group:

☐ Create a new security group

☒ Select an existing security group

FilterVPC security groups

Security Group ID	Name	Description	Actions
<input type="checkbox"/> sg-0bb0a9bc3e885adfb	AutoScaling-Security-Group-1	AutoScaling-Security-Group-1 (2020-06-15 12:00:39.275+05:30)	Copy to new
<input type="checkbox"/> sg-0b3772fb578fb44ce	AutoScaling-Security-Group-2	AutoScaling-Security-Group-2 (2020-06-15 15:18:53.000+05:30)	Copy to new
<input checked="" type="checkbox"/> sg-103a4f3e	default	default VPC security group	Copy to new
<input type="checkbox"/> sg-0b13f451747da2fc2	launch-wizard-1	launch-wizard-1 created 2020-05-12T23:27:45.924+05:30	Copy to new
<input type="checkbox"/> sg-0458b504a37badf44	launch-wizard-10	launch-wizard-10 created 2020-06-13T14:16:46.319+05:30	Copy to new
<input type="checkbox"/> sg-0fd12e18e2b9c22d6	launch-wizard-11	launch-wizard-11 created 2020-06-15T11:38:34.722+05:30	Copy to new
<input type="checkbox"/> sg-04b735293b2ccb9a7	launch-wizard-12	launch-wizard-12 created 2020-06-15T15:10:02.695+05:30	Copy to new
<input type="checkbox"/> sg-0f3b470cd95160c71	launch-wizard-13	launch-wizard-13 created 2020-06-15T20:33:05.606+05:30	Copy to new
<input type="checkbox"/> sg-0d9a46000ea95453f	launch-wizard-2	launch-wizard-2 created 2020-05-13T05:34:24.807+05:30	Copy to new

CancelPreviousNext: Configure Routing

Step 8: Choose the name of the target group to be my-target-group. Click on Next: Register Targets.

1. Configure Load Balancer2. Configure Security Settings3. Configure Security Groups4. Configure Routing5. Register Targets6. Review

Step 4: Configure Routing

Your load balancer routes requests to the targets in this target group using the protocol and port that you specify, and performs health checks on the targets using these health check settings. Note that each target group can be associated with only one load balancer.

Target group

Target group

New target group

Name

my-target-group

Target type

☒ Instance

☐ IP

☐ Lambda function

Protocol

HTTP

Port

80

Health checks

Protocol

HTTP

Path

/

CancelPreviousNext: Register Targets

Step 9: Choose instance A and instance B and click on Add to registered. Click on Next: Review.

1. Configure Load Balancer2. Configure Security Settings3. Configure Security Groups4. Configure Routing5. Register Targets6. Review

Step 5: Register Targets

Registered targets

To deregister instances, select one or more registered instances and then click Remove.

Remove

	Instance	Name	Port	State	Security groups	Zone
<input type="checkbox"/>	i-015104070505078ef	instanceA	80	running	default	us-east-1e
<input type="checkbox"/>	i-0de23b37012599b85	instanceB	80	running	default	us-east-1e

Instances

To register additional instances, select one or more running instances, specify a port, and then click Add. The default port is the port specified for the target group. If the instance is already registered on the specified port, you must specify a different port.

Add to registered on port80

Search Instances

	Instance	Name	State	Security groups	Zone	Subnet ID	Subnet CIDR
<input checked="" type="checkbox"/>	i-015104070505078ef	instanceA	running	default	us-east-1e	subnet-28f6cc16	172.31.48.0/20
<input checked="" type="checkbox"/>	i-0de23b37012599b85	instanceB	running	default	us-east-1e	subnet-28f6cc16	172.31.48.0/20

CancelPreviousNext: Review

Step 10: Review all the configurations and click on create

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Name

load -balancer

Add additional tags

▼ Application and OS Images (Amazon Machine Image)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Q

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type

ami-0ad21ae1d0696ad58 (64-bit (x86)) / ami-01f6c796d6dbc1e36 (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type

ami-0c2af51e265bd5e0e (64-bit (x86)) / ami-0c938b21c7e598cd0 (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

Ubuntu Pro - Ubuntu Server Pro 24.04 LTS (HVM), SSD Volume Type

ami-0b2adf5ee06537f94 (64-bit (x86)) / ami-01a47a9c8e9d1db3b (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

▼ Summary

Number of instances

1

Software Image (AMI)

Canonical, Ubuntu, 24.04 LTS, ...read more

ami-0ad21ae1d0696ad58

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance

Cancel

Launch instance

Review commands

Select ubuntu latest version.click advanced set

▼ Advanced details

Domain join directory

Select

Create new directory

IAM instance profile

Select

Create new IAM profile

Hostname type

IP name

DNS Hostname

☒ Enable IP name IPv4 (A record) DNS requests

☒ Enable resource-based IPv4 (A record) DNS requests

☐ Enable resource-based IPv6 (AAAA record) DNS requests

Instance auto-recovery

Select

Shutdown behavior

Select

docs.google.com/document/d/1abBZAHj0Mq5RFIb8v3lwO_fOXgqCWpqUEF3-GjuK2S4/edit

Elastic load balancer

File Edit View Tools Help

Outline

Steps to configure an Applicatio...

```
sudo systemctl start nginx
echo "<h1>Hello World from $(hostname -f)</h1>" >
/var/www/html/index.html

Or

#!/bin/bash
sudo apt update
sudo apt install apache2 wget unzip -y
wget https://www.tooplate.com/zip-templates/2132_clean_work.zip
unzip 2132_clean_work.zip
sudo cp -r 2132_clean_work/* /var/www/html/
sudo systemctl restart apache2
```

Copy the bash script and paste it in user data

Allow tags in metadata [Info](#)

User data - optional [Info](#)

Upload a file with your user data or enter it in the field.

```
sudo apt update
sudo apt install apache2 wget unzip -y
wget https://www.tooplate.com/zip-templates/2132_clean_work.zip
unzip 2132_clean_work.zip
sudo cp -r 2132_clean_work/* /var/www/html/
sudo systemctl restart apache2
```

Services

Search

[Alt+S]

2

Allow tags in metadata

Info

Select

User data - optional

Info

Upload a file with your user data or enter it in the field.

Choose file

```

sudo apt update
sudo apt install apache2 wget unzip -y
wget https://www.tooplate.com/zip-templates/2132_clean_work.zip
unzip 2132_clean_work.zip
sudo cp -r 2132_clean_work/* /var/www/html/
sudo systemctl restart apache2

```

☐ User data has already been base64 encoded

Summary

Number of instances

Info

1

Software Image (AMI)

Canonical, Ubuntu, 22.04 LTS, ...read more

ami-0c2af51e265bd5e0e

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier:

In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance

Cancel

Launch instance

Review commands

Instances (1/2) Info

Find Instance by attribute or tag (case-sensitive)

All states

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public I
<input type="checkbox"/>	efs-vm	i-0ac64f22fb76887fc	Stopped	t2.micro	-	View alarms +	ap-south-1a	-
<input checked="" type="checkbox"/>	vpc1	i-024aa7eac737fea15	Running	t2.micro	-	View alarms +	ap-south-1a	ec2-13-

Another instance created for another application. Follow the same steps

Ubuntu

```

#!/bin/bash
sudo apt update -y
sudo apt install nginx -y
sudo systemctl enable nginx
sudo systemctl start nginx
echo "<h1>Hello World from $(hostname -f)</h1>" >
/var/www/html/index.html

```

Or

User data - optional

Info

Upload a file with your user data or enter it in the field.

Choose file

```

sudo apt update -y
sudo apt install nginx -y
sudo systemctl enable nginx
sudo systemctl start nginx
echo "<h1>Hello World from $(hostname -f)</h1>" > /var/www/html/index.html

```

☐ User data has already been base64 encoded

Software Image (AMI)

Canonical, Ubuntu, 22.04 LTS, ...read more

ami-0c2af51e265bd5e0e

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance

Cancel

Launch instance

Review commands

EC2 Dashboard

EC2 Global View

Events

Instances

Instances

Instance Types

Launch Templates

Instances (1/3)

Info

Find Instance by attribute or tag (case-sensitive)

All states

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
efs-vm	i-0ac64f22fb76887fc	Stopped	t2.micro	-	View alarms +	ap-south-1a	-
<input checked="" type="checkbox"/> vpc1	i-024aa7eac737fea15	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1a	ec2-13-
<input type="checkbox"/> vpc2	i-0de9423acc73f435d	Pending	t2.micro	-	View alarms +	ap-south-1a	ec2-65-

2 instances created for 2 diff applications

Add inbound rule for port no:80 for both instance

Inbound rules

Info

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sg-r-04bdb7229143ae894	SSH	TCP	22	Custom	0.0.0.0/0
-	Custom TCP	TCP	80	Anywh...	0.0.0.0/0

Add rule

