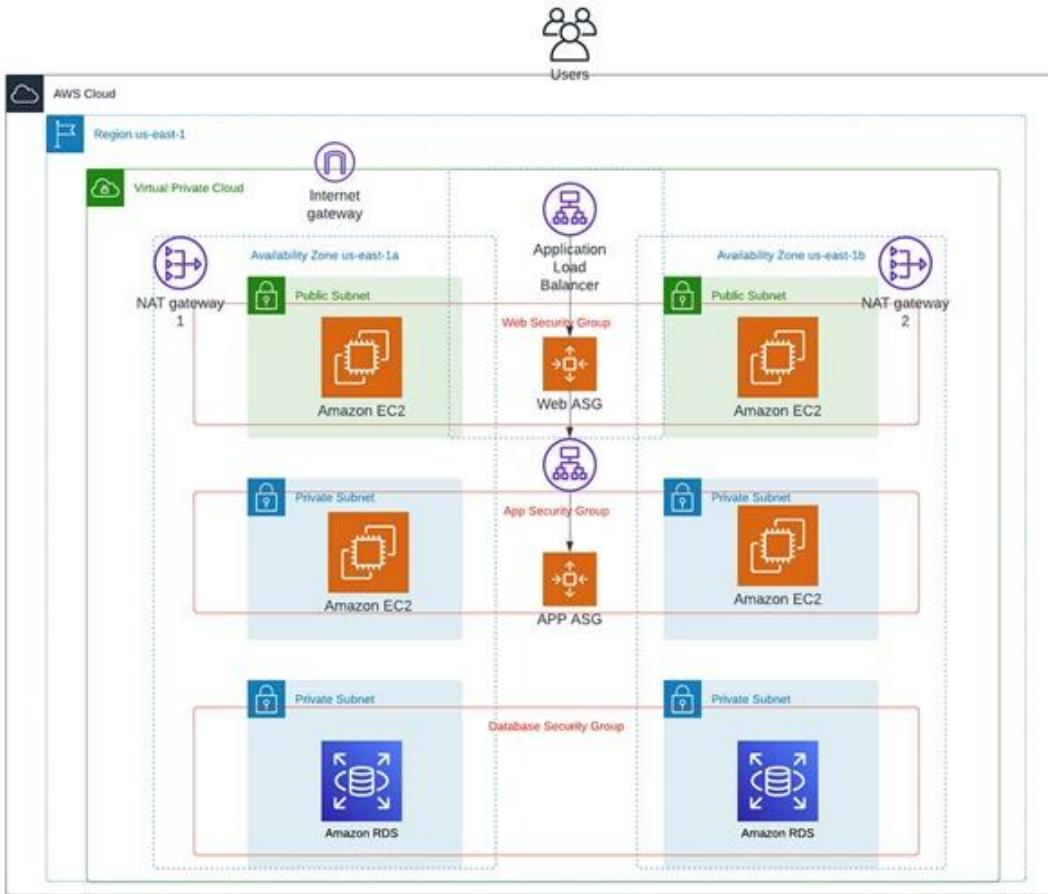


AWS THREE-TIRE ARCHITECTURE PROJECT



❖ What is a Three-Tier Architecture?

A Three-tier application architecture is a modular client-server architecture that consists three layers, namely are presentation tier, an application tier and a data tier.the presentation tier is a graphical user interface (GUI) that communicates with the other two tiers and the application tier handles logic and the data tier stores information.

❖ Benefits of a 3 Tier Architecture

1. Scalability: Each tier can scale independently, allowing organizations to optimize their resources and minimize costs.
2. Reliability: Each tier can be replicated across multiple servers, improving application availability and reliability.
3. Performance: By dividing the application into separate layers, 3-tier architecture reduces network traffic and enhances application performance.
4. Security: Each tier can have its own security group, allowing different organizations to implement customized security measures for each layer.

❖ Creating a VPC :

Log into the AWS account select California region and click the create VPC button and create VPC and I am select VPC only and give name and give CIDR block and then create VPC.

The screenshot shows the 'Create VPC' configuration page in the AWS Management Console. The 'VPC settings' section is active. Under 'Resources to create', the 'VPC only' option is selected. In the 'Name tag - optional' field, 'my-vpc-01' is entered. The 'IPv4 CIDR block' field contains '30.0.0.0/16'. Under 'IPv6 CIDR block', the 'No IPv6 CIDR block' option is selected. A green success message at the bottom states: 'You successfully created vpc-0ed1a6944be421ee3 / my-vpc-01'.

❖ Create subnets:

1. Click on SUBNETS & Click on create subnet & choose VPC ID (Own VPC not Default).
2. give subnet name & select availability zone (1b or 1c) & give IPv4 subnet CIDR BLOCK .
3. click on create subnet.
4. like that create 6 subnets – 2 public subnets in 1b & 1c zone and 4 private subnets – take 2 private subnets in 1b & remaining 2 private subnets in 1c zone.
5. some snapshots of subnets are added below

aws | Services | Search [Alt+S]

VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.

vpc-0ed1a6944be421ee3 (my-vpc-01) ▾

Associated VPC CIDRs

IPv4 CIDRs
30.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
public-subnet-1

The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US West (N. California) / us-west-1b ▾

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
30.0.0.0/16 ▾

IPv4 subnet CIDR block
30.0.0.0/24 256 IPs
< > ^ v

▼ Tags - optional

⌚ You have successfully created 1 subnet: subnet-059d3050d121f4e9e

VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.

vpc-0ed1a6944be421ee3 (my-vpc-01) ▾

Associated VPC CIDRs

IPv4 CIDRs
30.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
public-subnet-2

The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US West (N. California) / us-west-1c ▾

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
30.0.0.0/16 ▾

IPv4 subnet CIDR block
30.0.10.0/24 256 IPs
< > ^ v

Create subnet Info

VPC

VPC ID

Create subnets in this VPC.

vpc-0ed1a6944be421ee3 (my-vpc-01) ▾

Associated VPC CIDRs

IPv4 CIDRs

30.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name

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

private-subnet-1

The name can be up to 256 characters long.

Availability Zone Info

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

US West (N. California) / us-west-1b ▾

IPv4 VPC CIDR block Info

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

30.0.0.0/16 ▾

IPv4 subnet CIDR block

30.0.20.10/24

256 IPs

⌚ You have successfully created 1 subnet: subnet-0d473bc4ff06ed74

VPC

VPC ID

Create subnets in this VPC.

vpc-0ed1a6944be421ee3 (my-vpc-01) ▾

Associated VPC CIDRs

IPv4 CIDRs

30.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name

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

my-private-subnet-2

The name can be up to 256 characters long.

Availability Zone Info

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

US West (N. California) / us-west-1c ▾

IPv4 VPC CIDR block Info

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

30.0.0.0/16 ▾

IPv4 subnet CIDR block

30.0.12.10/22

1,024 IPs

⌚ You have successfully created 1 subnet: subnet-00db1c6a259290775

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.

vpc-0ed1a6944be421ee3 (my-vpc-01) ▾

Associated VPC CIDRs

IPv4 CIDRs
30.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

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

private-subnet-01

The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

US West (N. California) / us-west-1b ▾

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

30.0.0.0/16 ▾

IPv4 subnet CIDR block

30.0.25.0/22 1,024 IPs

< > ^ v

⌚ You have successfully created 1 subnet: subnet-0c4f3b4304b4481c9

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.

vpc-0ed1a6944be421ee3 (my-vpc-01) ▾

Associated VPC CIDRs

IPv4 CIDRs
30.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

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

private-subnet-02

The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

US West (N. California) / us-west-1c ▾

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

30.0.0.0/16 ▾

IPv4 subnet CIDR block

30.0.23.0/24 256 IPs

< > ^ v

⌚ You have successfully created 1 subnet: subnet-0c4f3b4304b4481c9

Available subnets (2/6)						
	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID	
<input checked="" type="checkbox"/>	public-subnet-1	subnet-059d3050d121f4e9e	30.0.0.0/24	-	Main (rtb-039383d19407558bd)	
<input checked="" type="checkbox"/>	public-subnet-2	subnet-05de870c45198f4a	30.0.10.0/24	-	Main (rtb-039383d19407558bd)	
<input type="checkbox"/>	private-subnet-1	subnet-0d473bcb4ff06ed74	30.0.20.0/24	-	Main (rtb-039383d19407558bd)	
<input type="checkbox"/>	private-subnet-2	subnet-00db1c6a259290775	30.0.12.0/22	-	Main (rtb-039383d19407558bd)	
<input type="checkbox"/>	private-subnet-01	subnet-0a79cf513b111d6f	30.0.24.0/22	-	Main (rtb-039383d19407558bd)	
<input type="checkbox"/>	private-subnet-02	subnet-0c4f3b4304b4481c9	30.0.23.0/24	-	Main (rtb-039383d19407558bd)	

❖ CREATE INTERNET GATEWAY AND ATTACH TO VPC:

click on internet gateway & create internet gateway and after the creation of internet gateway, click on internet gateway , click on actions & attach it to VPC and Snapshots of internet gateway are attached below

VPC > Internet gateways > Create internet gateway

Create internet gateway Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

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

Tags - optional
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
<input type="text" value="Name"/>	<input type="text" value="internet-gateway-1"/> <input type="button" value="Remove"/>
<input type="button" value="Add new tag"/>	
You can add 49 more tags.	

The following internet gateway was created: igw-07bbdabcd62472a8b - internet-gateway-1. You can now attach to a VPC to enable the VPC to communicate with the internet.

VPC dashboard > VPC > Internet gateways > igw-07bbdabcd62472a8b

igw-07bbdabcd62472a8b / internet-gateway-1

Details <small>Info</small>		Actions <small>▲</small>	
Internet gateway ID <input type="text" value="igw-07bbdabcd62472a8b"/>	State <input checked="" type="radio" value="Detached"/>	VPC ID <input type="text" value="-"/>	Owner <input type="text" value="010928185"/>
<input type="button" value="Attach to VPC"/>		<input type="button" value="Detach from VPC"/>	
<input type="button" value="Manage tags"/>		<input type="button" value="Delete"/>	
Tags			
<input type="text" value="Search tags"/>			
Key <input type="text" value="Name"/>	Value <input type="text" value="internet-gateway-1"/>	<input type="button" value="Manage tags"/>	
Name <input type="text" value="internet-gateway-1"/>		<input type="button" value="Delete"/>	

Attach to VPC (igw-07bbdabcd62472a8b) Info

VPC
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs
Attach the internet gateway to this VPC.

X

▶ AWS Command Line Interface command

Cancel Attach internet gateway

⌚ Internet gateway igw-07bbdabcd62472a8b successfully attached to vpc-0ed1a6944be421ee3

❖ CREATE NAT GATEWAY :

- 1.click on Nat gateway & click on create.
- 2.select PRIVATE SUBNET & choose connectivity type as PUBLIIC & Allocate ELASTIC IP .
- 3.Click on create NAT GATEWAY .

⌚ Elastic IP address 54.183.39.240 (eipalloc-003672d98cb5c7150) allocated.

VPC > NAT gateways > Create NAT gateway

Create NAT gateway Info

A highly available, managed Network Address Translation (NAT) service that instances in private subnets can use to connect to services in other VPCs, on-premises networks, or the internet.

NAT gateway settings

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

The name can be up to 256 characters long.

Subnet
Select a subnet in which to create the NAT gateway.

Connectivity type
Select a connectivity type for the NAT gateway.
 Public
 Private

Elastic IP allocation ID Info
Assign an Elastic IP address to the NAT gateway.
 ▼ Allocate Elastic IP

⌚ NAT gateway nat-07d1821c78500a404 | nat-gateway-1 was created successfully.

❖ CREATE ROUTE TABLES:

1. We have to create 2 route tables – one is PUBLIC & another one is PRIVATE.

2. goto route table – click on create route- select VPC & create route table.
3. click on route- actions-edit subnet associations-select PUBLIC SUBNETS – save associations.
4. create another route table as PRIVATE.
5. Select VPC – do edit subnet associations – select 4 private subnets – save associations
6. snapshots are attached below.

[VPC](#) > [Route tables](#) > Create route table

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.

vpc-0ed1a6944be421ee3 (my-vpc-01)

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 - <i>optional</i>
<input type="text" value="Name"/>	<input type="text" value="route-table-1"/>

[Add new tag](#)

You can add 49 more tags.

[Cancel](#) [Create route table](#)

⌚ Route table rtb-0003de7af1656562 | route-table-1 was created successfully.

[VPC dashboard](#) ✖ [Edit](#)

[EC2 Global View](#) ✖ [Edit](#)

[Filter by VPC](#) ✖ [Edit](#)

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
- Encryption

Updated routes for rtb-0003de7af1656562 / route-table-1 successfully

Details

[VPC](#) > [Route tables](#) > rtb-0003de7af1656562

rtb-0003de7af1656562 / route-table-1

Details Info

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-0003de7af1656562	<input checked="" type="checkbox"/> No	-	-
VPC	Owner ID		
vpc-0ed1a6944be421ee3 my-vpc-01	010928185144		

[Actions](#) ▾

- [Set main route table](#)
- [Edit subnet associations](#)
- [Edit edge associations](#)
- [Edit route propagation](#)
- [Edit routes](#)
- [Manage tags](#)
- [Delete](#)

Routes (2)

Destination	Target	Status	Propagated
0.0.0.0/0	igw-07bdabxd62472a8b	Active	No
30.0.0.0/16	local	Active	No

VPC > Route tables > rtb-0003de7af1656562 > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/6)						
Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID		
<input checked="" type="checkbox"/> public-subnet-1	subnet-059d3050d121f4e9e	30.0.0.0/24	-	Main (rtb-039383d19407558bd)		
<input checked="" type="checkbox"/> public-subnet-2	subnet-05dc0870c45198f4a	30.0.10.0/24	-	Main (rtb-039383d19407558bd)		
<input type="checkbox"/> private-subnet-1	subnet-0d473cb4f06ed74	30.0.20.0/24	-	Main (rtb-039383d19407558bd)		
<input type="checkbox"/> private-subnet-2	subnet-00db1c6a259290775	30.0.12.0/22	-	Main (rtb-039383d19407558bd)		
<input type="checkbox"/> private-subnet-01	subnet-0a79cf513b111d6f	30.0.24.0/22	-	Main (rtb-039383d19407558bd)		
<input type="checkbox"/> private-subnet-02	subnet-0c4f3b4304b4481c9	30.0.23.0/24	-	Main (rtb-039383d19407558bd)		

Selected subnets

subnet-059d3050d121f4e9e / public-subnet-1 subnet-05dc0870c45198f4a / public-subnet-2

Cancel Save associations

VPC dashboard > VPC > Route tables > rtb-0003de7af1656562

rtb-0003de7af1656562 / route-table-1

Details		Actions	
Route table ID	Main	Explicit subnet associations	Edge associations
rtb-0003de7af1656562	No	-	-
VPC	Owner ID	Set main route table	
vpc-0ed1a6944be421ee3 my-vpc-01	010928185144	Edit subnet associations	
		Edit edge associations	
		Edit route propagation	
		Edit routes	
		Manage tags	
		Delete	

Routes (1)

Both				Edit routes	
Destination	Target	Status	Propagated		
30.0.0.0/16	local	Active	No	< 1 >	

Edit routes

Destination	Target	Status	Propagated
30.0.0.0/16	local	Active	No
Q. 0.0.0.0/0	Internet Gateway	-	No
Q. igw-07bbddabcf52472a8t	X	-	-

Add route

Updated routes for rtb-0003de7af1656562 / route-table-1 successfully
You have successfully updated subnet associations for rtb-0003de7af1656562 / route-table-1.

Cancel Preview Save changes

VPC dashboard > VPC > Route tables (4)

Route tables (4) Info

You have successfully updated subnet associations for rtb-0003de7af1656562 / route-table-1.

Route tables (4)						
Name	Route table ID	Explicit subnet associations	Edge associations	Main		
-	rtb-0c84ede73597f6526	-	-	Yes		
-	rtb-0045f60e7e4e895b6	-	-	Yes		
-	rtb-039383d19407558bd	-	-	Yes		
route-table-1	rtb-0003de7af1656562	2 subnets	-	No		

7. click on public route table – edit routes – add rules- attach internet gateway – save changes.
8. for private route table – attach Nat gateway – save changes.
9. Now go to the subnets - click on public subnet -01, click on actions – edit subnet settings – ENABLE Auto assign public IPv4 address.
10. Do the same for remaining subnets also.

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	Remove
<input type="text" value="Name"/>	<input type="text" value="private-route-table"/>	<button>Remove</button>

Add new tag
You can add 49 more tags.

[Cancel](#)[Create route table](#)

✓ Route table rtb-0acb60077e3bcd19b | private-route-table was created successfully.

rtb-0acb60077e3bcd19b / private-route-table

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-0acb60077e3bcd19b	No	-	-
VPC	Owner ID	Edge associations	Manage tags
vpc-0ed1a6944be421ee3 my-vpc-01	010928185144	-	Delete

[Actions ▾](#)

[Set main route table](#)

[Edit subnet associations](#)

[Edit edge associations](#)

[Edit route propagation](#)

[Edit routes](#)

[Manage tags](#)

[Delete](#)

Routes

Destination	Target	Status	Propagated
30.0.0.0/16	local	Active	No

Available subnets (4/6)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
public-subnet-1	subnet-059d3050d121f4e9e	30.0.0.0/24	-	rtb-0003de7af1656562 / public-route-t...
public-subnet-2	subnet-05dcce870c45198f4a	30.0.10.0/24	-	rtb-0003de7af1656562 / public-route-t...
private-subnet-1	subnet-0d473bc4ff06ed74	30.0.20.0/24	-	Main (rtb-039383d19407558bd)
private-subnet-2	subnet-0db1c6a259290775	30.0.12.0/22	-	Main (rtb-039383d19407558bd)
private-subnet-01	subnet-0a7d9cf513b111d6f	30.0.24.0/22	-	Main (rtb-039383d19407558bd)
private-subnet-02	subnet-0c4f3b4304b4481c9	30.0.23.0/24	-	Main (rtb-039383d19407558bd)

Selected subnets

subnet-0d473bc4ff06ed74 / private-subnet-1 X subnet-0db1c6a259290775 / private-subnet-2 X subnet-0a7d9cf513b111d6f / private-subnet-01 X subnet-0c4f3b4304b4481c9 / private-subnet-02 X

[Cancel](#) [Save associations](#)

✓ You have successfully updated subnet associations for rtb-0acb60077e3bcd19b / private-route-table.

VPC dashboard > VPC > Route tables > rtb-0acb60077e3bcd19b

rtb-0acb60077e3bcd19b / private-route-table

Details				Actions	
Route table ID rtb-0acb60077e3bcd19b	Main No	Explicit subnet associations 4 subnets	Edge associations -	Set main route table	
VPC vpc-0ed1a6944be421ee3 my-vpc-01	Owner ID 010928185144			Edit subnet associations	
				Edit edge associations	
				Edit route propagation	
				Edit routes	
				Manage tags	
				Delete	

Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (1)

Routes (1)				Both	Edit routes
Destination	Target	Status	Propagated		
30.0.0.0/16	local	Active	No	< 1 >	

Edit routes

Destination: 30.0.0.0/16 Target: local Status: Active Propagated: No

Routes (1):

Destination	Target	Status	Propagated
Q 0.0.0.0/0	X NAT Gateway	-	No
Q na-07d1821c78500a404	X	-	No

Add route

Cancel Preview Save changes

⌚ Updated routes for rtb-0acb60077e3bcd19b / private-route-table successfully

▶ Details

HERE I GO TO subnets and click ACTION AND EDIT SUBNET SETTINGS TO ENABLE AUTO ASSIGN PUBLIC IPV4 ADDRESS:

I need to make sure '*Enable auto-assign public IPv4 address*' for all **subnets** so we can access its resources via the Internet.

VPC dashboard > Subnets (1/8) Info

Subnets (1/8) Info					
Find resources by attribute or tag					
Name	Subnet ID	State	VPC	IPv4 CIDR	Last updated
public-subnet-1	subnet-059d3050d121fe40e	Available	vpc-0ed1a6944be421ee3 my-vpc-01	30.0.0.0/24	4 minutes ago
public-subnet-2	subnet-05dce870x45198f4a	Available	vpc-0ed1a6944be421ee3 my-vpc-01	30.0.10.0/24	
-	subnet-07f302226c64af58b	Available	vpc-092ee8fd938ae62cb	172.31.10.0/20	
-	subnet-0aded705a0ac6f58e	Available	vpc-092ee8fd938ae62cb	172.31.16.0/20	
private-subnet-1	subnet-0dd473bc4ff06ed74	Available	vpc-0ed1a6944be421ee3 my-vpc-01	30.0.20.0/24	
private-subnet-2	subnet-00d1c16a259290775	Available	vpc-0ed1a6944be421ee3 my-vpc-01	30.0.12.0/22	
private-subnet-01	subnet-0a7d9cf513b111d6f	Available	vpc-0ed1a6944be421ee3 my-vpc-01	30.0.24.0/22	

Actions

- Create subnet
- View details
- Create flow log
- Edit subnet settings
- Edit IPv6 CDRs
- Edit network ACL association
- Edit route table association
- Edit CIDR reservations
- Share subnet
- Manage tags
- Delete subnet

Edit subnet settings Info

Subnet	
Subnet ID <input type="text"/> subnet-059d3050d121f4e9e	Name <input type="text"/> public-subnet-1

Auto-assign IP settings Info

Enable AWS to automatically assign a public IPv4 or IPv6 address to a new primary network interface for an instance in this subnet.

Enable auto-assign public IPv4 address Info

Enable auto-assign customer-owned IPv4 address Info
Option disabled because no customer owned pools found.

Resource-based name (RBN) settings Info

Specify the hostname type for EC2 instances in this subnet and optional RBN DNS query settings.

Enable resource name DNS A record on launch Info

Enable resource name DNS AAAA record on launch Info

Hostname type Info

Resource name

IP name

✓ You have successfully changed subnet settings:

- Enable auto-assign public IPv4 address

NOTE: HERE SAME PROCESS TO REMAINING FIVE SUBNETS

❖ Create SECURITY GROUPS:

1.we have to create TWO security groups.

2. Go to security groups - click on create security groups- select VPC – add INBOUND (SSH & HTTP) & OUTBOUND RULES (All traffic) – click on create security group.

3.snapshots are attached below

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info

security-group-1|

Name cannot be edited after creation.

Description Info

nothing

VPC Info

vpc-0ed1a6944be421ee3 (my-vpc-01)

Inbound rules Info

This security group has no inbound rules.

Add rule

VPC > Security Groups > sg-0d5c691184de9a581 - security-group-1 > Edit inbound rules

Edit inbound rules [Info](#)
Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info					
Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info
-	SSH	TCP	22	Anywhere... ▾	<input type="text" value="0.0.0.0"/> X
-	HTTP	TCP	80	Anywhere... ▾	<input type="text" value="0.0.0.0"/> X

[Add rule](#)

Cancel [Preview changes](#) **Save rules**

⌚ Security group (sg-0d5c691184de9a581 | security-group-1) was created successfully

► Details

VPC > Security Groups > sg-0cedaa05d45f45de6 - security-group-2 > Edit inbound rules

Edit inbound rules [Info](#)
Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info					
Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info
-	SSH	TCP	22	Anywhere... ▾	<input type="text" value="0.0.0.0"/> X
-	HTTP	TCP	80	Anywhere... ▾	<input type="text" value="0.0.0.0"/> X

[Add rule](#)

Cancel [Preview changes](#) **Save rules**

⌚ Security group (sg-0cedaa05d45f45de6 | security-group-2) was created successfully

► Details

❖ NOW LAUNCH TWO TEMPLATES:

➤ FIRST TEMPLATE NAME: public-template

1. Search EC2 – Click on LAUNCH TEMPLATES – Click on CREATE LAUNCH TEMPLATES.
2. Select AMI – UBUNTU & instance type - t2. Micro (1GB- Free Tier).
3. Select KEY PAIR – a new or existing.
4. In Network Settings I am not going to specify subnets, but security group (public-security-group-1) that I am created is selected. Make sure the proper VPC is selected.
5. Snapshots of Public Template are attached below.

Launch template name and description

Launch template name - *required*

public-template

Must be unique to this account. Max 128 chars. No spaces or special characters like '&', '*', '@'.

Template version description

nothing

Max 255 chars

Auto Scaling guidance | [Info](#)

Select this if you intend to use this template with EC2 Auto Scaling

Provide guidance to help me set up a template that I can use with EC2 Auto Scaling

► [Template tags](#)

► [Source template](#)

Launch template contents

Specify the details of your launch template below. Leaving a field blank will result in the field not being included in the launch template.

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

▼ **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

 [Search our full catalog including 1000s of application and OS images](#)

Recents

Quick Start

Don't include
in launch
template

Amazon
Linux


Ubuntu


Windows


Red Hat


SUSE Li




[Browse more AMIs](#)

Including AMIs from
AWS, Marketplace and
the Community

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type

ami-0d53d72369335a9d6 (64-bit (x86)) / ami-06098d756d39a2267 (64-bit (Arm))

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

Free tier eligible

Description

Ubuntu Server 24.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Architecture

AMI ID

64-bit (x86)

ami-0d53d72369335a9d6

Verified provider

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name

[Create new key pair](#)

▼ Network settings [Info](#)

Subnet [Info](#)

[Create new subnet](#)

When you specify a subnet, a network interface is automatically added to your template.

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

 Select existing security group Create security group

Security groups [Info](#)

 [Compare security group rules](#)

Success

Successfully created public-template(lt-0a0a99d81cb5f6494).

➤ SECOND TEMPLATE NAME: private-template

1. Create same as previous template, but at SECURITY GROUP select security group-2(private –sg)
2. Snapshots of PRIVATE TEMPLATE as attached below.

Launch template name and description

Launch template name - required

Must be unique to this account. Max 128 chars. No spaces or special characters like '&', '*', '@'.

Template version description

Max 255 chars

Auto Scaling guidance [Info](#)

Select this if you intend to use this template with EC2 Auto Scaling

Provide guidance to help me set up a template that I can use with EC2 Auto Scaling

► **Template tags**

► **Source template**

Launch template contents

Specify the details of your launch template below. Leaving a field blank will result in the field not being included in the launch template.

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

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.

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

Recents | **Quick Start**

Don't include in launch template	Amazon Linux	Ubuntu	Windows	Red Hat	SUSE Linux Enterprise Server
----------------------------------	--------------	--------	---------	---------	------------------------------

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type
ami-0d53d72369335a9d6 (64-bit (x86)) / ami-06098d756d39a2267 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

Description
Ubuntu Server 24.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Architecture 64-bit (x86) | **AMI ID** ami-0d53d72369335a9d6 | **Verified provider**

Instance type [Info](#) | [Get advice](#) | [Advanced](#)

Instance type

t2.micro Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand RHEL base pricing: 0.0282 USD per Hour
On-Demand SUSE base pricing: 0.0138 USD per Hour
On-Demand Windows base pricing: 0.0184 USD per Hour
On-Demand Linux base pricing: 0.0138 USD per Hour

All generations | Compare instance types

Additional costs apply for AMIs with pre-installed software

Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name swathi | [Create new key pair](#)

Network settings [Info](#)

Subnet [Info](#)

Don't include in launch template

Create new subnet

When you specify a subnet, a network interface is automatically added to your template.

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Select existing security group | Create security group

Security groups [Info](#)

Select security groups

security-group-2 sg-0cedaa05d45f45de6 X
VPC: vpc-0ed1a6944be421ee3

Compare security group rules

Success
Successfully created private-template([lt-05392e4e8f3822307](#)).

❖ Create an Auto scaling group :

➤ LAUNCH AUTO SCALINGS GROUPS TWO:(public and private)

1.In EC2, go to autoscaling group – click on create autoscaling group.

2.give name to ASG – Select PUBLIC TEMPLATE (which is already created)

3.In network settings - choose VPC – choose 2 public subnets.

4. After that click on NEXT.

5. We have to attach LOAD BALANCER to ASG.

Choose launch template Info

Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group.

Name

Auto Scaling group name

Enter a name to identify the group.

WEB ASG

Must be unique to this account in the current Region and no more than 255 characters.

Launch template Info

i For accounts created after May 31, 2023, the EC2 console only supports creating Auto Scaling groups with launch templates. Creating Auto Scaling groups with launch configurations is not recommended but still available via the CLI and API until December 31, 2023.

Launch template

Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.

public-template



[Create a launch template](#)

Network Info

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across the zones. The default VPC and default subnets are suitable for getting started quickly.

VPC

Choose the VPC that defines the virtual network for your Auto Scaling group.

vpc-0ed1a6944be421ee3 (my-vpc-01)



[Create a VPC](#)

Availability Zones and subnets

Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.

Select Availability Zones and subnets



us-west-1b | subnet-059d3050d121f4e9e (public-subnet-1)
30.0.0.0/16



us-west-1c | subnet-05dce870c45198f4a (public-subnet-2)
30.0.10.0/24



[Create a subnet](#)

Cancel

[Skip to review](#)

[Previous](#)

[Next](#)

Load balancing Info

Use the options below to attach your Auto Scaling group to an existing load balancer, or to a new load balancer that you define.

No load balancer

Traffic to your Auto Scaling group will not be fronted by a load balancer.

Attach to an existing load balancer

Choose from your existing load balancers.

Attach to a new load balancer

Quickly create a basic load balancer to attach to your Auto Scaling group.

Attach to a new load balancer

Define a new load balancer to create for attachment to this Auto Scaling group.

Load balancer type

Choose from the load balancer types offered below. Type selection cannot be changed after the load balancer is created. If you need a different type of load balancer than those offered here, visit the [Load Balancing console](#).

Application Load Balancer

HTTP, HTTPS

Network Load Balancer

TCP, UDP, TLS

Load balancer name

Name cannot be changed after the load balancer is created.

WEB ASG-1

6.Attach load balancer- choose application load balancer- LB name should be same as ASG , if you want to edit it you can edit the name.

7.select subnets – give PORT NO: 80 for HTTP – Select TARGET GROUP (new or existing).

8.Give HEALTH CHECK GRACE PERIOD as your wish.

Load balancer scheme

Scheme cannot be changed after the load balancer is created.

Internal

Internet-facing

Network mapping

Your new load balancer will be created using the same VPC and Availability Zone selections as your Auto Scaling group. You can select different subnets and add subnets from additional Availability Zones.

VPC

vpc-0ed1a6944be421ee3 [\[Edit\]](#)

my-vpc-01

Availability Zones and subnets

You must select a single subnet for each Availability Zone enabled. Only public subnets are available for selection to support DNS resolution.

us-west-1b

subnet-059d3050d121f4e9e



us-west-1c

subnet-05dce870c45198f4a



Listeners and routing

If you require secure listeners, or multiple listeners, you can configure them from the [Load Balancing console](#) after your load balancer is created.

Protocol

Port

Default routing (forward to)

HTTP

80

Create a target group



New target group name

An instance target group with default settings will be created.

Web-Asg-1-tg

Group size Info

Set the initial size of the Auto Scaling group. After creating the group, you can change its size to meet demand, either manually or by using automatic scaling.

Desired capacity type

Choose the unit of measurement for the desired capacity value. vCPUs and Memory(GiB) are only supported for mixed instances groups configured with a set of instance attributes.

Units (number of instances) ▾

Desired capacity

Specify your group size.

2

Scaling Info

You can resize your Auto Scaling group manually or automatically to meet changes in demand.

Scaling limits

Set limits on how much your desired capacity can be increased or decreased.

Min desired capacity

2

Equal or less than desired capacity

Max desired capacity

5

Equal or greater than desired capacity

9. Select Group size We want to set a minimum and maximum number of instances the ASG can provision:

- **Desired capacity:** 2
- **Minimum capacity:** 2
- **Maximum capacity:** 5

Once the ASG is created, I can go to our EC2 dashboard and see that two EC2 instances have been deployed.

Automatic scaling - optional

Choose whether to use a target tracking policy | Info

You can set up other metric-based scaling policies and scheduled scaling after creating your Auto Scaling group.

No scaling policies

Your Auto Scaling group will remain at its initial size and will not dynamically resize to meet demand.

Target tracking scaling policy

Choose a CloudWatch metric and target value and let the scaling policy adjust the desired capacity in proportion to the metric's value.

Scaling policy name

Target Tracking Policy

Metric type | Info

Monitored metric that determines if resource utilization is too low or high. If using EC2 metrics, consider enabling detailed monitoring for better scaling performance.

Average CPU utilization

Target value

50

Instance warmup | Info

50 seconds

Disable scale in to create only a scale-out policy

EC2 > Auto Scaling groups

Auto Scaling groups (1) <small>Info</small>							<input type="button" value="C"/>	Launch configurations	Launch templates	Actions ▾	<input type="button" value="Create Auto Sca"/>
<input type="text"/> Search your Auto Scaling groups											
Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Max					
WEB-ASG	public-template Version Default	2	-	2	2	5					

➤ **CREATE ANOTHER ASG AS PRIVATE:**

- 1.follow all the steps as above.
2. But at network settings, choose 2 private subnets .

Name

Auto Scaling group name
Enter a name to identify the group.

Must be unique to this account in the current Region and no more than 255 characters.

Launch template Info

ⓘ For accounts created after May 31, 2023, the EC2 console only supports creating Auto Scaling groups with launch templates. Creating Auto Scaling groups with launch configurations is not recommended but still available via the CLI and API until December 31, 2023.

Launch template
Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.

Create a launch template [\[i\]](#)

Version

Create a launch template version [\[i\]](#)

Network Info

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across the zones. The default VPC and default subnets are suitable for getting started quickly.

VPC
Choose the VPC that defines the virtual network for your Auto Scaling group.

Create a VPC [\[i\]](#)

Availability Zones and subnets
Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.

Select Availability Zones and subnets

us-west-1b | subnet-0d473bcb4ff06ed74 (private-subnet-1)
30.0.20.0/24

us-west-1c | subnet-00db1c6a259290775 (private-subnet-2)
30.0.12.0/22

Create a subnet [\[i\]](#)

Load balancing Info

Use the options below to attach your Auto Scaling group to an existing load balancer, or to a new load balancer that you define.

No load balancer
Traffic to your Auto Scaling group will not be fronted by a load balancer.

Attach to an existing load balancer
Choose from your existing load balancers.

Attach to a new load balancer
Quickly create a basic load balancer to attach to your Auto Scaling group.

Attach to a new load balancer

Define a new load balancer to create for attachment to this Auto Scaling group.

Load balancer type

Choose from the load balancer types offered below. Type selection cannot be changed after the load balancer is created. If you need a different type of load balancer than those offered here, visit the [Load Balancing console](#).

Application Load Balancer
HTTP, HTTPS

Network Load Balancer
TCP, UDP, TLS

Load balancer name

Name cannot be changed after the load balancer is created.

APP-ASG-1

Load balancer scheme

Scheme cannot be changed after the load balancer is created.

Internal

Internet-facing

VPC

vpc-0ed1a6944be421ee3 [Edit](#)

my-vpc-01

Availability Zones and subnets

You must select a single subnet for each Availability Zone enabled. Only public subnets are available for selection to support DNS resolution.

us-west-1b

subnet-0d473bcb4ff06ed74



us-west-1c

subnet-00db1c6a259290775



Listeners and routing

If you require secure listeners, or multiple listeners, you can configure them from the [Load Balancing console](#) after your load balancer is created.

Protocol	Port	Default routing (forward to)
HTTP	80	<input type="button" value="Create a target group"/> New target group name An instance target group with default settings will be created. APP-ASG-1-Tg

Tags - optional

Group size Info

Set the initial size of the Auto Scaling group. After creating the group, you can change its size to meet demand, either manually or by using automatic scaling.

Desired capacity type

Choose the unit of measurement for the desired capacity value. vCPUs and Memory(GiB) are only supported for mixed instances groups configured with a set of instance attributes.

Units (number of instances)

Desired capacity

Specify your group size.

2

Scaling Info

You can resize your Auto Scaling group manually or automatically to meet changes in demand.

Scaling limits

Set limits on how much your desired capacity can be increased or decreased.

Min desired capacity

2

Equal or less than desired capacity

Max desired capacity

5

Equal or greater than desired capacity

Automatic scaling - optional

4.Successfully created TWO AUTO SCALING GROUPS.

The screenshot shows the AWS Auto Scaling Groups page. At the top, a green banner indicates: "APP-ASG, 1 Scaling policy, 1 Load balancer, 1 Target group, 1 Listener created successfully. 1 new target group has been attached to ASG." Below the banner, the page title is "Auto Scaling groups (2) Info". There is a search bar labeled "Search your Auto Scaling groups". A toolbar at the top right includes "Launch configurations", "Launch templates", "Actions", and a prominent orange "Create Auto Scaling group" button. The main table lists two Auto Scaling groups:

Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Max	Availability Zones
APP-ASG	private-template Version Default	0	Updating capacity...	2	2	5	us-west-1b, us-west-1c
WEB-ASG	public-template Version Default	2	-	2	2	5	us-west-1b, us-west-1c

5.Now go to EC2 dashboard- click on instances

6.we should see four EC2 instances running.

The screenshot shows the AWS Instances page. The title is "Instances (4) Info". A toolbar at the top right includes "Last updated less than a minute ago", "Connect", "Instance state", "Actions", and a yellow "Launch instances" button. The main table lists four EC2 instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Pub.
i-0978bd36f7b6c28e3	Running	t2.micro	2/2 checks passed	View alarms +	us-west-1b	-	3.1t	
i-0e391385529974c62	Running	t2.micro	2/2 checks passed	View alarms +	us-west-1b	-	54.	
i-0bcf2f481f407c00b	Running	t2.micro	2/2 checks passed	View alarms +	us-west-1c	-	52.t	
i-0eee3f5be44389dac	Running	t2.micro	2/2 checks passed	View alarms +	us-west-1c	-	54.t	

7.Give the names to those instances as – public-1, public-2, private-1 & private-2.

The screenshot shows the AWS Instances page. The title is "Instances (1/4) Info". A toolbar at the top right includes "Last updated less than a minute ago", "Connect", "Instance state", "Actions", and a yellow "Launch instances" button. The main table lists four EC2 instances with names assigned:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Pub.
public-1	i-0978bd36f7b6c28e3	Running	t2.micro	2/2 checks passed	View alarms +	us-west-1b	-	3.1t
private-1	i-0e391385529974c62	Running	t2.micro	2/2 checks passed	View alarms +	us-west-1b	-	54.15
public-2	i-0bcf2f481f407c00b	Running	t2.micro	2/2 checks passed	View alarms +	us-west-1c	-	52.53
private-2	i-0eee3f5be44389dac	Running	t2.micro	2/2 checks passed	View alarms +	us-west-1c	-	54.67

➤ PUBLIC1 INSTANCE CONNECT TO THE WEB:

8. let's go to its public instance and connect to ssh -i link connect to EC2 server.I connect to ubuntu server and next below steps follows

- ✧ **Sudo** -to become a root user
- ✧ **apt update -y && apt install apache2 -y && cd /var/www/html** -update packages and install apache2 and path
- ✧ **Ls** -list
- ✧ **rm index.html** -to remove html file
- ✧ **vi index.html** – enter – press i – insert date ---:x (to save) – enter
- ✧ **Systemctl status apache2** -to check the server status
- ✧ **Ping google.com** - to check whether the server is ping or not.

9.Snapshots are given below

10.Copy the PUBLIC IP address & paste it in google chrome.

11.It will shows the data which we inserted.

```
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1012-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of Mon Aug 26 19:32:55 UTC 2024

  System load:  0.08          Processes:           111
  Usage of /:   26.0% of 6.71GB  Users logged in:      0
  Memory usage: 23%            IPv4 address for enX0: 30.0.0.181
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

85 updates can be applied immediately.
30 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Mon Aug 26 19:19:36 2024 from 13.52.6.116
ubuntu@ip-30-0-0-181:~$ sudo -i
root@ip-30-0-0-181:~# apt update -y && apt install apache2 -y
Hit:1 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Hit:3 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Fetched 126 kB in 1s (230 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
100 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
```

```

apache2 is already the newest version (2.4.58-1ubuntu8.4).
0 upgraded, 0 newly installed, 0 to remove and 100 not upgraded.
root@ip-30-0-0-181:~# cd /var/www/html
root@ip-30-0-0-181:/var/www/html# ls
index.html
root@ip-30-0-0-181:/var/www/html# rm index.html
root@ip-30-0-0-181:/var/www/html# vi index.html
root@ip-30-0-0-181:/var/www/html# systemctl status apache2
● apache2.service - The Apache HTTP Server
    Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
    Active: active (running) since Mon 2024-08-26 19:12:28 UTC; 22min ago
      Docs: https://httpd.apache.org/docs/2.4/
      Main PID: 2430 (apache2)
        Tasks: 55 (limit: 1130)
       Memory: 10.9M (peak: 11.1M)
         CPU: 186ms
      CGroup: /system.slice/apache2.service
              ├─2430 /usr/sbin/apache2 -k start
              ├─2433 /usr/sbin/apache2 -k start
              └─2434 /usr/sbin/apache2 -k start

Aug 26 19:12:28 ip-30-0-0-181 systemd[1]: Starting apache2.service - The Apache HTTP Server...
Aug 26 19:12:28 ip-30-0-0-181 apachectl[2429]: AH00558: apache2: Could not reliably determine the server's fully qualified name, using ip-30-0-0-181.
Aug 26 19:12:28 ip-30-0-0-181 systemd[1]: Started apache2.service - The Apache HTTP Server.

root@ip-30-0-0-181:/var/www/html# ping google.com
PING google.com (142.251.46.206) 56(84) bytes of data.
64 bytes from nug04s45-in-f14.1e100.net (142.251.46.206): icmp_seq=1 ttl=118 time=1.89 ms
64 bytes from nug04s45-in-f14.1e100.net (142.251.46.206): icmp_seq=2 ttl=118 time=1.88 ms
64 bytes from nug04s45-in-f14.1e100.net (142.251.46.206): icmp_seq=3 ttl=118 time=1.92 ms
64 bytes from nug04s45-in-f14.1e100.net (142.251.46.206): icmp_seq=4 ttl=118 time=1.87 ms
64 bytes from nug04s45-in-f14.1e100.net (142.251.46.206): icmp_seq=5 ttl=118 time=1.86 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 1.861/1.883/1.922/0.021 ms
root@ip-30-0-0-181:/var/www/html#

```



this is a nginx public-1 server

NOW CONNECT TO THE PRIVATE INSTANCE THROUGH THE PUBLIC INSTANCE:

1.Follow the steps as mentioned in the snapshots.

2.Successfully connected to the PRIVATE INSTANCE

```

root@ip-30-0-0-181:/var/www/html# vi swathi.pem
root@ip-30-0-0-181:/var/www/html# chmod 400 "swathi.pem"
root@ip-30-0-0-181:/var/www/html# ssh -i "swathi.pem" ubuntu@30.0.20.185
The authenticity of host '30.0.20.185 (30.0.20.185)' can't be established.
ED25519 key fingerprint is SHA256:ZgSwz+2zIg3og7aVLjQzq6ro/RP5EbgXcPaVW5EtDUo.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '30.0.20.185' (ED25519) to the list of known hosts.
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1012-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Mon Aug 26 19:40:23 UTC 2024

 System load:  0.0          Processes:           104
 Usage of /:   22.7% of 6.71GB   Users logged in:     0
 Memory usage: 20%          IPv4 address for enx0: 30.0.20.185
 Swap usage:   0%
 
Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-30-0-20-185:~$ 

```

❖ CREATE SUBNET GROUP:

To create a database first you need you to create a subnet group

- 1.select create subnet group on rds dashboard
- 2.give a name to new subnet group-select vpc
- 3.add availability zones (us-west-1b & us-west-1c)

Subnet group details

Name
You won't be able to modify the name after your subnet group has been created.

Must contain from 1 to 255 characters. Alphanumeric characters, spaces, hyphens, underscores, and periods are allowed.

Description

VPC
Choose a VPC identifier that corresponds to the subnets you want to use for your DB subnet group. You won't be able to choose a different VPC identifier after your subnet group has been created.

Add subnets

Availability Zones
Choose the Availability Zones that include the subnets you want to add.

Subnets
Choose the subnets that you want to add. The list includes the subnets in the selected Availability Zones.

⌚ Successfully created DB-subnet. [View subnet group](#)

- 4.successfully created a subnet group

⌚ Successfully created DB-subnet. [View subnet group](#)

Subnet groups (3)						
<input type="text" value="Filter by subnet group"/>				<input type="button" value="C"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
<input type="checkbox"/>	Name	Description	Status	VPC		
<input type="checkbox"/>	db-subnet	allow	<input checked="" type="checkbox"/> Complete	vpc-0ed1a6944be421ee3		

4. And goto security groups and select edit inbounds and select mysql

Edit inbound rules info
Inbound rules control the incoming traffic that's allowed to reach the instance.

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-01151640efcf539766	SSH	TCP	22	Custom	<input type="text" value="0.0.0.0"/> <input type="button" value="Delete"/>
sgr-02ec25249ef9b5f1a	HTTP	TCP	80	Custom	<input type="text" value="0.0.0.0"/> <input type="button" value="Delete"/>
...	MYSQL/Aurora	TCP	3306	Anywhere...	<input type="text" value="0.0.0.0"/> <input type="button" value="Delete"/>

⌚ Inbound security group rules successfully modified on security group (sg-0d5c691184de9a581 | security-group-1)
► Details

❖ CREATE DATABASE:

- 1.select database on rds dashboard and click create database
- 2.choose STANDARD in creation method and MYSQL in engine methods
- 3.select FREE TIER in template
4. choose SELF MANAGED in settings and give PASSWORD
- 5.go to connectivity and choose CONNECT TO EC2 INSTANCE and select public instance
- 6.we don't have to give vpc and db subnet group it will take by default
- 7.choose existing security groups and select both public (public-security-group) and private (private-security-group) security groups

Create database

Choose a database creation method [Info](#)

Standard create
You set all of the configuration options, including ones for availability, security, backups, and maintenance.

Easy create
Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Engine options

Engine type [Info](#)

Aurora (MySQL Compatible)

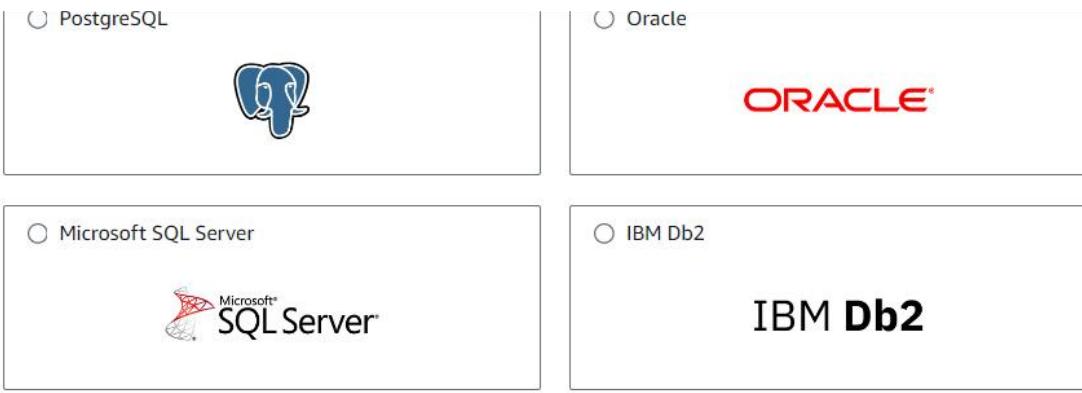
Aurora (PostgreSQL Compatible)

MySQL

MariaDB

PostgreSQL

Oracle



Edition

MySQL Community

Engine version [Info](#)

View the engine versions that support the following database features.

▼ Hide filters

Show versions that support the Amazon RDS Optimized Writes [Info](#)

Amazon RDS Optimized Writes improves write throughput by up to 2x at no additional cost.

Engine Version

MySQL 8.0.35

Enable RDS Extended Support [Info](#)

Amazon RDS Extended Support is a [paid offering](#). By selecting this option, you consent to being charged for this offering if you are running your database major version past the RDS end of standard support date for that version. Check the end of standard support date for your major version in the [RDS for MySQL documentation](#).

Credentials management

You can use AWS Secrets Manager or manage your master user credentials.

Managed in AWS Secrets Manager - *most secure*
RDS generates a password for you and manages it throughout its lifecycle using AWS Secrets Manager.

Self managed
Create your own password or have RDS create a password that you manage.

Auto generate password

Amazon RDS can generate a password for you, or you can specify your own password.

Master password [Info](#)

Password strength Strong

Minimum constraints: At least 8 printable ASCII characters. Can't contain any of the following symbols: / ' " @

Confirm master password [Info](#)

Instance configuration

The DB instance configuration options below are limited to those supported by the engine that you selected above.

DB instance class [Info](#)

▼ Hide filters

- Show instance classes that support Amazon RDS Optimized Writes [Info](#)
Amazon RDS Optimized Writes improves write throughput by up to 2x at no additional cost.
- Include previous generation classes
- Standard classes (includes m classes)
 - Memory optimized classes (includes r and x classes)

Connectivity [Info](#)



Compute resource

Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

- Don't connect to an EC2 compute resource
Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.

- Connect to an EC2 compute resource
Set up a connection to an EC2 compute resource for this database.

EC2 instance [Info](#)

Choose the EC2 instance to add as the compute resource for this database. A VPC security group is added to this EC2 instance. A VPC security group is also added to the database with an inbound rule that allows the EC2 instance to access the database.

i-0acd8d3bf3f511fc2
public-1



Some VPC settings can't be changed when a compute resource is added

Adding an EC2 compute resource automatically selects the VPC, DB subnet group, and public access settings for this database. To allow the EC2 instance to access the database, a VPC security group rds-ec2-X is added to the database and another called ec2-rds-X to the EC2 instance. You can remove the new security group for the database only by removing the compute resource.

Virtual private cloud (VPC) [Info](#)

Choose the VPC. The VPC defines the virtual networking environment for this DB instance.

No Dual compatible VPCs



Only VPCs with a corresponding DB subnet group are listed.

Public access [Info](#)

- Yes
RDS assigns a public IP address to the database. Amazon EC2 instances and other resources outside of the VPC can connect to your database. Resources inside the VPC can also connect to the database. Choose one or more VPC security groups that specify which resources can connect to the database.

- No
RDS doesn't assign a public IP address to the database. Only Amazon EC2 instances and other resources inside the VPC can connect to your database. Choose one or more VPC security groups that specify which resources can connect to the database.

VPC security group (firewall) [Info](#)

Choose one or more VPC security groups to allow access to your database. Make sure that the security group rules allow the appropriate incoming traffic.

- Choose existing
Choose existing VPC security groups

- Create new
Create new VPC security group

Additional VPC security group

Choose one or more options

security-group-2 X | security-group-1 X

Amazon RDS will add a new VPC security group rds-ec2-1 to allow connectivity with your compute resource.

Availability Zone [Info](#)



Certificate authority - optional [Info](#)

Using a server certificate provides an extra layer of security by validating that the connection is being made to an Amazon database. It does so by checking the server certificate that is automatically installed on all databases that you provision.

rds-ca-rsa2048-g1 (default)
Expiry: May 20, 2061



8. successfully database is created

❖ Take DB SNAPSHOT :

1.Go to rds dashboard - select snapshot –click on take snapshot

2.select db instance and give a new name to snapshot

3.click on take snapshot

RDS > Snapshots > Take snapshot

Take DB Snapshot

Preferences
To take a DB Snapshot, choose a database and name your DB Snapshot.

Snapshot type
 DB instance
 DB cluster

DB instance
DB Instance Identifier. This is the unique key that identifies a DB Instance.
database

Snapshot name
Identifier for the DB Snapshot.
DB-SNAPSHOT

Snapshot identifier is case insensitive, but stored as all lower-case, as in "mysnapshot". Cannot be null, empty, or blank. Must contain from 1 to 255 alphanumeric characters or hyphens. First character must be a letter. Cannot end with a hyphen or contain two consecutive hyphens.

Cancel **Take snapshot**

4.successfully snapshot is created

Snapshots			
Manual	System	Shared with me	Public
Backup service			
Exports in Amazon S3			
Manual snapshots (1)			
<input type="button" value="Filter by manual snapshots"/>			
<input type="checkbox"/> Snapshot name	DB instance or cluster	Snapshot creation time	DB instance created time
<input type="checkbox"/> db-snapshot	database	-	August 26, 2024, 11:30 (UTC+05:30)
<input type="button" value="Actions"/> <input type="button" value="Take snapshot"/>			

➤ MYSQL installation :

After the DB has been created, i'll need the database endpoint DNS to establish a connection from the public instance.

To install mysql use this commands

Sudo -i

Sudo apt update

Sudo apt install mysql-server

Sudo systemctl start mysql.server

After install to use this commands

```
mysql -h YOUR_DB_ENDPOINT -u YOUR_DB_USERNAME -p
```

enter the password you chose when creating the DB.

Successfully login to mysql database

Mysql> show databases;

- once you complete giving the commands it displays as following in below snapshots

```
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1012-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of Tue Aug 27 11:15:31 UTC 2024

System load: 0.08      Processes:          109
Usage of /: 36.8% of 6.71GB  Users logged in: 0
Memory usage: 59%        IPv4 address for enx0: 30.0.0.181
Swap usage: 0%

* Ubuntu Pro delivers the most comprehensive open source security and
  compliance features.

https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

61 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

*** System restart required ***
Last login: Tue Aug 27 06:13:53 2024 from 13.52.6.115
ubuntu@ip-30-0-0-181:~$ sudo -i
root@ip-30-0-0-181:~# sudo apt update
Hit:1 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Hit:3 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Get:5 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [468 kB]
Get:6 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [337 kB]
```

```
Get:7 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Hit:3 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Get:5 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [468 kB]
Get:6 http://us-west-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [337 kB]
Fetched 932 kB in 1s (1144 kB/s)
Reading package lists... Done
Building dependency tree... Done
Building dependency tree... Done
Reading state information... Done
79 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@ip-30-0-0-181:~# sudo apt install mysql-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
mysql-server is already the newest version (8.0.39-Ubuntu0.24.04.2).
0 upgraded, 0 newly installed, 0 to remove and 79 not upgraded.
root@ip-30-0-0-181:~# sudo systemctl start mysql.service
root@ip-30-0-0-181:~# mysql -h database.ctegomk2gg59.us-west-1.rds.amazonaws.com -P 3306 -u admin -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 26
Server version: 8.0.35 Source distribution

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

```
mysql> show databases;
+-----+
| Database      |
+-----+
| information_schema |
| mysql          |
| performance_schema |
| sys            |
+-----+
4 rows in set (0.00 sec)
```

```
mysql> create database vcube128;
Query OK, 1 row affected (0.00 sec)
```

```
mysql> use vcube128
Database changed
mysql> show databases;
+-----+
| Database      |
+-----+
| information_schema |
| mysql          |
| performance_schema |
| sys            |
| vcube128       |
+-----+
5 rows in set (0.00 sec)
```

```
mysql> |
```

THE END