

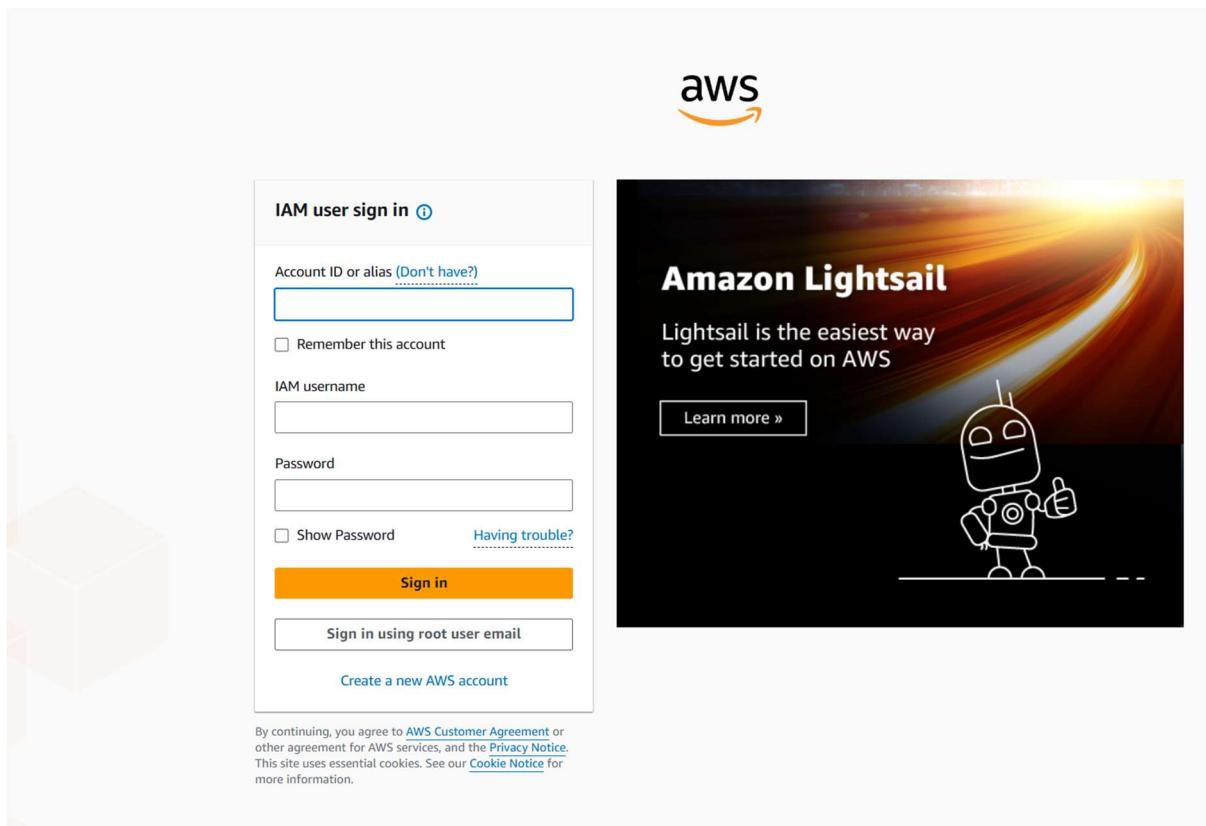
Name :Roshan Saral Kumar(CLOUD-COMPUTING-INTERN)
DATE:23-10-2025

TASK 3

- **Task 3: Create and Configure a Virtual Private Cloud (VPC) with Subnets**
 - **Objective:- To learn how cloud networking works by creating a Virtual Private Cloud (VPC) with public and private subnets, and enabling controlled internet access.**
 - **This task teaches the backbone of secure cloud architecture and how resources are isolated and protected in the cloud.**
-

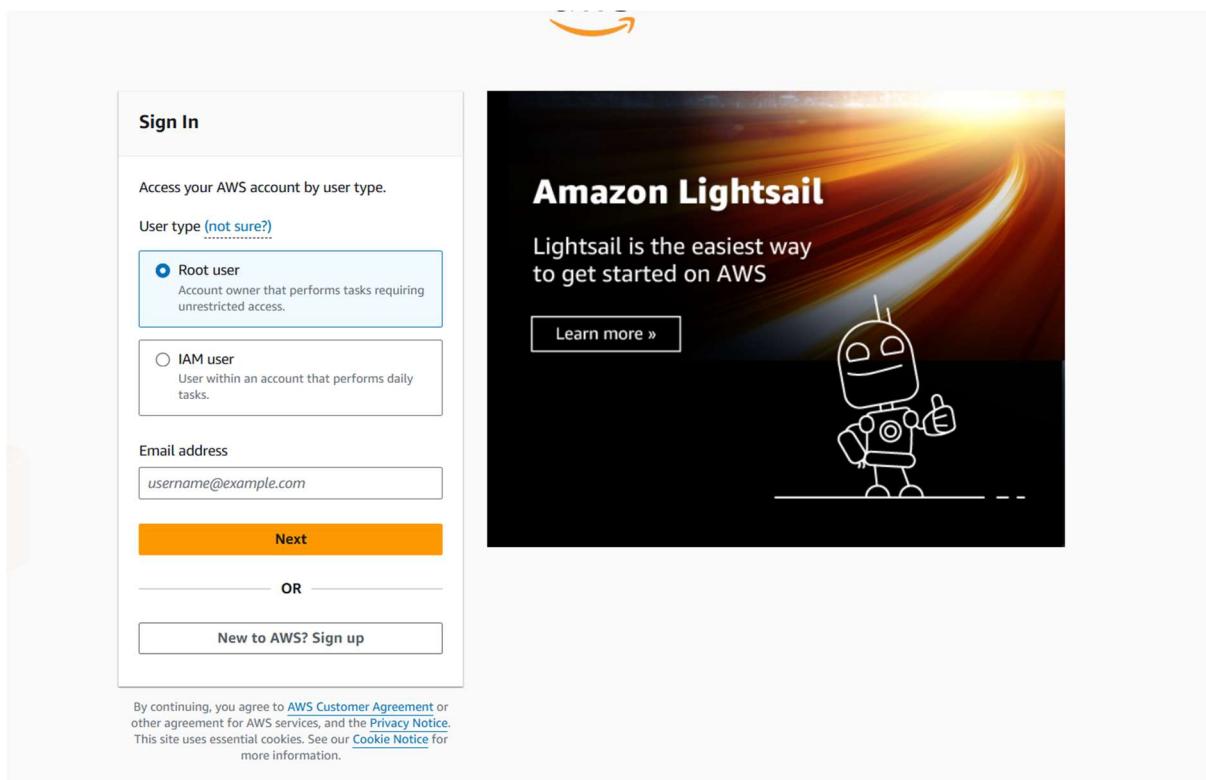
TOOLS USED:- AWS Free Tier (Preferred) – VPC, Subnets, Route Tables, Internet Gateway, Security Groups

- **THIS IS THE SIGN IN CONSOLE PAGE AND IAM USING SIGN USING ROOT USER EMAIL (ROOT USER MEANS I HAVE ACCESS TO ALL THE SERVICES OF AWS IF IT IS AN IAM (IDENTITY AND ACCESS MANAGEMENT USER THEN THE USER WILL HAVE ACCESS TO ONLY A LIMITED NUMBER OF SERVICES THAT AWS OFFERS AND THE IAM USERS WILL HAVE IAM POLICIES ATTACHED TO THEM SO ONLY THOSE SERVICES THEY WILL BE ABLE TO USE) CURRENTLY LOGGING IN AS ROOT USER EMAIL.**



The image shows the AWS IAM User Sign In page. At the top right is the AWS logo. Below it is a sidebar with the title "IAM user sign in ⓘ". The main form contains fields for "Account ID or alias (Don't have?)", "Remember this account", "IAM username", "Password", and "Show Password". There is also a link "Having trouble?". A large orange "Sign in" button is centered. Below the button are links for "Sign in using root user email" and "Create a new AWS account". At the bottom of the page is a small legal notice about cookie usage.

- AFTER CLICKING ON SIGN IN USING ROOT USER EMAIL I WILL GET THIS PAGE WHERE I HAVE TO ENTER MY EMAIL-ID. AND AS WE CAN SEE ROOT USER IS SELECTED BY DEFAULT. WE CAN ALSO SELECT IAM USER IN THIS PAGE IN CASE IF THERE IS A CHANGE.

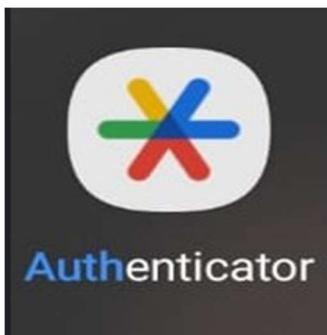


The image shows the AWS Sign In page. At the top right is the AWS logo. Below it is a sidebar with the title "Sign In". The main form asks "Access your AWS account by user type." It has two options: "Root user" (selected) and "IAM user". Below these are fields for "Email address" (containing "username@example.com") and a large orange "Next" button. To the right of the form is a sidebar for "Amazon Lightsail" with the text "Lightsail is the easiest way to get started on AWS" and a "Learn more »" button. At the bottom of the page is a small legal notice about cookie usage.

- AFTER ENTERING OUR EMAIL WE NEED TO GIVE OUR PASSWORD

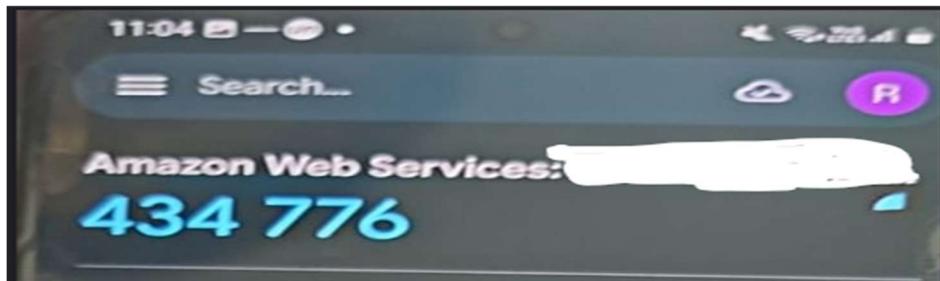
The image shows two side-by-side screenshots. The left screenshot is of the AWS Root user sign-in page, which asks for a password. The right screenshot is of the Amazon Lightsail landing page, which features a cartoon robot and a 'Learn more' button.

- SINCE I HAVE AN AWS ACCOUNT ALREADY CREATED I ACTUALLY MADE AN MFA FOR MY ROOT USER . MFA STANDS FOR (MULTI-FACTOR AUTHENTICATION CODE) IT ACTS AS A DOUBLE LAYER PROTECTION FOR OUR ROOT USER OTHERWISE WE CAN GET HACKED SO ALREADY PROVIDE AN EXTRA LAYER OF PROTECTION TO BE ON THE SAFER SIDE.
- MFA CODE IS GIVEN BY TOTEM TOKENS OR U CAN ALSO USE THE “GOOGLE AUTHENTICATOR APP” IN YOUR MOBILE WHICH IS MOSTLY PREFERRED.

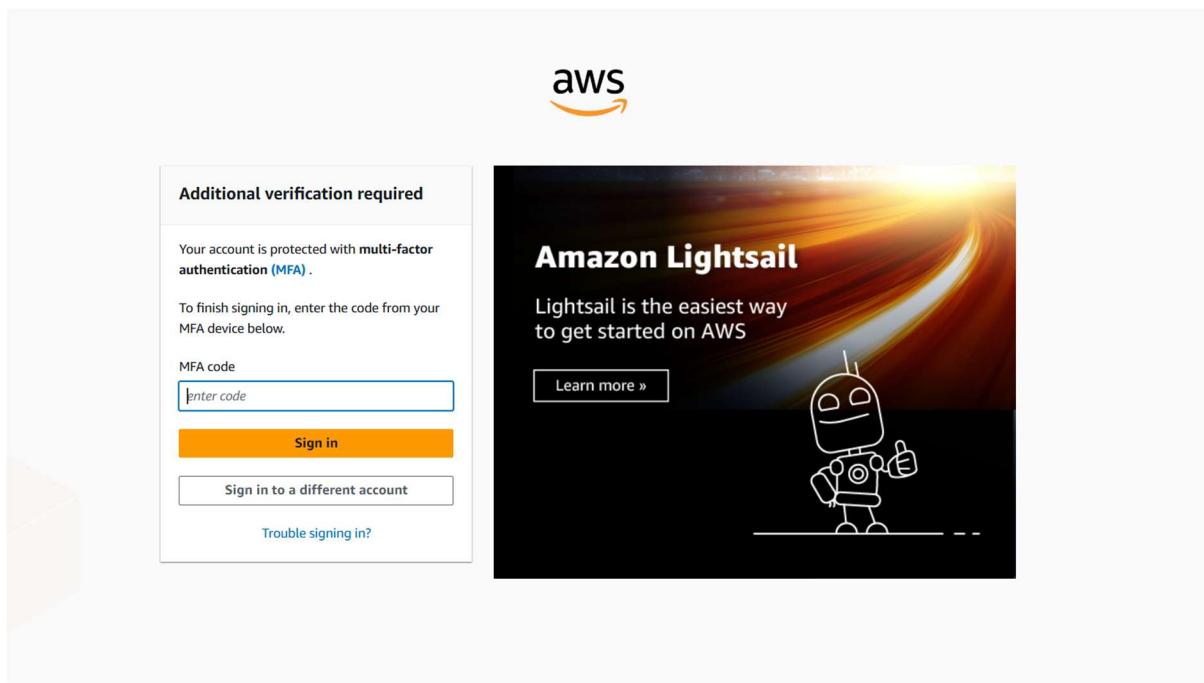


- THIS APP IS IN MY MOBILE AND I HAVE TO GIVE THE MFA CODE WHICH IS ASKED FOR THE VERIFICATION OF ROOT USER.
- ONCE I HAVE CLICKED ON THIS APP I WILL SEE THE BELOW SCREEN IN MY MOBILE.

- THE SCREEN IN MY MOBLIE LOOKS LIKE THIS:-THE CONTENT WHICH IAM HIDING USING A WHITE COLOR IS MY PRIVATE INFORMATION OF MY ACCOUNT WHICH CANNOT BE SHARED BUT HIS IS HOW A SIMPLE MFA CODE LOOKS LIKE AND THE MFA CODE KEEPS ON CHANGING ON A DAILY BASIS.ALWAYS USE MFA TO ENSURE ENHANCED SECURITY.



- THIS IS THE CODE THAT I HAVE TO ENTER IN MY AWS WEB BROWSER IN THE BELOW IMAGE IT IS SHOWN.



- AFTER SIGNING IN WE ENTER THE AWS MANAGEMENT CONSOLE AND THE DEFAULT REGION IS NORTH VIRGINIA THAT IS “us-east-1” WE CAN SELECT DIFFERENT REGIONS. IN THE IMAGE IT IS CLEARLY SHOWN IN THE RIGHT HAND SIDE WHICH REGION IAM CURRENTLY WORKING IN. THE BELOW IMAGE SHOWS THE SERVICES WHICH I VISITED AND THE CURRENT REGION WHICH IAM WORKING IN.
- TERMINOLOGIES:-
- Region:- It is a geothermal location which consists of a group of AZs (AVAILABILITY ZONES) and the network of a region is called a VPC(VIRTUAL PRIVATE CLOUD).
- AZ(Availability Zone):- they are a group of data centers. the network of a Az is a subnet.
- Edge Location:- it is a location in between various Azs or it is found at the boundary of an az In order to cache the incoming data acts like a storage for easier retrieval.

PLS NOTE CHANGE STARTS FROM HERE BELOW:-

- NOTE:-WE ARE WORKING IN THE PUBLIC SUBNET THAT IS “ap-south-1” if we are working in any azs it will show ap-south-1a,ap-south-1b and so on. We can check the azs in our aws management console itself that is given in below figure.

SO NOW FOR THE VPC SETTINGS IAM CURRENTLY WORKING IN THE MUMBAI REGION SO IAM USING “ap-south-1”.

HERE WE WILL BE ABLE TO SEE THE SUBNETS IN THE VPC DASHBOARD IF WE CLICK ON SUBNETS THEN TOTALLY THERE ARE 3 SUBNETS THAT IS PRIVATE SUBNETS FROM “ap-south-1a” to “ap-south-1c” totally we have 3 private subnets or we can also say we have 3 azs under Asia pacific (MUMBAI) REGION THAT IS “AP-SOUTH-1” REGION. This is provided by aws itself by default we cannot create any Availability Zones.

Logging into aws amangement console and searching for VPC(VIRTUAL PRIVATE CLOUD)

THIS IS THE AWS MANAGEMENT CONSOLE AFTER LOGGING IN CURRENTLY WORKING IN MUMBAI(ap-south-1) the below image shows that

The screenshot shows the AWS Management Console Home page. At the top right, the region is set to "Asia Pacific (Mumbai)". The left sidebar lists recently visited services: EC2, IAM, VPC, Lightsail, S3, AWS Health Dashboard, CloudWatch, and Elastic Kubernetes Service. The main content area is divided into several sections:

- Welcome to AWS**: Includes links to "Getting started with AWS", "Training and certification", and "AWS Builder Center".
- AWS Health**: Shows 0 open issues (Past 7 days), 0 scheduled changes (Upcoming and past 7 days), and 0 other notifications (Past 7 days).
- Cost and usage**: Displays a total credit balance of \$118.68 USD. It shows current month costs at \$1.20 (▲ 2,900%) and forecasted month end costs at \$1.23 (▲ 2,975%).
- Applications**: Shows 0 applications. A button to "Create application" is present.
- Regions**: A sidebar listing available regions categorized by continent:
 - United States**: N. Virginia, Ohio, N. California, Oregon.
 - Asia Pacific**: Hyderabad, Mumbai (highlighted in blue), Osaka, Seoul, Singapore, Sydney, Tokyo.
 - Canada**: Central.
 - Europe**: Frankfurt, Ireland, London, Paris, Stockholm.
 - South America**: São Paulo.A note states: "There are 16 Regions that are not enabled for this account."

SEARCH FOR VPC IN THE AWS MANAGEMENT CONSOLE:-

The screenshot shows the AWS Management Console search interface. The search bar at the top contains the query "VPC". Below the search bar, there are two main sections: "Services" and "Features".

Services section:

- VPC** Isolated Cloud Resources
- AWS Global View** AWS Global View provides a global dashboard and search functionality that lets you ...
- AWS Firewall Manager** Central management of firewall rules

Features section:

- Dashboard** ■ VPC feature
- Route 53 VPCs** ■ Route 53 feature
- VPC links** ■ API Gateway feature

Below these sections, there is a message about cross-Region search:

Looking for resources in other Regions?
You can enable cross-Region search for resources across all Regions in your account by specifying an aggregator index.

Enable cross-Region search [\[?\]](#)

At the bottom, there is a feedback section:

Were these results helpful?

[Yes](#) [No](#)

Resource details:

vpc-062ab221c16cb443d
■ VPC vpc

Region:

Asia Pacific (Mumbai) ap-south-1

HERE THIS IS THE VPC DASHBOARD SHOWN BELOW IT GIVES PRIVATE SYUBNETS , REGIONS , NETWORK ACLS , ROUTE TABLE ETC SHOWN IN BELW IMAGE.

The screenshot shows the AWS VPC Dashboard for the Asia Pacific region. The left sidebar includes links for VPC dashboard, AWS 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, NAT gateways, Peering connections, Route servers), Security (Network ACLs, Security groups), and PrivateLink and Lattice (Getting started, Endpoints, Endpoint services, Service networks, Lattice services, Resource configurations, Resource gateways, Target groups). The main content area displays 'Resources by Region' for Mumbai, listing VPCs (1), Subnets (3), Route Tables (1), Internet Gateways (1), Egress-only Internet Gateways (0), DHCP option sets (1), Endpoints (0), Instance Connect Endpoints (0), NAT Gateways (0), VPC Peering Connections (0), Network ACLs (1), Security Groups (2), Customer Gateways (0), Virtual Private Gateways (0), Site-to-Site VPN Connections (0), and Running Instances (0). A 'Service Health' box indicates no issues. On the right, there are sections for Settings (Block Public Access, Zones, Console Experiments) and Additional Information (VPC Documentation, All VPC Resources, Forums, Report an Issue). An 'AWS Network Manager' section provides an overview and a link to get started. A 'Site-to-Site VPN Connections' section explains how Amazon VPC enables connecting isolated resources within the AWS Cloud.

VPC dashboard

[Create VPC](#) [Launch EC2 Instances](#)

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

Resources by Region

You are using the following Amazon VPC resources

VPCs	Mumbai 1	NAT Gateways	Mumbai 0
Subnets	Mumbai 3	VPC Peering Connections	Mumbai 0
Route Tables	Mumbai 1	Network ACLs	Mumbai 1
Internet Gateways	Mumbai 1	Security Groups	Mumbai 2
Egress-only Internet Gateways	Mumbai 0	Customer Gateways	Mumbai 0
DHCP option sets	Mumbai 1	Virtual Private Gateways	Mumbai 0
Endpoints	Mumbai 0	Site-to-Site VPN Connections	Mumbai 0
Instance Connect Endpoints	Mumbai 0	Running Instances	Mumbai 0

Service Health

[View complete service health details](#)

Settings

- [Block Public Access](#)
- [Zones](#)
- [Console Experiments](#)

Additional Information

- [VPC Documentation](#)
- [All VPC Resources](#)
- [Forums](#)
- [Report an Issue](#)

AWS Network Manager

AWS Network Manager provides tools and features to help you manage and monitor your network on AWS. Network Manager makes it easier to perform connectivity management, network monitoring and troubleshooting, IP management, and network security and governance.

[Get started with Network Manager](#)

Site-to-Site VPN Connections

Amazon VPC enables you to use your own isolated resources within the AWS Cloud, and then connect

WHEN WE CLICK ON VPC WE HAVE ALREADY A DEFAULT VPC AVAILABLE.

The screenshot shows the AWS VPC console. At the top, there is a search bar labeled "Find VPCs by attribute or tag". Below it is a table with columns: Name, VPC ID, State, Block Public..., IPv4 CIDR, IPv6 CIDR, DHCP option set, Main route table, and Mair. One row is selected, showing "vpc-062ab221c16cb443d" with "Available" state and "Off" for Block Public Access. The Main route table is "rtb-070801c956006d3ac" and the DHCP option set is "dopt-013e439bf3b4783d".

Below the table, a detailed view for "vpc-062ab221c16cb443d" is shown. It includes sections for VPC ID, DNS resolution, Main network ACL, and IPv6 CIDR. On the right, there are sections for State, Block Public Access, DHCP option set, IPv4 CIDR, Network Address Usage metrics, and other network settings like DNS hostnames, Main route table, IPv6 pool, and Owner ID.

THE PRIVATE SUBNETS OF THE REGION IS AS SHOWN BELOW THAT IS FROM “ap-south-1a” to “ap-south-1c”.

The screenshot shows the AWS VPC Subnets console. At the top, there is a search bar labeled "Find subnets by attribute or tag". Below it is a table with columns: Name, Subnet ID, State, VPC, Block Public..., IPv4 CIDR, IPv6 CIDR, and IPv6 CIDR association ID. Three subnets are listed: "subnet-00baaf85838381c59f" (State Available, VPC vpc-062ab221c16cb443d, IPv4 CIDR 172.31.0.0/20), "Subnet-0a4785f80a36418ea" (State Available, VPC vpc-062ab221c16cb443d, IPv4 CIDR 172.31.32.0/20), and "subnet-0185d2cbbf97fc399" (State Available, VPC vpc-062ab221c16cb443d, IPv4 CIDR 172.31.16.0/20).

THESE ARE THE PRIVATE SUBNETS AVILABLE IN MUMBAI REGION TO REGION THE SUBNETS VARIES WE CANNOT DECIDE ON THE AZ THAT IS WE CANNOT CREATE AN AVAILABILITY ZONE IT IS CREATED BY AWS FOR THAT REGION BY DEFAULT.

CREATING VPC THAT IS VIRTUAL PRIVATE CLOUD :-HERE HTER ARE TWO WAYS IN WHICH WE CAN CREATE THE VPC ONE IS THE MANUAL WAY WE HAVE TO ENETER THE OTHER ONE IS VPC AND MORE WHICH GIVES US THE PREVIEW TABLE AND ALL BY DEFAULT . BUT TODAY IAM GOING TO SHOW THE CREATION MANUALLY PROVIDED IN THE STEPS OF ELEVATE-LABS.

THIS BELOW OPTION INDICATES VPC ONLY AND WE HAVE TO CREATE EVERYHTING MANUALLY THAT IS CONNECTION OF INTERNET GATEWAY AND ALL IF WE WANT A FASTER TASK AND CREATE VPC IMMEDIATELY THEN GO FOR VPC AND MORE.

VPC ONLY OPTION IAM GOING TO USE.

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

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

IPv4 CIDR block Info
 IPv4 CIDR manual input IPAM-allocated IPv4 CIDR block

IPv4 CIDR

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

IPv6 CIDR block Info
 No IPv6 CIDR block IPAM-allocated IPv6 CIDR block Amazon-provided IPv6 CIDR block IPv6 CIDR owned by me

Tenancy Info

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.
No tags associated with the resource

Add tag
You can add 50 more tags

AFTER EDITING THE NAME OF THE VPC AND CHOOSING THE IPV4 CIDR BLOCK AND DEFAULTLY WE ARE NOT USING IPV6 ADDRESS IF WE WANT WE CAN USE DEPENDING ON THE RQUIREMENTS.

WHEN TO USE IPV4 AND IPV6:-

Scenario	Use IPv4 When...	Use IPv6 When...
Enterprise Network Setup	You're integrating with older hardware, legacy software, or internal systems that only support IPv4.	You're deploying a new infrastructure with modern routers, switches, and cloud-native services that support IPv6.
IoT Deployment	You have a small number of devices and NAT (Network Address Translation) is acceptable.	You're deploying thousands of IoT devices and need unique global addresses without NAT.
Web Hosting	Your clients or users primarily access your site from IPv4-only networks.	You want global reach, better routing, and future-proofing for mobile and international users.
Cloud Services (e.g., AWS, Azure)	You're using EC2 instances or S3 buckets with default IPv4 configurations.	You're scaling across regions, using IPv6-enabled load balancers, and optimizing for performance and security.
Security Compliance	You rely on traditional firewalls and VPNs that are IPv4-centric.	You need built-in IPsec support and end-to-end encryption with IPv6.
Mobile Networks	Your carrier or app backend still uses IPv4.	You're targeting 5G networks and mobile devices that natively support IPv6.
Global Expansion	Your current user base is IPv4-heavy (e.g., internal enterprise users).	You're expanding to regions like Asia or Africa where IPv6 adoption is higher.
DNS and Domain Setup	You only need A records (IPv4).	You want to add AAAA records for IPv6 and support dual-stack DNS.

RECENT ADVANCEMENTS IN IPV4 AND IPV6

Category	IPv4 Advancements	IPv6 Advancements
Address Management	Enhanced NAT techniques and address reclamation to extend IPv4 usability	SLAAC and DHCPv6 improvements for dynamic, scalable address assignment
Security	Improved firewall and VPN integration; anomaly detection tools	Native IPsec support; better end-to-end encryption without NAT
Routing	Optimized BGP and OSPF for legacy networks	OSPFv3 and BGP extensions for faster, scalable routing
Cloud Integration	Continued support in AWS, Azure, GCP with IPv4 defaults	Full IPv6 support in EC2, S3, Kubernetes, and load balancers
IoT & Mobile	IPv4 with NAT for small-scale IoT deployments	IPv6 for massive IoT networks and 5G mobile compatibility
Transition Tools	NAT64, DNS64, 464XLAT refined for IPv6 bridging	Dual-stack and IPv6-only data centers gaining traction
Global Adoption	IPv4 still dominant but facing exhaustion	Mandates and incentives in India, China, US for IPv6 rollout
Education & Certification	IPv4 remains core in networking exams	IPv6 labs added to Cisco, AWS, and cloud certifications
Performance	Kernel-level QoS and fragmentation handling improvements	Simplified headers and efficient routing for real-time apps

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 - optional
Creates a tag with a key of 'Name' and a value that you specify.
roshans_elevate labs_vpc

IPv4 CIDR block [Info](#)
 IPv4 CIDR manual input IPAM-allocated IPv4 CIDR block

IPv4 CIDR
10.0.0.0/16
CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)
 No IPv6 CIDR block IPAM-allocated IPv6 CIDR block Amazon-provided IPv6 CIDR block IPv6 CIDR owned by me

Tenancy [Info](#)
Default

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
<input type="text"/> Name	<input type="text"/> roshans_elevate labs_vpc X Remove tag

[Add tag](#)
You can add 49 more tags

[Cancel](#) [Preview code](#) [Create VPC](#)

AFTER ALL THE EDITING I WILL CCLIK ON CREATE VPC . THE VPC CIDR BLOCK IS **10.0.0.0/16 WHICH MENAS THAT THE FIRST 16 BITS IS FIXED AND THE REMAINING STARTS FROM 0 TO 255 AND THEN AFTER 255 IT ISAGIN 1.0 , 1.1 , 1.2 ,**

1.255 HERE FINAL IP ADDRESS IS LIKE THIS THAT IS 10.0.255.255/16

THE NUMBER OF IP ADDRESSES IS :- 255 X 255 BY MULTYPLYING WE GET AROUND 65,025 IP ADDRESSES THAT IS APPROXIEMATELY. IF 32 BITS ARE FIXED THEN WE HAVE ONE SINGLE IP ADDRESS.WE CAN SEE THAT ONCE I CLICKED ON CREATE VPC IT WAS CREATED IN THE BELOW FIGURE.

You successfully created vpc-04e14667aadc10df3 / roshans_elevate labs_vpc [X](#)

vpc-04e14667aadc10df3 / roshans_elevate labs_vpc [Actions](#)

Details		Block Public Access		DNS hostnames	
VPC ID	vpc-04e14667aadc10df3	State	Available	Disabled	Main route table rtb-04a9633f2a04ccde8
DNS resolution	Enabled	Tenancy	default		IPv6 pool -
Main network ACL	acl-00f50c3de649d595d	Default VPC	No		Owner ID 51626664533
IPv6 CIDR (Network border group)	-	Network Address Usage metrics	Disabled		
Resource map CIDRs Flow logs Tags Integrations					

Resource map [Info](#)

VPC	Subnets (0)	Route tables (1)	Network Connections (0)
Your AWS virtual network roshans_elevate labs_vpc	Subnets within this VPC	Route network traffic to resources rtb-04a9633f2a04ccde8	Connections to other networks

[Show all details](#)

NOW IAM GOING TO CREATE MY SUBNETS:-SUBNETS CAN BE PRIVATE OR PUBLIC SUBNETS.

Name	VPC ID	State	Block Public...	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route table	
-	vpc-062ab221c16cb443d	Available	Off	172.31.0.0/16	-	dopt-013e43a9bf3b478...	rtb-070801c956006d3ac	ad-C
roshans_elevatelabs_vpc	vpc-04e14667aadc10df3	Available	Off	10.0.0.0/16	-	dopt-013e43a9bf3b478...	-	-

GO TO THE LEFT SIDE PANNEL AND SELECT SUBNETS OPTION.

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	IPv6 CIDR	IPv6 CIDR association ID
-	subnet-00ba85838381c59f	Available	vpc-062ab221c16cb443d	Off	172.31.0.0/20	-	-
-	subnet-0a4785f80a36418ea	Available	vpc-062ab221c16cb443d	Off	172.31.32.0/20	-	-
-	subnet-0185d2chbf97fc399	Available	vpc-062ab221c16cb443d	Off	172.31.16.0/20	-	-

THE ABOVE FIGURE SHOWS ALL DEFAULT SUBNETS HERE IAM GOING TO CREATE THE SUBNETS MANUALLY AS PER THE GUIDELINES AS PER THE GUIDELINES OF ELEVATE LABS.

AFTER U ARE CLICKING ON CREATE SUBNET MAKE SURE THAT U CHANGETHE VPC ID TO YOUR VPC ID THAT IS 10.0.0.0/16 VPC.

ONCE WE HAVE CLICKED ON OUR VPC ID WE GET THE BELOW IMAGE

Create subnet [Info](#)

VPC

VPC ID
Create subnets in this VPC.

vpc-04e14667aadc10df3 (roshans_elevatelabs_vpc) ▾

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

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.
roshsub_1_elevatelabs

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.
Asia Pacific (Mumbai) / aps1-az1 (ap-south-1a) ▾

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.
10.0.0.0/16 ▾

IPv4 subnet CIDR block
10.0.1.0/24 256 IPs
< > ^ v

IF WE SEE CAREFULLY IN THE IPV4 SUBNET CIDR BLOCK WE GET 256 IPS FOR 10.0.1.0/24 THIS IS A PUBLIC SUBNET WHICH IAM GOING TO CREATE FOR (ap-south-1a)

THIS SUBNET CURRENTLY WHICH I CREATED IS PRIVATE SUBNET BUT GIVEN NAME AS PUBLIC. TO MAKE IT PUBLIC I HAVE TO AUTO ASSIGN THE IP AND ATTACH THE INTERNET GATEWAY. THIS I HAVE TO DO AND CURRENTLY THIS USBNET IS IN ap-south-1a

The screenshot shows the AWS Subnets page with a green header message: "You have successfully created 1 subnet: subnet-07beb24b686ba19e6". Below the header, there's a search bar and a "Create subnet" button. The main table lists one subnet:

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	IPv6 CIDR	IPv6 CIDR association ID
rosh_sub1_elevatelabs_public	subnet-07beb24b686ba19e6	Available	vpc-04e14667aadcc10df3 rosh...	Off	10.0.1.0/24	-	-

AFTER DOING THIS NOW I AM GOING TO CREATE MY PRIVATE SUBNET THAT IS SUBNET 2 IN ap-south-1b so if use overall I am creating my subnets in separate availability zones which is mostly preferred. Because even if one AZ goes down the other AZ will be there for backup and for restoring the data. The below figure shows the private subnet.

The screenshot shows the "Create subnet" wizard. The first step, "VPC", is completed with the VPC ID "vpc-04e14667aadcc10df3 (roshans_elevatelabs_vpc)". The second step, "Associated VPC CIDRs", shows the IPv4 CIDR "10.0.0.0/16". The third step, "Subnet settings", is currently active. It shows "Subnet 1 of 1" with a name "rosh_sub2_elevatelabs" and an availability zone "Asia Pacific (Mumbai) / aps1-az3 (ap-south-1b)". The IPv4 CIDR block is set to "10.0.0.0/16" and the IPv4 subnet CIDR block is set to "10.0.2.0/24".

IF PEOPLE ASK ME AFTER CREATING THE NAMES AS PUBLIC AND PRIVATE AS ARE THEY REALLY PUBLIC AND PRIVATE THEN I WOULD SAY NO WHY BECAUSE WE HAVE TO CREATE THE INTERNET GATEWAY AND ROUTING FOR THE SUBNETS ONCE THIS IS DONE THEN WE CAN DEFINITELY SAY THAT THE SUBNET1 IS A PUBLIC SUBNET AND SUBNET 2 IS A PRIVATE SUBNET.

<input type="checkbox"/>	-	subnet-00ba8f85338381c59f	Available	vpc-062ab221c16cb443d	Off	172.31.0.0/20	-	-
<input type="checkbox"/>	-	subnet-0a4785f80a36418ea	Available	vpc-062ab221c16cb443d	Off	172.31.32.0/20	-	-
<input type="checkbox"/>	-	subnet-0185d12cbff97fc399	Available	vpc-062ab221c16cb443d	Off	172.31.16.0/20	-	-
<input type="checkbox"/>	rosh_sub1_elevate labs_public	subnet-07beb24b686ba19e6	Available	vpc-04e14667aadc10df3 rosh...	Off	10.0.1.0/24	-	-
<input checked="" type="checkbox"/>	rosh_sub2_elevate labs_private	subnet-098b6aaac45db34ad	Available	vpc-04e14667aadc10df3 rosh...	Off	10.0.2.0/24	-	-

We have created two private subnets now iam going to create my internet gateway for the public subnet that is sub 1 once we attach the internet gateway to a subnet in aws the subnet becomes public and the one where the internet gateway is not attached becomes the private subnet.

IAM NAVIGATING TO THE INTERNET GATEWAY AND IAM GOING TO CREATE THE INTERNET GATEWAY.(DEFAULT INTERNET GATEWAY) SHOWN BELOW

Internet gateways (1) Info			
<input type="text"/> Find internet gateways by attribute or tag			
<input type="checkbox"/> Name	▼ Internet gateway ID	▼ State	▼ VPC ID
<input type="checkbox"/> -	igw-07d899456ba8f9f5b	Attached	vpc-062ab221c16cb443d

NOW IAM GOING TO CLICK ON 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="ROSH_SUNETS_IGW_ELEVATELABS"/> X Remove

[Add new tag](#)
You can add 49 more tags.

Cancel Create internet gateway

The following internet gateway was created: igw-08d814355cbdbbdd4 - ROSH_SUNETS_IGW_ELEVATELABS. You can now attach to a VPC to enable the VPC to communicate with the internet.

igw-08d814355cbdbbdd4 / ROSH_SUNETS_IGW_ELEVATELABS

Actions ▾

Details <small>Info</small>	
Internet gateway ID igw-08d814355cbdbbdd4	State Detached
VPC ID -	Owner 518286664533

Tags

Manage tags

[Search tags](#)

Key	Value
Name	ROSH_SUNETS_IGW_ELEVATELABS

OUR INTERNET GATEWAY IS CREATED. NOW I HAVE TO ATTACH THE INTERNET GATEWAY TO THE VPC SO WE WILL DO THIS BY USING THE DROP DOWN OPTIONS IN ACTIONS BUTTON ON THE RIGHT HAND SIDE OF THE INTERNET GATEWAY DASHBOARD WHERE IT IS WRITTEN “ATTACH TO VPC”.

VPC > Internet gateways

Internet gateways (1/2) Info

Actions ▾ Create internet gateway

Name	Internet gateway ID	State	VPC ID	Owner
-	igw-07d899456ba8f915b	Attached	vpc-062ab21c16cb445d	518286664533
<input checked="" type="checkbox"/> ROSH_SUNETS_IGW_ELEVATELABS	igw-08d814355cbdbbdd4	Detached	-	518286664533

AFTER U CLICK ON ATTACH TO VPC WE GET THESE PARAMETERS.

SELECTING MY OWN VPC ID WHICH I CREATED.

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.

Select a VPC

vpc-04e14667aad10df3 - roshans_elevate labs_vpc

AWS Command Line Interface command

Cancel **Attach internet gateway**

Attach to VPC (igw-08d814355cbdbbdd4) 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.



▼ AWS Command Line Interface command

You can perform the same actions on this page by using the AWS Command Line Interface (CLI) tools. [Learn more](#) [?]

Platform

Choose the platform from which you'll be running this command. The command parameters may be specified differently depending on the platform. Learn more about [specifying parameter values](#) [?].



CLI command

If you're using the AWS CLI tools, you can copy and paste this command - which includes the parameters you specified on this page - into your command line prompt or terminal. Learn more about the available [AWS CLI commands](#) [?].

```
aws ec2 attach-internet-gateway --vpc-id "vpc-04e14667aadc10df3" --internet-gateway-id "igw-08d814355cbdbbdd4" --region ap-south-1
```

IF WE WANT TO HAVE CONTROL OVER OTHER CLIS WE CAN MENTION HERE BUT NOW IAM LEAVING IT AS DEFAULT.

THE MAJOR TASK IS DONE THAT IS ATTACHING THE INTERNET GATEWAY TO THE VPC IS DONE.(WITHOUT WHICH WE WILL NOT HAVE INTERNET ACCESS FOR OUR REGION OR WE CAN SAY THE NETWORK OF OUR REGION THAT IS A VPC WILL NOT BE THERE SO WE WILL NOT BE ABLE TO ACCESS THE PUBLIC SUBNET OR THE PRIVATE SUBNET BECAUSE THESE REQUIRE INTERNET ACCESS . PRIVATE SUBNET WE WILL NOT BE ABLE TO ACCESS BUT WE CAN ACCESS IT IF WE USE A BASTION HOST OR JUMP SERVER FROM THE PUBLIC SUBNET.THIS IS EXPLAINED IN MY OTHER FILE PROJECT WHERE I LAUNCHED THE WEBSITE OR APPLICATION FROM MY PRIVATE SUBNET.BUT NOW THIS IS WHAT AS PER THE GUIDELINES IAM DOING.)

Internet gateway igw-08d814355cbdbbdd4 successfully attached to vpc-04e14667aadc10df3 X

igw-08d814355cbdbbdd4 / ROSH_SUNETS_IGW_ELEVATELABS Actions ▾

Details <small>Info</small>		VPC ID	Owner
Internet gateway ID	igw-08d814355cbdbbdd4	vpc-04e14667aadc10df3 roshans_elevatelabs_vpc	518286664533
State	Attached		

Tags Manage tags

Key	Value
Name	ROSH_SUNETS_IGW_ELEVATELABS

NOW AFTER DOING THIS I HAVE CREATED MY OWN ROUTE TABLE MANUALLY HERE IAM TRYING TO ACCESS THE PUBLIC SUBNET AND WANT O GIVE SOME ANSWER WHICH I WILL SHOW LATER BUT INITIALLY A ROUTE TABLE IS CREATED AS SHOWN IN THE BELOW FIGURE USING THE SAME VPC ID FOR MY VPC WHICH I CREATED NOT THE DEAFULT ONE DON'T USE THE DEFAULT ONE.

ROUTE TABLE CREATED USING THIS NAME

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
<input type="text" value="Q_ Name"/>	<input type="text" value="Q_ RT-01-ELEVATERLABS"/> X Remove

Add new tag

You can add 49 more tags.

Cancel Create route table

AFTER EDITING I HAVE CREATED SUCCESSFULLY.

Route table rtb-051f656f1ba398f51 | RT-01-ELEVATE-LABS was created successfully. X

rtb-051f656f1ba398f51 / RT-01-ELEVATE-LABS Actions ▾

Details Info

Route table ID <input type="text" value="rtb-051f656f1ba398f51"/>	Main <input type="checkbox"/>	Explicit subnet associations -	Edge associations -
VPC <input type="text" value="vpc-04e14667aadc10df3 roshans_elevatelabs_vpc"/>	Owner ID <input type="text" value="518286664533"/>		

Routes Subnet associations Edge associations Route propagation Tags

Routes (1) Both ▾ Edit routes

Destination		Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	Create Route Table	

NOW AFTER THIS IN ROUTE TABLES → EDIT ROUTES IAM EDITING THE ROUTES VIA THIS INFORMATION THAT IS PROVIDING ALL TRAFFIC MEANING 0.0.0.0/0 TO THE INTERNET GATEWAY.

Edit routes

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	CreateRouteTable
Q_ 0.0.0.0/0	X Internet Gateway	-	No	CreateRoute
	Q igw-	X		
	Use: "igw-"			
	igw-08d814355cbd8dd4 (ROSH_SUNETS_IGW_ELEVATELABS)			
	Add route			
				Remove

THE INTERNET GATEWAY WHICH I BUILT IAM SELECTING.WE CAN SEE IN THE ABOVE FIGURE.

I HAVE UPDATED THE ROUTE TABLE WITH THE INTERNET GATEWAY ROUTING THAT IS GIVING ALL TRAFFIC 0.0.0.0/0 TO THE INTERNET GATEWAY.

⌚ Updated routes for rtb-051f656f1ba398f51 / RT-01-ELEVATE-LABS successfully Details																				
rtb-051f656f1ba398f51 / RT-01-ELEVATE-LABS																				
Actions																				
Details Info																				
<table border="1"> <tr> <td>Route table ID</td> <td>Main</td> <td>Explicit subnet associations</td> <td>Edge associations</td> </tr> <tr> <td>rtb-051f656f1ba398f51</td> <td><input checked="" type="checkbox"/> No</td> <td>-</td> <td>-</td> </tr> <tr> <td>VPC</td> <td>Owner ID</td> <td></td> <td></td> </tr> <tr> <td>vpc-04e14667aadcc10df3 roshans_elevatelabs_vpc</td> <td>518286664533</td> <td></td> <td></td> </tr> </table>					Route table ID	Main	Explicit subnet associations	Edge associations	rtb-051f656f1ba398f51	<input checked="" type="checkbox"/> No	-	-	VPC	Owner ID			vpc-04e14667aadcc10df3 roshans_elevatelabs_vpc	518286664533		
Route table ID	Main	Explicit subnet associations	Edge associations																	
rtb-051f656f1ba398f51	<input checked="" type="checkbox"/> No	-	-																	
VPC	Owner ID																			
vpc-04e14667aadcc10df3 roshans_elevatelabs_vpc	518286664533																			
Routes Subnet associations Edge associations Route propagation Tags																				
Routes (2)																				
<table border="1"> <thead> <tr> <th>Destination</th> <th>Target</th> <th>Status</th> <th>Propagated</th> <th>Route Origin</th> </tr> </thead> <tbody> <tr> <td>0.0.0.0/0</td> <td>igw-08d814355cbd8dd4</td> <td>Active</td> <td>No</td> <td>Create Route</td> </tr> <tr> <td>10.0.0.0/16</td> <td>local</td> <td>Active</td> <td>No</td> <td>Create Route Table</td> </tr> </tbody> </table>					Destination	Target	Status	Propagated	Route Origin	0.0.0.0/0	igw-08d814355cbd8dd4	Active	No	Create Route	10.0.0.0/16	local	Active	No	Create Route Table	
Destination	Target	Status	Propagated	Route Origin																
0.0.0.0/0	igw-08d814355cbd8dd4	Active	No	Create Route																
10.0.0.0/16	local	Active	No	Create Route Table																
Edit routes																				

NOW AFTER THIS IAM GOING TO GO FOR SUBNET ASSOCIATIONS IN THE SUBNET SECTION.SO NOW HERE I HAVE CONFIGURED THE ROUTE TABLE ASSOCIATIONS SUCCESSFULLY.

Subnet (subnet-07beb24b686ba19e6) has been successfully associated with route table (rtb-051f656f1ba398f51).

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	IPv6 CIDR	IPv6 CIDR association ID
-	subnet-00baef85838381c59f	Available	vpc-062ab221c16cb443d	Off	17.231.0.0/20	-	-
-	subnet-0a4785f80a36418ea	Available	vpc-062ab221c16cb443d	Off	17.231.32.0/20	-	-
-	subnet-0185d2cbbf97fc399	Available	vpc-062ab221c16cb443d	Off	17.231.16.0/20	-	-
<input checked="" type="checkbox"/> rosh_sub1_elevatelabs_public	subnet-07beb24b686ba19e6	Available	vpc-04e14667aad10df3 rosh...	Off	10.0.1.0/24	-	-
<input type="checkbox"/> rosh_sub2_elevatelabs_private	subnet-098b6aaac45db34ad	Available	vpc-04e14667aad10df3 rosh...	Off	10.0.2.0/24	-	-

subnet-07beb24b686ba19e6 / rosh_sub1_elevatelabs_public

Details | Flow logs | Route table | Network ACL | CIDR reservations | Sharing | Tags

Details

Subnet ID	subnet-07beb24b686ba19e6	Subnet ARN	arn:aws:ec2:ap-south-1:518286664533:subnet/subnet-07beb24b686ba19e6	State	Available	Block Public Access	Off
IPv4 CIDR	10.0.1.0/24	Available IPv4 addresses	251	IPv6 CIDR	-	IPv6 CIDR association ID	-
Availability Zone	ap-s1-a2z1 (ap-south-1a)	Network border group	ap-south-1	VPC	vpc-04e14667aad10df3 roshans_elevatelabs_vpc	Route table	rtb-051f656f1ba398f51 RT-01-ELEVATE-LABS
Network ACL	acl-00f50c3de649d595d	Default subnet	No	Auto-assign public IPv4 address	No	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	Hostname type	IP name	Resource name DNS A record	Disabled
Resource name DNS AAAA record				Owner			

IAM CREATING A PRIVATE ROUTE TABLE FOR THE PRIVATE SUBNET AND IAM NOT GOING TO ADD ANY INTERNET ACCESS TO THE PRIVATE SUBNET.THAT IS IAM NOT GOING TO ADD ROUTE 0.0.0.0/0 TO THE PRIVATE SUBNET.

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
<input type="text" value="Name"/>	<input type="text" value="RT-01-ELEVATE-LABS-PRIVATE"/> X Remove

[Add new tag](#)
You can add 49 more tags.

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

Route table rtb-096b232164ea60c74 | RT-02-ELEVATE-LABS-PRIVATE was created successfully.

rtb-096b232164ea60c74 / RT-02-ELEVATE-LABS-PRIVATE

[Actions ▾](#)

Details		Info	
Route table ID	rtb-096b232164ea60c74	Main	Explicit subnet associations
VPC	vpc-04e14667aadcc10df3 roshans_elevate labs_vpc	No	-
Owner ID	518286664533	Edge associations	-

[Routes](#) [Subnet associations](#) [Edge associations](#) [Route propagation](#) [Tags](#)

Routes (1)					
<input type="text"/> Filter routes				Both ▾ Edit routes	
Destination	Target	Status	Propagated	Route Origin	Create Route Table
10.0.0.0/16	local	Active	No		

ONCE WE HAVE CREATED THIS ROUTE TABLE WE HAVE TO GO TO THE SUBNET ASSOCIATIONS BUT THERE IN SUBNET WE HAVE ROUTE ASSOCIATIONS SO GO THERE AND CHANGE IF WE WANT BUT NOW WE HAVE TO ATTACH THIS ROUTE TO OUR PRIVATE SUBNET.

IN SUBNET 2 IAM NOT ADDING ANY ROUTES OR GATEWAYS AND MAKING IT AS A PRIVATE SUBNET AND HERE IAM JUST ADDING OR ATTACHING MY PRIVATE ROUTE TABLE.

Subnet route table settings

Subnet ID
subnet-098b6aac45db34ad

Route table ID
rtb-096b232164ea60c74 (RT-02-ELEVATE-LABS-PRIVATE) [C](#)

Routes (1)					
<input type="text"/> Filter routes				Both ▾ Edit routes	
Destination	Target				
10.0.0.0/16	local				

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

HERE I HAVE SUCCESSFULLY ADDED THE PRIVATE ROUTE TABLE.

Subnet (1/5) Info

Last updated less than a minute ago Actions Create subnet

Find subnets by attribute or tag

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	IPv6 CIDR	IPv6 CIDR association ID
-	subnet-00baef85838381c59f	Available	vpc-062ab221c16cb445d	Off	172.31.0.0/20	-	-
-	subnet-0a4785f80a36418ea	Available	vpc-062ab221c16cb445d	Off	172.31.32.0/20	-	-
-	subnet-0185d2cbff97fc399	Available	vpc-062ab221c16cb445d	Off	172.31.16.0/20	-	-
rosh_sub1_elevatelabs_public	subnet-07beb24b6866ba19e6	Available	vpc-04e14667aadcc10df3 rosh...	Off	10.0.1.0/24	-	-
<input checked="" type="checkbox"/> rosh_sub2_elevatelabs_private	subnet-098b6aaac45db34ad	Available	vpc-04e14667aadcc10df3 rosh...	Off	10.0.2.0/24	-	-

subnet-098b6aaac45db34ad / rosh_sub2_elevatelabs_private

Details

Subnet ID	subnet-098b6aaac45db34ad	Subnet ARN	arn:aws:ec2:ap-south-1:518286664533:subnet/subnet-098b6aaac45db34ad	State	Available
IPv4 CIDR	10.0.2.0/24	Available IPv4 addresses	251	IPv6 CIDR	-
Availability Zone	aps1-az3 (ap-south-1b)	Network border group	ap-south-1	VPC	vpc-04e14667aadcc10df3 roshans_elevatelabs_vpc
Network ACL	acl-00f50c3de649d595d	Default subnet	No	Auto-assign public IPv4 address	No
Auto-assign customer-owned IPv4 address	No	Customer-owned IPv4 pool	-	Outpost ID	-

Block Public Access

IPv6 CIDR association ID -

Route table rtb-096b232164ea60c74 | RT-02-ELEVATE-LABS-PRIVATE

Auto-assign IPv6 address No

IPv4 CIDR reservations -

IN ROUTES IAM JUST GOING TO SELECT 0.0.0.0/0 AND TARGET IAM NOT GIVING ANYTHING SO CANNOT ACCESS THE INTERNET GATEWAY.WHICH MEANS SUNET 2 WILL NOT RECEIVE THE INTERNET ACCESS.

THE ERROR WHEN I TRIED TO SAVE MY CHANGES WAS WE HAVE TO SPECIFY THE TARGET GROUP SO DOONT SPECIFY CURRENTLY ANYTHING U CAN JUST LEAVE IT AS IT IS THAT IS DEFAULT WITHOUT ANYTHING TO BE SAVED . TO ACCESS THE PRIVATE SUBNET WE CAN USE BASTION HOST OR JUMP SERVER WHICH IS GIVEN IN MY OTHER FILE PROJECT IN WHICH I DEPLOYED AN APPLICATION FROM MY PRIVATE SUBNET.

Edit routes

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	CreateRouteTable
Q 0.0.0.0/0	<input style="border: 1px solid red; color: red; background-color: white; width: 100%; height: 20px; margin-top: 5px;" type="text" value="local"/>	-	No	CreateRoute

Add route Remove Cancel Preview Save changes

NEXT AFTER DOING ALL THESE THINGS THE MAJOR IMPORTANT FACTOR IS ENABLING OR AUTO ASSIGNING THE PUBLIC IPV4 ADDRESS ASSIGNS THIS FOR THE PUBLIC SUBNET NOT FOR THE PRIVATE SUBNET.

- 1) Go to Subnets → Select your Public Subnet
- 2) Click Actions → Modify auto-assign IP settings
- 3) Check Auto-assign IPv4 address
- 4) Save

Edit subnet settings [Info](#)

Subnet

Subnet ID [subnet-07beb24b686ba19e6](#)

Name [rosh_sub1_elevatelabs_public](#)

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

DNS64 settings
Enable DNS64 to allow IPv6-only services in Amazon VPC to communicate with IPv4-only services and networks.

Enable DNS64 [Info](#)

JUST ENABLE AUTO ASSIGN PUBLIC IPV4 ADDRESS.

Edit subnet settings [Info](#)

Subnet

Subnet ID [subnet-07beb24b686ba19e6](#)

Name [rosh_sub1_elevatelabs_public](#)

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

DNS64 settings
Enable DNS64 to allow IPv6-only services in Amazon VPC to communicate with IPv4-only services and networks.

Enable DNS64 [Info](#)

NOW AFTER THIS WE WILL BE GETTING THE INTERNET ACCESS FOR SUBNET 1 AND NOT FOR SUBNET 2.

Edit subnet settings Info

Subnet

Subnet ID	Name
subnet-07beb24b686ba19e6	rosh_sub1_elevatelabs_public

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.

<input checked="" type="checkbox"/> Enable auto-assign public IPv4 address <small>Info</small>
<input type="checkbox"/> Enable auto-assign customer-owned IPv4 address <small>Info</small> 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.

<input type="checkbox"/> Enable resource name DNS A record on launch <small>Info</small>
<input type="checkbox"/> Enable resource name DNS AAAA record on launch <small>Info</small>

Hostname type Info

<input type="radio"/> Resource name
<input checked="" type="radio"/> IP name

DNS64 settings
Enable DNS64 to allow IPv6-only services in Amazon VPC to communicate with IPv4-only services and networks.

<input type="checkbox"/> Enable DNS64 <small>Info</small>

CLICK ON SAVE.REST EVERYTHING KEEP IT AS DEFAULT.

WE HAVE SUCCESSFULLY ASSIGNED THE PUBLIC IPV4 ADDRESS.

You have successfully changed subnet settings:

- Enable auto-assign public IPv4 address

Subnets (1/5) Info

Last updated less than a minute ago [Actions](#) [Create subnet](#)

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	IPv6 CIDR	IPv6 CIDR association ID
-	subnet-0a4785f80a36418ea	Available	vpc-062ab221c16cb443d	<input type="radio"/> Off	172.31.32.0/20	-	-
-	subnet-0185d2ccb97fc399	Available	vpc-062ab221c16cb443d	<input type="radio"/> Off	172.31.16.0/20	-	-
<input checked="" type="checkbox"/> rosh_sub1_elevatelabs_public	subnet-07beb24b686ba19e6	Available	vpc-04e14667aadcc10df3 rosh...	<input type="radio"/> Off	10.0.1.0/24	-	-
-	subnet-098b6aaac45db34ad	Available	vpc-04e14667aadcc10df3 rosh...	<input type="radio"/> Off	10.0.2.0/24	-	-

subnet-07beb24b686ba19e6 / rosh_sub1_elevatelabs_public

[Details](#) [Flow logs](#) [Route table](#) [Network ACL](#) [CIDR reservations](#) [Sharing](#) [Tags](#)

Details

Subnet ID subnet-07beb24b686ba19e6	Subnet ARN arn:aws:ec2:ap-south-1:518286664533:subnet/subnet-07beb24b686ba19e6	State Available	Block Public Access <input type="radio"/> Off
IPv4 CIDR 10.0.1.0/24	IPv6 CIDR -	IPv6 CIDR association ID -	Route table rtb-051f656f1ba39bf51 RT-01-ELEVATE-LABS-PUBLIC
Availability Zone aps1-az1 (ap-south-1a)	Network border group ap-south-1	VPC vpc-04e14667aadcc10df3 roshans_elevatelabs_vpc	Auto-assign IPv6 address No
Network ACL acl-00f50c3de649d595d	Default subnet No	Customer-owned IPv4 pool -	IPv4 CIDR reservations -
Auto-assign customer-owned IPv4 address No	Customer-owned IPv4 pool -	Hostname type IP name	Resource name DNS A record Disabled
IPv6 CIDR reservations -	IPv6-only No		

SO WHAT I HAVE CREATED I CAN SHOW IN MY PREVIEW DIAGRAM IN MY OWN VPC WHICH I CREATED WHICH GIVES THE CIDR BLOC VPC NAME CONFIGURATIONS,SUBNET DETAILS

PREVIEW DIAGRAM:-

Your VPCs (1/2) [Info](#)

Last updated 13 minutes ago [Actions](#) [Create VPC](#)

Name	VPC ID	State	Block Public...	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route table	
ync-062ab221c16cb443d	Available	Off	172.31.0.0/16	-	dopt-013e43a9bf3b478...	rtb-070801c956006d3ac	acl-C	
roshans_elevatelabs_vpc	Available	Off	10.0.0.0/16	-	dopt-013e43a9bf3b478...	rtb-04a9633f2a04ccde8	acl-C	

vpc-04e14667aadcd10df3 / roshans_elevatelabs_vpc

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

Resource map [Info](#)

Show all details

```

graph LR
    VPC[Your AWS virtual network  
roshans_elevatelabs_vpc] --- Subnets[Subnets (2)  
Subnets within this VPC]
    Subnets --- apsouth1a[ap-south-1a  
rosh_sub1_elevatelabs_public]
    Subnets --- apsouth1b[ap-south-1b  
rosh_sub2_elevatelabs_private]
    apsouth1a --- RT02[RT-02-ELEVATE-LABS-PRIVATE]
    apsouth1b --- RT01[RT-01-ELEVATE-LABS-PUBLIC]
    RT02 --- NC[ROSH_SUNETS_IGW_ELEVATELABS]
    RT01 --- NC
  
```

ARCHITECTURE SETUP (RESOURCE MAP IN VPC)

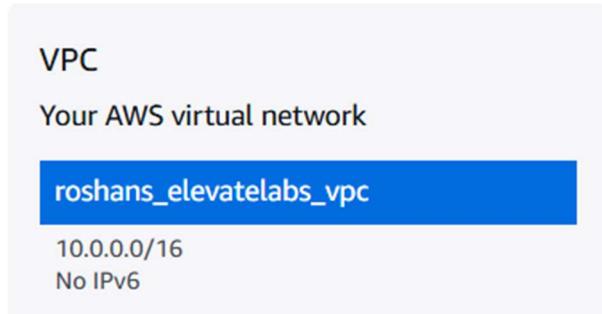
Details [Resource map](#) CIDs | Flow logs | Tags | Integrations

Resource map [Info](#)

```

graph LR
    VPC[Your AWS virtual network  
roshans_elevatelabs_vpc] --- Subnets[Subnets (2)  
Subnets within this VPC]
    Subnets --- apsouth1a[ap-south-1a  
rosh_sub1_elevatelabs_public]
    Subnets --- apsouth1b[ap-south-1b  
rosh_sub2_elevatelabs_private]
    apsouth1a --- RT02[RT-02-ELEVATE-LABS-PRIVATE]
    apsouth1b --- RT01[RT-01-ELEVATE-LABS-PUBLIC]
    RT02 --- NC[ROSH_SUNETS_IGW_ELEVATELABS]
    RT01 --- NC
  
```

VPC name:- roshans_elevatelabs_vpc



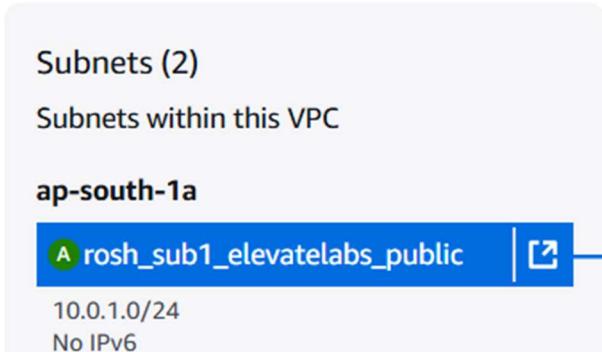
CIDR block:- 10.0.0.0/16 (VPC)

Subnet 1 :- 10.0.1.0/24
Subnet 2: 10.0.2.0/24

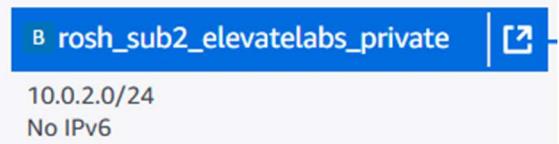
Subnet details

Subnet 1 has internet gateway which allows all traffic(0.0.0.0/0)

Subnet 2 has internet gateway which does not allow traffic and does not have an internet gateway so private can be accessed via bastion host or jump server.



ap-south-1b



Routing configuration:-

PUBLIC ROUTE TABLE:-

<input checked="" type="checkbox"/>	RT-01-ELEVATE-LABS-PUBLIC	rtb-051f656f1ba398f51	subnet-07beb24b686ba1...	-	No	vpc-04e14667aadc10df3 rosh...	518286664533
<input type="checkbox"/>	RT-02-ELEVATE-LABS-PRIVATE	rtb-096b232164ea60c74	subnet-098b6aaac45db3...	-	No	vpc-04e14667aadc10df3 rosh...	518286664533

rtb-051f656f1ba398f51 / RT-01-ELEVATE-LABS-PUBLIC

[Details](#) | [Routes](#) | [Subnet associations](#) | [Edge associations](#) | [Route propagation](#) | [Tags](#)

Details

Route table ID: rtb-051f656f1ba398f51
VPC: vpc-04e14667aadc10df3 | roshans_elevatelabs_vpc

Main: No
Owner ID: 518286664533

Explicit subnet associations: subnet-07beb24b686ba19e6 / rosh_sub1_elevatelabs_public

Edge associations: -

PRIVATE ROUTE TABLE:-

<input checked="" type="checkbox"/>	RT-02-ELEVATE-LABS-PRIVATE	rtb-096b232164ea60c74	subnet-098b6aaac45db3...	-	No	vpc-04e14667aadc10df3 rosh...	518286664533
-------------------------------------	----------------------------	-----------------------	--------------------------	---	----	---------------------------------	--------------

rtb-096b232164ea60c74 / RT-02-ELEVATE-LABS-PRIVATE

[Details](#) | [Routes](#) | [Subnet associations](#) | [Edge associations](#) | [Route propagation](#) | [Tags](#)

Details

Route table ID: rtb-096b232164ea60c74
VPC: vpc-04e14667aadc10df3 | roshans_elevatelabs_vpc

Main: No
Owner ID: 518286664533

Explicit subnet associations: subnet-098b6aaac45db3ad / rosh_sub2_elevatelabs_private

Edge associations: -

Public route table configurations:-

rtb-051f656f1ba398f51 / RT-01-ELEVATE-LABS-PUBLIC

[Details](#) | [Routes](#) | [Subnet associations](#) | [Edge associations](#) | [Route propagation](#) | [Tags](#)

Routes (2)

Filter routes

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-08d814355cbd8dd4	Active	No	Create Route
10.0.0.0/16	local	Active	No	Create Route Table

Both | [Edit routes](#)

Private route table configurations:-

rtb-096b232164ea60c74 / RT-02-ELEVATE-LABS-PRIVATE

[Details](#) | [Routes](#) | [Subnet associations](#) | [Edge associations](#) | [Route propagation](#) | [Tags](#)

Routes (1)

Filter routes

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	Create Route Table

Both | [Edit routes](#)

SO NOW THE QUESTION ARRISSES WHY NOT THE SAME ROUTE TABLE FOR BOTH SUBNETS WHAT ARE THE BENEFITS AND DEFECTS OF USING THE SAME ROUTE TABLE FOR PUBLIC AND PRIVATE SUBNET ?

ANSWER

Aspect	Separate Route Tables	Shared Route Table
Security	Public subnet exposed, private subnet isolated	Both subnets risk exposure if IGW is added
Clarity	Easy to understand and document	Ambiguous subnet roles
Control	Fine-grained routing per subnet	One-size-fits-all routing
NAT Gateway Support	Private subnet can route via NAT	Not possible without separate table
Compliance	Aligns with AWS Well-Architected Framework	May violate segmentation principles

Using the Same Route Table for Both Subnets

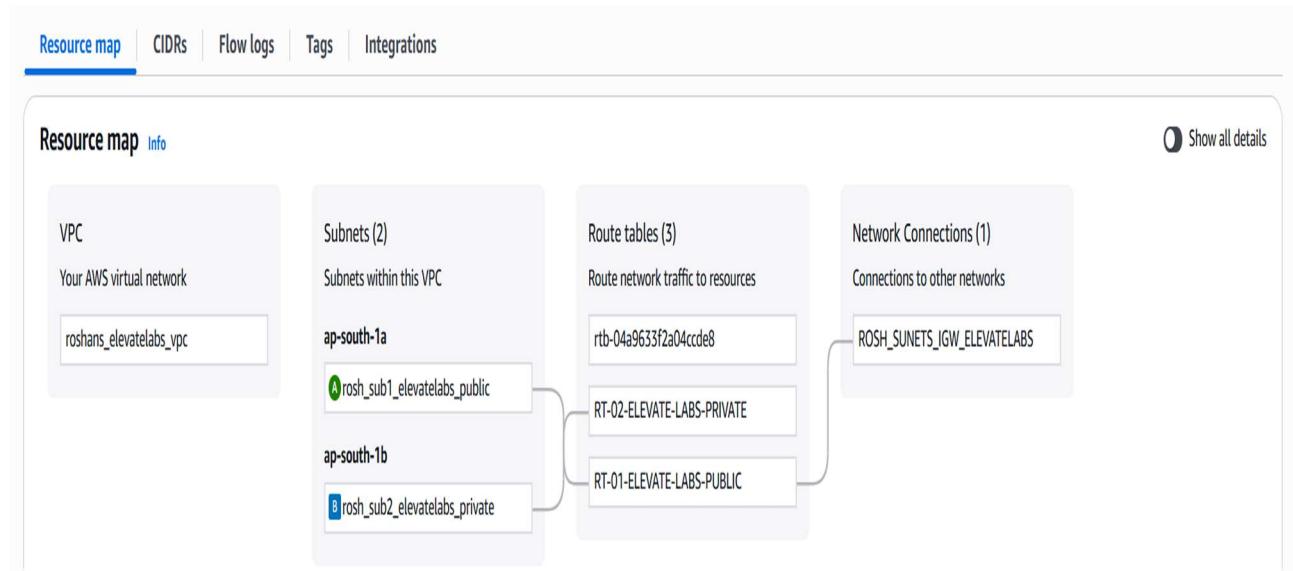
Benefits:-

- **Simplicity:** Fewer resources to manage; easier for small test environments.
- **Faster Setup:** One-time configuration for routing rules.
- **Cost-Free:** No extra charges for creating multiple route tables.

Drawbacks:-

- **Security Risk:** If the route table includes $0.0.0.0/0 \rightarrow$ IGW, both subnets get internet access—even the private one.
- **Harder to Audit:** You lose clarity on which subnet is meant to be public vs private.
- **No NAT Gateway Support:** You can't route private subnet traffic through a NAT Gateway without a separate route table.
- **Poor Scalability:** As your architecture grows (e.g., adding VPN, peering, or hybrid cloud), shared route tables become a bottleneck.
- **Fails Best Practices:** AWS recommends subnet isolation for production workloads, especially for sensitive services like databases.

FINAL ARCHITECTURE LOOKS LIKE THIS:-



CONCLUSION IS : I WAS ABLE TO UNDERSTAND HOW TO SETUP THE CONFIGURATIONS FOR MY OWN VPC AND HOW TO ATTACH AN INTERNET GATEWAY AND HOW TO ESTABLISH A ROUTE TABLE TO ROUTE THE TRAFFIC TO THE REQUIRED DESTINATION IN MY OTHER FILE I HAVE CLEARLY SHOWN HOW TO ACCESS THE PRIVATE SUBNET YOU CAN PLS USE THIS LINK FOR MY PROFILE F PROJECTS WHICH I DO INDEPENDENTLY.

Link is :- <http://github.com/Roshan-saral> to know more about the tools which I have used and also the bastion host to access the private subnet to deploy an application via the private subnet. I have used the concept of auto scaling groups to scale up or scale down the resources depending on the traffic and the demand. Thanks for this project could understand a lot.

RECENT ADVANCEMENTS IN VPC:-

Feature	Benefit	Use Case
VPC Lattice	Zero-trust, app-layer routing	Microservices, multi-account
IPAM Tiers	Scalable IP management	Multi-region VPCs
CloudTrail Endpoint Logs	Network visibility	Security auditing
IPv6 Dual-Stack	Future-proofing	Global apps, mobile
Service Network Endpoints	Simplified cross-account access	SaaS, internal APIs
Resource Gateways	Secure resource sharing	Private workloads

WHEN TO USE PUBLIC AND PRIVATE SUBNET:-

Scenario	Use Public Subnet	Use Private Subnet
Hosting a website	EC2 instance needs to be accessible from the internet	✗ Not suitable — no direct internet access
SSH access (bastion host)	Bastion host must be reachable from your local machine	Backend EC2 accessed via bastion in public subnet
Load balancer (ALB/NLB)	Public-facing load balancer requires internet traffic	Internal load balancer for private services
Database (e.g., RDS)	✗ Never — databases should not be exposed	✓ Ideal — isolated and secure
Application backend	✗ Avoid — backend logic should be protected	✓ Best for internal APIs and services
Outbound-only access (e.g., updates)	Direct internet access via public IP	Use NAT Gateway for secure outbound access
Sensitive data processing	✗ Risk of exposure	✓ Ensures compliance and isolation
Monitoring tools	Tools needing external connectivity (e.g., CloudWatch agent)	Internal metrics collection or logging agents

Summary:-

- **Public Subnet:** Use for resources that need inbound internet access (web servers, bastion hosts).
- **Private Subnet:** Use for resources that need isolation or outbound-only access (databases, internal apps).