

Production-Grade Cloud Networking Project

AWS VPC Design with Multi-Size Subnets & Controlled Internet Access

STEP 1: Steps to open **VPC** in AWS Console :

1. Login to **AWS** Console.
2. Make sure the region is **Asia Pacific (Mumbai)**.
3. In the search bar, type **VPC**.
4. Click on **VPC – Isolated Cloud Resources**.
5. You will be redirected to the **VPC Dashboard**.
6. From left menu you can create:
 - o VPC
 - o Subnets
 - o Route Tables
 - o Internet Gateway
 - o NAT Gateway
 - o Security Groups
 - o NACLs



STEP 2: create a **VPC**, next steps:

1. Click **Create VPC**.
2. Select **VPC only**.
3. Enter CIDR (example: 10.0.0.0/16).
4. Click **Create VPC**.

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

VPC only

VPC and more

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

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

IPv4 CIDR

 CIDR block must start from between /16 and /28.

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

Tenancy [Info](#)

VPC encryption control (\$) [Info](#)
 instant mode provides visibility into encrypted traffic without blocking traffic. It can't make present unencrypted traffic. Additional charges apply [Learn more](#)
 None
 Monitor mode
 See which resources in your VPC are encrypted but allow the creation of unencrypted instances.
 Enforce mode
 Requires all resources, except instances in your VPC to be encryption-capable and blocks creation of unencrypted resources.

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 tag](#)

[Add tag](#) You can add 40 more tags.

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

STEP 3: Create and attach an Internet Gateway (IGW) in AWS:

[Search](#) [\[AH-5\]](#) [All Services](#) [My Services](#)

[Internet gateway](#) > [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
 Create 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** [Remove](#)

[Add new tag](#) You can add 40 more tags.

[Cancel](#) [Create internet gateway](#)

A. Create Internet Gateway

1. Go to **VPC Dashboard**.
2. Click **Internet Gateways** (left menu).
3. Click **Create internet gateway**.
4. Enter **Name tag** → Aja IGW
5. (Optional) Add tags.
6. Click **Create internet gateway**.

B. Attach Internet Gateway to VPC

Name	Internet gateway ID	Status	VPC ID
Aja IGW	igw-0003846d1fb63203a	Attached	vpc-0ef0f81562027a67bbf7b4c30c
IBM vPC	igw-0c248c299772ac4	Unattached	-

7. Select the created IGW
8. Click **Actions** → **Attach to VPC**.
9. Choose your VPC (example: Aja-VPC or 10.0.0.0/16).
10. Click **Attach internet gateway**.

C. Add Route to Public Subnet

11. Go to **Route Tables**.
12. Select your **Public Route Table**.
13. Click **Edit routes** → **Add route**.
14. Destination: 0.0.0.0/0
15. Target: **Internet Gateway (Aja IGW)**.
16. Click **Save routes**.

Now your **public subnet has internet access**.

STEP 4: To create the Subnet

1. Go to **VPC Dashboard**.
2. Click **Subnets** → **Create subnet**.
3. Select your **VPC** (example: 10.0.0.0/16).
4. Under **Subnet 1 of 3**:
 - **Subnet name:** SHARED
 - **Availability Zone:** Select **No preference** (or choose ap-south-1a if needed)
 - **IPv4 VPC CIDR block:** 10.0.0.0/16
 - **IPv4 subnet CIDR block:** 10.0.0.0/19
(This gives 8,192 IPs)
5. Tags (optional):
 - Key: Name
 - Value: SHARED
6. Click **Create subnet**.

If you are creating 6 subnets.

Subnets (8) Info

ID: Each identifies the subnet's IP range.

Name	Subnet ID	Status	VPC	Block Range... <small>IPv4 CIDR</small>	IPv4 CIDR	IPv6 CIDR
IBM DB subnet	subnet-01eef0f112e1e0ca	Available	vpc-0973a982952a406d	10.0.16.0/24	10.0.16.0/24	-
VWU	subnet-01eef0f112e1e0ca	Available	vpc-0973a982952a406d	10.0.16.0/22	10.0.16.0/22	-
SHARED	subnet-01eef0f112e1e0ca	Available	vpc-0973a982952a406d	10.0.0.0/19	10.0.0.0/19	-
EDDP	subnet-01eef0f112e1e0ca	Available	vpc-0973a982952a406d	10.0.40.0/23	10.0.40.0/23	-
PLATFOR	subnet-01eef0f112e1e0ca	Available	vpc-0973a982952a406d	10.0.42.0/24	10.0.42.0/24	-
IBM APP subnet	subnet-01eef0f112e1e0ca	Available	vpc-0973a982952a406d	10.0.44.0/24	10.0.44.0/24	-
APP	subnet-01eef0f112e1e0ca	Available	vpc-0973a982952a406d	10.0.45.0/24	10.0.45.0/24	-
ADMN	subnet-01eef0f112e1e0ca	Available	vpc-0973a982952a406d	10.0.46.0/24	10.0.46.0/24	-

Select a subnet

Subnet 1 of 3

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

SHARED

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.

No preference

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

10.0.0.0/16

IPv4 subnet CIDR block

10.0.0.0/19 8,192 IPs

< > ^ v

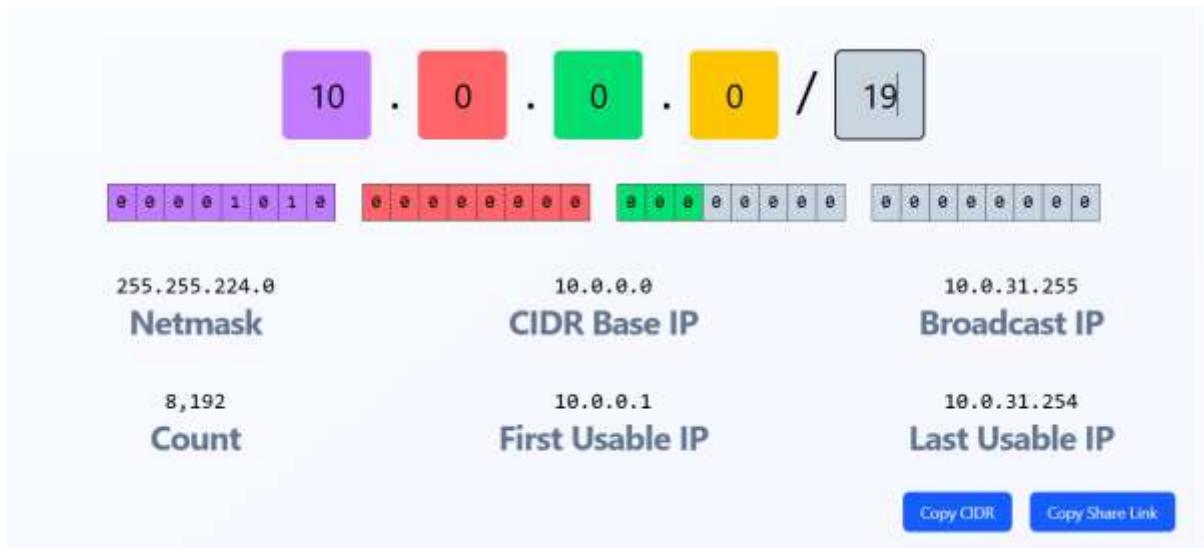
Tags - optional

Key	Value - optional
<input type="text" value="Name"/> Name	<input type="text" value="SHARED"/> SHARED

Add new tag

You can add 49 more tags.

Remove



Subnet 2 of 3

Subnet name

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

PLATFORM

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.

No preference



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.

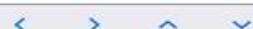
10.0.0.0/16



IPv4 subnet CIDR block

10.0.32.0/20

4,096 IPs



▼ Tags - optional

STEP 5 : Create Route Table

1. Go to **VPC Dashboard**.
2. Click **Route Tables** (left side).
3. Click **Create route table**.
4. In **Name**: AJA Public RT
5. Select **VPC**: Aja VPC (10.0.0.0/16)
6. Tags:
 - o Key: Name
 - o Value: AJA Public RT
7. Click **Create route table**.

B. Add Internet Route

8. Select the created route table (AJA Public RT).
9. Go to **Routes** tab → Click **Edit routes**.
10. Click **Add route**:
 - o Destination: 0.0.0.0/0
 - o Target: **Internet Gateway (Aja IGW)**
11. Click **Save routes**.

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	Actions
<input type="text" value="Name"/>	<input type="text" value="AIA Public RT"/> <small>X</small> <small>Remove</small>	<small>Add new tag</small>

You can add 49 more tags.

Cancel **Create route table**

Select	Route table name	Status	Propagated	Owner	Last modified
<input checked="" type="checkbox"/>	AIA Private RT	rb-0ac69d51db894d3a58	-	Yes	vpc-0ed59142dc97ad1ee AIA ... 914970130631
<input type="checkbox"/>	-	rb-09a33d16bb406adef67	-	Yes	vpc-087bcbfbf975db97f4 IBM ... 914970130631
<input type="checkbox"/>	-	rb-0f55fd49b0ca4ff743	-	Yes	vpc-07ecf576849c8663 914970130631
<input checked="" type="checkbox"/>	AIA Public RT	rb-0c70708fc20388725	-	No	vpc-0ed59142dc97ad1ee AIA ... 914970130631

C. Associate with Public Subnet

12. Go to **Subnet associations** tab.
13. Click **Edit subnet associations**.
14. Select your **Public subnet**.
15. Click **Save associations**.

Now your public subnet can access the internet.

VPC > Route tables

VPC dashboard <

AWS Global View (1)

Filter by VPC

Virtual private cloud

- Your VPCs
- Subnets
- Route tables**
- Internet gateways
- Transit-only internet gateways
- DHCP option sets
- Route Plots
- Managed prefix lists
- NAT gateways
- Pending connections
- Route servers

Security

- Network ACLs
- Security groups

PrivateLink and Latency

- Getting started
- Endpoints
- Endpoint services

Route tables (1/6) **rtb-0c7d708fca3088723 / AIA Public RT**

Actions | Create route table

Last updated 3 minutes ago

Name	Route Table ID	Explicit subnet associations	Edge associations	Main	VPC	Owner ID
IBM Route APP	rtb-0290a0a793a1e159	subnet-0230a0a793a1e159	-	No	vpc-033a09f75da37141801	914970130631
IBM Route DB	rtb-0077a180a153a5d1	subnet-0000a0a793a1e159	-	No	vpc-033a09f75da37141801	914970130631
AIA Private RT	rtb-0972a1193a0a910	-	-	Yes	vpc-0ed19142a37ea7141801	914970130631
-	rtb-29a0a0a793a1e159	-	-	Yes	vpc-033a09f75da37141801	914970130631
-	rtb-0077a180a153a5d1	-	-	Yes	vpc-033a09f75da37141801	914970130631
AIA Public RT	rtb-0c7d708fca3088723	-	-	No	vpc-0ed19142a37ea7141801	914970130631

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

Explicit subnet associations (0)

Filter subnet associations

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
WEB	subnet-08e1ef139067e91ae	10.0.56.0/22	-	Main rtb-0ad6f
SHARED	subnet-053bb05258fbfa1	10.0.0.0/19	-	Main rtb-0ad6f
EDGE	subnet-01796265d5c47a55	10.0.60.0/23	-	Main rtb-0ad6f
PLATFORM	subnet-0afef0fa15771ad1e	10.0.32.0/20	-	Main rtb-0ad6f
APP	subnet-007511bd4a05264f	10.0.48.0/21	-	Main rtb-0ad6f
ADMIN	subnet-0fec2a0a95088724	10.0.62.0/24	-	Main rtb-0ad6f

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/6)

Filter subnet associations

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
WEB	subnet-08e1ef139067e91ae	10.0.56.0/22	-	Main rtb-0ad6f
SHARED	subnet-053bb05258fbfa1	10.0.0.0/19	-	Main rtb-0ad6f
EDGE	subnet-01796265d5c47a55	10.0.60.0/23	-	Main rtb-0ad6f
PLATFORM	subnet-0afef0fa15771ad1e	10.0.32.0/20	-	Main rtb-0ad6f
APP	subnet-007511bd4a05264f	10.0.48.0/21	-	Main rtb-0ad6f
ADMIN	subnet-0fec2a0a95088724	10.0.62.0/24	-	Main rtb-0ad6f

Selected subnets

subnet-0fec2a0a95088724 / ADMIN X | subnet-01796265d5c47a55 / EDGE X

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

You have successfully updated subnet associations for rtb-0ac69d51d094d8a38 / AIA-Private-RT.

Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC	Owner ID
IBM Route APP	rtb-0000000000000000	subnet-0000000000000000	-	No	vpc-0000000000000000	91497013661
IBM Route On	rtb-0000000000000000	subnet-0000000000000000	-	No	vpc-0000000000000000	91497013661
AIA-Private-RT	rtb-0ac69d51d094d8a38	-	-	Yes	vpc-0000000000000000	91497013661
-	rtb-0000000000000000	-	-	Yes	vpc-0000000000000000	91497013661
-	rtb-0000000000000000	-	-	Yes	vpc-0000000000000000	91497013661
AIA-Public-RT	rtb-0000000000000000	2 subnets	-	No	vpc-0000000000000000	91497013661

STEP 6: To add Internet Gateway route:

1. Go to **VPC Dashboard**
2. Click **Route Tables**
3. Select your route table
4. Click **Routes tab**
5. Click **Edit routes**

Now add this:

6. Click **Add route**
7. In **Destination** → enter **0.0.0.0/0**
8. In **Target** → select **Internet Gateway (igw-xxxxxx)**

You will see:

- 10.0.0.0/16 → local (already there, don't change)
- 0.0.0.0/0 → igw-xxxxxx

9. Click **Save changes**

Now this subnet becomes **Public Subnet** (it has internet access).

Edit routes

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	CreateRouteTable
Q. 0.0.0.0	X			
Q. 0.0.0.0	Internet Gateway		No	CreateRoute
Q. igw-000ded6dcf8637034	X			
Use "igw-000ded6dcf8637034"				
igw-000ded6dcf8637034 (Aja VPC)				

Add route **Remove** **Cancel** **Preview** **Save changes**

STEP 7: You are in **Route Table → Edit routes**.

Right now it has only one rule:

10.0.0.0/16 → local

This means:

- All computers (EC2) inside your VPC can talk to each other.
- They **cannot go to the internet** yet.

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	CreateRouteTable
Q. 0.0.0.0	X			

Add route **Cancel** **Preview** **Save changes**

STEP 8: Instance creation for Validation and Testing

Simple steps to launch EC2 in your VPC:

1. Go to **EC2 → Instances → Launch instance**
2. Select **AMI: Ubuntu 24.04**
3. Select **Instance type: t3.micro**
4. In **Network settings**:
 - o VPC: **Aja VPC (10.0.0.0/16)**
 - o Subnet: **WEB (Public Subnet)**
 - o Auto-assign Public IP: **Enable**

5. Create Security Group:
 - Allow SSH (22) from 0.0.0.0/0
6. Select or create Key Pair
7. Click Launch instance

Network settings

VPC - required [info](#)
vpc-0ad593142d597ad7ee (A/p Vpc)
10.0.0.0/16

Subnet [info](#)
subnet-0f9aefc5258867d974
VPC: vpc-0ad593142d597ad7ee Owner: 914977130311 Availability Zone: ap-south-1a (ami-0f9aefc5258867d974)
IP addresses available: 10119 CIDR: 10.0.0.0/16/27/28

Create new subnet [info](#)

Auto-assign public IP [info](#)
Enable

Firewall (security groups) [info](#)
A security group is a set of network rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group [info](#)

Select existing security group [info](#)

Security group name - required [info](#)
Launch-wizard-5

This security group will be applied to all network interfaces. The name can't be edited after the security group is created. Max length is 32 characters. Valid characters: a-z, A-Z, 0-9, spaces, and '-' (0x2D)- (0x2F)

Description - required [info](#)
Launch-wizard-5 created 2026-01-28T11:42:37.967Z

Inbound Security Group Rules:

Security group rule 1 (TCP 22, 0.0.0.0/0)

[Remove](#)

Summary

Number of instances [info](#)
1

Software image (AMI) [info](#)
Canonical, Ubuntu, 24.04, ami-0... (latest)
ami-0f9aefc5258867d974

Virtual server type (instance type) [info](#)
t3.micro

Firewall (security group) [info](#)
New security group

Storage (volume) [info](#)
1 volume(s) - 8 GB

[Create](#) [Launch instance](#) [Preview code](#)

Private Subnet Validation

- EC2 instances in Web/App/Platform/Shared:
 - Cannot reach the internet
 - Can communicate internally

Why: No route to IGW exists



Network settings

VPC - required [info](#)
vpc-0ad593142d597ad7ee (A/p Vpc)
10.0.0.0/16

Subnet [info](#)
subnet-0f9aefc5258867d974
VPC: vpc-0ad593142d597ad7ee Owner: 914977130311 Availability Zone: ap-south-1a (ami-0f9aefc5258867d974)
IP addresses available: 10119 CIDR: 10.0.0.0/16/27/28

Create new subnet [info](#)

Auto-assign public IP [info](#)
Enable

Firewall (security groups) [info](#)
A security group is a set of network rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group [info](#)

Select existing security group [info](#)

Security group name - required [info](#)
Launch-wizard-6

This security group will be applied to all network interfaces. The name can't be edited after the security group is created. Max length is 32 characters. Valid characters: a-z, A-Z, 0-9, spaces, and '-' (0x2D)- (0x2F)

Description - required [info](#)
Launch-wizard-6 created 2026-01-28T11:42:38.516Z

[Remove](#)

Summary

Number of instances [info](#)
1

Software image (AMI) [info](#)
Canonical, Ubuntu, 24.04, ami-0... (latest)
ami-0f9aefc5258867d974

Virtual server type (instance type) [info](#)
t3.micro

Firewall (security group) [info](#)
New security group

Storage (volume) [info](#)
1 volume(s) - 8 GB

[Create](#) [Launch instance](#) [Preview code](#)

Public Subnet Validation

- EC2 instances in Admin/Edge can:
 - Resolve DNS
 - Reach external IPs
 - Access the internet

Why: Route table contains 0.0.0.0/0 → IGW

```
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-10-0-62-248:~$
```