

AWS VPC creation

VPC and subnets

Name	Default	Adjustable	Comments
VPCs per Region	5	Yes 	Increasing this quota increases the quota on internet gateways per Region by the same amount. You can increase this limit so that you can have hundreds of VPCs per Region.
Subnets per VPC	200	Yes 	
IPv4 CIDR blocks per VPC	5	Yes  (up to 50)	This primary CIDR block and all secondary CIDR blocks count toward this quota.
IPv6 CIDR blocks per VPC	5	Yes  (up to 50)	The number of /56 CIDRs you can allocate to a single VPC.

Elastic IP addresses

Name	Default	Adjustable	Comments
Elastic IP addresses per Region	5	Yes 	This quota applies to individual AWS account VPCs and shared VPCs.
Elastic IP addresses per public NAT gateway	2	Yes 	

Gateways

Name	Default	Adjustable	Comments
Egress-only internet gateways per Region	5	Yes 	To increase this quota, increase the quota for VPCs per Region. You can attach only one egress-only internet gateway to a VPC at a time.
Internet gateways per Region	5	Yes 	To increase this quota, increase the quota for VPCs per Region. You can attach only one internet gateway to a VPC at a time.
NAT gateways per Availability Zone	5	Yes 	NAT gateways only count toward your quota in the <code>pending</code> , <code>active</code> , and <code>deleting</code> states.
Private IP address quota per NAT gateway	8	Yes 	You can assign private IP addresses only to private NAT gateways.
Carrier gateways per VPC	1	No	

Network ACLs

Name	Default	Adjustable	Comments
Network ACLs per VPC	200	Yes 	You can associate one network ACL to one or more subnets in a VPC.
Rules per network ACL	20	Yes 	This quota determines both the maximum number of inbound rules and the maximum number of outbound rules. This quota can be increased up to a maximum of 40 inbound rules and 40 outbound rules (for a total of 80 rules), but network performance might be impacted.

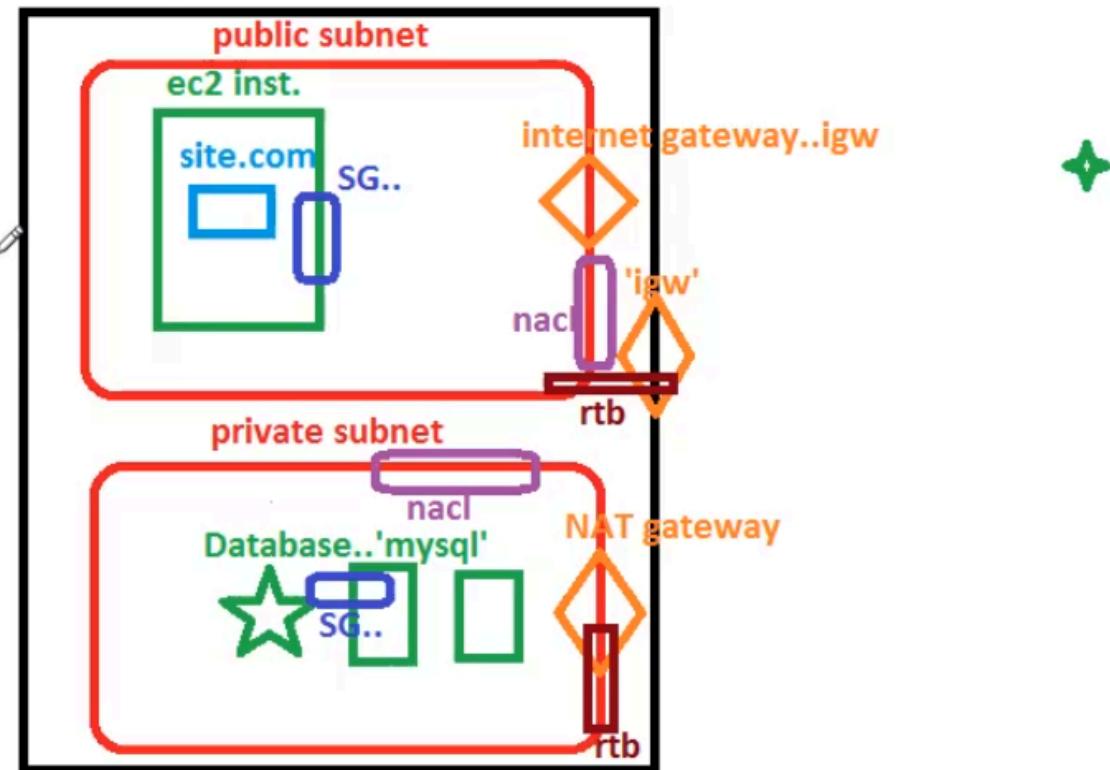
Route tables

Name	Default	Adjustable	Comments
Route tables per VPC	200	Yes 	The main route table counts toward this quota. Note that if you request a quota increase for route tables, you may also want to request a quota increase for subnets. While route tables can be shared with multiple subnets, a subnet can only be associated with a single route table.
Routes per route table (non-propagated routes)	50	Yes 	You can increase this quota up to a maximum of 1,000; however, network performance might be impacted. This quota is enforced separately for IPv4 routes and IPv6 routes. If you have more than 125 routes, we recommend that you paginate calls to describe your route tables for better performance.
Propagated routes per route table	100	No	If you require additional prefixes, advertise a default route.

Security groups

Name	Default	Adjustable	Comments
VPC security groups per Region	2,500	Yes 	This quota applies to individual AWS account VPCs and shared VPCs. If you increase this quota to more than 5,000 security groups in a Region, we recommend that you paginate calls to describe your security groups for better performance.
Inbound or outbound rules per security group	60	Yes 	This quota is enforced separately for IPv4 rules and IPv6 rules. Therefore, for an account with the default quota of 60 rules, a security group can have 60 inbound rules for IPv4 traffic and 60 inbound rules for IPv6 traffic. For more information, see Security group size . A quota change applies to both inbound and outbound rules. This quota multiplied by the quota for security groups per network interface cannot exceed 1,000.
Security groups per network interface	5	Yes  (up to 16)	This quota multiplied by the quota for rules per security group cannot exceed 1,000.

VPC..



- VPC is collection of subnets
- Two types of subnet are there : public subnet & private subnet
- Public subnet purpose : we create resources in a public subnet (resources like instance), because any public user/any user can access the resources.
- Private subnet purpose : we create a database (mysql) in a private subnet, because the database needs to be very secure and can not be accessed publicly. so public users can not access the database. we can also create instances/databases in private subnets, so no public user can access them.
- Suppose I have deployed a website in a public subnet's ec2 instance, then the user will request the information, then that request for the info is sent to the database from the public subnet's ec2 instance, and info is sent back to the public subnets website and then forwarded to the user.
- Can a user directly access the resource (database, instance) in a private subnet?
-> NO

- How to differentiate whether a subnet is public or private?

-> using gateways

Internet gateway : it is attached to the public subnet, it lets you access the resources publicly.

NAT gateway : it is attached to the private subnet.

This NAT gateway makes the private subnet more secure.

HOW? -> if a public user tries to access the private subnet, it rejects, it allows the resource in only one way. -> resources can access the internet through NAT gateway, but the internet can not access the resources in private subnets.

- Why does VPC need an internet gateway?

-> The internet gateway is connected at two levels, namely the VPC (Virtual Private Cloud) and subnet levels. This configuration is essential because instances within the VPC send requests to a NAT (Network Address Translation) device. The NAT device then forwards these requests to the VPC's internet gateway, which ultimately routes the traffic to the broader internet.

- Internet gateway :internet -> IGW -> resources -> IGW -> internet (two way communication in public subnet via IGW)

- How does the user/internet access the database?

-> user request is sent to the IGW of VPC then IGW of subnet then private subnet, the response from private subnet is sent back to the public subnet and then to the user.

- Security Group: security grp are attach at instance lvl
Both private and public resources have security groups.

- NACL : NACL is attached at subnet lvl, for both public and private subnet.

- User -> public subnet

User -> IGW -> public NACL (inbound rule in NACL, allowing this request) -> public instance SG (instance lvl, and inbound rule in SG, allowing this request)

- User -> private subnet

user -> IGW -> public NACL (inbound rule in NACL, allowing this request) -> public instance SG (instance lvl, and inbound rule in SG, allowing this request) -> private NACL (inbound rule in NACL, allowing this request) -> private instance SG (instance lvl, and inbound rule in SG, allowing this request) -> resource (response) -> private instance SG

(instance lvl, and outbound rule in SG, allowing this request) -> private NACL (outbound rule in NACL, allowing this request) -> public instance SG (instance lvl, and outbound rule in SG, allowing this request) -> public NACL (outbound rule in NACL, allowing this request) -> IGW -> user

- How to attach gateways to subnets?
-> route tables

Route tables : bridge between gateways to the subnets

Public subnet ->route tables-> IGW

Private subnet ->route tables-> NAT

Today

=====

```
--VPC..virtual private cloud
--VPC and components/Arch./steps
  1.create vpc
  2.create subnet(public,private)
  3.create gateways..igw,nat
  4.route tables
  5.attach gateways to subnets via rtb
  6.create SG
  7.create nacl
  8.associate nacl to subnet and SG to resource(inst.)
```

Sure, I can explain these fundamental concepts related to networking in the context of Amazon Web Services (AWS) and similar cloud environments:

1. ****VPC (Virtual Private Cloud):****

- A VPC is a logically isolated section of the AWS cloud where you can launch AWS resources such as EC2 instances, RDS databases, and more.
- It allows you to define your own network topology, including IP address ranges, subnets, route tables, and security settings.
- VPCs provide control over your network environment and can be connected to your on-premises data centres or other VPCs.

2. ****Subnet:****

- Subnets are subdivisions of a VPC's IP address range. They allow you to segment your VPC into smaller, more manageable networks.
- Each subnet is associated with a specific Availability Zone (AZ), and resources launched in a subnet are placed in the corresponding AZ.
- Subnets can be either public (accessible from the internet) or private (not

accessible from the internet).

3. **IP Addresses (Internet Protocol Addresses):**

- IP addresses are unique numerical labels assigned to devices on a network to identify and communicate with each other.

- In AWS, you can allocate IP addresses to instances, load balancers, and other resources. Two types of IP addresses are commonly used: private IPs (within a VPC) and public IPs (for internet-facing resources).

4. **Security Groups:**

- Security Groups are virtual firewalls that control inbound and outbound traffic for AWS resources.

- They are stateful, meaning that if you allow inbound traffic from a specific IP, the corresponding outbound reply traffic is automatically allowed.

- You can attach security groups to EC2 instances and other AWS resources to define the rules governing traffic to and from those resources.

5. **Routing Tables:**

- Routing tables determine how network traffic is directed within a VPC.

- Each subnet is associated with a routing table that specifies the routes for traffic leaving that subnet.

- Routing tables contain rules that determine whether traffic should be sent locally within the VPC or forwarded to other destinations, such as an Internet Gateway or VPN connection.

6. **Internet Gateway:**

- An Internet Gateway (IGW) is a horizontally scalable, highly available AWS resource that allows communication between instances in your VPC and the internet.

- It serves as a gateway for traffic going in and out of your VPC to and from the internet.

- To enable internet access for resources in a VPC, you must attach an IGW to the VPC and configure appropriate routing.

7. **Network Access Control Lists (NACLs):**

- NACLs are network-level security devices that act as a firewall for controlling inbound and outbound traffic at the subnet level.

- Unlike security groups, NACLs are stateless, meaning you must define both inbound and outbound rules separately.

- NACLs are less granular than security groups but can provide an additional layer of security for your VPC.

Can we attach an internet gateway to a private subnet?

-> No

What is a NAT gateway?

-> A Network Address Translation (NAT) gateway is a networking component that allows resources in a private subnet to access the internet while keeping their individual IP addresses hidden. It acts as an intermediary, translating private IP addresses to a single public IP address when communicating with the internet, providing an extra layer of security.

Why do we need an internet gateway at the VPC level?

-> An Internet Gateway is needed at the VPC (Virtual Private Cloud) level to enable communication between resources within your VPC and the internet. It acts as a bridge, allowing instances in your VPC to access and send data to and from the public internet. This is essential for scenarios like web servers serving content to users, downloading updates, or interacting with external APIs.

Why is a NAT gateway more secure than an internet gateway?

-> Because NAT allows traffic in one way , whereas an internet gateway allows traffic in both ways.

How do we differentiate private subnet and public subnet?

-> Private Subnet:

- Resources within a private subnet typically don't have direct internet access.
- They are used for sensitive services like databases or backend servers.
- Communication with the internet is usually mediated through a NAT gateway or NAT instance.
- Private subnets have route tables that direct outbound traffic to the NAT gateway for internet access.

Public Subnet:

- Resources in a public subnet can have direct internet access.
- These are commonly used for front-facing services like web servers.
- They can communicate directly with the Internet through an Internet Gateway.
- Public subnets have route tables that direct outbound traffic to the Internet Gateway.

What is VPC and VPC more?

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

-> VPC means only VPC will get created

VPC and more means VPC as well as other components will get created.

Other components mean -> Subjects, nacl, etc

Which process should we follow ideally and why?

-> VPC only, because we can configure things on our own in VPC only. But if we select VPC and more all things are default, just one click and all things will get created.

What are the different ways we can create VPC?

- > 1)VPC
- 2)VPC and more
- 3>Terraform

What is a CIDR block?

IPv4 CIDR block Info

Determine the starting IP and the size of your VPC using CIDR notation.

10.0.0.0/16

65,536 IPs

What is 65536 IPs ?

It is the capacity.

10.0.0.0/16 => (32-16) -> 2 pow 16 => 65536

10.0.0.0/8..32-8...2pow24..16M
ex: 10.0.0.0/16..32-16..2pow16..65536
10.0.0.0/24..32-24..2pow8..256

Only 10.0.0.0/16 (this is class b type), 10.0.0.0/24 (this is class c type) is provided by cloud, 10.0.0.0/8 (this is class a type) is very big range, so no cloud provides this much CIDR range

-> CIDR block decides ip range.

The CIDR block decides how many instances can be launched in your VPC.

Again no of resources that can be deployed in the public or private subnet are decided by CICD

EXAMPLE

Your CICD block value is 16000 . Then your public + private subnet cannot deploy resources more than 16000.

Can we attach multiple NACL to the same subnet?

-> YES

Can we assign two security groups to a instance

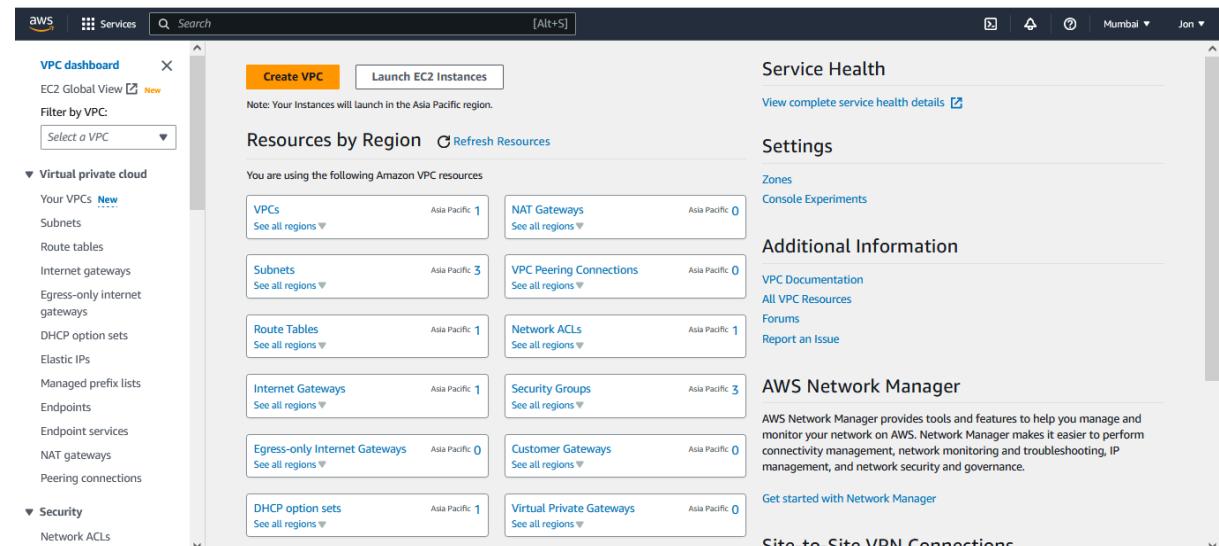
-> YES

Steps to create VPC

1.Creating VPC using VPC and more option

STEP 1

VPC dashboard -> Create VPC



The screenshot shows the AWS VPC dashboard. At the top, there is a 'Create VPC' button and a 'Launch EC2 Instances' button. Below this, a note says 'Note: Your Instances will launch in the Asia Pacific region.' The main area is titled 'Resources by Region' with a 'Refresh Resources' button. It lists various Amazon VPC resources with their counts in the Asia Pacific region: VPCs (1), Subnets (3), Route Tables (1), Internet Gateways (1), Egress-only Internet Gateways (0), DHCP option sets (1), Security Groups (3), Customer Gateways (0), and Virtual Private Gateways (0). To the right, there are sections for 'Service Health', 'Settings' (with 'Zones' and 'Console Experiments' sub-sections), 'Additional Information' (with 'VPC Documentation', 'All VPC Resources', 'Forums', and 'Report an Issue' links), 'AWS Network Manager' (with a description and 'Get started with Network Manager' link), and 'Site-to-Site VPN Connections'.

STEP 2

Create VPC ->VPC settings -> Select VPC and more

The screenshot shows the 'Create VPC' page in the AWS Management Console. On the left, under 'VPC settings', there are two radio button options: 'VPC only' (unchecked) and 'VPC and more' (checked). Below this are sections for 'Name tag auto-generation' (checked for 'Auto-generate' and set to 'project'), 'IPv4 CIDR block' (set to '10.0.0.0/16' with 65,536 IPs), and 'IPv6 CIDR block' (unchecked for 'No IPv6 CIDR block'). On the right, the 'Preview' section shows a network diagram for a VPC named 'project-vpc'. It includes a 'VPC' node, 'Subnets (4)' (ap-south-1a, ap-south-1b, project-subnet-public1-ap-south-1a, project-subnet-private1-ap-south-1a), and 'Route tables (3)' (project-rtb-public, project-rtb-private1, project-rtb-private2). Arrows indicate the connections between the VPC, subnets, and route tables.

STEP 3

Give name or else you can keep auto generated

The screenshot shows the 'Name tag auto-generation' section. It includes a description: 'Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.' Below is a checked checkbox for 'Auto-generate' and a text input field containing 'tmp'.

Decide CIDR value

STEP 4

The screenshot shows the 'IPv4 CIDR block' section. It includes a description: 'Determine the starting IP and the size of your VPC using CIDR notation.' Below is a text input field containing '10.0.0.0/24' with '256 IPs' indicated to its right. Below the input field is a numeric slider with arrows for adjusting the CIDR value.

The screenshot shows the 'IPv6 CIDR block' section. It includes a radio button for 'No IPv6 CIDR block' (selected) and an unchecked radio button for 'Amazon-provided IPv6 CIDR block'.

***** Out Of 256 only 251 are available for us , 5 are reserved for AWS**

STEP 5

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

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

1

2

3

► [Customize AZs](#)

▼ [Customize AZs](#)

First availability zone

ap-south-1a



Second availability zone

ap-south-1b



(You can even customise the availability zone)

***** If you have 2 subnets then you have to select 2 availability zones. And make sure that both the availability zones are different . Different subnets have different availability zones.**

STEP 6

Select 2 public and 2 private subnets.

Number of public subnets [Info](#)

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

0

2

Number of private subnets [Info](#)

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

0

2

4

► [Customize subnets CIDR blocks](#)

STEP 7

Click create VPC

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

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

VPC endpoints [Info](#)
 Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

None	S3 Gateway
------	------------

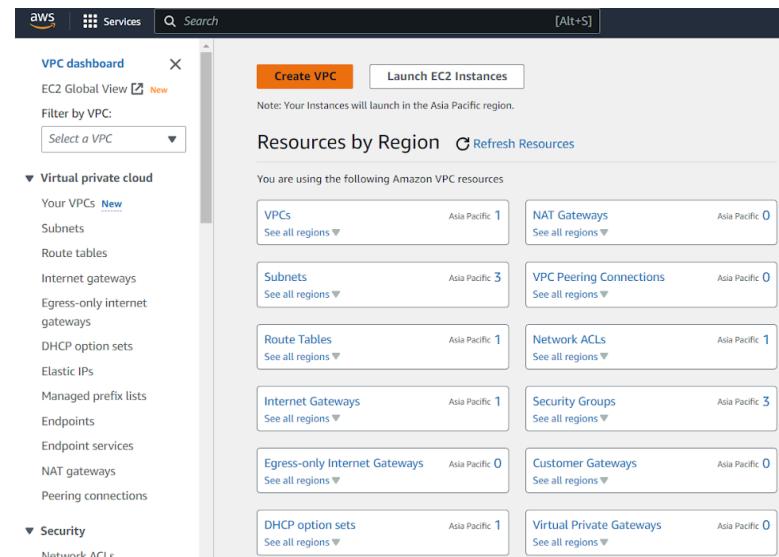
DNS options [Info](#)
 Enable DNS hostnames
 Enable DNS resolution

► Additional tags

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

2. Creating Customised VPC

Services -> search for VPC -> create VPC



The screenshot shows the AWS VPC dashboard. At the top, there are buttons for 'Create VPC' and 'Launch EC2 Instances'. A note says 'Note: Your Instances will launch in the Asia Pacific region.' Below this is a section titled 'Resources by Region' with a 'Refresh Resources' button. The resources listed are:

- VPCs: Asia Pacific: 1
- NAT Gateways: Asia Pacific: 0
- Subnets: Asia Pacific: 3
- VPC Peering Connections: Asia Pacific: 0
- Route Tables: Asia Pacific: 1
- Network ACLs: Asia Pacific: 1
- Internet Gateways: Asia Pacific: 1
- Security Groups: Asia Pacific: 3
- Egress-only Internet Gateways: Asia Pacific: 0
- Customer Gateways: Asia Pacific: 0
- DHCP option sets: Asia Pacific: 1
- Virtual Private Gateways: Asia Pacific: 0

On the left sidebar, there are sections for '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) and 'Security' (Network ACLs).

or

Services -> search for VPC -> Virtual Private Cloud -> Your VPCs -> create VPC

Your VPCs (1) Info						
Actions Create VPC						
<input type="text"/> Find resources by attribute or tag						
Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHC	
-	vpc-0f8f0da2d5913c923	Available	172.31.0.0/16	-	dopt	Actions

Two VPC must not have same CIDR

Services -> search for VPC -> Virtual Private Cloud -> Your VPCs -> create VPC -> VPC only

VPC > Your VPCs > Create VPC

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.

adhi-vpc

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

IPv4 CIDR
20.0.0.0/16

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

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*
Name adhi-vpc [Remove tag](#)

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

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

Successfully created VPC

2. Creating Subnets

Services -> search for VPC -> Virtual Private Cloud -> Subnets -> create subnet

VPC dashboard X

EC2 Global View New

Filter by VPC: Select a VPC

Virtual private cloud New

Your VPCs New

Subnets

Subnets (3) Info

Find resources by attribute or tag

Actions Create subnet

< 1 > @

<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR
<input type="checkbox"/>	-	subnet-0941d6d773441c43a	Available	vpc-0f8f0da2d5913c923	172.31.16.0/20
<input type="checkbox"/>	subnet-0012fc7f26a13991c	subnet-0012fc7f26a13991c	Available	vpc-0f8f0da2d5913c923	172.31.32.0/20
<input type="checkbox"/>	subnet-07a68b1b3fc828cf5	subnet-07a68b1b3fc828cf5	Available	vpc-0f8f0da2d5913c923	172.31.0.0/20

choosed recently created VPC

aws | Services Q Search [Alt+S]

[VPC](#) > [Subnets](#) > [Create subnet](#)

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.
vpc-00784dd42f224120d (adhi-vpc)

Associated VPC CIDRs
IPv4 CIDRs
20.0.0.0/16

creating public subnet

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
adhi-vpc-subnet-pub

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) / ap-south-1a

IPv4 CIDR block Info
Q 20.0.10.0/24 X

Tags - optional

Key Q Name X	Value - optional Q adhi-vpc-subnet-pub X Remove
---	--

Add new tag

You can add 49 more tags.

Remove

Add new subnet

Cancel Create subnet

click on add new subnet

creating private subnet

Subnet 2 of 2

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

adhi-vpc-subnet-pv

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) / ap-south-1a

Use: "20.0.11.0/24"

X

▼ Tags - optional

Key <div style="border: 1px solid #ccc; padding: 5px; width: 100%;">Q Name</div> <div style="border: 1px solid #ccc; padding: 5px; width: 100%; text-align: right;">X</div>	Value - optional <div style="border: 1px solid #ccc; padding: 5px; width: 100%;">Q adhi-vpc-subnet-pv</div> <div style="border: 1px solid #ccc; padding: 5px; width: 100%; text-align: right;">X Remove</div>
--	--

Add new tag

You can add 49 more tags.

Remove

Add new subnet

These are just names, public and private. Now these two are the same subnets, we will make them public or private later on by using gateways.

Subnets (2) Info						
<input type="text" value="Find resources by attribute or tag"/> Actions Create subnet						
Subnet ID = subnet-09dc4614ec1993817		Subnet ID = subnet-07ee4c40b71ecb2e4		Clear filters « 1 » ⚙️		
□	Name	Subnet ID	State	VPC	IPv4 CIDR	⋮
<input type="checkbox"/>	adhi-vpc-subnet-pv	subnet-07ee4c40b71ecb2e4	Available	vpc-00784dd42f224120d adhi...	20.0.11.0/24	⋮
<input type="checkbox"/>	adhi-vpc-subnet-pub	subnet-09dc4614ec1993817	Available	vpc-00784dd42f224120d adhi...	20.0.10.0/24	⋮

3. Creating Gateways

1. Internet gateway for VPC

Services -> search for VPC -> Virtual Private Cloud -> Internet gateways -> create internet gateway



<input checked="" type="checkbox"/>	Name	Internet gateway ID	State	VPC ID	Owner
<input checked="" type="checkbox"/>	—	igw-048fea7fbe8fe8154	Attached	vpc-0f8f0da2d5913c923	115185172188

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="adhi-vpc-internet-gateway"/>

[Add new tag](#)

You can add 49 more tags.

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

internet gateway created

now we have to attach that gateway to the VPC

The following internet gateway was created: igw-074d6d528cf07ae60 - adhi-vpc-internet-gateway. You can now attach to a VPC to enable the VPC to communicate with the internet.

Name	Internet gateway ID	State	VPC ID
adhi-vpc-internet-g...	igw-074d6d528cf07ae60	Attached	vpc-0f8f0da2d5913c923

[Actions](#) [Create](#)

[View details](#) [Attach to VPC](#) [Detach from VPC](#) [Manage tags](#) [Delete internet gateway](#)

VPC > Internet gateways > Attach to VPC (igw-074d6d528cf07ae60)

Attach to VPC (igw-074d6d528cf07ae60) Info

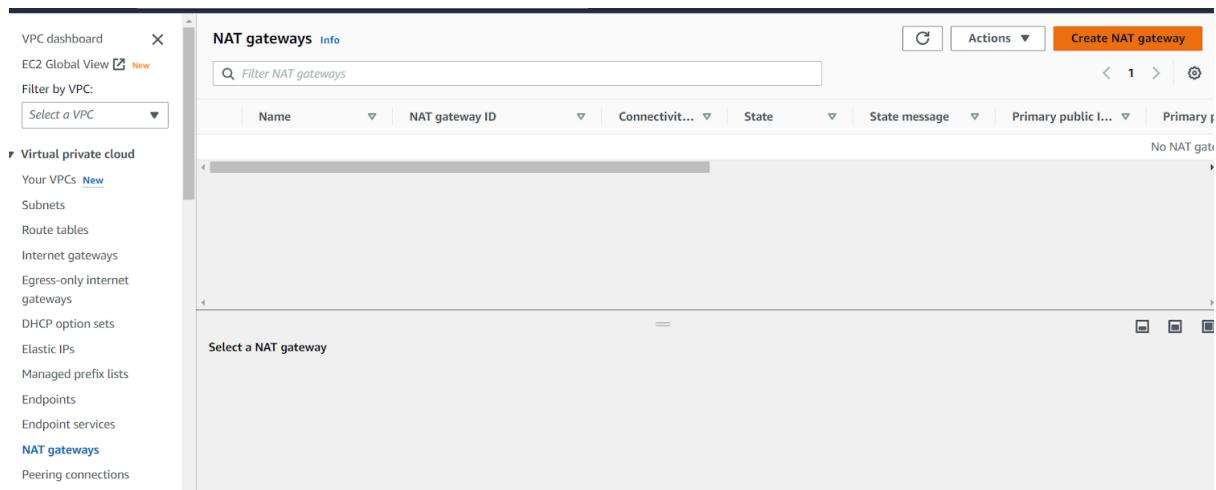
VPC
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs
Attach the internet gateway to this VPC.

[AWS Command Line Interface command](#)

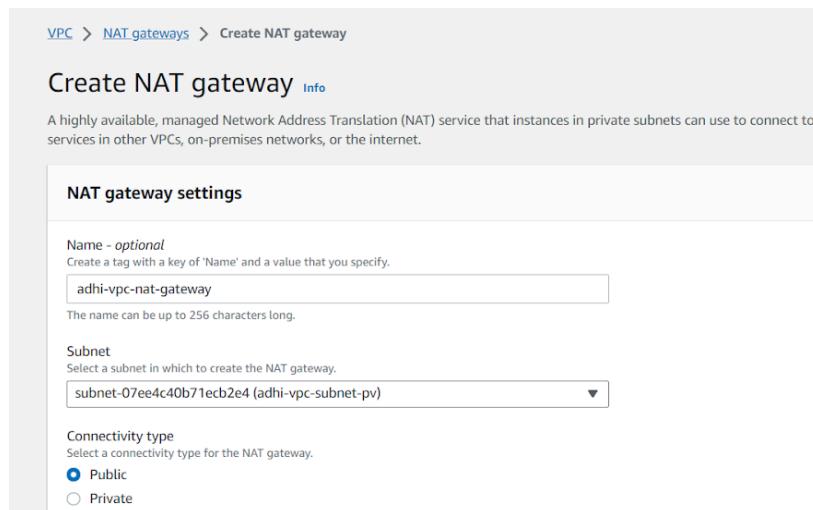
[Cancel](#) [Attach internet gateway](#)

2. NAT gateway



The screenshot shows the AWS VPC dashboard with the 'NAT gateways' section selected. The list table is empty, indicating 'No NAT gateways found'. A prominent orange 'Create NAT gateway' button is located in the top right corner of the list area.

In NAT, we have option to attach the subnet while creating NAT, so here we will select **adhi-vpc-subnet-pv**



The screenshot shows the 'Create NAT gateway' wizard. Step 1: NAT gateway settings. The 'Name' field is set to 'adhi-vpc-nat-gateway'. The 'Subnet' dropdown is set to 'subnet-07ee4c40b71ecb2e4 (adhi-vpc-subnet-pv)'. The 'Connectivity type' section shows 'Public' selected. The wizard has three steps: 'Create NAT gateway', 'Allocate elastic IP', and 'Review and Create'.

click on allocate elastic ip -> create NAT

Elastic IP allocation ID [Info](#)
Assign an Elastic IP address to the NAT gateway.

eipalloc-073dd3a28a18fa018

[Allocate Elastic IP](#)

► Additional settings [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.

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="adhi-vpc-nat-gateway"/>

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

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

4. Creating Route tables

VPC dashboard [X](#)
EC2 Global View [New](#)

Filter by VPC: [Select a VPC](#)

Virtual private cloud
Your VPCs [New](#)
Subnets
Route tables

Route tables (2) [Info](#)

[Find resources by attribute or tag](#)

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

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
<input type="checkbox"/>	-	rtb-07a31a1702c682190	-	-	Yes	vpc-00784dd42f224120
<input type="checkbox"/>	-	rtb-01641c7dee81ba28e	-	-	Yes	vpc-0f8f0da2d5913c92

1. creating route table for public subnet

[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.

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="adhi-vpc-subnet-pub-rtb"/>

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

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

2. creating route table for private subnet

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.

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="adhi-vpc-subnet-pv-rtb"/> X Remove
Add new tag	

You can add 49 more tags.

Cancel Create route table

5. Attach gateways to subnet via rtb

For public

VPC dashboard X

EC2 Global View New

Filter by VPC: Select a VPC

Virtual private cloud

Your VPCs New

Subnets

Route tables

Internet gateways

Egress-only internet gateways

DHCP option sets

Elastic IPs

Route tables (1/4) Info

Route table rtb-051e6282f6c5fcc58 | adhi-vpc-subnet-pv-rtb was created successfully.

Name	Route table ID	Explicit subnet associations	Edge associations
adhi-vpc-subnet-pub-rtb	rtb-0717f911607e6d75e	-	-
adhi-vpc-subnet-pv-rtb	rtb-051e6282f6c5fcc58	-	-

rtb-0717f911607e6d75e / adhi-vpc-subnet-pub-rtb

Actions Create route table

- View details
- Set main route table
- Edit subnet associations 4
- Edit edge associations 4
- Edit route propagation 4
- Edit routes
- Manage tags
- Delete route table
- Troubleshoot
- Trace network reachability

VPC > Route tables > rtb-0717f911607e6d75e > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/2)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
adhi-vpc-subnet-pv	subnet-07ee4c40b71ecb2e4	20.0.11.0/24	-	rtb-0717f911607e6d75e / adhi-vpc-su...
adhi-vpc-subnet-pub	subnet-09dc4614ec1993817	20.0.10.0/24	-	Main (rtb-07a31a1702c682190)

Selected subnets

subnet-09dc4614ec1993817 / adhi-vpc-subnet-pub X

Cancel Save associations

For private

The screenshot shows the AWS VPC Route Tables page. In the main table, the route table 'adhi-vpc-subnet-pv-rtb' is selected. A context menu is open on the right, and the 'Edit subnet associations' option is highlighted in blue. The menu also includes other options like 'View details', 'Set main route table', 'Edit edge associations', 'Edit route propagation', 'Edit routes', 'Manage tags', 'Delete route table', 'Troubleshoot', and 'Trace network reachability'.

The screenshot shows the 'Edit subnet associations' dialog box. Under 'Available subnets (1/2)', the subnet 'adhi-vpc-subnet-pv' is selected. Under 'Selected subnets', the subnet 'subnet-07ee4c40b71ecb2e4 / adhi-vpc-subnet-pv' is listed. At the bottom right, there are 'Cancel' and 'Save associations' buttons.

it is associated, we can do this like below mentioned...

The screenshot shows the AWS VPC Route Tables page. The 'adhi-vpc-subnet-pv-rtb' route table is selected. Below the main table, there is a section titled 'EXPLICIT SUBNET ASSOCIATIONS (1)'. It shows a table with one entry: 'adhi-vpc-subnet-pub' associated with 'subnet-09dc4614ec1993817' and '20.0.10.0/24'.

Route tables (1/4) [Info](#)

Find resources by attribute or tag

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associa...
<input type="checkbox"/>	-	rtb-07a31a1702c682190	-
<input type="checkbox"/>	-	rtb-01641c7dee81ba28e	-
<input type="checkbox"/>	adhi-vpc-subnet-pub-rtb	rtb-0717f911607e6d75e	subnet-09dc4614ec199...
<input checked="" type="checkbox"/>	adhi-vpc-subnet-pv-rtb	rtb-051e6282f6c5fcc58	subnet-07ee4c40b71ecb...

rtb-051e6282f6c5fcc58 / adhi-vpc-subnet-pv-rtb

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

Explicit subnet associations (1)

Find subnet association

<input type="checkbox"/>	Name	Subnet ID	IPv4 CIDR
<input type="checkbox"/>	adhi-vpc-subnet-pv	subnet-07ee4c40b71ecb2e4	20.0.11.0/24

adding routes

1. for public route table

route tables -> pub rtb -> routes -> edit routes

Route tables (1/4) [Info](#)

Find resources by attribute or tag

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

[<](#) [1](#) [>](#) [@](#)

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associati...	Edge associations	Main	VPC
<input type="checkbox"/>	-	rtb-07a31a1702c682190	-	-	Yes	vpc-00784dd42f224
<input type="checkbox"/>	-	rtb-01641c7dee81ba28e	-	-	Yes	vpc-0f8f0da2d5913c
<input checked="" type="checkbox"/>	adhi-vpc-subnet-pub-rtb	rtb-0717f911607e6d75e	subnet-09dc4614ec1993...	-	No	vpc-00784dd42f224
<input type="checkbox"/>	adhi-vpc-subnet-pv-rtb	rtb-051e6282f6c5fcc58	subnet-07ee4c40b71ecb...	-	No	vpc-00784dd42f224

rtb-0717f911607e6d75e / adhi-vpc-subnet-pub-rtb

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

Routes (1)

[Edit routes](#)

Destination	Target	Status	Propagated
20.0.0.0/16	local	Active	No
0.0.0.0/0	igw-074d6d528cf07ae60	-	No

this is how we attach internet gateways to subnets

gateway attached to subnet successfully

Name	Subnet ID	State	VPC
adhi-vpc-subnet-pub	subnet-09dc4614ec1993817	Available	vpc-00784dd42f224120d adhi...
adhi-vpc-subnet-pv	subnet-07ee4c40b71ecb2e4	Available	vpc-00784dd42f224120d adhi...
subnet-0012fc7f26a13991c	subnet-0012fc7f26a13991c	Available	vpc-0f8f0da2d5913c923
subnet-07a68b1b3fc828cf5	subnet-07a68b1b3fc828cf5	Available	vpc-0f8f0da2d5913c923

Destination	Target
20.0.0.0/16	local
0.0.0.0/0	igw-074d6d528cf07ae60

same for private rtb, we will attach private rtb to private subnet

VPC dashboard X

EC2 Global View New

Filter by VPC: Select a VPC

Virtual private cloud

Your VPCs New

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

Route tables (1/4) Info

Find resources by attribute or tag

Route table ID

Name

Explicit subnet associations

Edge associations

Main

VPC

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
-	rtb-07a31a1702c682190	-	-	Yes	vpc-00784dd42f2241
-	rtb-01641c7dee81ba28e	-	-	Yes	vpc-0f8f0da2d5913c9
adhi-vpc-subnet-pub-rtb	rtb-0717f911607e6d75e	subnet-09dc4614ec1993...	-	No	vpc-00784dd42f2241
adhi-vpc-subnet-pv-rtb	rtb-051e6282f6c5fcc58	subnet-07ee4c40b71ecb...	-	No	vpc-00784dd42f2241

rtb-051e6282f6c5fcc58 / adhi-vpc-subnet-pv-rtb

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

Explicit subnet associations (1)

Find subnet association

Name

Subnet ID

IPv4 CIDR

IPv6 CIDR

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
adhi-vpc-subnet-pv	subnet-07ee4c40b71ecb2e4	20.0.11.0/24	-

VPC dashboard X

EC2 Global View New

Filter by VPC: Select a VPC

Virtual private cloud

Your VPCs New

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

Route tables (1/4) Info

Find resources by attribute or tag

Route table ID

Name

Explicit subnet associations

Edge associations

Main

VPC

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
-	rtb-07a31a1702c682190	-	-	Yes	vpc-00784dd42f2241
-	rtb-01641c7dee81ba28e	-	-	Yes	vpc-0f8f0da2d5913c9
adhi-vpc-subnet-pub-rtb	rtb-0717f911607e6d75e	subnet-09dc4614ec1993...	-	No	vpc-00784dd42f2241
adhi-vpc-subnet-pv-rtb	rtb-051e6282f6c5fcc58	subnet-07ee4c40b71ecb...	-	No	vpc-00784dd42f2241

rtb-051e6282f6c5fcc58 / adhi-vpc-subnet-pv-rtb

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

Routes (1)

Edit routes

and select NAT

VPC > Route tables > rtb-051e6282f6c5fcc58 > Edit routes

Edit routes

Destination	Target	Status	Propagated
20.0.0.0/16	Q local X Active	No	
Q 0.0.0.0/0	Q nat-031701a0922bd1e81 X -	No	Remove

Add route

Cancel Preview Save changes

we can verify this like below...

subnets -> select private subnet -> route table

Subnets (1/5) [Info](#)

Find resources by attribute or tag

Name	Subnet ID	State	VPC	IPv4 CIDR
-	subnet-0941d6d773441c45a	Available	vpc-0f8f0da2d5913c923	172.31.16.0/20
<input checked="" type="checkbox"/> adhi-vpc-subnet-pv	subnet-07ee4c40b71ecb2e4	Available	vpc-00784dd42f224120d adhi...	20.0.10.0/24
<input type="checkbox"/> adhi-vpc-subnet-pub	subnet-09dc4614ec1993817	Available	vpc-00784dd42f224120d adhi...	20.0.10.0/24
<input type="checkbox"/> subnet-0012fc7f26a13991c	subnet-0012fc7f26a13991c	Available	vpc-0f8f0da2d5913c923	172.31.32.0/20
<input type="checkbox"/> subnet-07a68b1b3fc828cf5	subnet-07a68b1b3fc828cf5	Available	vpc-0f8f0da2d5913c923	172.31.0.0/20

subnet-07ee4c40b71ecb2e4 / adhi-vpc-subnet-pv

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

Route table: [rtb-051e6282f6c5fcc58](#) / adhi-vpc-subnet-pv-rtb

Routes (2)

Filter routes

Destination	Target
20.0.0.0/16	local
0.0.0.0/0	nat-031701a0922bd1e81

6. Create NACL

Security -> NACL -> create NACL

1. create public NACL

VPC > Network ACLs > Create network ACL

Create network ACL [Info](#)

A network ACL is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet.

Network ACL settings

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

VPC
VPC to use for this network ACL.

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 49 more tags

[Cancel](#) [Create network ACL](#)

1. create private NACL

VPC > Network ACLs > Create network ACL

Create network ACL Info

A network ACL is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet.

Network ACL settings

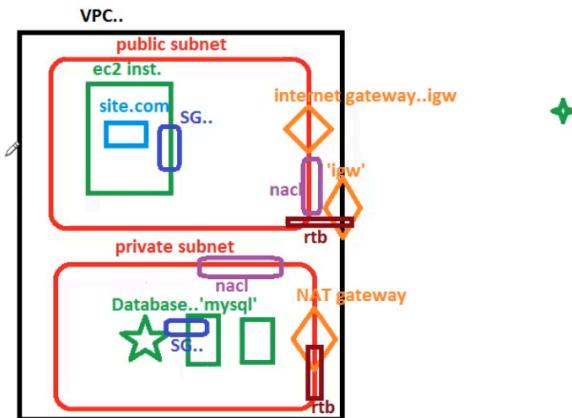
Name - *optional*
Creates a tag with a key of 'Name' and a value that you specify.
adhi-vpc-nacl-pv

VPC
VPC to use for this network ACL.
vpc-00784dd42f224120d (adhi-vpc)

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="button" value="X"/>	<input type="text" value="adhi-vpc-nacl-pv"/> <input type="button" value="X"/>

You can add 49 more tags



Editing inbound rules of NACL

1. for public NACL

select public NACL -> inbound rules -> edit inbound rules

just adding some random rules

2. for private NACL

select private NACL -> inbound rules -> edit inbound rules

Network ACLs (1/4) [Info](#)

Find resources by attribute or tag

[Actions](#) [Create network ACL](#)

Name	Network ACL ID	Associated with	Default	VPC ID
-	acl-0824b14b04b52eb66	3 Subnets	Yes	vpc-0f8f0da2d5913c923
-	acl-03efb6b89c9c87726	2 Subnets	Yes	vpc-00784dd42f224120d / adhi-vpc
adhi-vpc-nacl-pub	acl-0a0d673abe13feded	-	No	vpc-00784dd42f224120d / adhi-vpc
<input checked="" type="checkbox"/> adhi-vpc-nacl-pv	acl-038a66c63806f2087	-	No	vpc-00784dd42f224120d / adhi-vpc

acl-038a66c63806f2087 / adhi-vpc-nacl-pv

[Details](#) [Inbound rules](#) [Outbound rules](#) [Subnet associations](#) [Tags](#)

[Run Reachability Analyzer](#)

Inbound rules (1) [Edit inbound rules](#)

i want only adhi-vpc-subnet-pub can access my private NACL, so i will select public subnet and copy IPv4 CIDR

VPC dashboard [X](#)

EC2 Global View [New](#)

Filter by VPC: [Select a VPC](#)

Virtual private cloud

Your VPCs [New](#)

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

Subnets (1/5) [Info](#)

Find resources by attribute or tag

[Actions](#) [Create subnet](#)

Name	Subnet ID	State	VPC	IPv4 CIDR
-	subnet-0941d6d773441c45a	Available	vpc-0f8f0da2d5913c923	172.31.16.0/20
adhi-vpc-subnet-pv	subnet-07ee4c40b71ecb2e4	Available	vpc-00784dd42f224120d adhi...	20.0.11.0/24
<input checked="" type="checkbox"/> adhi-vpc-subnet-pub	subnet-09dc4614ec1993817	Available	vpc-00784dd42f224120d adhi...	20.0.10.0/24
subnet-0012fc7f26a13991c	subnet-0012fc7f26a13991c	Available	vpc-0f8f0da2d5913c923	172.31.32.0/20
subnet-07a68b1b3fc828cf5	subnet-07a68b1b3fc828cf5	Available	vpc-0f8f0da2d5913c923	172.31.0.0/20

subnet-09dc4614ec1993817 / adhi-vpc-subnet-pub

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

Details

Subnet ID subnet-09dc4614ec1993817	Subnet ARN arn:aws:ec2:ap-south-1:115185172188:subnet/subnet-09dc4614ec1993817	State Available	IPv4 CIDR 20.0.10.0/24
Available IPv4 addresses 251		Availability Zone ap-south-1a	Availability Zone ID ap-south-1a

and paste it here.

i want only my database to access my private NACL

VPC > Network ACLs > acl-038a66c63806f2087 / adhi-vpc-nacl-pv > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the VPC.

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	MySQL/Aurora (3306)	TCP (6)	3306	20.0.10.0/24	Allow
101	Oracle (1521)	TCP (6)	1521	20.0.10.0/24	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

[Add new rule](#) [Sort by rule number](#)

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

we have successfully set up NACL inbound and outbound rules

now we will associate our NACL to subnets

1. for public NACL

VPC dashboard X

EC2 Global View New

Filter by VPC: Select a VPC

Virtual private cloud

Your VPCs New

Subnets

Route tables

Internet gateways

Egress-only internet

Network ACLs (1/10) Info

[Create network ACL](#)

Name	Network ACL ID	Associated with	Default
acl-03a325964bb52f69f	subnet-053756ab8eabf75ea / vpc2-prv-subnet	Yes	
acl-0f9c5c5f5e06cd89	subnet-0f0ee90bdd21d6a73 / vpc1-prv-subnet	Yes	
sakshi-vpc-nacl-pub	acl-0deb3d242c8d14277	No	
acl-03efb6b89c9c87726	2 Subnets	Yes	
sakshi-vpc-nacl-pv	acl-034bd4479cd47842a	No	
adhi-vpc-nacl-pub	acl-0a0d673abe13feded	No	

[View details](#)

[Edit inbound rules](#)

[Edit outbound rules](#)

[Edit subnet associations](#)

[Manage tags](#)

[Delete network ACLs](#)

[Troubleshoot](#)

[Trace network reachability](#)

VPC > Network ACLs > acl-0a0d673abe13feded / adhi-vpc-nacl-pub > Edit subnet associations

Edit subnet associations Info

Change which subnets are associated with this network ACL.

Available subnets (1/2)

Name	Subnet ID	Associated with	Availability Zone	IPv4 CIDR	IPv6 CIDR
adhi-vpc-subnet-pv	subnet-07ee4c40b71ecb2e4	acl-05efb6b89c9c87726	ap-south-1a	20.0.11.0/24	-
adhi-vpc-subnet-pub	subnet-09dc4614ec1993817	acl-03efb6b89c9c87726	ap-south-1a	20.0.10.0/24	-

Selected subnets

subnet-09dc4614ec1993817 / adhi-vpc-subnet-pub X

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

2. same for private NACL

Network ACLs (1/10) [Info](#)

Find resources by attribute or tag

Name	Network ACL ID	Associated with	Default
<input checked="" type="checkbox"/> adhi-vpc-nacl-pv	acl-038a66c63806f2087	–	No
<input type="checkbox"/> –	acl-0d2e7d4db16af57d8	2 Subnets	Yes
<input type="checkbox"/> vpc1-pub-nacl	acl-05b2630709206b9ec	–	No
<input type="checkbox"/> –	acl-0824b14b04b52eb66	3 Subnets	Yes
<input type="checkbox"/> –	acl-03a325964bb52f69f	subnet-053756ab8abf75ea / vpc2-prv-subnet	Yes
<input type="checkbox"/> –	acl-0f9c5c5f65e06cd89	subnet-0f0ee90bdd21d6a73 / vpc1-dub-subnet	Yes

Actions ▾ [Create network](#)

- [View details](#)
- [Edit inbound rules](#)
- [Edit outbound rules](#)
- [Edit subnet associations](#) (highlighted in blue)
- [Manage tags](#)
- [Delete network ACLs](#)
- [Troubleshoot](#)
- [Trace network reachability](#)

VDC-U0a80Uc4Zt90857c/U / VDC1

VPC > Network ACLs > acl-038a66c63806f2087 / adhi-vpc-nacl-pv > Edit subnet associations [Info](#)

Edit subnet associations [Info](#)

Change which subnets are associated with this network ACL.

Available subnets (1/2)

Name	Subnet ID	Associated with	Availability Zone	IPv4 CIDR	IPv6 CIDR
<input checked="" type="checkbox"/> adhi-vpc-subnet-pv	subnet-07ee4c40b71ecb2e4	acl-03efb6b89c9c87726	ap-south-1a	20.0.11.0/24	–
<input type="checkbox"/> adhi-vpc-subnet-pub	subnet-09dc4614ec1993817	acl-0a0d673abe15feded / adhi...	ap-south-1a	20.0.10.0/24	–

Selected subnets

subnet-07ee4c40b71ecb2e4 / adhi-vpc-subnet-pv	X
---	-------------------

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

how to disassociate subnet

VPC dashboard [X](#)

EC2 Global View [New](#)

Filter by VPC: [Select a VPC](#)

Virtual private cloud

Your VPCs [New](#)

Subnets

Route tables

Route tables (1/11) [Info](#)

Find resources by attribute or tag

Name	Route table ID	Explicit subnet associations	Edge associations
<input checked="" type="checkbox"/> adhi-vpc-subnet-pv-rtb	rtb-051e6282f6c5fcc58	subnet-07ee4c40b71ecb...	–
<input type="checkbox"/> –	rtb-07a31a1702c682190	–	–
<input type="checkbox"/> –	rtb-0bb4879711026ebc9	–	–
<input type="checkbox"/> –	rtb-038f4c972a759b632	–	–
<input type="checkbox"/> –	rtb-0ddc0ff7e967983e	–	–

Actions ▾ [Create route table](#)

- [View details](#)
- [Set main route table](#)
- [Edit subnet associations](#) (highlighted in blue)
- [Edit edge associations](#)
- [Edit route propagation](#)
- [Edit routes](#)
- [Manage tags](#)
- [Delete route table](#)

VPC > Route tables > rtb-051e6282f6c5fcc58 > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

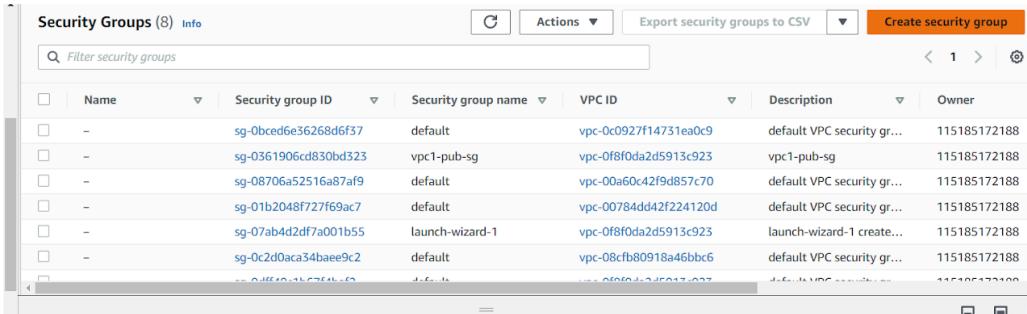
Available subnets (2)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input type="checkbox"/> adhi-vpc-subnet-pv	subnet-07ee4c40b71ecb2e4	20.0.11.0/24	–	rtb-051e6282f6c5fcc58 / adhi-vpc-sub...
<input type="checkbox"/> adhi-vpc-subnet-pub	subnet-09dc4614ec1993817	20.0.10.0/24	–	rtb-0717f911607e6d75e / adhi-vpc-su...

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

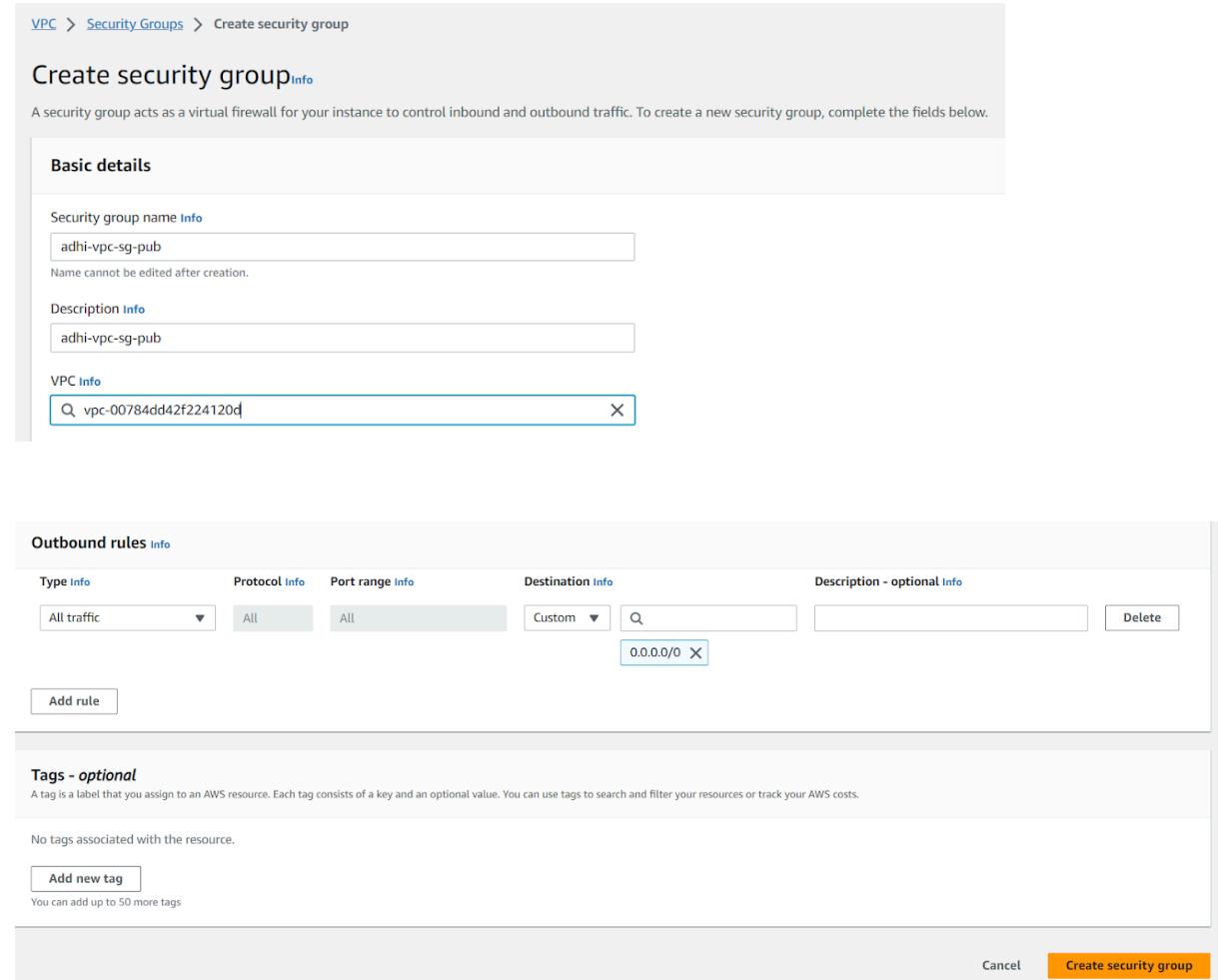
7. Create Security groups

click on **create security group**



Security Groups (8) info						
	Name	Security group ID	Security group name	VPC ID	Description	Owner
<input type="checkbox"/>	-	sg-0bcd6e36268d6f37	default	vpc-0c0927f14731ea0c9	default VPC security gr...	115185172188
<input type="checkbox"/>	-	sg-0361906cd830bd323	vpc1-pub-sg	vpc-0f8f0da2d5913c923	vpc1-pub-sg	115185172188
<input type="checkbox"/>	-	sg-08706a52516a87af9	default	vpc-00a60c42f9d857c70	default VPC security gr...	115185172188
<input type="checkbox"/>	-	sg-01b2048f727f69ac7	default	vpc-00784dd42f224120d	default VPC security gr...	115185172188
<input type="checkbox"/>	-	sg-07ab4d2df7a001b55	launch-wizard-1	vpc-0f8f0da2d5913c923	launch-wizard-1 create...	115185172188
<input type="checkbox"/>	-	sg-0c2d0aca34baee9c2	default	vpc-08fb80918a46bbc6	default VPC security gr...	115185172188

1. Public



VPC > [Security Groups](#) > Create security group

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](#)
adhi-vpc-sg-pub

Name cannot be edited after creation.

Description [Info](#)
adhi-vpc-sg-pub

VPC Info
Q vpc-00784dd42f224120d

Outbound rules [info](#)

Type Info	Protocol Info	Port range Info	Destination Info	Description - optional Info
All traffic	All	All	Custom <input type="button" value="Custom"/> <input type="text" value="0.0.0.0/0"/> <input type="button" value="X"/>	<input type="button" value="Delete"/>

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.

No tags associated with the resource.

You can add up to 50 more tags

Security Groups (1/9) Info						
	Name	Security group ID	Security group name	VPC ID	Description	Owner
<input type="checkbox"/>	-	sg-01b2048f727f69ac7	default	vpc-00784dd42f224120d	default VPC security gr...	115185172188
<input type="checkbox"/>	-	sg-07ab4d2df7a001b55	launch-wizard-1	vpc-0f8f0da2d5913c923	launch-wizard-1 create...	115185172188
<input type="checkbox"/>	-	sg-0c2d0aca34baee9c2	default	vpc-08cfb80918a46bbc6	default VPC security gr...	115185172188
<input type="checkbox"/>	-	sg-0df49c1b67f4baef2	default	vpc-0f8f0da2d5913c923	default VPC security gr...	115185172188
<input checked="" type="checkbox"/>	-	adhi-vpc-sg-pub	5	vpc-00784dd42f224120d	adhi-vpc-sg-pub	115185172188
<input type="checkbox"/>	-	adhi-vpc-sg-pub	ba	vpc-0f8f0da2d5913c923	launch-wizard-2 create...	115185172188
<input type="button" value="Cancel"/> <input type="button" value="Save"/>						
sg-0f8c8dd27!						

1. Private

VPC > [Security Groups](#) > Create security group

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic.

Basic details

Security group name [Info](#)
adhi-vpc-sg-pv

Name cannot be edited after creation.

Description [Info](#)
adhi-vpc-sg-pv

VPC Info
vpc-00784dd42f224120d

Outbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Destination Info	Description - optional Info
All traffic	All	All	Custom	0.0.0.0/0

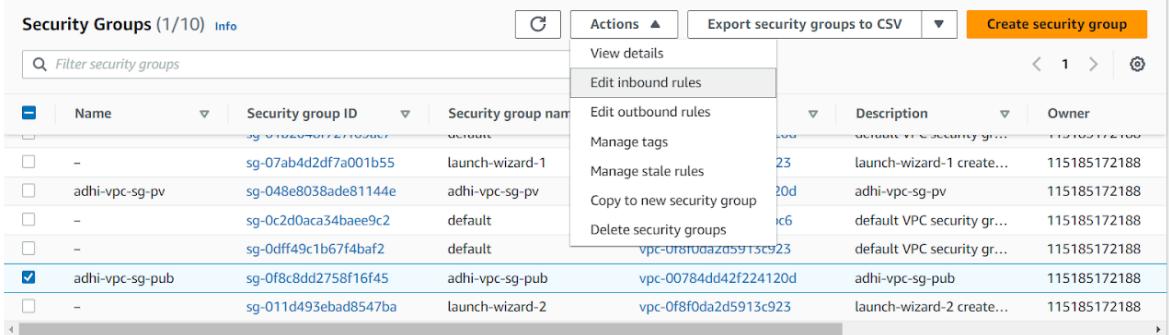
Tags - optional
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
Name	adhi-vpc-sg-pv

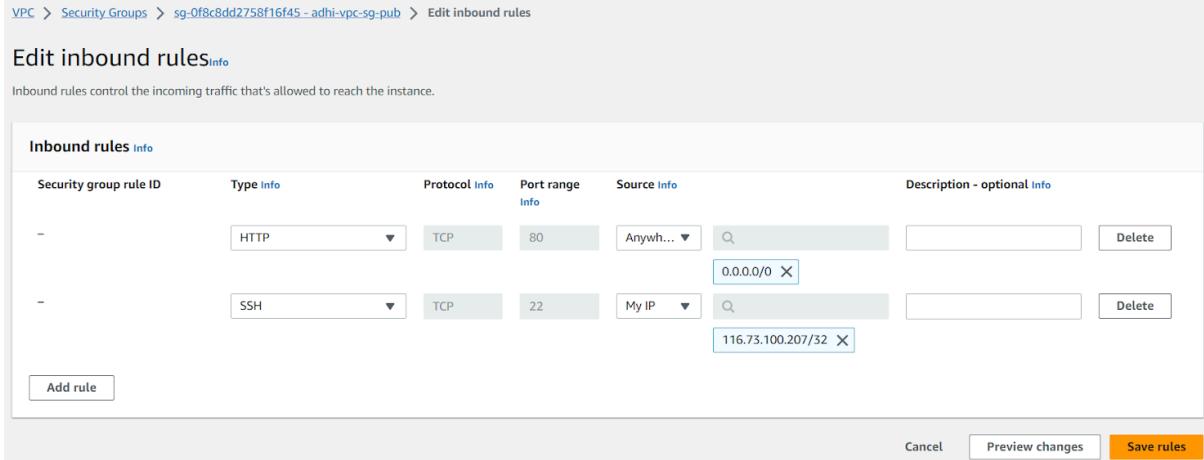
You can add up to 49 more tags

now we will change inbound rules

1. public



The screenshot shows the AWS VPC Security Groups list. A context menu is open over a selected security group named 'adhi-vpc-sg-pub'. The menu options are: View details, Edit inbound rules (which is highlighted in grey), Edit outbound rules, Manage tags, Manage stale rules, Copy to new security group, and Delete security groups. The security group table lists several entries, including 'adhi-vpc-sg-pub' and 'default'.



The screenshot shows the 'Edit inbound rules' configuration page for the security group 'adhi-vpc-sg-pub'. The page displays two existing rules:

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info	Description - optional
-	HTTP	TCP	80	Anywhere	0.0.0.0/0
-	SSH	TCP	22	My IP	116.73.100.207/32

At the bottom of the page are buttons for 'Add rule', 'Cancel', 'Preview changes', and 'Save rules'.

2. private

Security Groups (1/12) Info				Actions ▲	Export security groups to CSV	Create security group
				View details		
				Edit inbound rules		
Name	Security group ID	Security group name			Description	Owner
sg-0c2d0aca34baee9c2	sg-0c2d0aca34baee9c2	default			ic6	default VPC security gr...
sg-0dff49c1b67f4baf2	sg-0dff49c1b67f4baf2	default			23	default VPC security gr...
<input checked="" type="checkbox"/> adhi-vpc-sg-pv	sg-048e8038ade81144e	adhi-vpc-sg-pv			20d	adhi-vpc-sg-pv
sg-011d493ebad8547ba	sg-011d493ebad8547ba	launch-wizard-2			vpc-0f8c8dd2758f16f45	launch-wizard-2 create...
adhi-vpc-sg-pub	sg-0f8c8dd2758f16f45	adhi-vpc-sg-pub			vpc-00784dd42f224120d	adhi-vpc-sg-pub
vpc2-prv-sg	sg-073fc3e43e7ed376b	vpc2-prv-sg			vpc-08cfb80918a46bbc6	vpc2-prv-sg

VPC > Security Groups > sg-048e8038ade81144e - adhi-vpc-sg-pv > 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
-	MySQL/Aurora	TCP	3306	Custom	<input type="text"/> sg-0f8c8dd2758f16f45 X
-	Oracle-RDS	TCP	1521	Custom	<input type="text"/> sg-0f8c8dd2758f16f45 X

[Add rule](#)

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

here, in source, we have added security group of public subnet, in source field

8. Associate NACL to subnet and SG to resource

We have already associated NACL to subnet in step 6

And to associate SG to resource, we have to launch the instances into our custom VPC and then associate SG to resource

Go the EC2 -> Launch instance

1. Public

EC2 > Instances > Launch an instance

Launch an instance Info

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

Name and tags Info

Name [Add additional tags](#)

Application and OS Images (Amazon Machine Image) Info

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

Quick Start

Summary

Number of instances Info

Software Image (AMI)

Provided by Red Hat, Inc.
ami-008b85aa3ff5c1b02

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 10 GiB

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

Cancel
Launch instance

Instance type Info

Instance type **t2.micro** Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true

On-Demand Linux pricing: 0.0124 USD per Hour

On-Demand Windows pricing: 0.017 USD per Hour

On-Demand RHEL pricing: 0.0724 USD per Hour

On-Demand SUSE pricing: 0.0124 USD per Hour

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 - *required* [Create new key pair](#)

Network settings Info

Network Info vpc-0f8f0da2d5913c923

Summary

Number of instances Info

Software Image (AMI)

Provided by Red Hat, Inc.
ami-008b85aa3ff5c1b02

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 10 GiB

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

Cancel
Launch instance

Network settings -> Edit

VPC : adhi-vpc

Subnet : adhi-vpc-subnet-pub

Auto-assign public ip : Enable

Firewall : Select existing security group -> adhi-vpc-sg-pub -> launch instance

Availability zones of instance totally depend upon the zones of the subnet, we can not change the availability zones of the instance while creating. While creating an instance, when we select the subnet, then the same zone is applicable for the instance too.

Private ip is in the range of CIDR of public

we can cross check everything for this instance now, our instance is created in our vpc, subnets, and in our security group.

1. Private

EC2 -> Instances -> Launch an instance

Launch an instance [Info](#)
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)
Name Add additional tags

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

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

Quick Start
Amazon Linux macOS Ubuntu Windows Red Hat SUSE Li > Browse more AMIs

Instance type [Info](#)
Instance type Family: t2 1 vCPU 1 GiB Memory Current generation: true Free tier eligible All generations Compare instance types

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 - required Create new key pair

Network settings [Info](#)
Edit Network [Info](#)

Summary
Number of instances [Info](#)
Software Image (AMI)
Provided by Red Hat, Inc.
ami-008b85aa3ff5c1b02
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 10 GiB
ⓘ Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance

Cancel Review commands

▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-00784dd42f224120d (adhi-vpc)
20.0.0.0/16

Subnet Info

subnet-07ee4c40b71ecb2e4
adhi-vpc-subnet-pv

Subnet ID: vpc-00784dd42f224120d Owner: 115185172188 Availability Zone: ap-south-1a IP addresses available: 250 CIDR: 20.0.11.0/24

Auto-assign public IP [Info](#)

Disable

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.

[Create security group](#)
OR
 [Select existing security group](#)

Common security groups [Info](#)

Select security groups

adhi-vpc-sg-pv sg-048e8038ade81144e

VPC: vpc-00784dd42f224120d

Security groups that you add or remove here will be added to or removed from all your network interfaces.

► Advanced network configuration

▼ Summary

Number of instances [Info](#)

1

Software Image (AMI) [Info](#)

Provided by Red Hat, Inc. ami-008b85aa3ff5c1b02

Virtual server type (instance type)

t2.micro

Firewall (security group)

adhi-vpc-sg-pv

Storage (volumes)

1 volume(s) - 10 GiB

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

[Cancel](#)
[Launch instance](#)

click on **Launch instance**