Codec Technologies : 1-Month Cloud Internship

Name :Prakhar Anil Sharma

Major Project : Virtual Private Cloud (VPC) with Secure Architecture

Objective: Design a secure network architecture using VPC.

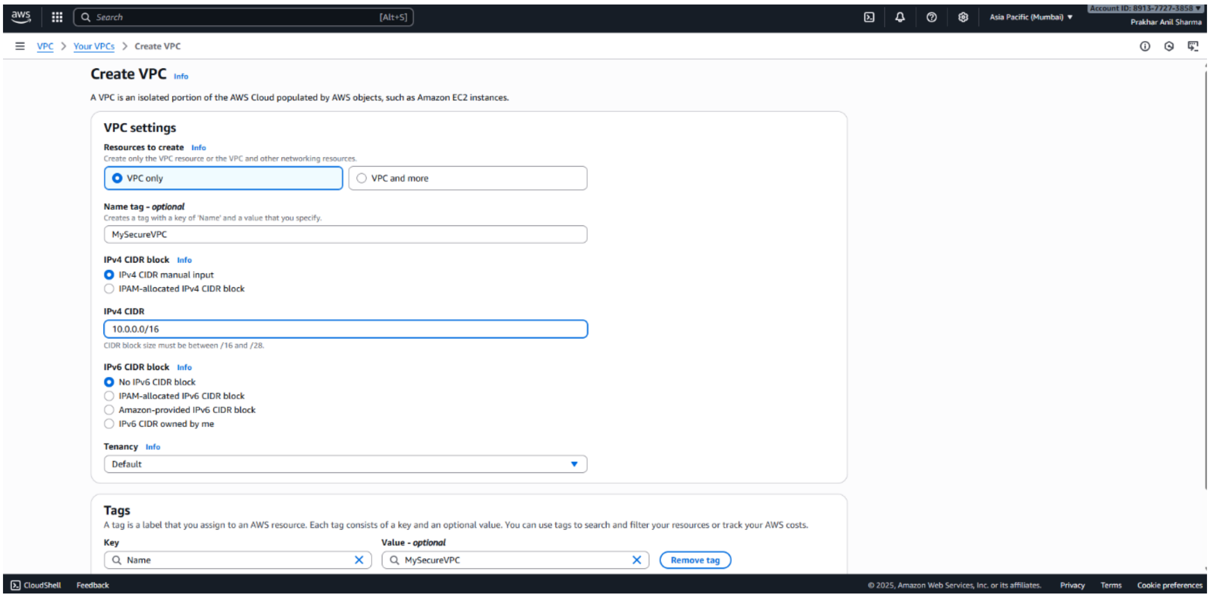
Guidelines:

Create public and private subnets.

Setup NAT Gateway, Security Groups, NACLs.

Deploy a web app in private subnet with bastion host access.

Step – 1] Go to AWS Management Console and login to it .
Step – 2] Search VPC service , and go to your VPC .
Step – 3] Click create VPC .
Step – 4] Choose VPC only, and Name the VPC .
Step – 5] Select IPv4 CIDR manually input .
Step – 6] Add IPv4 CIDR .
Step – 7] Select No IPv6 CIDR block .
Step - 8] Select Tenancy Default .
Step – 9] Click create VPC .



Create VPC

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

VPC settings

Resources to create
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.
MySecureVPC

IPv4 CIDR block
● 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
● No IPv6 CIDR block
○ IPAM-allocated IPv6 CIDR block
○ Amazon-provided IPv6 CIDR block
○ IPv6 CIDR owned by me

Tenancy
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.

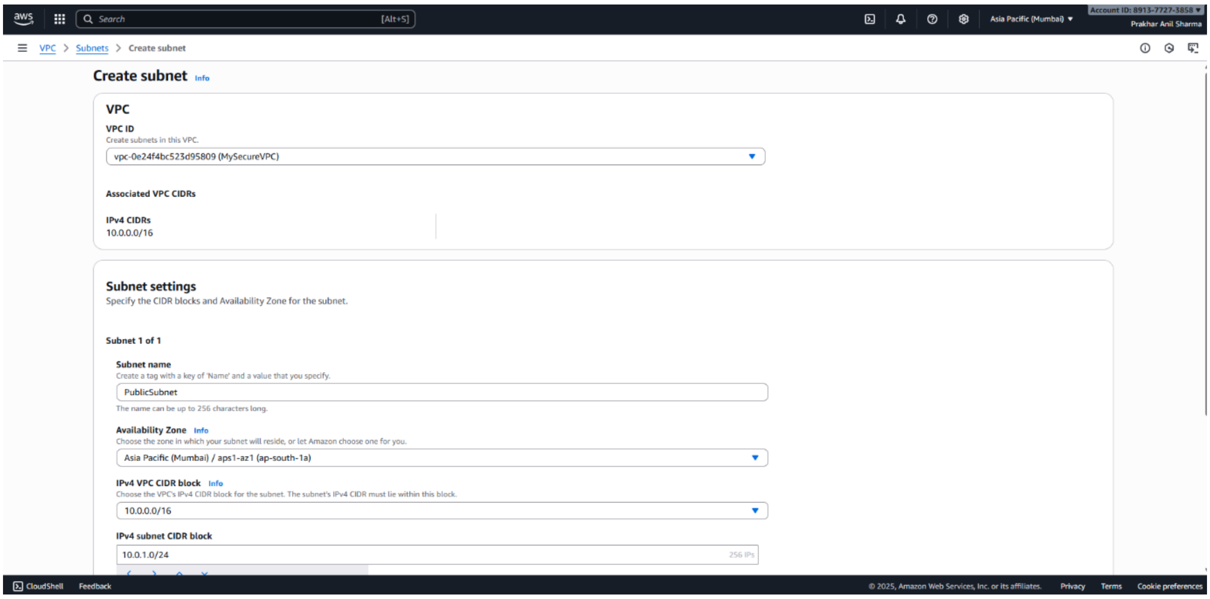
Key: Name
Value - *optional*: MySecureVPC
Remove tag

Step – 10] In the left navigation menu, Click Subnets.
Step – 11] Click Create subnet .
Step – 12] In Subnet setting ,Name and create Public Subnet .
Step – 13] Input the IPv4 subnet CIDR block .

Codec Technologies : 1-Month Cloud Internship

Name :Prakhar Anil Sharma

Major Project : Virtual Private Cloud (VPC) with Secure Architecture



VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.
vpc-0e24f4bc523d95809 (MySecureVPC)

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

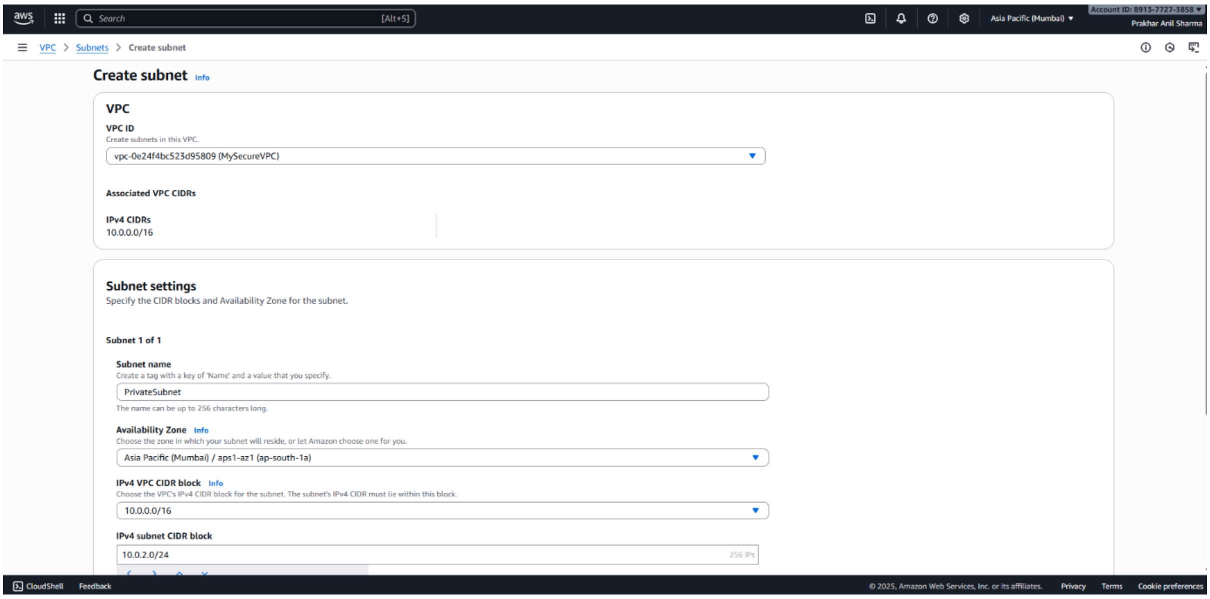
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
PublicSubnet
The name can be up to 256 characters long.

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

Step – 14] Click Create subnet .
Step – 15] In Subnet setting ,Name and create Private Subnet .
Step – 16] Input the IPv4 subnet CIDR block .



VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.
vpc-0e24f4bc523d95809 (MySecureVPC)

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

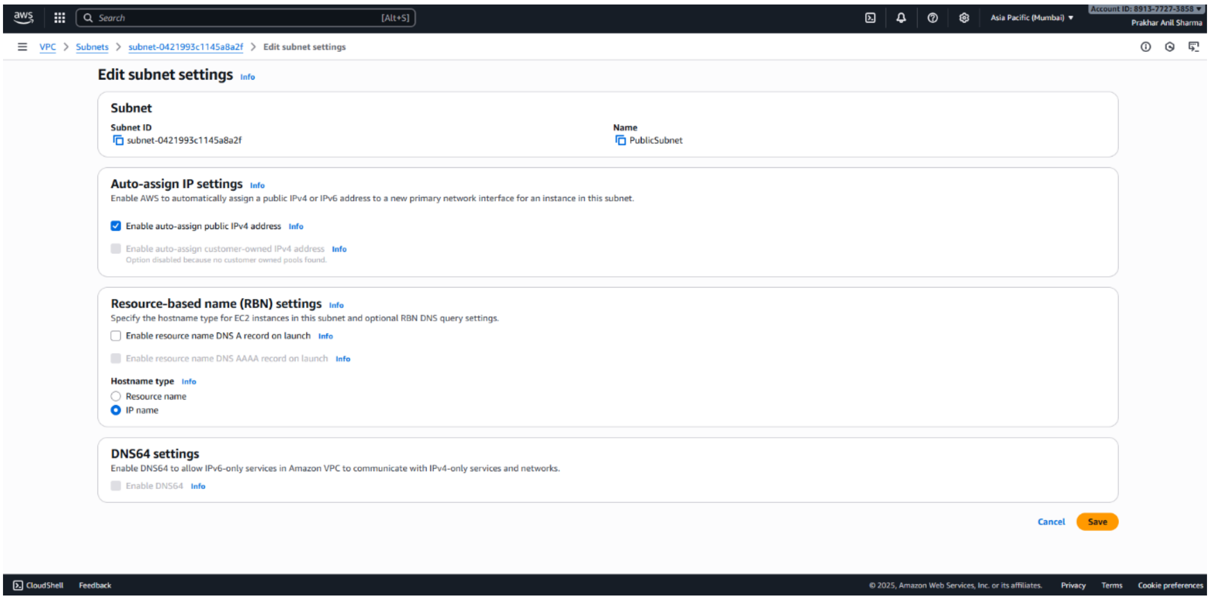
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
PrivateSubnet
The name can be up to 256 characters long.

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
10.0.2.0/24 256 IPs

Step – 17] Now go to the Public Subnet and enable auto assign public IPv4 .


aws
Search [Alt+S]
Asia Pacific (Mumbai) ▾
Account ID: 8913-7727-3858 ▾
Prakhar Anil Sharma
VPC > Subnets > subnet-0421993c1145a8a2f > Edit subnet settings
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Edit subnet settings Info

Subnet

Subnet ID: subnet-0421993c1145a8a2f

Name: PublicSubnet

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

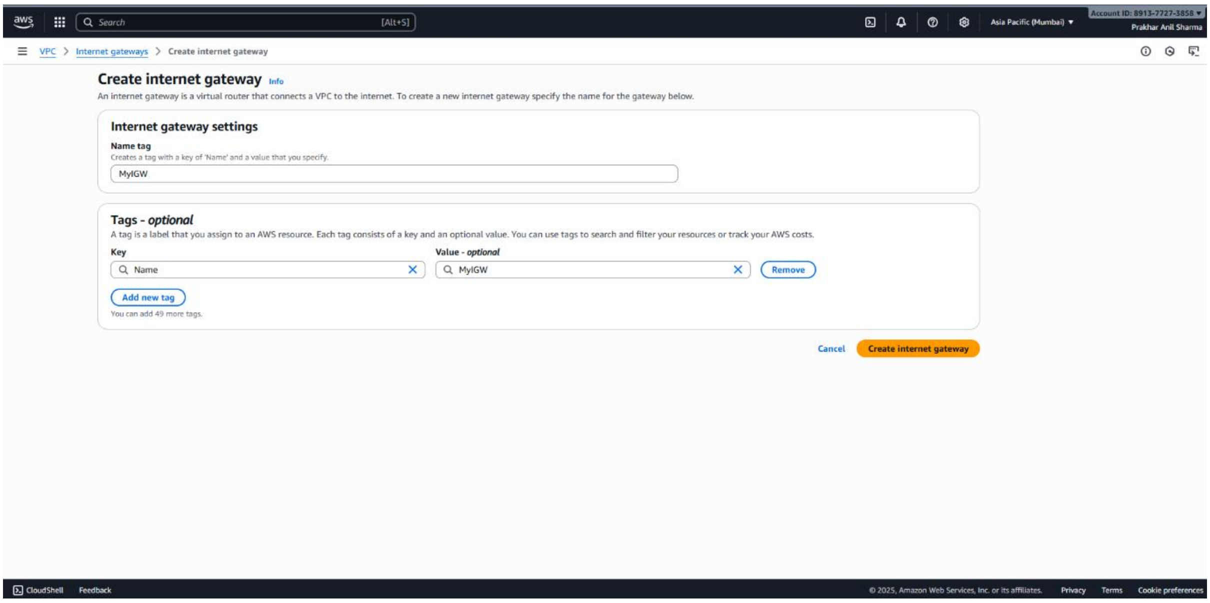
Cancel Save

Step – 18] In the left navigation menu, Click Internet gateway.

Step – 19] Click create internet gateway.

Step – 20] Name it .

Step – 21] Click create internet gateway .


aws
Search [Alt+S]
Asia Pacific (Mumbai) ▾
Account ID: 8913-7727-3858 ▾
Prakhar Anil Sharma
VPC > Internet gateways > Create internet gateway
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

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.
MyIGW

Tags - *optional*

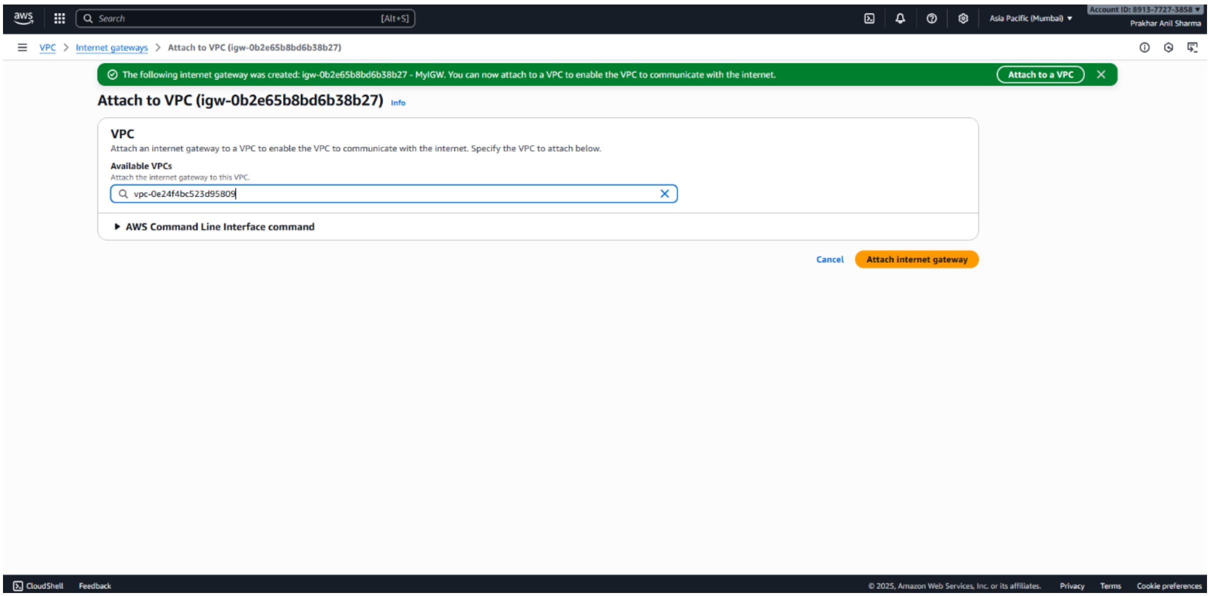
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*	
Name	MyIGW	Remove

Add new tag
You can add 49 more tags.

Cancel Create internet gateway

Step – 22] Attach it with VPC .



The following internet gateway was created: igw-0b2e65b8bd6b38b27 - MyIGW. You can now attach to a VPC to enable the VPC to communicate with the internet.

Attach to VPC (igw-0b2e65b8bd6b38b27)

VPC

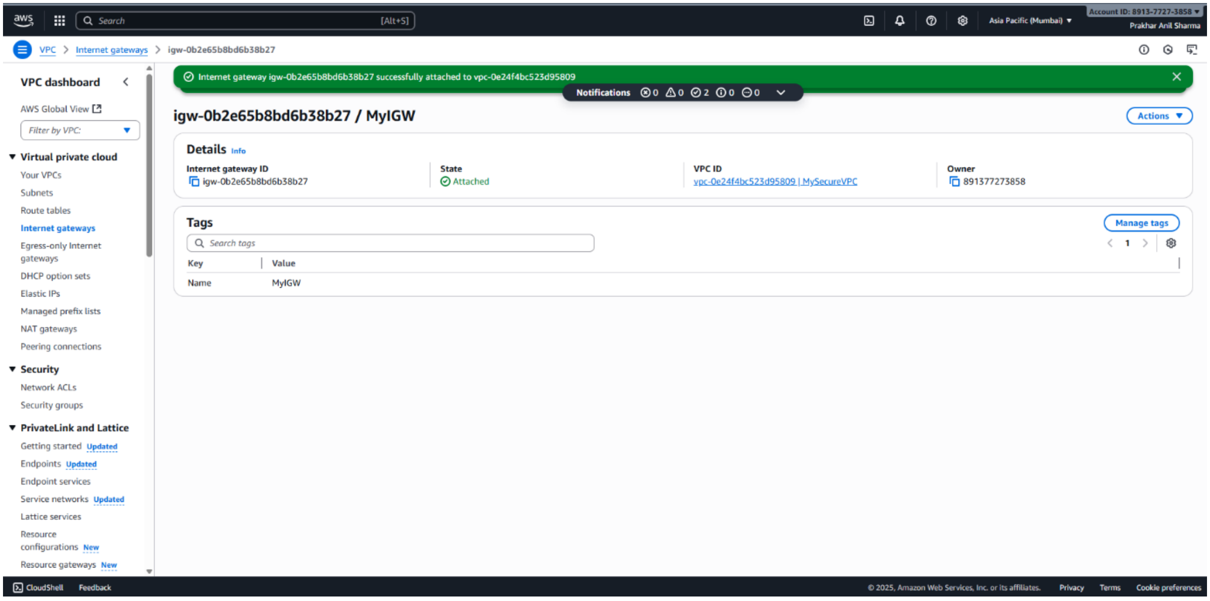
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

vpc-0e24f4bc523d95809

▸ AWS Command Line Interface command



Internet gateway igw-0b2e65b8bd6b38b27 successfully attached to vpc-0e24f4bc523d95809

igw-0b2e65b8bd6b38b27 / MyIGW

Details

Internet gateway ID	State	VPC ID	Owner
igw-0b2e65b8bd6b38b27	Attached	vpc-0e24f4bc523d95809 | MySecureVPC	891377273858

Tags

Key	Value
Name	MyIGW

Step – 23] Now in the navigation menu, go to NAT gateway .

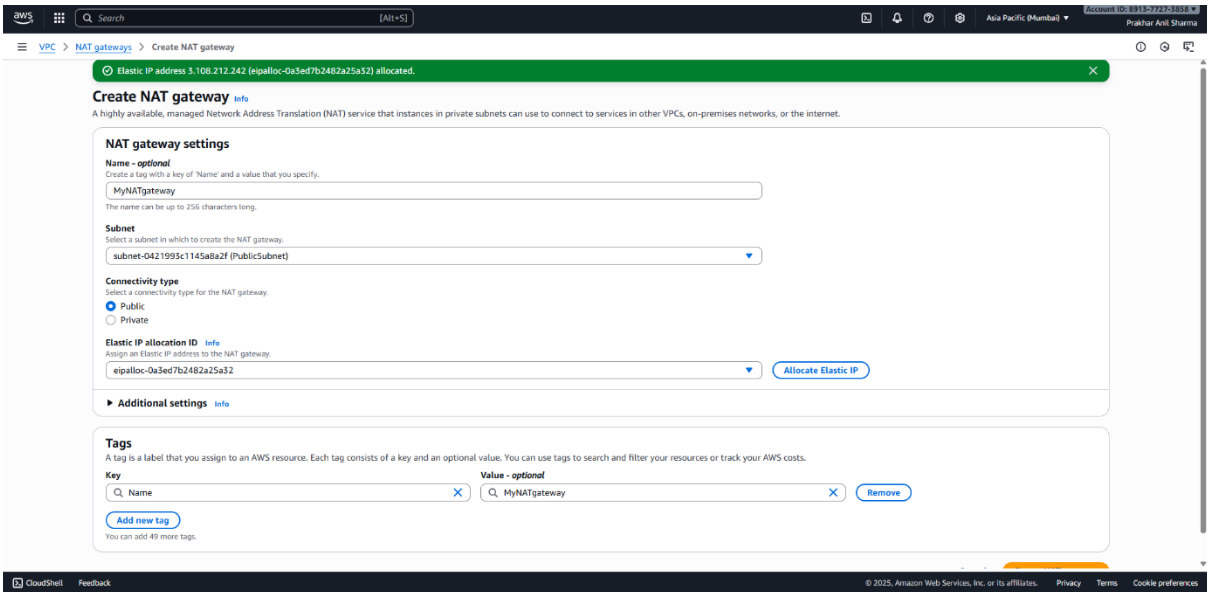
Step - 24] Click create NAT gateway .

Step - 25] Name it .

Step – 26] Select Public Subnet , with Public connectivity .

Step – 27] Select Elastic IP from dropdown .

Step - 28] Click create .



aws
Search [Alt+S]
Asia Pacific (Mumbai) ▾
Account ID: 8913-7727-3858 ▾
Prakhar Anil Sharma
VPC > NAT gateways > Create NAT gateway

Elastic IP address 3.108.212.242 (eipalloc-0a3ed7b2482a25a32) allocated.

Create NAT gateway Info

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

NAT gateway settings

Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.
MyNATgateway
The name can be up to 256 characters long.

Subnet
Select a subnet in which to create the NAT gateway.
subnet-0421993c1145a8a2f (PublicSubnet)

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

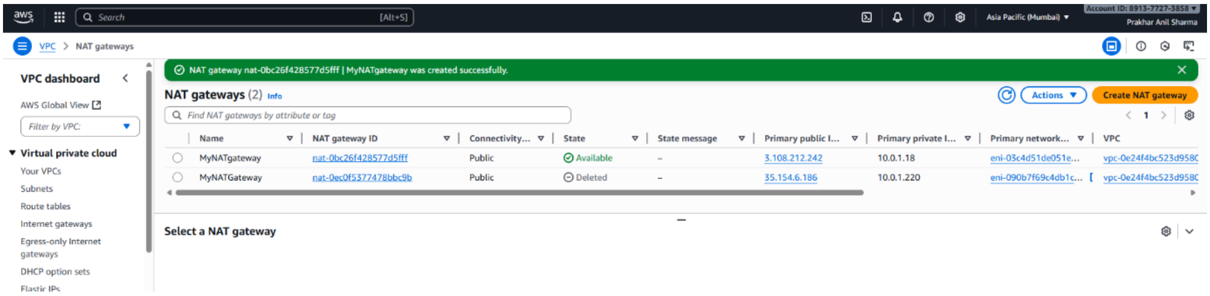
Elastic IP allocation ID Info
Assign an Elastic IP address to the NAT gateway.
eipalloc-0a3ed7b2482a25a32

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	MyNATgateway

You can add 49 more tags.



NAT gateway nat-0bc26f428577d5fff | MyNATgateway was created successfully.

NAT gateways (2) Info

	Name	NAT gateway ID	Connectivity...	State	State message	Primary public I...	Primary private I...	Primary network...	VPC
○	MyNATgateway	nat-0bc26f428577d5fff	Public	Available	–	3.108.212.242	10.0.1.18	eni-03c4d51de051e...	vpc-0e24f4bc523d958C
○	MyNATGateway	nat-0ec0f5377478bbc9b	Public	Deleted	–	35.154.6.186	10.0.1.220	eni-090b7f69c4db1c...	vpc-0e24f4bc523d958C

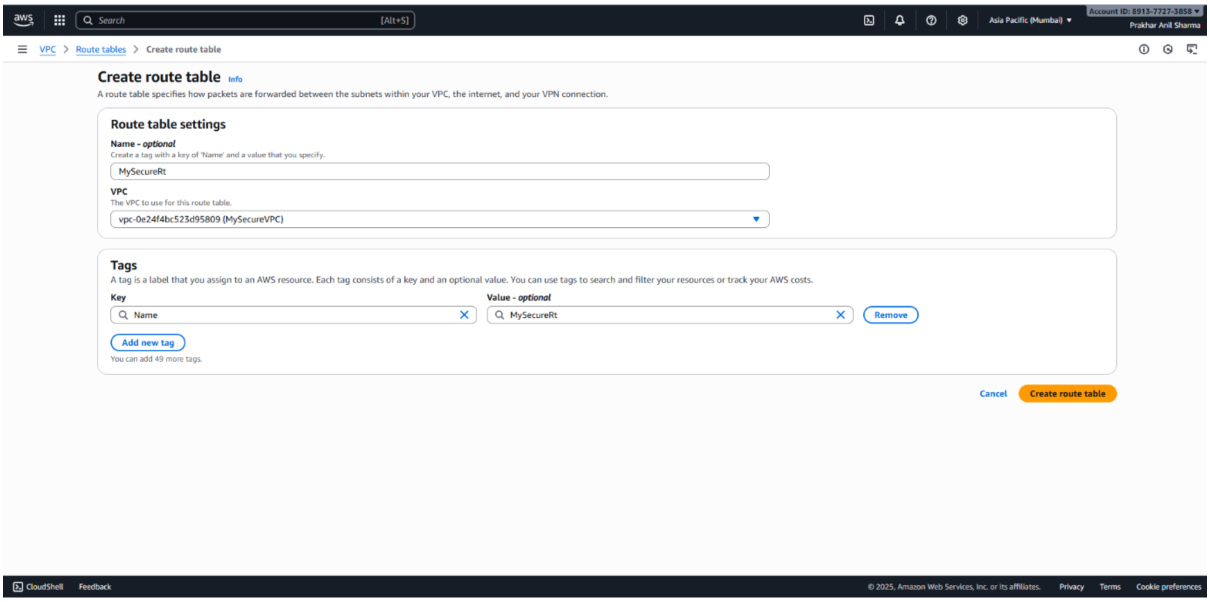
Select a NAT gateway

Step – 29] In navigation menu, go to Route table .

Step – 30] Click create route table .

Step – 31] Select VPC .

Step – 32] Click create .



VPC > Route tables > Create route table

Create route table

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*: MySecureRt

VPC: vpc-0e24f4bc523d95809 (MySecureVPC)

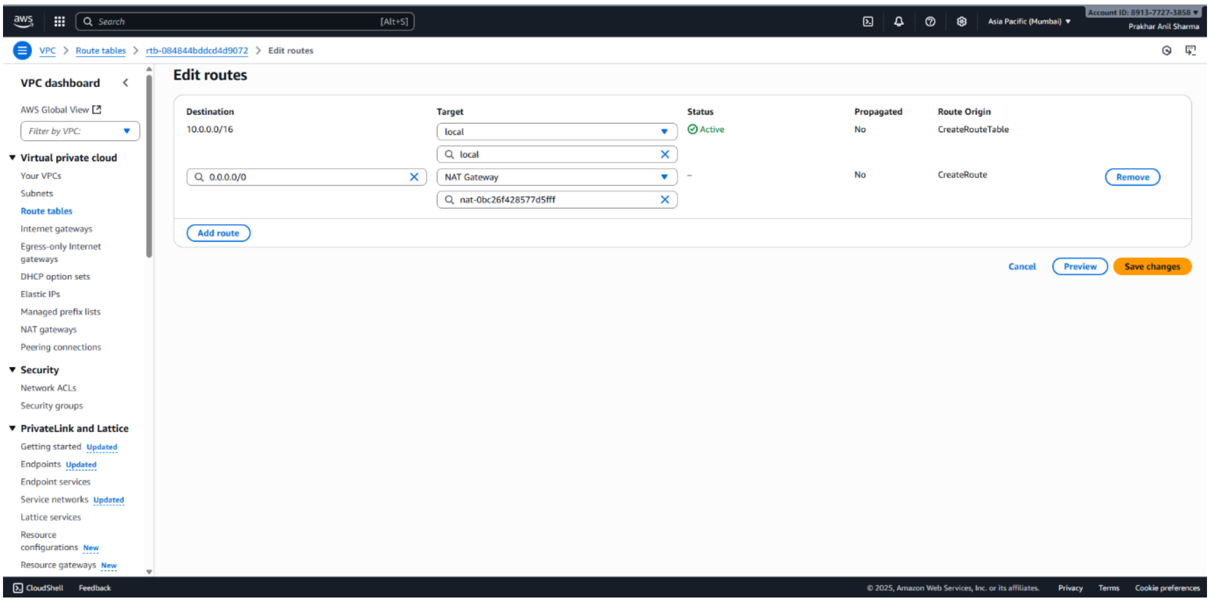
Tags

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	MySecureRt

You can add 49 more tags.

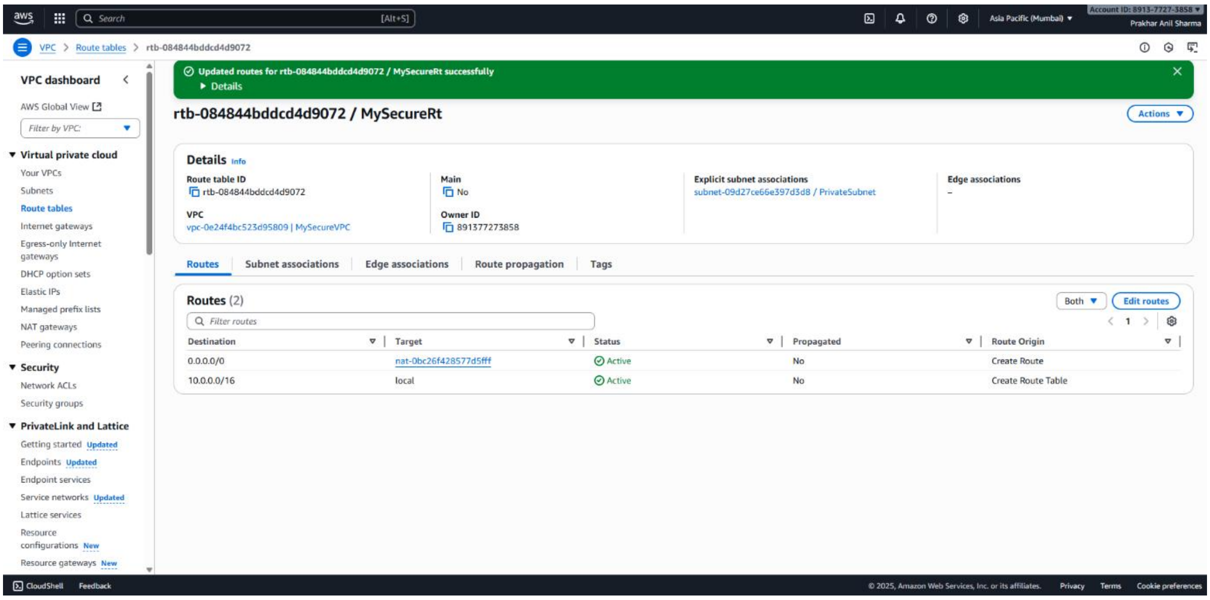
Step – 33] Go to route table ,Click edit routes.
Step - 34] Select destination 0.0.0.0/0 and target as NAT gateway.
Step – 35] Click save changes.



VPC > Route tables > rtb-084844bddcd4d9072 > Edit routes

Edit routes

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local local	Active	No	CreateRouteTable
0.0.0.0/0	NAT Gateway nat-0bc26f428577d5fff	-	No	CreateRoute



Updated routes for rtb-084844bddcd4d9072 / MySecureRt successfully

rtb-084844bddcd4d9072 / MySecureRt

Details

Route table ID: rtb-084844bddcd4d9072

Main: No

Explicit subnet associations: subnet-09d27ce66e397d3d8 / PrivateSubnet

Edge associations: –

VPC: vpc-0e24f4bc523d95809 | MySecureVPC

Owner ID: 891377273858

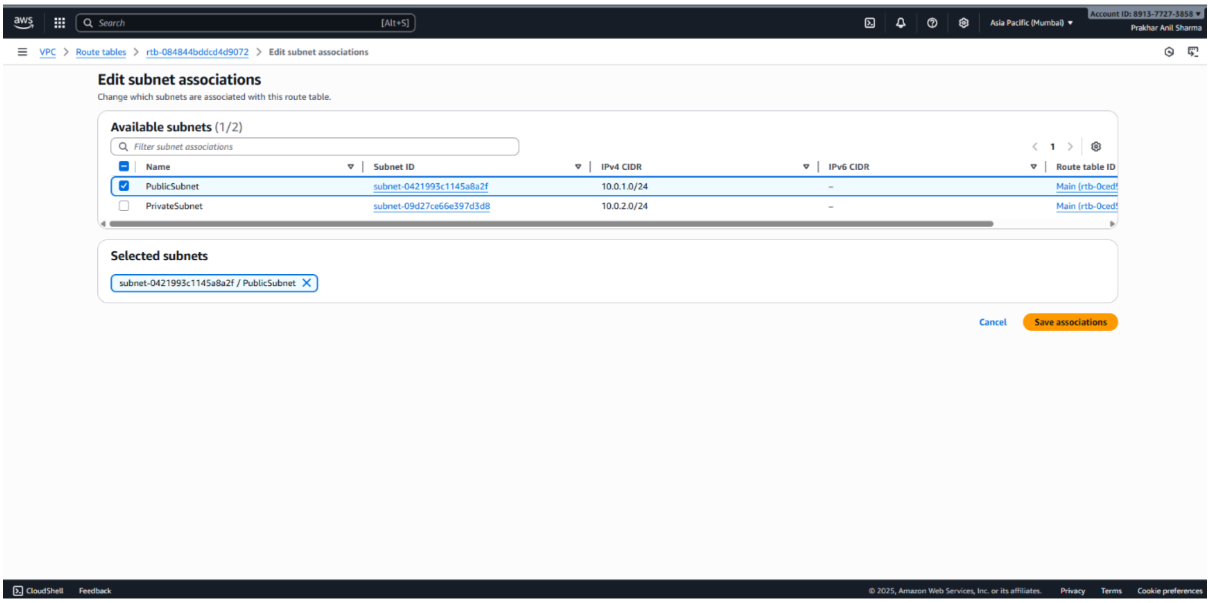
Routes (2)

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	nat-0bc26f428577d5fff	Active	No	Create Route
10.0.0.0/16	local	Active	No	Create Route Table

Step – 36] Go to subnet association, Click edit .

Step – 37] Select Public Subnet , Click save association.

Step – 38] Select Private Subnet , Click save association.


VPC > Route tables > rtb-084844bddcd4d9072 > Edit subnet associations
Filter subnet associations
Cancel
Save associations
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Edit subnet associations

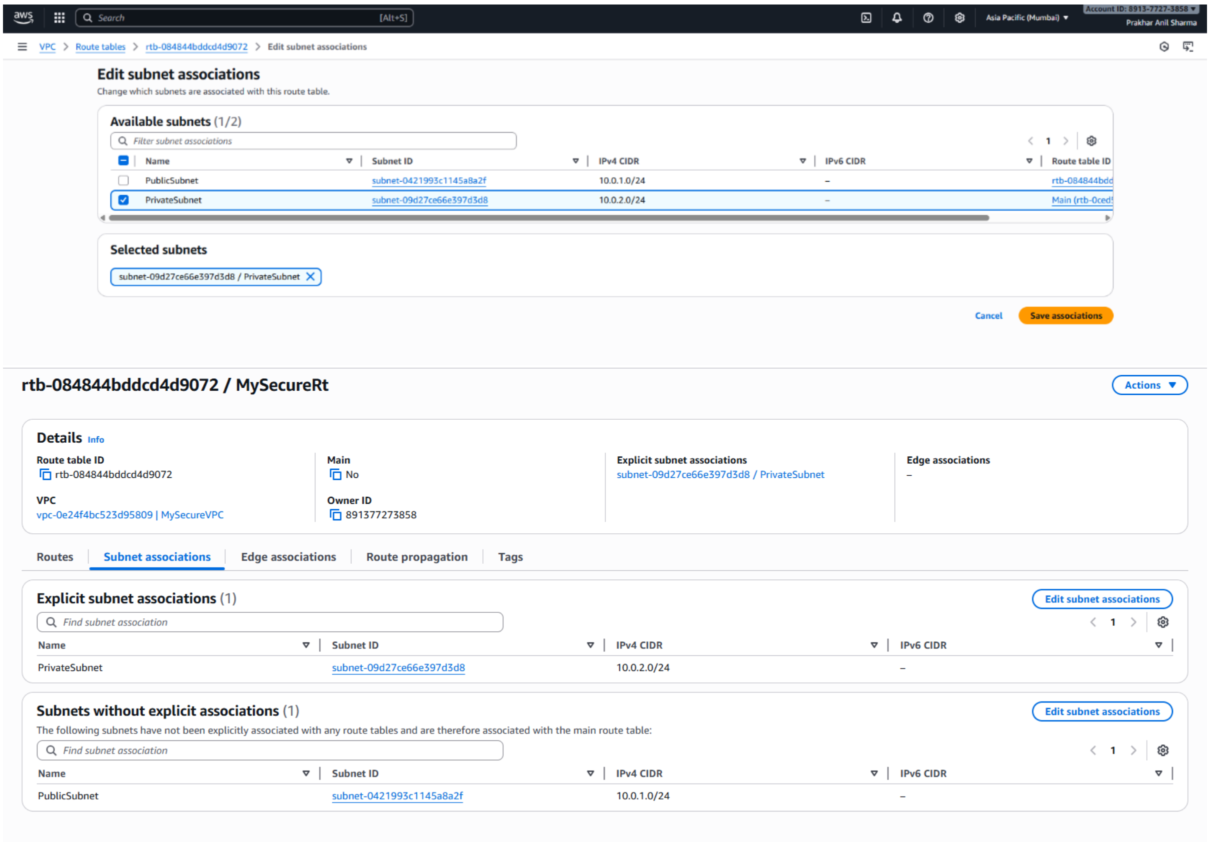
Change which subnets are associated with this route table.

Available subnets (1/2)

	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
☑	PublicSubnet	subnet-0421993c1145a8a2f	10.0.1.0/24	–	Main (rtb-0ced!
□	PrivateSubnet	subnet-09d27ce66e397d3d8	10.0.2.0/24	–	Main (rtb-0ced!

Selected subnets

subnet-0421993c1145a8a2f / PublicSubnet



aws
Search [Alt+S]
Asia Pacific (Mumbai) ▾
Account ID: 8913-7727-3858 ▾
Prakhar Anil Sharma
VPC > Route tables > rtb-084844bddcd4d9072 > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/2)

Filter subnet associations

	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
□	PublicSubnet	subnet-0421993c1145a8a2f	10.0.1.0/24	–	rtb-084844bdd
☑	PrivateSubnet	subnet-09d27ce66e397d3d8	10.0.2.0/24	–	Main (rtb-0ced

Selected subnets

subnet-09d27ce66e397d3d8 / PrivateSubnet ✕

rtb-084844bddcd4d9072 / MySecureRt

Details Info

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-084844bddcd4d9072	No	subnet-09d27ce66e397d3d8 / PrivateSubnet	–
VPC	**Owner ID**		
vpc-0e24f4bc523d95809 | MySecureVPC	891377273858		

Explicit subnet associations (1)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
PrivateSubnet	subnet-09d27ce66e397d3d8	10.0.2.0/24	–

Subnets without explicit associations (1)

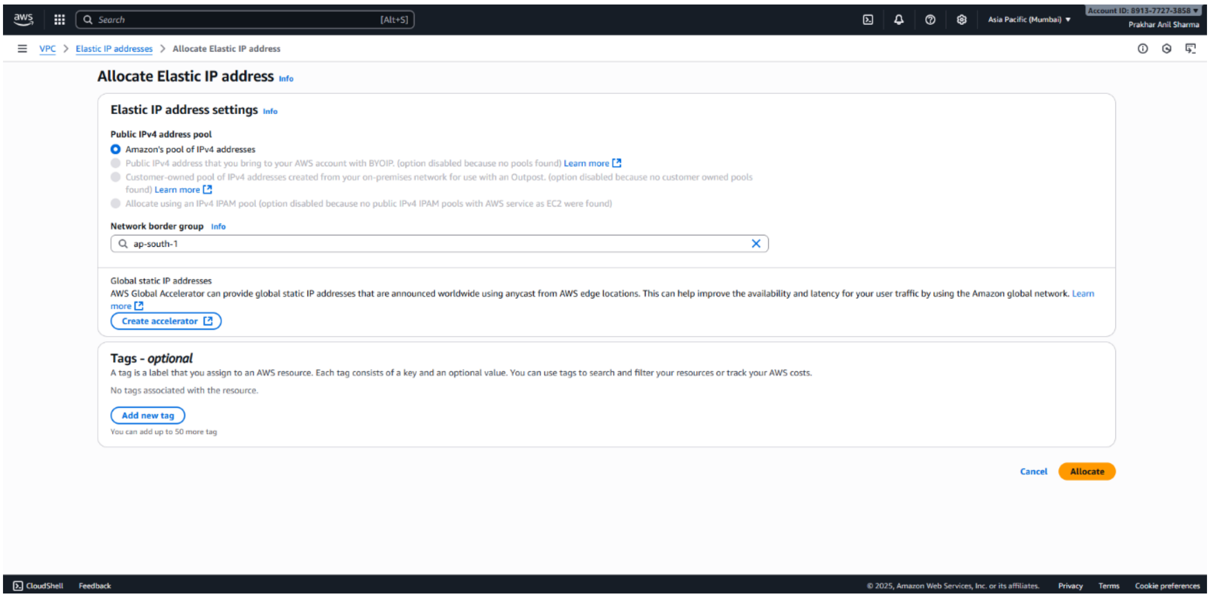
The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
PublicSubnet	subnet-0421993c1145a8a2f	10.0.1.0/24	–

Step – 39] Go to navigation menu, Click Elastic IP address.

Step – 40] Click allocate elastic IP address .

Step – 41] Click allocate .



VPC > Elastic IP addresses > Allocate Elastic IP address

Allocate Elastic IP address Info

Elastic IP address settings Info

Public IPv4 address pool

● Amazon's pool of IPv4 addresses

○ Public IPv4 address that you bring to your AWS account with BYOIP. (option disabled because no pools found) Learn more

○ Customer-owned pool of IPv4 addresses created from your on-premises network for use with an Outpost. (option disabled because no customer owned pools found) Learn more

○ Allocate using an IPv4 IPAM pool (option disabled because no public IPv4 IPAM pools with AWS service as EC2 were found)

Network border group Info

ap-south-1

Global static IP addresses

AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. Learn more

Create accelerator

Tags - *optional*

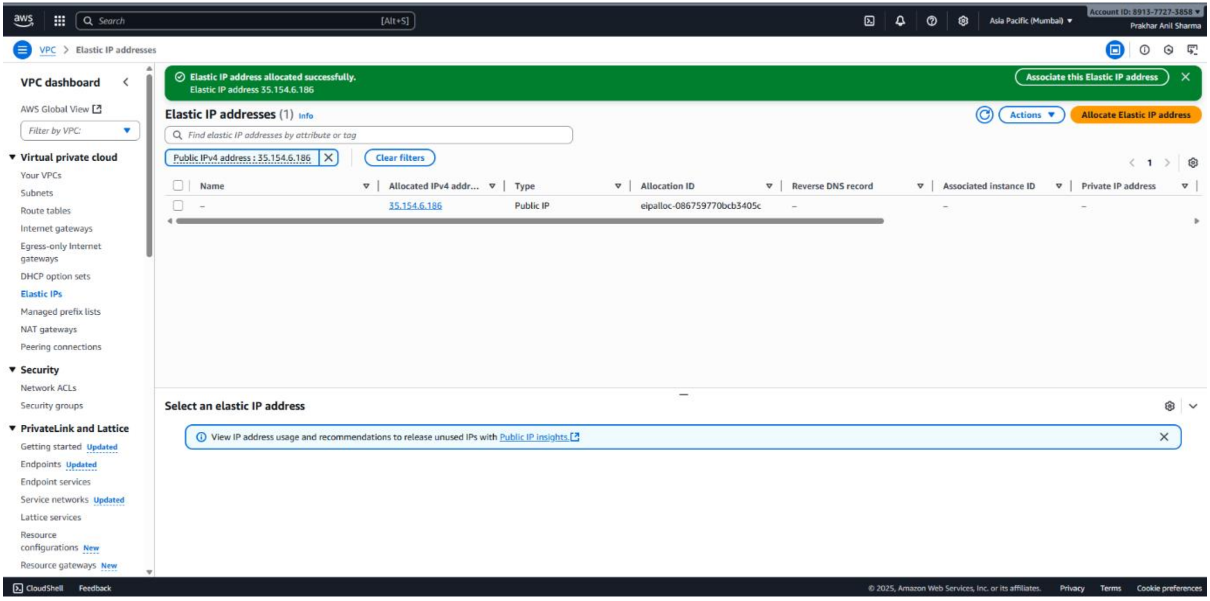
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

Add new tag

You can add up to 50 more tag

Cancel Allocate



VPC > Elastic IP addresses

Elastic IP address allocated successfully.
Elastic IP address 35.154.6.186

Elastic IP addresses (1) Info

Public IPv4 address : 35.154.6.186

Name	Allocated IPv4 addr...	Type	Allocation ID	Reverse DNS record	Associated instance ID	Private IP address
–	35.154.6.186	Public IP	eipalloc-086759770bcb3405c	–	–	–

Select an elastic IP address

Step – 42] Go to search box, search EC2.

Step – 43] Click EC2, Click create Instance.

Step – 44] Name it.

Step – 45] Select ami as Amazon Linux .

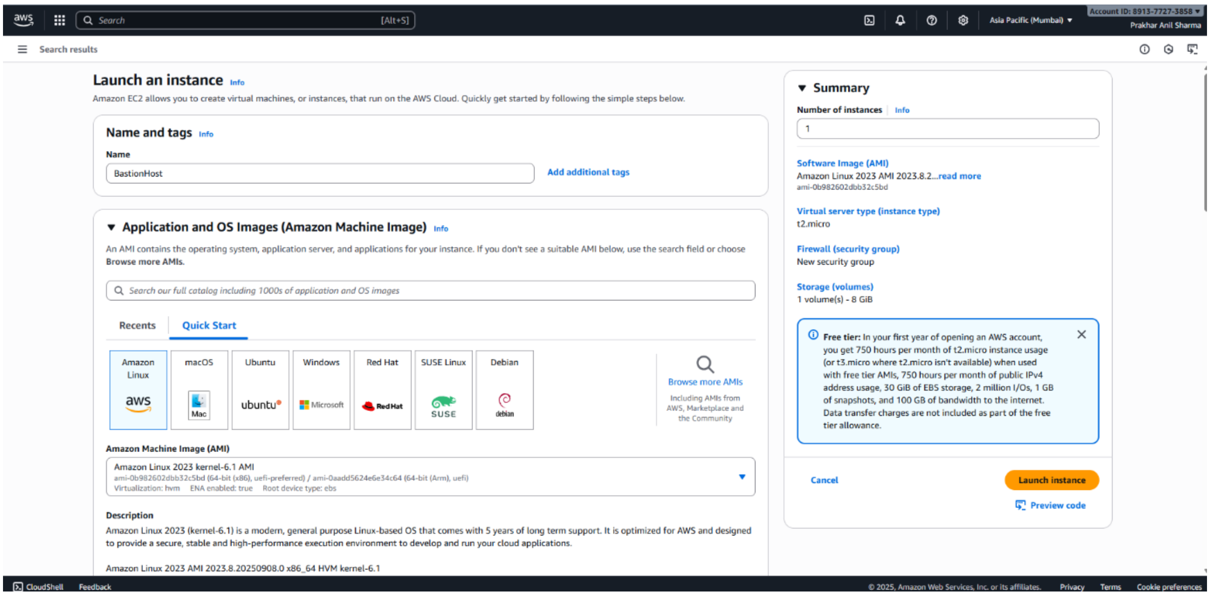
Step – 46] Select instance type as t2.micro.

Step – 47] Create Key Pair.

Step – 48] In network setting, Select VPC .

Step – 49] Select Public Subnet .

Step – 50] Enable Auto assign IP.



Launch an instance

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

Name and tags

Name: BastionHost

Application and OS Images (Amazon Machine Image)

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose Browse more AMIs.

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

Amazon Machine Image (AMI)

Amazon Linux 2023 kernel-6.1 AMI
ami-0b982602dbb32c5bd (64-bit (x86), uefi-preferred) / ami-0aadd5624e6e34c64 (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 (kernel-6.1) is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Amazon Linux 2023 AMI 2023.8.20250908.0 x86_64 HVM kernel-6.1

Summary

Number of instances: 1

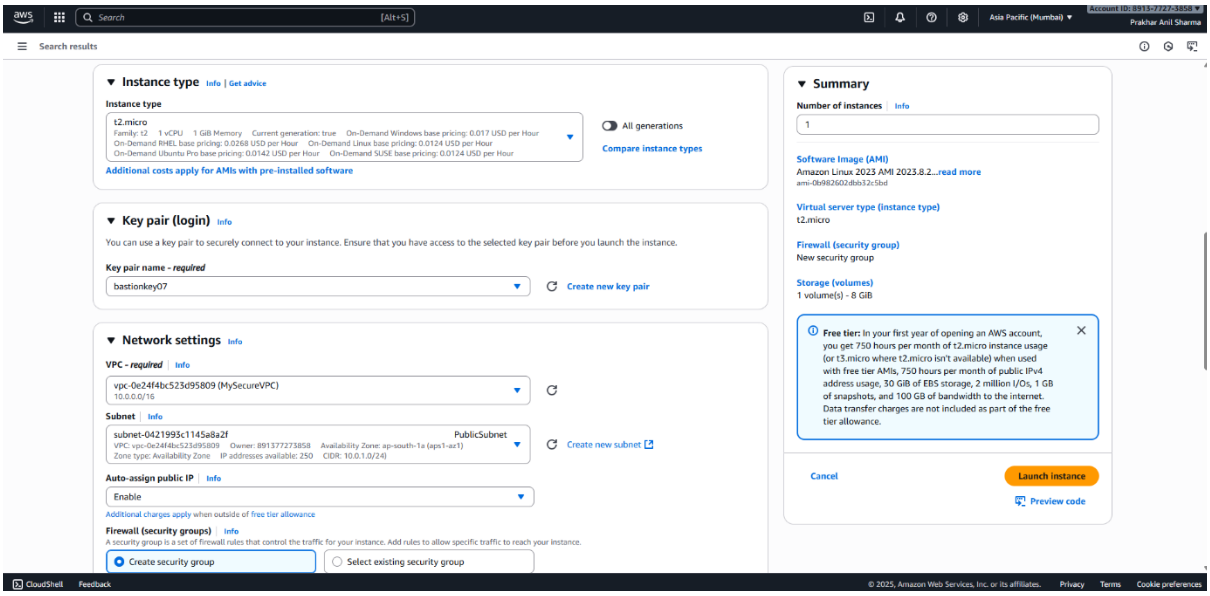
Software Image (AMI)
Amazon Linux 2023 AMI 2023.8.2...read more
ami-0b982602dbb32c5bd

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet. Data transfer charges are not included as part of the free tier allowance.



▼ Instance type

Instance type
t2.micro
Family: t2 1 vCPU 1 GiB Memory Current generation: true On-Demand Windows base pricing: 0.017 USD per Hour
On-Demand RHEL base pricing: 0.0268 USD per Hour On-Demand Linux base pricing: 0.0124 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0142 USD per Hour On-Demand SUSE base pricing: 0.0124 USD per Hour

Additional costs apply for AMIs with pre-installed software

▼ Key pair (login)

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*: bastionkey07

▼ Network settings

VPC - *required*: vpc-0e24f4bc523d95809 (MySecureVPC)
10.0.0.0/16

Subnet: subnet-0421993c1145a8a2f PublicSubnet
VPC: vpc-0e24f4bc523d95809 Owner: 891377273858 Availability Zone: ap-south-1a (aps1-az1)
Zone type: Availability Zone IP addresses available: 250 CIDR: 10.0.1.0/24)

Auto-assign public IP: Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups)
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 ○ Select existing security group

▼ Summary

Number of instances: 1

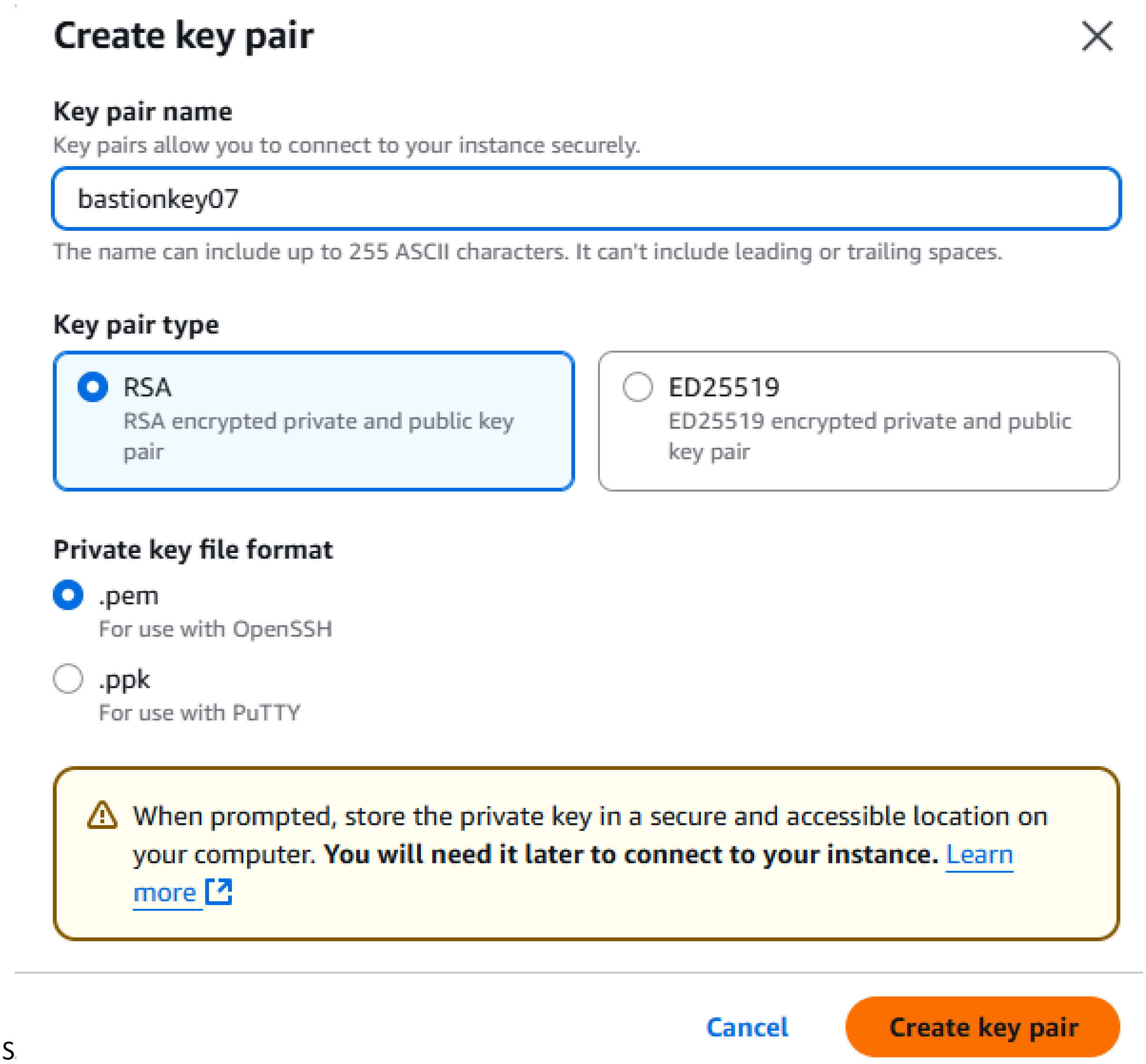
Software Image (AMI)
Amazon Linux 2023 AMI 2023.8.2...read more
ami-0b982602dbb32c5bd

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet. Data transfer charges are not included as part of the free tier allowance.



Create key pair

Key pair name

Key pairs allow you to connect to your instance securely.

bastionkey07

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

● RSA
RSA encrypted private and public key pair

○ ED25519
ED25519 encrypted private and public key pair

Private key file format

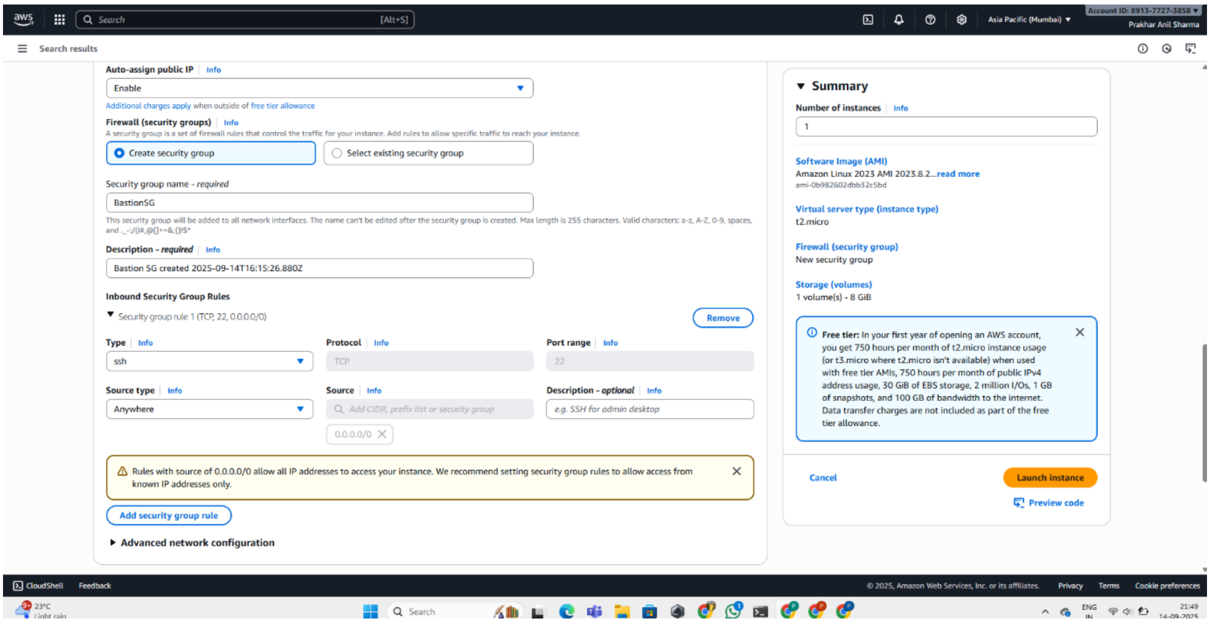
● .pem
For use with OpenSSH

○ .ppk
For use with PuTTY

⚠ When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** Learn more

S

Step – 51] Create Security Group .
Step – 52] Name it .
Step – 53] Set SSH as Inbound rule .
Step – 54] Click Launch instance .



Auto-assign public IP: Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups)

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 ○ Select existing security group

Security group name - *required*: BastionSG

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - *required*: Bastion SG created 2025-09-14T16:15:26.880Z

Inbound Security Group Rules

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

Type: ssh

Protocol: TCP

Port range: 22

Source type: Anywhere

Source: Add CIDR, prefix list or security group — 0.0.0.0/0

Description - *optional*: e.g. SSH for admin desktop

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.8.2...read more ami-0b982602dbb32c5bd

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet. Data transfer charges are not included as part of the free tier allowance.

Step – 55] Create another Instance.

Step – 56] Name it.

Step – 57] Select ami as Amazon Linux .

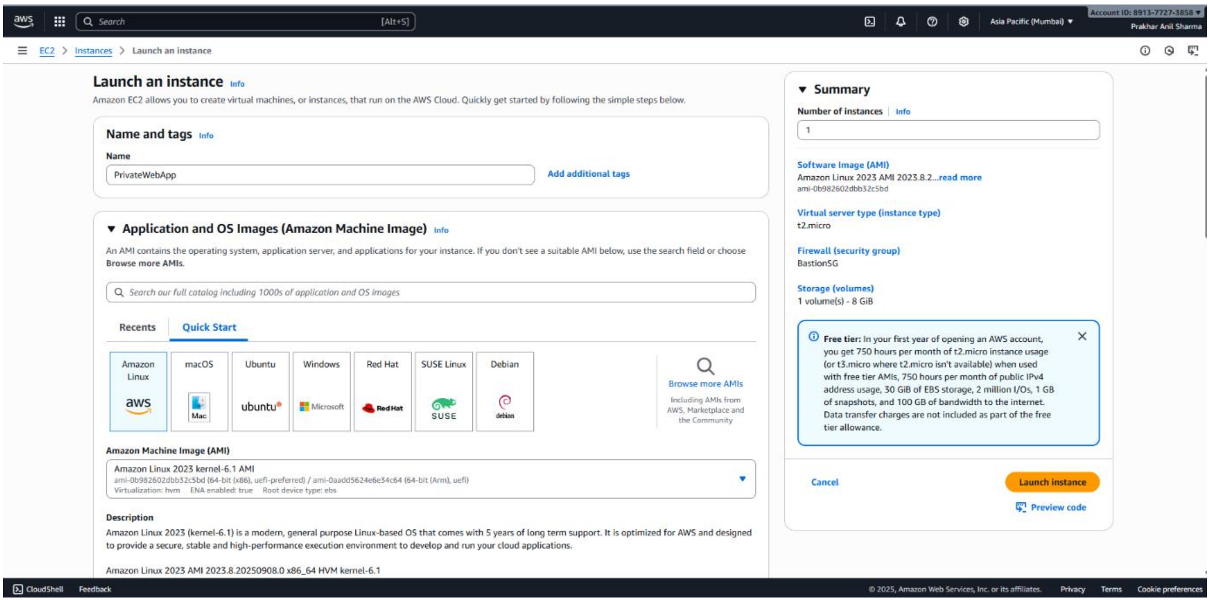
Step – 58] Select instance type as t2.micro.

Step – 59] Select Key Pair.

Step – 60] In network setting, Select VPC .

Step – 61] Select Private Subnet .

Step – 62] Disable Auto assign IP.



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: PrivateWebApp

Add additional tags

▼ Application and OS Images (Amazon Machine Image) Info

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose Browse more AMIs.

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

Recents | Quick Start

Amazon Linux | macOS | Ubuntu | Windows | Red Hat | SUSE Linux | Debian

Browse more AMIs
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 kernel-6.1 AMI
ami-0b982602dbb32c5bd (64-bit (x86), uefi-preferred) / ami-0aadd5624e6e34c64 (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 (kernel-6.1) is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Amazon Linux 2023 AMI 2023.8.20250908.0 x86_64 HVM kernel-6.1

▼ Summary

Number of instances | Info: 1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.8.2...read more
ami-0b982602dbb32c5bd

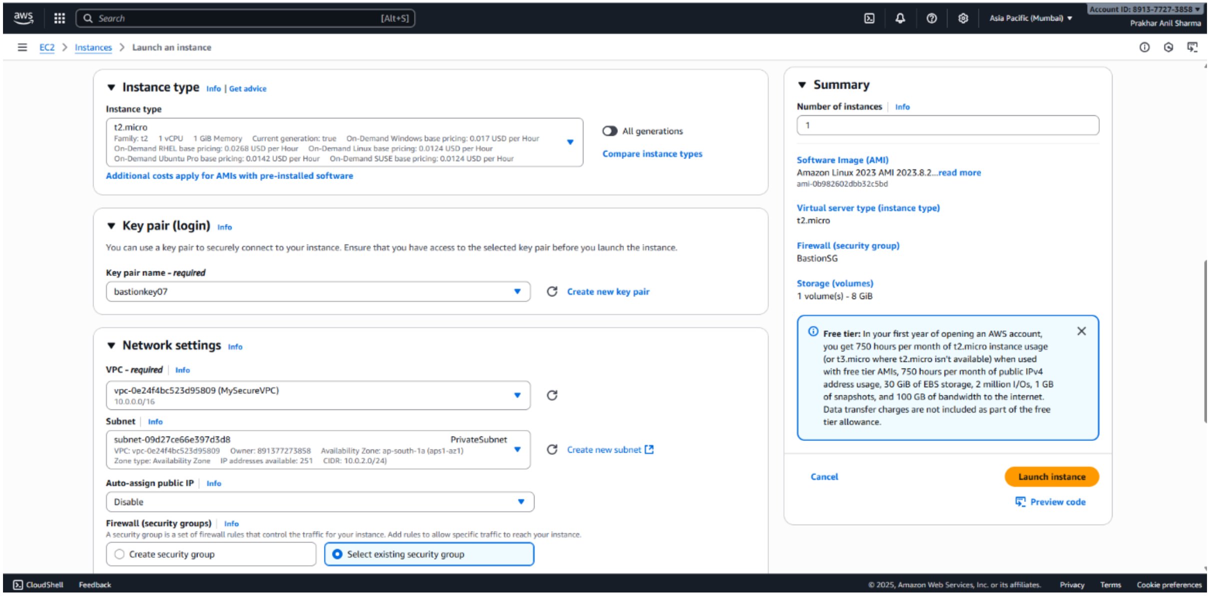
Virtual server type (instance type)
t2.micro

Firewall (security group)
BastionSG

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet. Data transfer charges are not included as part of the free tier allowance.

Cancel | Launch instance | Preview code



EC2 > Instances > Launch an instance

▼ Instance type Info | Get advice

Instance type

t2.micro
Family: t2 1 vCPU 1 GiB Memory Current generation: true On-Demand Windows base pricing: 0.017 USD per Hour
On-Demand RHEL base pricing: 0.0268 USD per Hour On-Demand Linux base pricing: 0.0124 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0142 USD per Hour On-Demand SUSE base pricing: 0.0124 USD per Hour

All generations | Compare instance types

Additional costs apply for AMIs with pre-installed software

▼ Key pair (login) Info

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

Key pair name - *required*: bastionkey07

Create new key pair

▼ Network settings Info

VPC - *required* | Info
vpc-0e24f4bc523d95809 (MySecureVPC)
10.0.0.0/16

Subnet | Info
subnet-09d27ce66e397d3d8 PrivateSubnet
VPC: vpc-0e24f4bc523d95809 Owner: 891377273858 Availability Zone: ap-south-1a (aps1-az1)
Zone type: Availability Zone IP addresses available: 251 CIDR: 10.0.2.0/24)

Create new subnet

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 ● Select existing security group

▼ Summary

Number of instances | Info: 1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.8.2...read more
ami-0b982602dbb32c5bd

Virtual server type (instance type)
t2.micro

Firewall (security group)
BastionSG

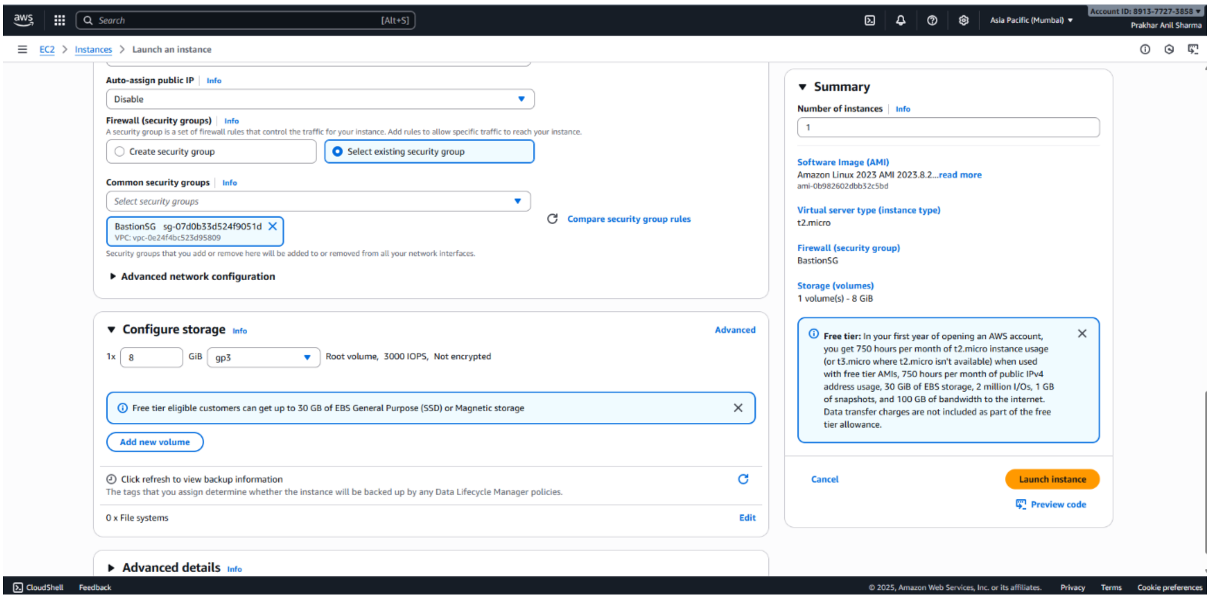
Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet. Data transfer charges are not included as part of the free tier allowance.

Cancel | Launch instance | Preview code

Step – 63] Select existing Security Group .

Step – 64] Click Launch instance .



EC2 > Instances > Launch an instance

Auto-assign public IP: Disable

Firewall (security groups)

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 ● Select existing security group

Common security groups: Select security groups

BastionSG sg-07d0b33d524f9051d
VPC: vpc-0e24f4bc523d95809

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

Configure storage

1x 8 GiB gp3 Root volume, 3000 IOPS, Not encrypted

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Click refresh to view backup information

The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems

Summary

Number of instances: 1

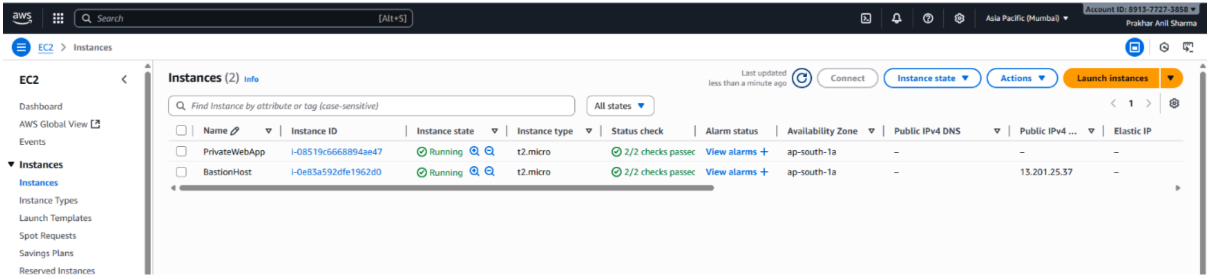
Software Image (AMI): Amazon Linux 2023 AMI 2023.8.2...read more
ami-0b982602dbb32c5bd

Virtual server type (instance type): t2.micro

Firewall (security group): BastionSG

Storage (volumes): 1 volume(s) - 8 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet. Data transfer charges are not included as part of the free tier allowance.

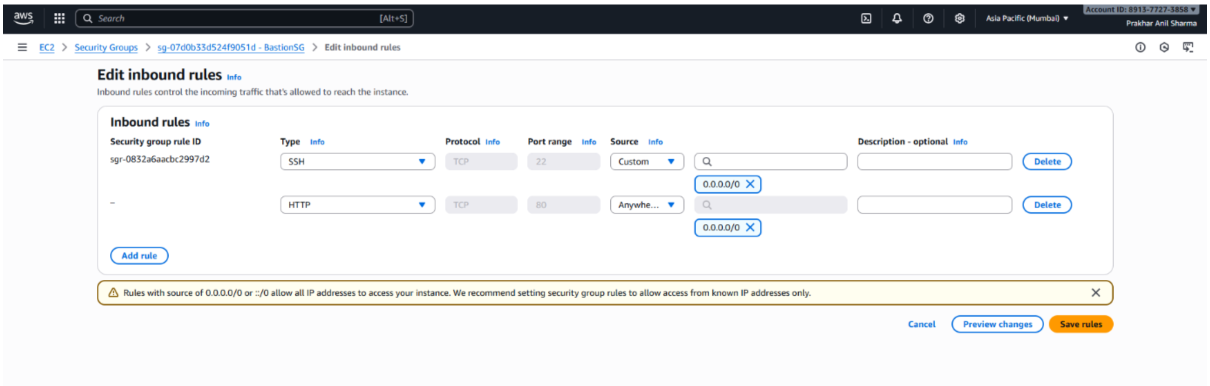


EC2 > Instances

Instances (2)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
PrivateWebApp	i-08519c6668894ae47	Running	t2.micro	2/2 checks passec	View alarms +	ap-south-1a	–	–	–
BastionHost	i-0e83a592dfe1962d0	Running	t2.micro	2/2 checks passec	View alarms +	ap-south-1a	–	13.201.25.37	–

Step – 65] Now go the security group and add HTTP in inbound rule.



EC2 > Security Groups > sg-07d0b33d524f9051d - BastionSG > Edit inbound rules

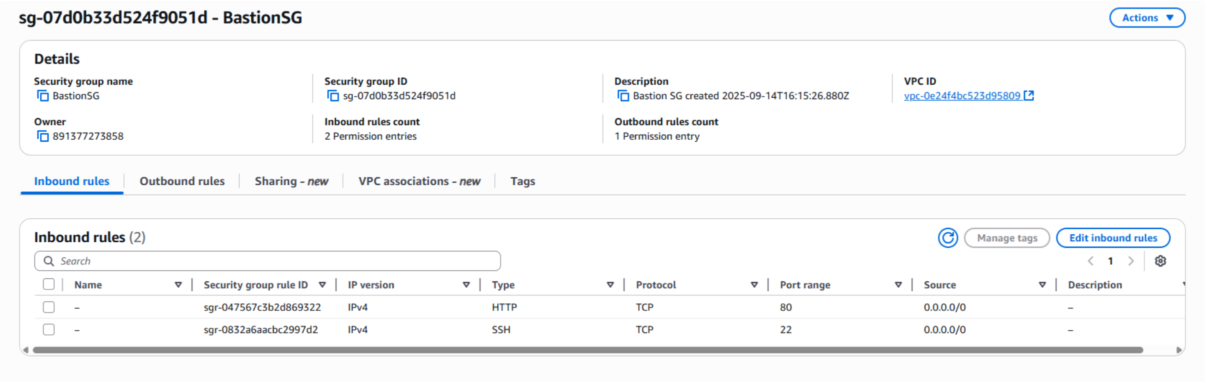
Edit inbound rules

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

Inbound rules

Security group rule ID	Type	Protocol	Port range	Source		Description - optional
sgr-0832a6aacbc2997d2	SSH	TCP	22	Custom	0.0.0.0/0	
–	HTTP	TCP	80	Anywhe...	0.0.0.0/0	

Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.



sg-07d0b33d524f9051d - BastionSG

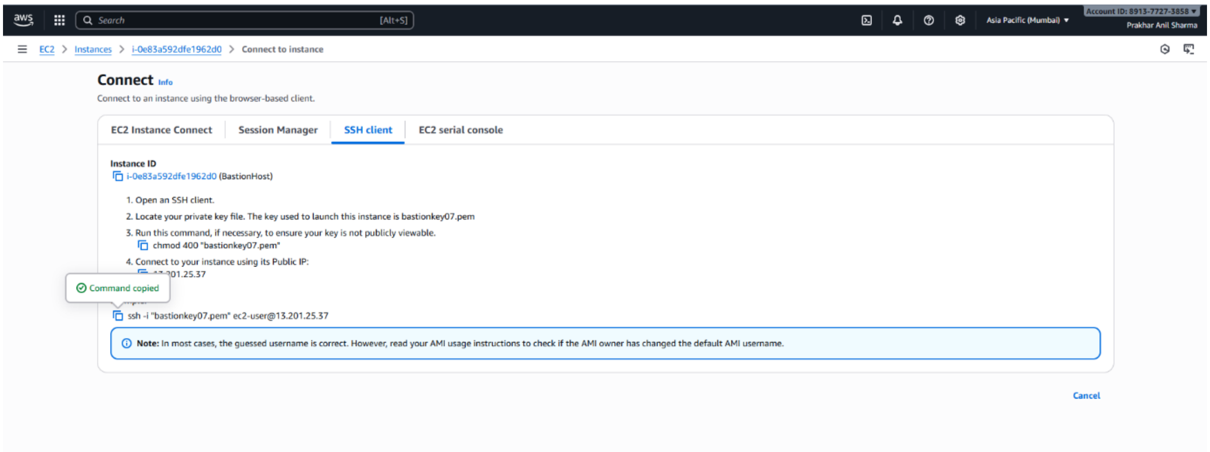
Details

Security group name: BastionSG
Security group ID: sg-07d0b33d524f9051d
Description: Bastion SG created 2025-09-14T16:15:26.880Z
VPC ID: vpc-0e24f4bc523d95809
Owner: 891377273858
Inbound rules count: 2 Permission entries
Outbound rules count: 1 Permission entry

Inbound rules (2)

□	Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
□	–	sgr-047567c3b2d869322	IPv4	HTTP	TCP	80	0.0.0.0/0	–
□	–	sgr-0832a6aacbc2997d2	IPv4	SSH	TCP	22	0.0.0.0/0	–

Step – 66] Now go to instances, Connect the bastion server using SSH client .



aws
Search [Alt+S]
Asia Pacific (Mumbai) ▼
Account ID: 8913-7727-3858 ▼
Prakhar Anil Sharma
EC2 > Instances > i-0e83a592dfe1962d0 > Connect to instance

Connect Info

Connect to an instance using the browser-based client.

Instance ID
i-0e83a592dfe1962d0 (BastionHost)

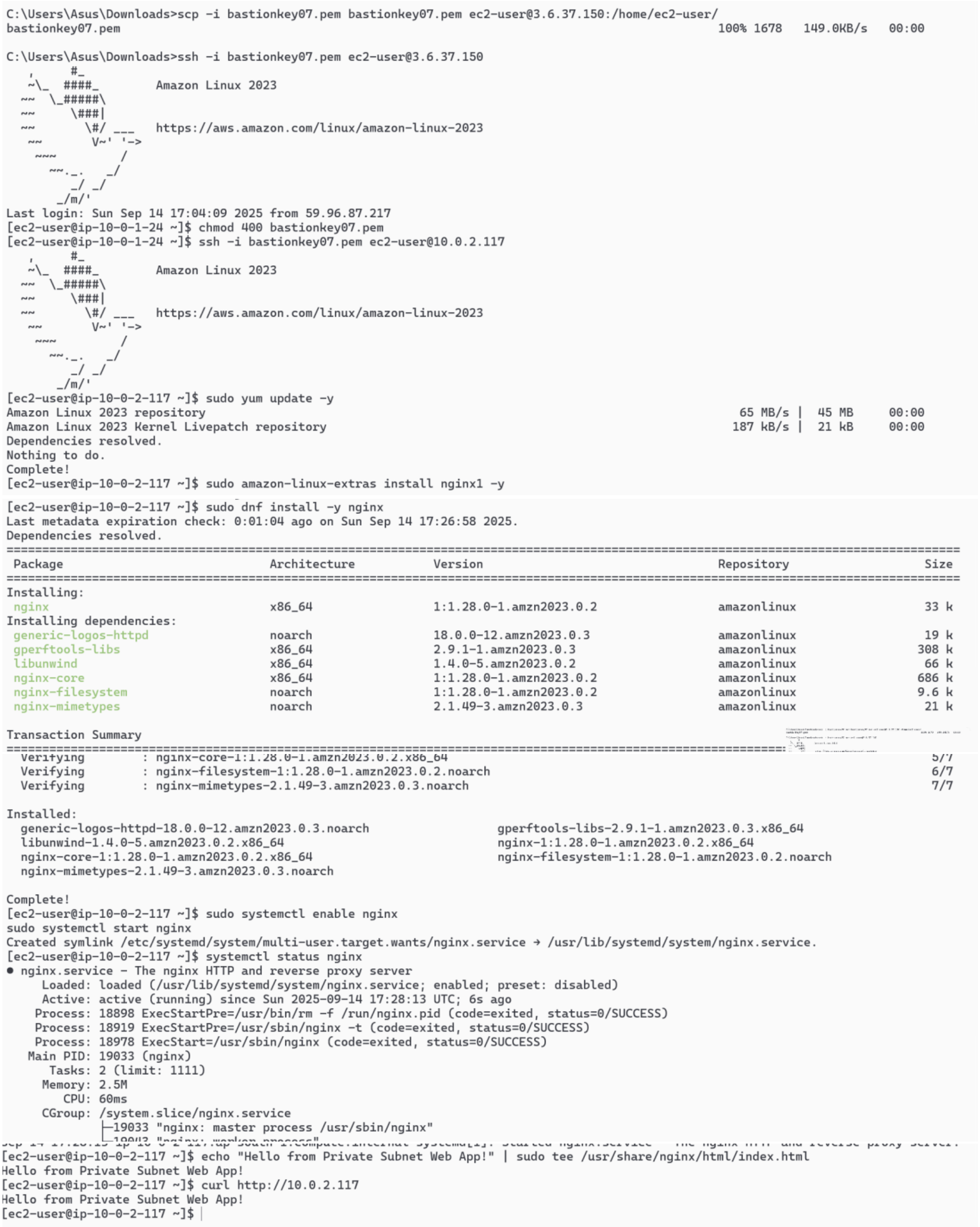
1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is bastionkey07.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
   chmod 400 "bastionkey07.pem"
4. Connect to your instance using its Public IP:
   01.25.37

```
ssh -i "bastionkey07.pem" ec2-user@13.201.25.37
```

Note: In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

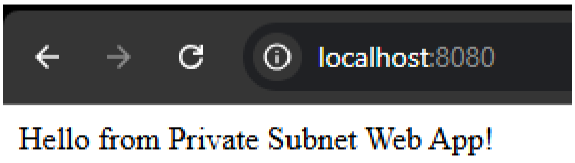
Step – 67] Now run the following command to host the website from private to public subnet .

```
- ssh -i "bastionkey07.pem" -L 8080:10.0.2.117:80 ec2-user@3.6.37.150
- ssh -i bastionkey07.pem ec2-user@3.6.37.150
- chmod 400 bastionkey07.pem
- ssh -i bastionkey07.pem ec2-user@10.0.2.117
- sudo yum update -y

- sudo amazon-linux-extras install nginx1 -y

- sudo systemctl start nginx

- sudo systemctl enable nginx

- echo "Hello from Private Subnet Web App!" | sudo tee /usr/share/nginx/html/index.html
- curl http://10.0.2.117
```



```
C:\Users\Asus\Downloads>scp -i bastionkey07.pem bastionkey07.pem ec2-user@3.6.37.150:/home/ec2-user/
bastionkey07.pem                                                                        100% 1678   149.0KB/s   00:00

C:\Users\Asus\Downloads>ssh -i bastionkey07.pem ec2-user@3.6.37.150
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Sun Sep 14 17:04:09 2025 from 59.96.87.217
[ec2-user@ip-10-0-1-24 ~]$ chmod 400 bastionkey07.pem
[ec2-user@ip-10-0-1-24 ~]$ ssh -i bastionkey07.pem ec2-user@10.0.2.117
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-10-0-2-117 ~]$ sudo yum update -y
Amazon Linux 2023 repository                                                              65 MB/s |  45 MB     00:00
Amazon Linux 2023 Kernel Livepatch repository                                            187 kB/s |  21 kB     00:00
Dependencies resolved.
Nothing to do.
Complete!
[ec2-user@ip-10-0-2-117 ~]$ sudo amazon-linux-extras install nginx1 -y
[ec2-user@ip-10-0-2-117 ~]$ sudo dnf install -y nginx
Last metadata expiration check: 0:01:04 ago on Sun Sep 14 17:26:58 2025.
Dependencies resolved.
=====================================================================================================================================
 Package                           Architecture           Version                                Repository                  Size
=====================================================================================================================================
Installing:
 nginx                             x86_64                 1:1.28.0-1.amzn2023.0.2                amazonlinux                 33 k
Installing dependencies:
 generic-logos-httpd               noarch                 18.0.0-12.amzn2023.0.3                 amazonlinux                 19 k
 gperftools-libs                   x86_64                 2.9.1-1.amzn2023.0.3                   amazonlinux                308 k
 libunwind                         x86_64                 1.4.0-5.amzn2023.0.2                   amazonlinux                 66 k
 nginx-core                        x86_64                 1:1.28.0-1.amzn2023.0.2                amazonlinux                686 k
 nginx-filesystem                  noarch                 1:1.28.0-1.amzn2023.0.2                amazonlinux                9.6 k
 nginx-mimetypes                   noarch                 2.1.49-3.amzn2023.0.3                  amazonlinux                 21 k

Transaction Summary
=====================================================================================================================================
  Verifying        : nginx-core-1:1.28.0-1.amzn2023.0.2.x86_64                                                              5/7
  Verifying        : nginx-filesystem-1:1.28.0-1.amzn2023.0.2.noarch                                                        6/7
  Verifying        : nginx-mimetypes-2.1.49-3.amzn2023.0.3.noarch                                                           7/7

Installed:
  generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch                  gperftools-libs-2.9.1-1.amzn2023.0.3.x86_64
  libunwind-1.4.0-5.amzn2023.0.2.x86_64                              nginx-1:1.28.0-1.amzn2023.0.2.x86_64
  nginx-core-1:1.28.0-1.amzn2023.0.2.x86_64                          nginx-filesystem-1:1.28.0-1.amzn2023.0.2.noarch
  nginx-mimetypes-2.1.49-3.amzn2023.0.3.noarch

Complete!
[ec2-user@ip-10-0-2-117 ~]$ sudo systemctl enable nginx
sudo systemctl start nginx
Created symlink /etc/systemd/system/multi-user.target.wants/nginx.service → /usr/lib/systemd/system/nginx.service.
[ec2-user@ip-10-0-2-117 ~]$ systemctl status nginx
● nginx.service - The nginx HTTP and reverse proxy server
     Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: disabled)
     Active: active (running) since Sun 2025-09-14 17:28:13 UTC; 6s ago
    Process: 18898 ExecStartPre=/usr/bin/rm -f /run/nginx.pid (code=exited, status=0/SUCCESS)
    Process: 18919 ExecStartPre=/usr/sbin/nginx -t (code=exited, status=0/SUCCESS)
    Process: 18978 ExecStart=/usr/sbin/nginx (code=exited, status=0/SUCCESS)
   Main PID: 19033 (nginx)
      Tasks: 2 (limit: 1111)
     Memory: 2.5M
        CPU: 60ms
     CGroup: /system.slice/nginx.service
             ├─19033 "nginx: master process /usr/sbin/nginx"
             └─19043 "nginx: worker process"
Sep 14 17:28:13 ip-10-0-2-117.ap-south-1.compute.internal systemd[1]: Started nginx.service - The nginx HTTP and reverse proxy server.
[ec2-user@ip-10-0-2-117 ~]$ echo "Hello from Private Subnet Web App!" | sudo tee /usr/share/nginx/html/index.html
Hello from Private Subnet Web App!
[ec2-user@ip-10-0-2-117 ~]$ curl http://10.0.2.117
Hello from Private Subnet Web App!
[ec2-user@ip-10-0-2-117 ~]$
```

Step – 68] Now you see the message on new browser tab by pasting the web link .



localhost:8080

Hello from Private Subnet Web App!