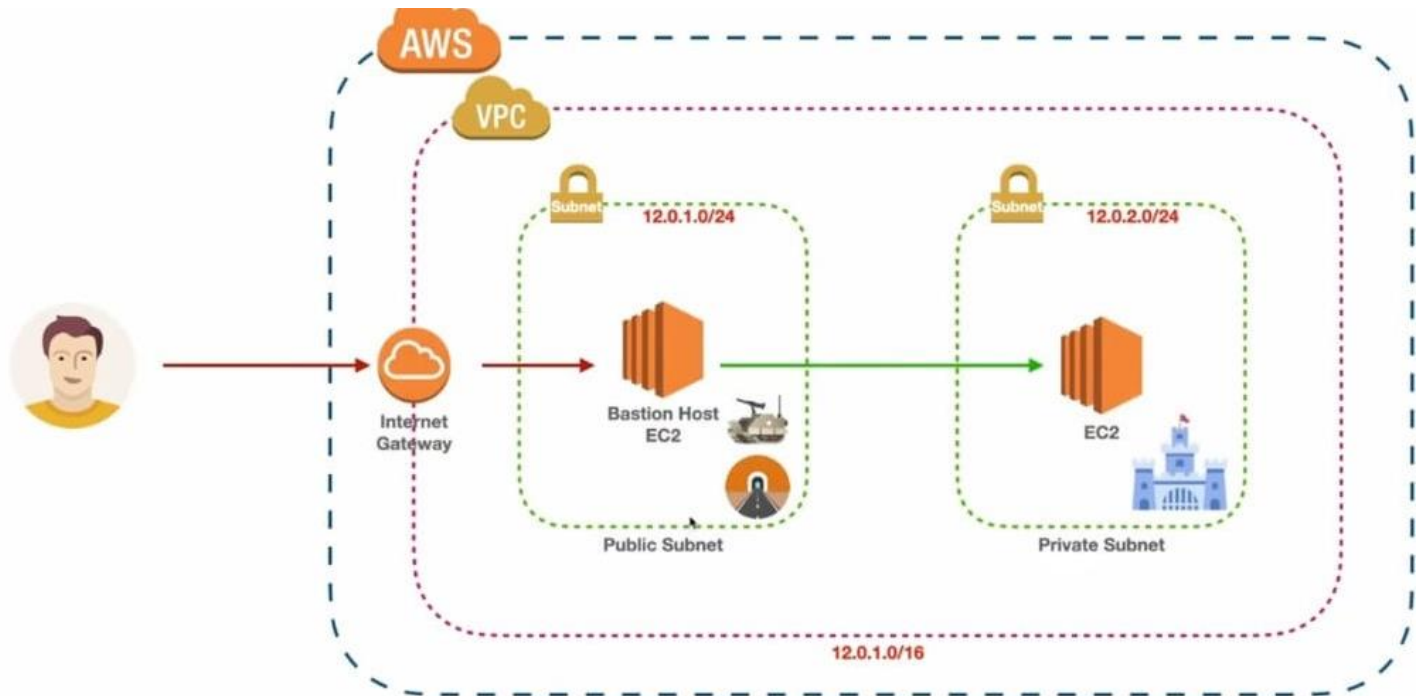


AWS Bastion Host:

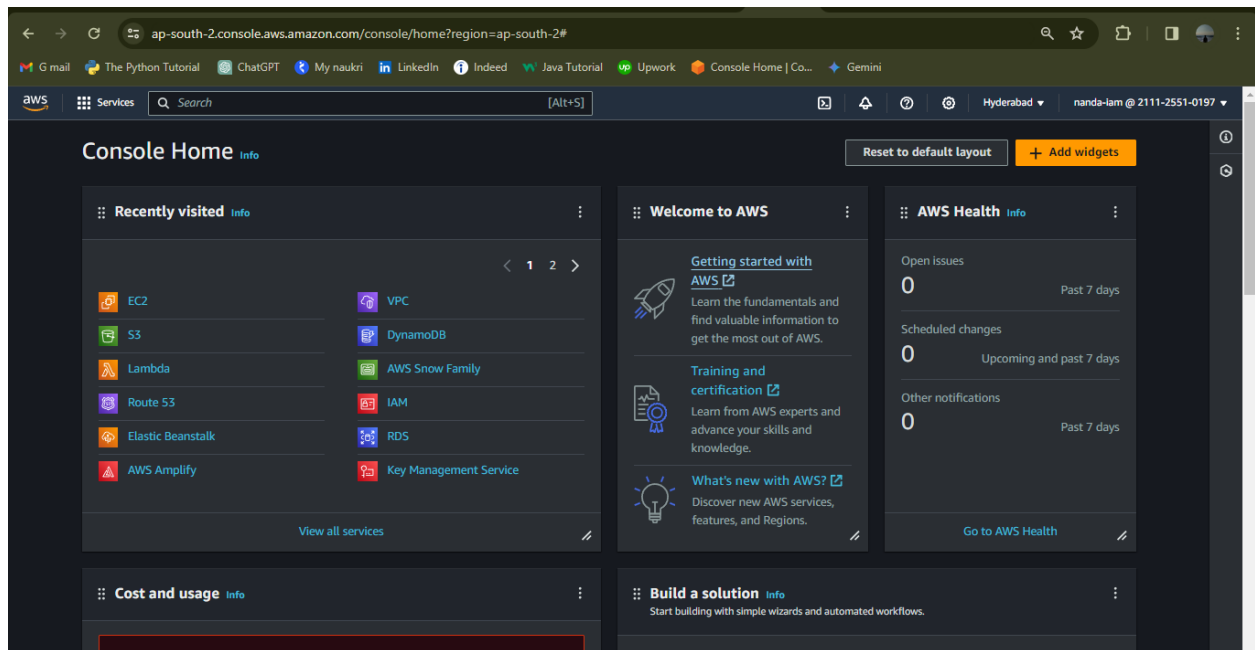
Created By : Nandakumar

This solution sets up the following



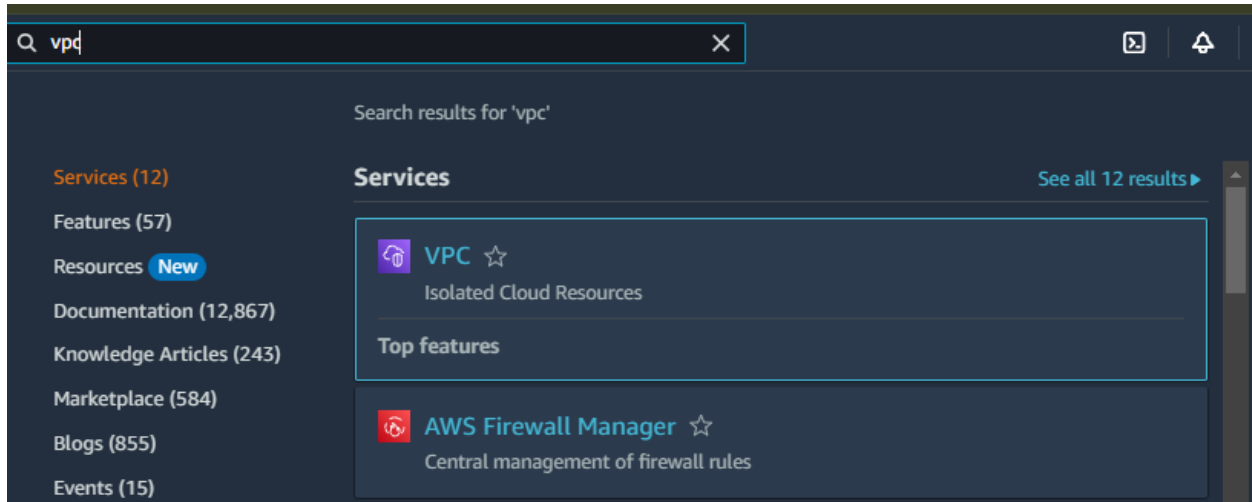
Step 1: Log in to AWS Console

- Navigate to the AWS Management Console at <https://console.aws.amazon.com/>.
- Log in using your credentials.



Step 2: Go to the VPC Dashboard

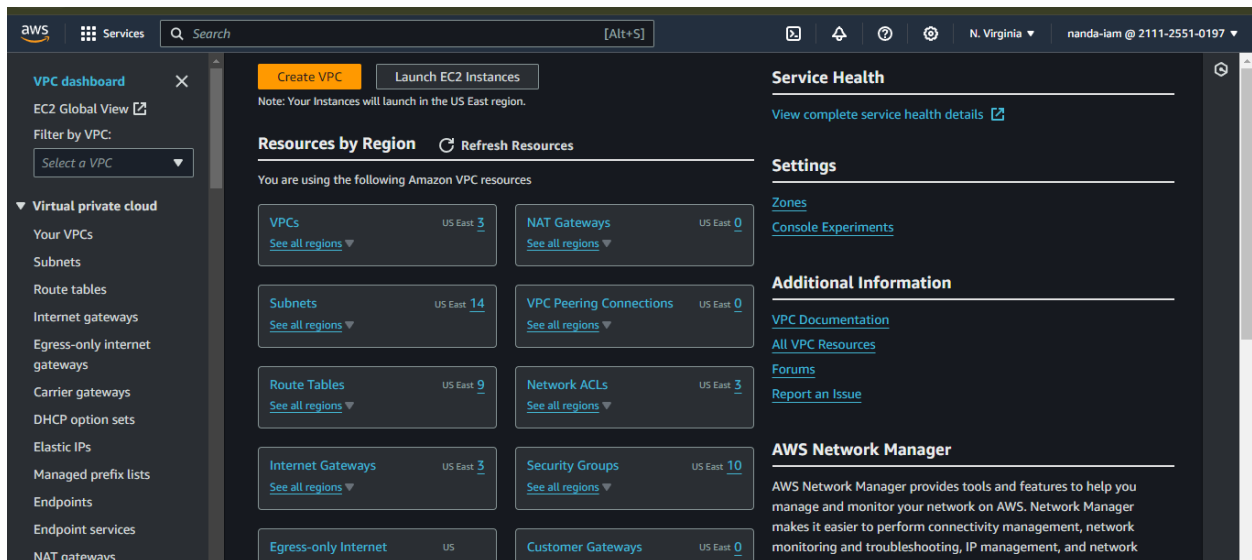
- In the AWS Management Console, search for "VPC" in the services search bar, or navigate to the Networking & Content Delivery section and click on "VPC".



- You'll land on the VPC Dashboard.

Step 3: Create a VPC

- Click on the "Create VPC" button.



- In the Create VPC wizard, you'll be prompted to fill out details:
- Name tag: Give your VPC a descriptive name of Bastion_VPC
- IPv4 CIDR block: Define the IP address range for your VPC, e.g., 12.0.0.0/16.

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.

Bastion_VPC

IPv4 CIDR block Info

☒ IPv4 CIDR manual input ☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

12.0.0.0/16

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

- IPv6 CIDR block: Optionally, you can assign an IPv6 CIDR block.
- Tenancy: Choose default unless you have specific requirements.
- Click on "Create".

IPv6 CIDR block Info

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

Tenancy Info

Default

Tags

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

Key	Value - optional	
Q Name X	Q Bastion_VPC X	Remove tag

Add tag

You can add 49 more tags

Cancel Create VPC

- You will see the status that your VPC is launching below.

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHC
Bastion_VPC	vpc-02bf120be199dd9de	Available	12.0.0/16	-	dopt

Step 4: Create Internet Gateway (IGW) (if needed)

- If you want your VPC to have internet access:
- Go to "Internet Gateways" in the VPC Dashboard.
- Click on "Create internet gateway"

Name	Internet gateway ID	State	VPC ID	Owner
-	igw-086874a8ff66e06d1	Attached	vpc-0dc153d5476a3d4aa	211125510197

- Provide a name for the internet gateway and click on "Bastion-internet-gateway".

Create internet gateway Info

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

Internet gateway settings

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

Bastion-internet-gateway

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.

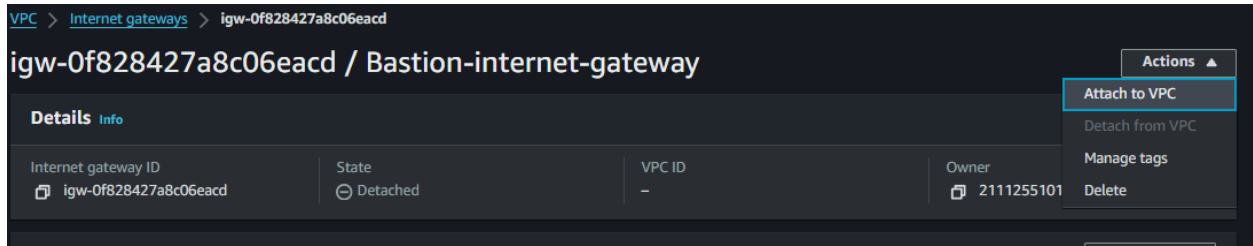
Key	Value - optional	
Name	Bastion-internet-gateway	Remove

Add new tag

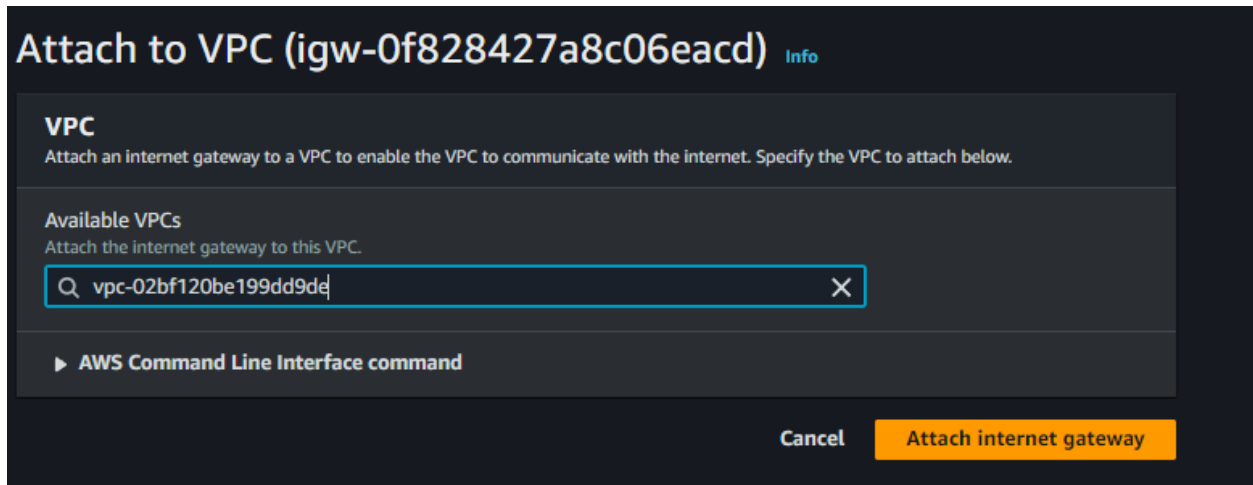
You can add 49 more tags.

Cancel **Create internet gateway**

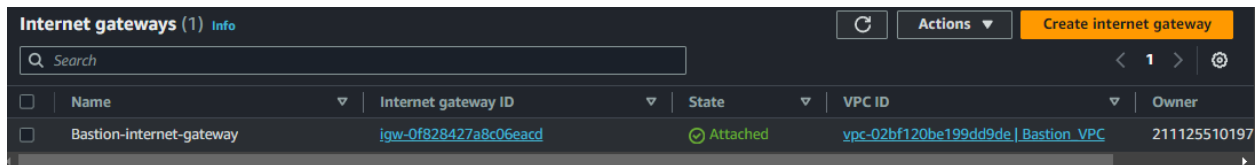
- Select the newly created internet gateway and click on "Attach to VPC".



- Choose your VPC and click on "Attach".

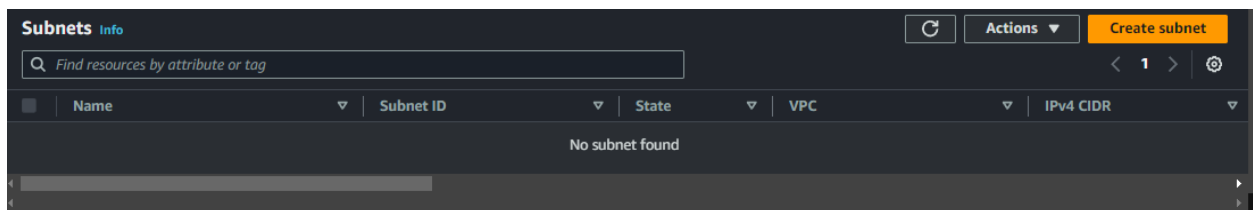


- You will see the status that your internet gateway is launching below.



Step 5: Create Subnets

- Sure, let's create both public and private subnets within the VPC.
- After creating the VPC, click on "Subnets" in the VPC Dashboard.
- Click on "Create subnet"



- VPC: Choose the VPC you created earlier.

VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.

vpc-02bf120be199dd9de (Bastion_VPC) ▼

Associated VPC CIDRs

- Name Tag: Bastion-public-4a
- Availability Zone: Select an availability zone. For example, ap-southeast-4a.
- IPv4 CIDR block: Define the IP address range for the subnet within the VPC CIDR block. For instance, if your VPC CIDR block is 12.0.0.0/16, you can define your public subnet as 12.0.1.0/24.

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

Bastion-public-4a

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 (Melbourne) / ap-southeast-4a ▼

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.

12.0.0.0/16 ▼

IPv4 subnet CIDR block

12.0.1.0/24 256 IPs

< > ^ v

- Name Tag: Bastion-private-4b
- Availability Zone: Select an availability zone. For example, ap-southeast-4b.
- IPv4 CIDR block: Define the IP address range for the subnet within the VPC CIDR block. For instance, if your VPC CIDR block is 12.0.0.0/16, you can define your public subnet as 12.0.2.0/24.

Subnet 2 of 2

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

Bastion-Private-4b

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 (Melbourne) / ap-southeast-4b

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.

12.0.0.0/16

IPv4 subnet CIDR block

12.0.2.0/24 256 IPs

< > ^ v

- Click on "Create subnet".

Add new subnet

Cancel **Create subnet**

- After completing the steps, AWS will create the public and private subnet, and you'll see it listed in the Subnets section of the VPC Dashboard

You have successfully created 2 subnets: subnet-0070b01b98a74bae1, subnet-0ac131e0f5157114f

Subnets (2) [Info](#)

Find resources by attribute or tag

Subnet ID: subnet-0070b01b98a74bae1 Subnet ID: subnet-0ac131e0f5157114f Clear filters

	Name	Subnet ID	State	VPC	IPv4 CIDR
<input type="checkbox"/>	Bastion-public-4a	subnet-0070b01b98a74bae1	Available	vpc-02bf120be199dd9de Bast...	12.0.1.0/24
<input type="checkbox"/>	Bastion-Private-4b	subnet-0ac131e0f5157114f	Available	vpc-02bf120be199dd9de Bast...	12.0.2.0/24

Step 6: Create Route Table of Public and Private

- Click on "Create route table".

Route tables (2) [Info](#)

Find resources by attribute or tag

Create route table

	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC	Own.
	rtb-0285786a11c2b1e3e	-	-	Yes	vpc-0dc153d5476a3d4aa	2111
	rtb-0e25f1957d09b9211	-	-	Yes	vpc-02bf120be199dd9de Bast...	2111

- Provide a name for the of Bastion-public-route
- Then select your VPC.
- Click on "Create".

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

Bation-Route

VPC
The VPC to use for this route table.

vpc-02bf120be199dd9de (Bastion_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 - optional	
Q Name X	Q Bation-Route X	Remove

Add new tag

You can add 49 more tags.

Cancel Create route table

- Provide a name for the of Bastion-Private-route
- Then select your VPC.
- Click on "Create".

Route table settings

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

bastion-private-route

VPC
The VPC to use for this route table.

vpc-02bf120be199dd9de (Bastion_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.

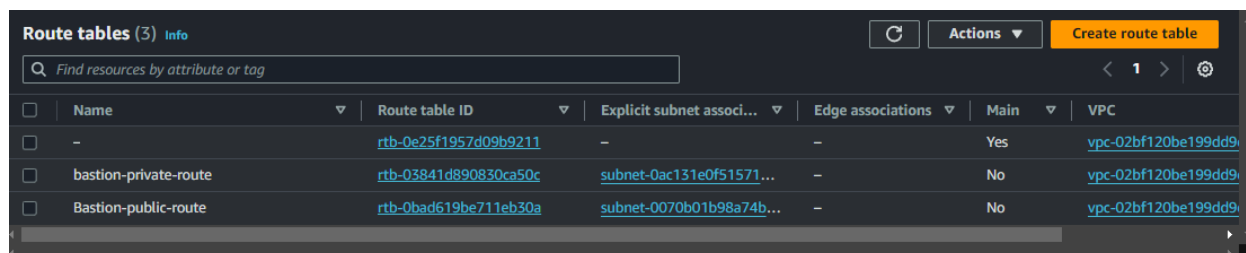
Key	Value - optional	
Q Name X	Q bastion-private-route X	Remove

Add new tag

You can add 49 more tags.

Cancel Create route table

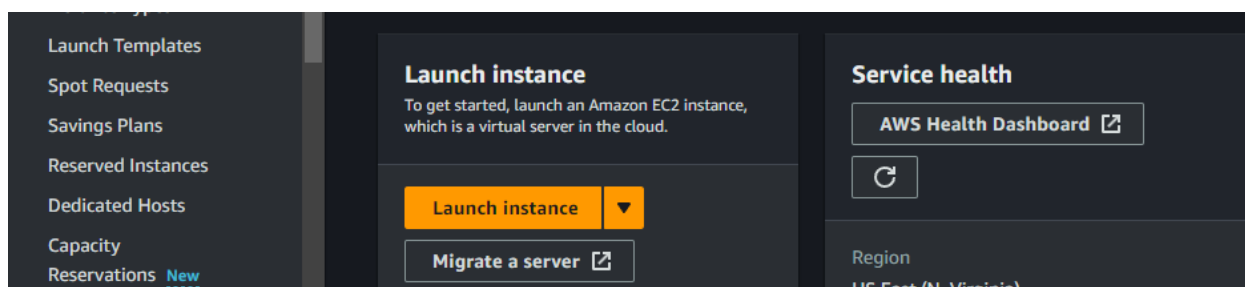
You will see the status that your Creating Route table is below.



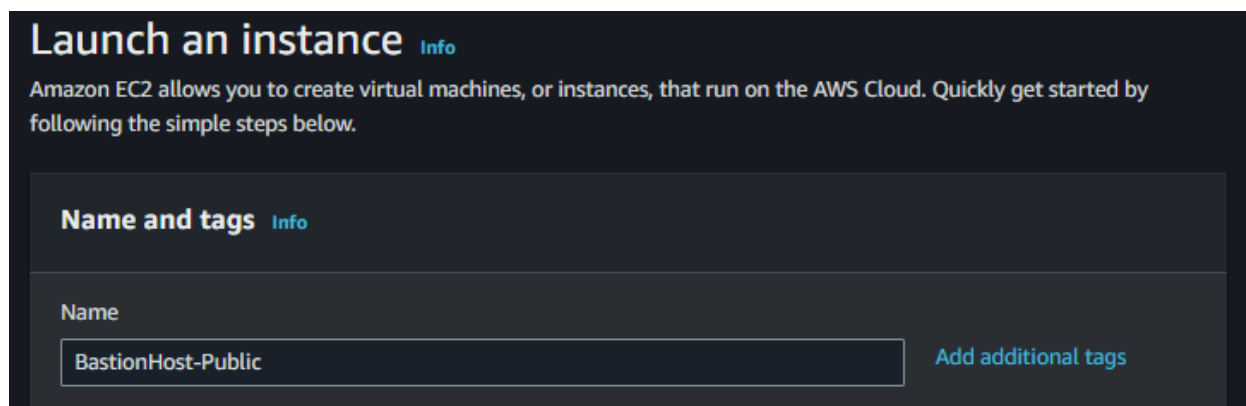
<input type="checkbox"/>	Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
<input type="checkbox"/>	-	rtb-0e25f1957d09b9211	-	-	Yes	vpc-02bf120be199dd9...
<input type="checkbox"/>	bastion-private-route	rtb-03841d890830ca50c	subnet-0ac131e0f51571...	-	No	vpc-02bf120be199dd9...
<input type="checkbox"/>	Bastion-public-route	rtb-0bad619be711eb30a	subnet-0070b01b98a74b...	-	No	vpc-02bf120be199dd9...

Step 7: Create instance Public and Private

- Go to the EC2 Dashboard by searching for "EC2" in the services search bar or navigating to Compute > EC2.
- In the EC2 Dashboard, click on the "Launch Instance" button.



- Provide a name for the of BastionHost-Public



The screenshot shows the 'Launch an instance' wizard in the AWS Management Console. The first step is 'Name and tags'. It includes a description: '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.' Below this is a form for the instance name, which is currently 'BastionHost-Public'. There is also a link to 'Add additional tags'.

- Choose an Amazon Machine Image (AMI) based on your requirements. You can select from the AWS Marketplace, AWS Community AMIs, or your own custom AMIs.
- Click on "Select" once you've chosen an Ubuntu AMI

▼ **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
aws


Ubuntu
ubuntu

Windows
Microsoft

Red Hat
Red Hat

SUSE Linux
SUSE

Debian
debian



[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type
ami-08b65f49f52d12d21 (64-bit (x86)) / ami-0302cb3ea1d64e309 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible ▼

Description

- Select an instance type based on your workload requirements. Instances vary in terms of CPU, memory, storage, and networking capabilities.

▼ **Instance type** [Info](#) | [Get advice](#)

Instance type

t3.micro
Family: t3 2 vCPU 1 GiB Memory Current generation: true
On-Demand Linux base pricing: 0.0132 USD per Hour
On-Demand RHEL base pricing: 0.0732 USD per Hour
On-Demand SUSE base pricing: 0.0132 USD per Hour
On-Demand Windows base pricing: 0.0224 USD per Hour

Free tier eligible ▼

☒ All generations

[Compare instance types](#)

- Create a new key pair to securely connect to your instance via SSH.
- Provide a Key pair name is Bastionhost
- Key Pair type is RSA
- Key file format is .pem
- Click on "Create Key pair"

Create key pair

Key pair name

Key pairs allow you to connect to your instance securely.

Bastionhost

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](#)

Cancel

Create key pair

▼ 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

Bastionhost

↻ [Create new key pair](#)

- Configure Network Settings
- Select the VPC you want to use from the Bastion_VPC.
- Choose the subnet within the selected the Bastion-public-4a
- Auto-assign Public IP: Choose whether you want to assign a public IP address to the instance. Options are "Use subnet setting (Enable or Disable)" or "Enable" or "Disable" specifically for this instance.

VPC - required | [Info](#)

vpc-02bf120be199dd9de (Bastion_VPC)
12.0.0.0/16

Subnet | [Info](#)

subnet-0070b01b98a74bae1 **Bastion-public-4a**
VPC: vpc-02bf120be199dd9de Owner: 211125510197
Availability Zone: ap-southeast-4a IP addresses available: 251 CIDR: 12.0.1.0/24

Auto-assign public IP | [Info](#)

Enable

Additional charges apply when outside of **free tier allowance**

- Create a new security group for your instance Name is BastionHost-public.

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

Security group name - required

BastionHost-Public

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 | [Info](#)

Public host

- This defines the inbound and outbound traffic rules.
- Review the configuration of your instance to ensure everything is correct.
- Click on "Launch".

Description - required | [Info](#)

Public host

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0) [Remove](#)

Type	Protocol	Port range	Source type	Source	Description - optional
ssh	TCP	22	Anywhere	0.0.0.0/0	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.

[Add security group rule](#)

► **Advanced network configuration**

▼ **Configure storage** | [Info](#) [Advanced](#)

Summary

Number of instances | [Info](#)

1

Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
ami-08b65f49f52d12d21

Virtual server type (instance type)
t3.micro

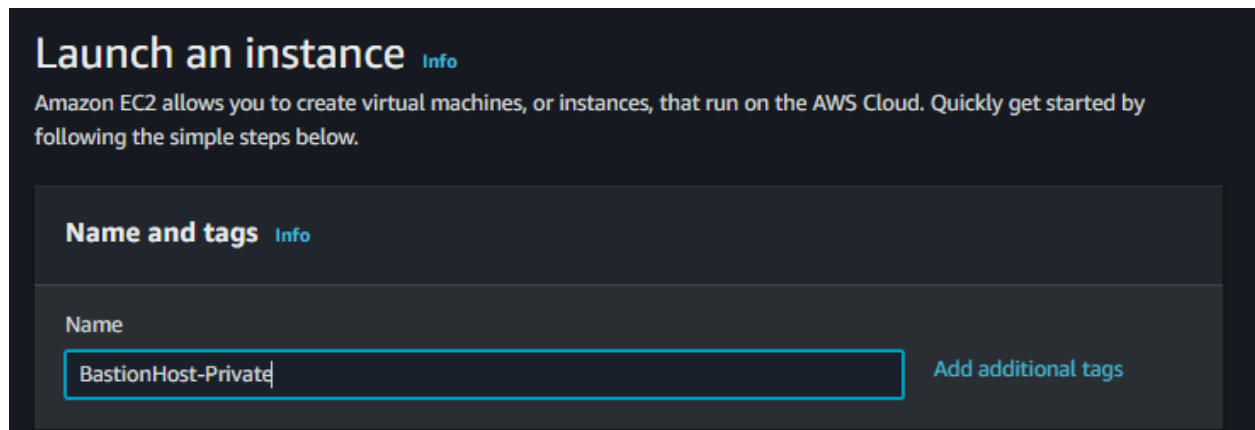
Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 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](#)

- Provide a name for the of BastionHost-Private



Launch an instance [Info](#)

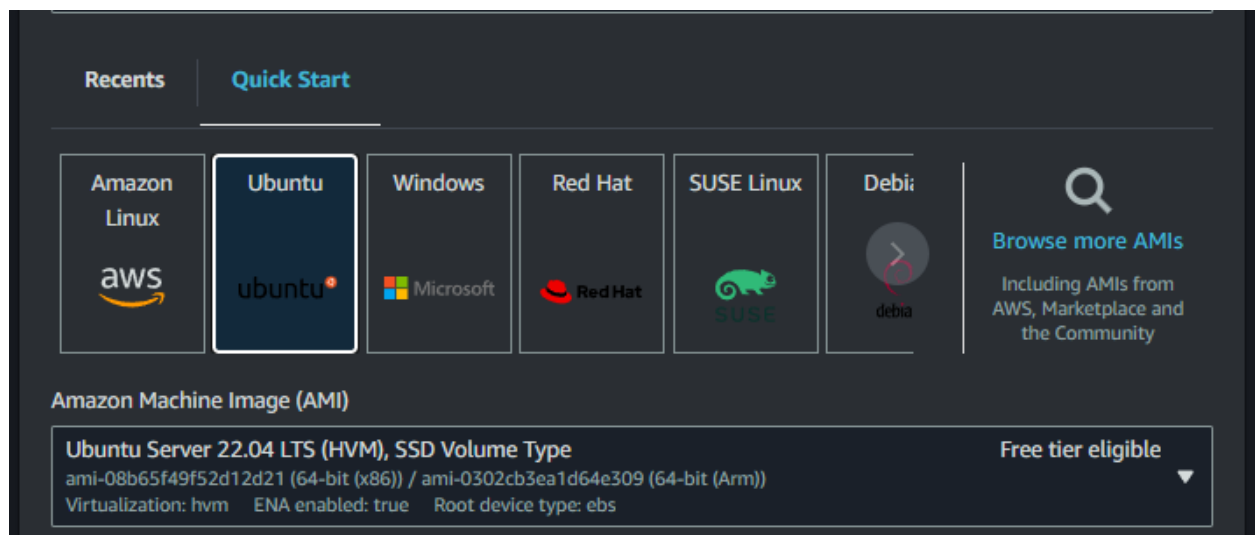
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name

BastionHost-Private [Add additional tags](#)

- Choose an Amazon Machine Image (AMI) based on your requirements. You can select from the AWS Marketplace, AWS Community AMIs, or your own custom AMIs.
- Click on "Select" once you've chosen an Ubuntu AMI



Recents **Quick Start**

Amazon Linux **Ubuntu** Windows Red Hat SUSE Linux Debian

aws ubuntu Microsoft Red Hat SUSE debia

[Browse more AMIs](#)
Including AMIs from AWS, Marketplace and the Community

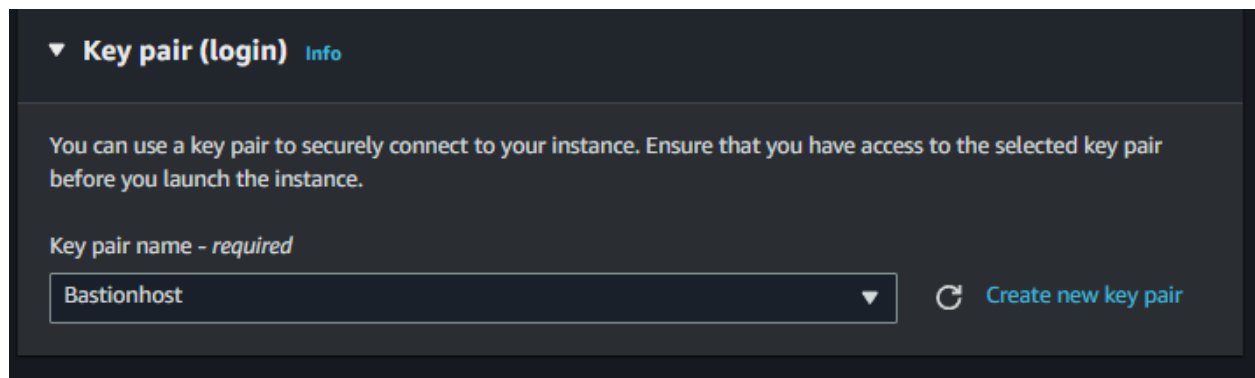
Amazon Machine Image (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type **Free tier eligible**

ami-08b65f49f52d12d21 (64-bit (x86)) / ami-0302cb3ea1d64e309 (64-bit (Arm))

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

- Choose an existing key pair of "Bastionhost" to securely connect to your instance via SSH



▼ 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*

Bastionhost [Create new key pair](#)

- Configure Network Settings

- Select the VPC you want to use from the Bastion_VPC.
- Choose the subnet within the selected the Bastion-Private-4b.
- Auto-assign Public IP: Choose whether you want to assign a public IP address to the instance. Options are "Use subnet setting (Enable or Disable)" or "Enable" or "Disable" specifically for this instance.

The screenshot shows the 'Network' tab of the AWS EC2 instance configuration page. It includes three sections: 'VPC - required' with a dropdown set to 'vpc-02bf120be199dd9de (Bastion_VPC)' and a refresh button; 'Subnet' with a dropdown set to 'subnet-0ac131e0f5157114f' (Bastion-Private-4b) and a 'Create new subnet' button; and 'Auto-assign public IP' with a dropdown set to 'Disable'.

- Create a new security group for your instance Name is BastionHost-Private
- This defines the inbound and outbound traffic rules.
- Review the configuration of your instance to ensure everything is correct.
- Click on "Launch".

The screenshot shows the 'Security' tab of the AWS EC2 instance configuration page. It includes a 'Create security group' button, a 'Security group name' field set to 'BastionHost-private', a 'Description' field, and a table for 'Inbound Security Group Rules' with one rule for SSH on port 22. A 'Summary' panel on the right shows instance details like 'Number of instances: 1', 'Software Image (AMI): Canonical, Ubuntu, 22.04 LTS', 'Virtual server type (instance type): t3.micro', and 'Storage (volumes): 1 volume(s) - 8 GiB'. At the bottom, there is a 'Free tier' notification and 'Cancel' and 'Launch instance' buttons.

- click on Instances You will see like below. Instance state is Running.
- You can click on the Instance ID to see more details about your instance.

Instances (2) Info							
Find Instance by attribute or tag (case-sensitive)				All states	< 1 > ⚙		
<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input type="checkbox"/>	BastionHost-Public	i-0621a3231b8ca6369	Running	t3.micro	2/2 checks passed	View alarms +	ap-southeast-4a
<input type="checkbox"/>	BastionHost-Private	i-019a564f2c5d1f0f3	Running	t3.micro	2/2 checks passed	View alarms +	ap-southeast-4b

Step 8: Connect the Bastion Host

- Open a terminal window on your local machine.
- Creating a key pair (bastionhost.pem):
- The first line `vi bastionhost.pem` uses the vi text editor to create a new file named "bastionhost.pem". You can use any text editor you are comfortable with.
- Setting permissions on the key pair:
- The line `chmod 400 "bastionhost.pem"` changes the permissions of the "bastionhost.pem" file. The `chmod` command is used to modify file permissions in Unix-based systems. Here, "400" sets the permissions so that only the owner of the file has read, write, and execute permissions. This restricts access to the private key file for enhanced security.

```
ubuntu@ip-12-0-1-39:~$ vi Bastionhost.pem
ubuntu@ip-12-0-1-39:~$ chmod 400 "Bastionhost.pem"
```

- Connecting to the bastion host:
- The line `ssh -i "bastionhost.pem" ubuntu@12.0.2.227` initiates an SSH connection to the server with the IP address 12.0.2.227. Here's a breakdown of the options used:
- `-i "bastionhost.pem"` : This option specifies the path to the private key file "bastionhost.pem" that you created in step 1.
- `ubuntu@` : This specifies the username to use for login. In this case, it's "ubuntu".
- `12.0.2.227` : This is the IP address of the server you want to connect to.

```
ubuntu@ip-12-0-1-39:~$ ssh -i "Bastionhost.pem" ubuntu@12.0.2.227
The authenticity of host '12.0.2.227 (12.0.2.227)' can't be established.
ED25519 key fingerprint is SHA256:Cve3AhqZM2j4EPL51e0fmV617gujEBgku8vfiXACbRU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

- you should be connected to the public EC2 instance from your local machine via the bastion host and the Private EC2 instance.

```
ubuntu@ip-12-0-2-227:~$ exit
logout
Connection to 12.0.2.227 closed.
ubuntu@ip-12-0-1-39:~$
```