

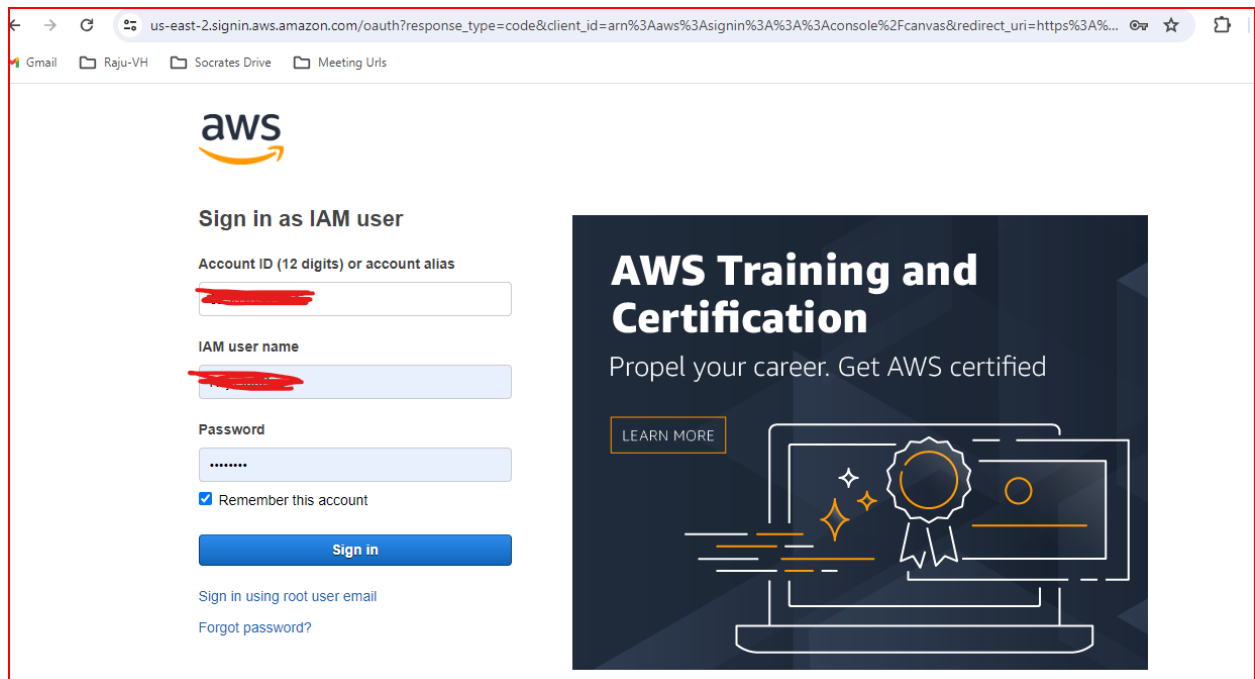
# Setup EC2 And VPC – AWS

## In this Document Covered these

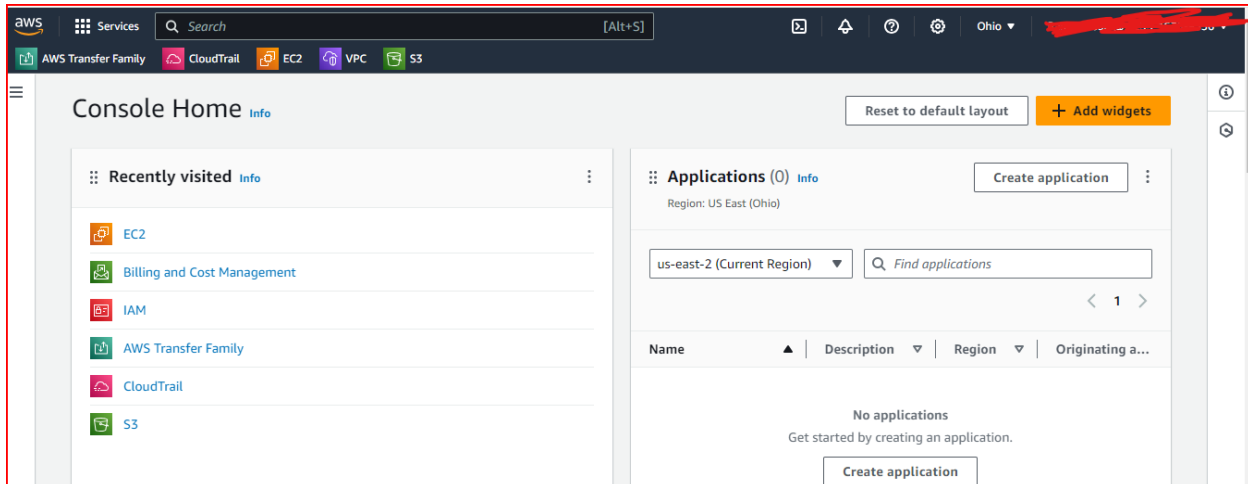
- 1 How to connect private ip address of aws ec2 instance
2. How many methods we have to connect instance
3. Complete setup of VPC- Subnets, Route tables, IGW, NAT.

## Launch EC2 VM :

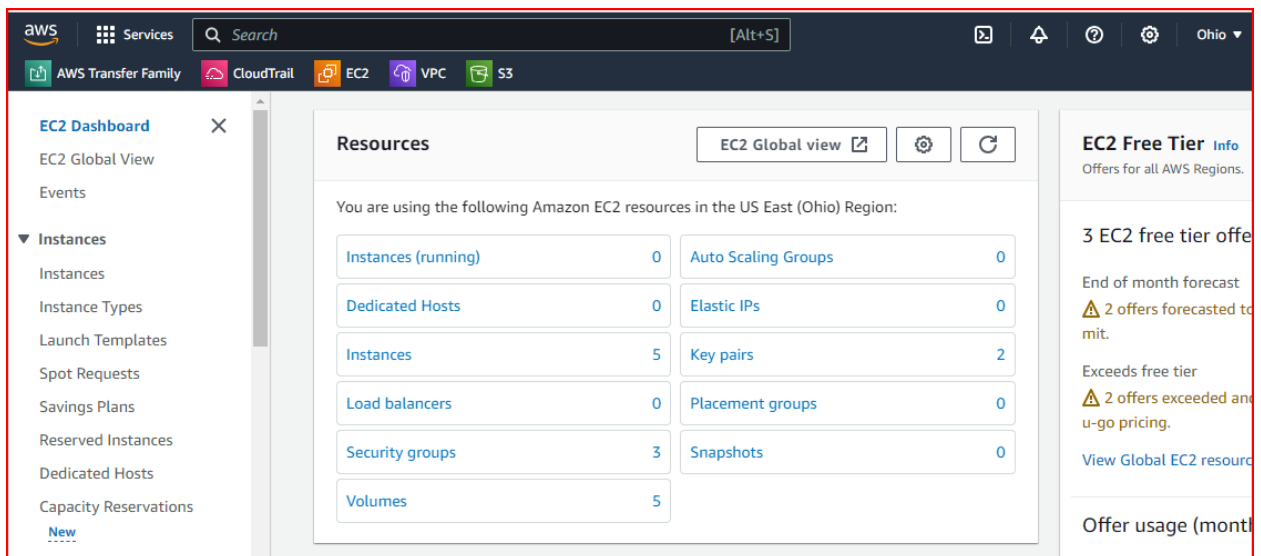
Step1: Login to AWS Console with user credentials



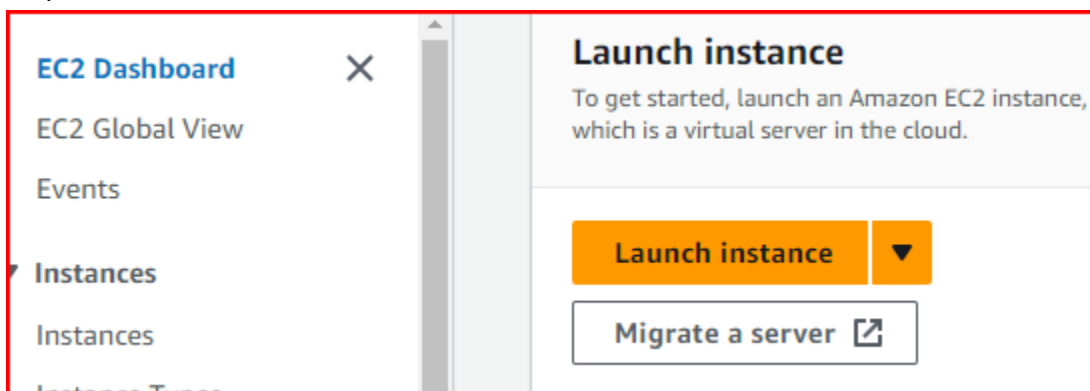
Step 2: After login into the account then go to home page of aws console



Step 3 : search ec2 home page



Step 4: Launch instance



Give the instance name as per requirement

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

### ▼ Summary

Number of instances [Info](#)

Software Image (AMI)  
Amazon Linux 2023 AMI 2023.3.2...[read more](#)  
ami-0ee4f2271a4df2d7d

Virtual server type (instance type)  
t2.micro

Firewall (security group)  
New security group

Storage (volumes)

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

Choose the AMI image like below as per requirement under drop down menu

Amazon Linux  
aws

macOS  
Mac

Ubuntu  
ubuntu

Windows  
Microsoft

Red Hat  
Red Hat

SUSE Linux  
SUS

[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-05fb0b8c1424f266b (64-bit (x86)) / ami-0748d13ffbc370c2b (64-bit (Arm))  
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible ▼

### Description

Canonical, Ubuntu, 22.04 LTS, amd64 jammy image build on 2023-12-07

Architecture

AMI ID  
ami-05fb0b8c1424f266b

Verified provider

Choose instance type as per requirement

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

Instance type

t2.micro

Free tier eligible

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

On-Demand Linux base pricing: 0.0116 USD per Hour

On-Demand SUSE base pricing: 0.0116 USD per Hour

On-Demand Windows base pricing: 0.0162 USD per Hour

On-Demand RHEL base pricing: 0.0716 USD per Hour

☐ All generations

[Compare instance types](#)

[Additional costs apply for AMIs with pre-installed software](#)

Due to security connectivity of the instance key pair is generated . here if key pair is generated choose that in drop down menu otherwise create new key pair .pem or .ppk files these file stored in local machine under download folder.

▼ 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*

Select

▼

↻

[Create new key pair](#)

Choose the vpc and security group

If the firewall is an existing security group choose default otherwise create a new security group as per requirement to allow or block the ports and ips.

▼ Network settings [Info](#)

Edit

Network [Info](#)

vpc-074e7529444273a39

Subnet [Info](#)

No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)

Enable

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

We'll create a new security group called 'launch-wizard-3' with the following rules:

☒ Allow SSH traffic from

Helps you connect to your instance

Anywhere  
0.0.0.0/0

☐ Allow HTTPS traffic from the internet

vpc-074e7529444273a39

Subnet [Info](#)

No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)

Enable

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

Common security groups [Info](#)

Select security groups

default sg-0f9a098d3a9cdae40 ✕  
VPC: vpc-074e7529444273a39

↻ Compare security group rules

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

Size of the instance i.e volume

▼ **Configure storage** [Info](#)

Advanced

1 x  GiB  ▼ Root volume (Not encrypted)

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

×

Add new volume

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance

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 [Edit](#)

If added in the extra details choose advanced options under instance creation setup.

▼ **Advanced details** [Info](#)

Domain join directory [Info](#)

Select ▼

↻

Create new directory [↗](#)

IAM instance profile [Info](#)

Select ▼

↻

Create new IAM profile [↗](#)

Hostname type [Info](#)

IP name ▼

DNS Hostname [Info](#)

☒ Enable IP name IPv4 (A record) DNS requests

☒ Enable resource-based IPv4 (A record) DNS requests

☐ Enable resource-based IPv6 (AAAA record) DNS requests

Instance auto-recovery [Info](#)

Select ▼

Shutdown behavior [Info](#)

Stop ▼

Stop - Hibernate behavior [Info](#)

Select ▼

Termination protection [Info](#)

Select ▼

Stop protection [Info](#)

Select ▼


Detailed CloudWatch monitoring [Info](#)

Select ▼

Elastic GPU [Info](#)

Elastic inference [Info](#)

☐ Add Elastic Inference accelerators

 Amazon Elastic Inference is no longer available to new customers. For new and existing customers, we recommend using an alternative, such as AWS Inferentia, which offers better performance at a lower cost. [Learn more](#)

Credit specification [Info](#)

Select ▼

Placement group [Info](#)

Select ▼

 [Create new placement group](#) 

EBS-optimized instance [Info](#)

Disable ▼

Purchasing option [Info](#)

☒ None

Capacity reservation [Info](#)

Select ▼

Tenancy [Info](#)

Select ▼

RAM disk ID [Info](#)

Select ▼

Kernel ID [Info](#)

Select ▼

Nitro Enclave [Info](#)

Select ▼

Nitro Enclaves are not compatible with instance types that have less than 2 vCPUs.

License configurations [Info](#)

Select ▼



Specify CPU options

The selected instance type does not support CPU options.

AMD SEV-SNP [Info](#)

Select ▼

AMD SEV-SNP is not supported with the selected instance type and the selected AMI.

Metadata accessible [Info](#)


Enabled ▼

Metadata transport

Select ▼

Metadata version [Info](#)

V2 only (token required) ▼

 For V2 requests, you must include a session token in all instance metadata requests. Applications or agents that use V1 for instance metadata access will break.

Metadata response hop limit [Info](#)



Here Under User data we need to insert the bash or any script to install the packages directly while on launching

Metadata response hop limit

Info

2

Allow tags in metadata

Info

Select

User data - optional

Info

Upload a file with your user data or enter it in the field.

Choose file

Summary

▼ Summary

Number of instances

Info

1

Software Image (AMI)

Canonical, Ubuntu, 22.04 LTS, ...[read more](#)

ami-05fb0b8c1424f266b

Virtual server type (instance type)

t2.micro

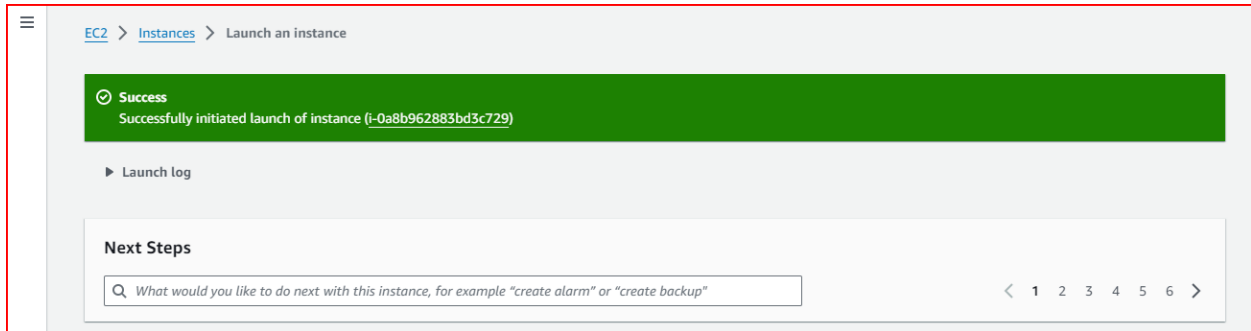
Firewall (security group)

default

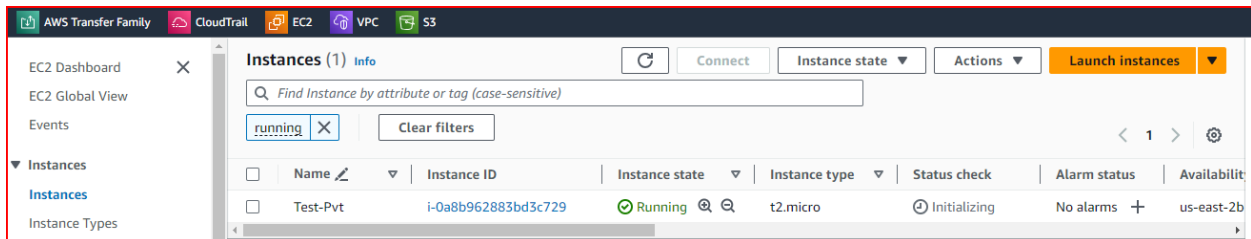
Storage (volumes)

Cancel

Launch instance

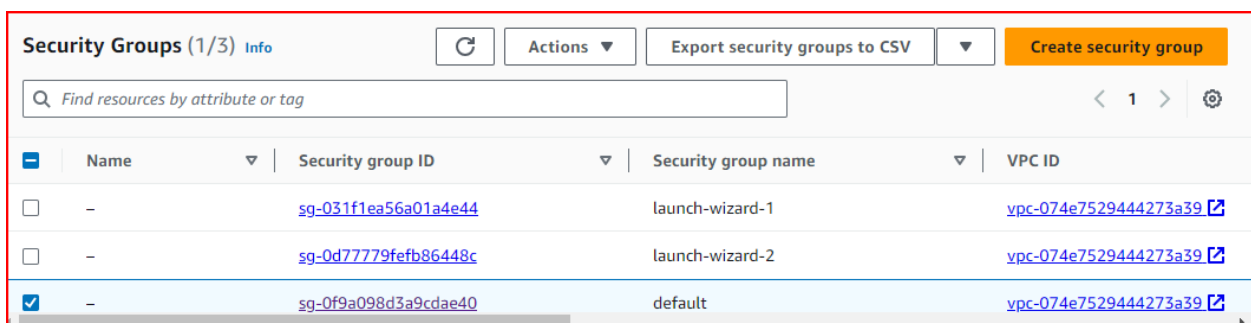
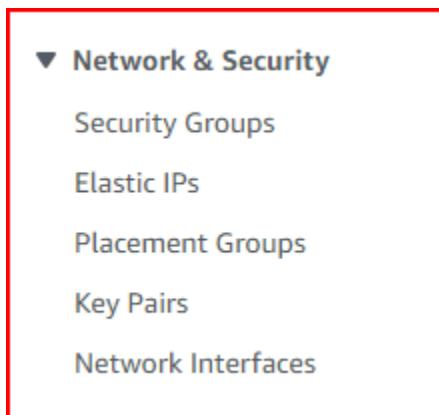


## Step 5: Instance is running



## Step 6 : adding the security group inbound and outbound rules

At ec2 dashboard goto network and security choose security groups



Here under inbound rules add custom tcp port 22 why because port 22 is default ssh connection

Inbound rules

**Inbound rules** [Info](#)

Security group rule ID	Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>	
sgr-04a79c12b1d5db2b1	All traffic ▼	All	All	Cus... ▼	0.0.0.0/0	Delete
sgr-0f29b5e6ac0041c43	SSH ▼	TCP	22	Cus... ▼	172.31.29.194/32	Delete

[Add rule](#)

Outbound rules all traffic

**Outbound rules** [Info](#)

Outbound rules (1)

[Manage tags](#) [Edit outbound rules](#)

<input type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol
<input type="checkbox"/>	-	sgr-07e9c22c802e1974b	IPv4	All traffic	All

Step 7 : Any changes in ec2 instance goto actions

**Instances (1)** [Info](#)

[Connect](#) [Instance state](#)

[running](#) [Clear filters](#)

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	State
<input type="checkbox"/>	Test-Pvt	i-0a8b962883bd3c729	Running	t2.micro	✓

**Actions**

- Connect
- View details
- Manage instance state
- Instance settings
- Networking
- Security
- Image and templates
- Monitor and troubleshoot

[Launch instances](#)

Step 8:

**MobaXterm**


Terminal Sessions View X server Tools Games Settings Macros Help

Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help


Session settings

SSH Telnet Rsh Xdmcp RDP VNC FTP SFTP Serial File Shell Browser Mosh Aws S3 WSL

Basic SSH settings

Remote host \*  ☐ Specify username   Port 22

Advanced SSH settings Terminal settings Network settings Bookmark settings


Secure Shell (SSH) session 

OK Cancel

Session settings

SSH Telnet Rsh Xdmcp RDP VNC FTP SFTP Serial File Shell Browser Mosh Aws S3 WSL

Basic SSH settings



Remote host \* 172.17.0.1 ☒ Specify username ubuntu   Port 22

Advanced SSH settings Terminal settings Network settings Bookmark settings

☒ X11-Forwarding ☒ Compression Remote environment: Interactive shell

Execute command:  ☐ Do not exit after command ends

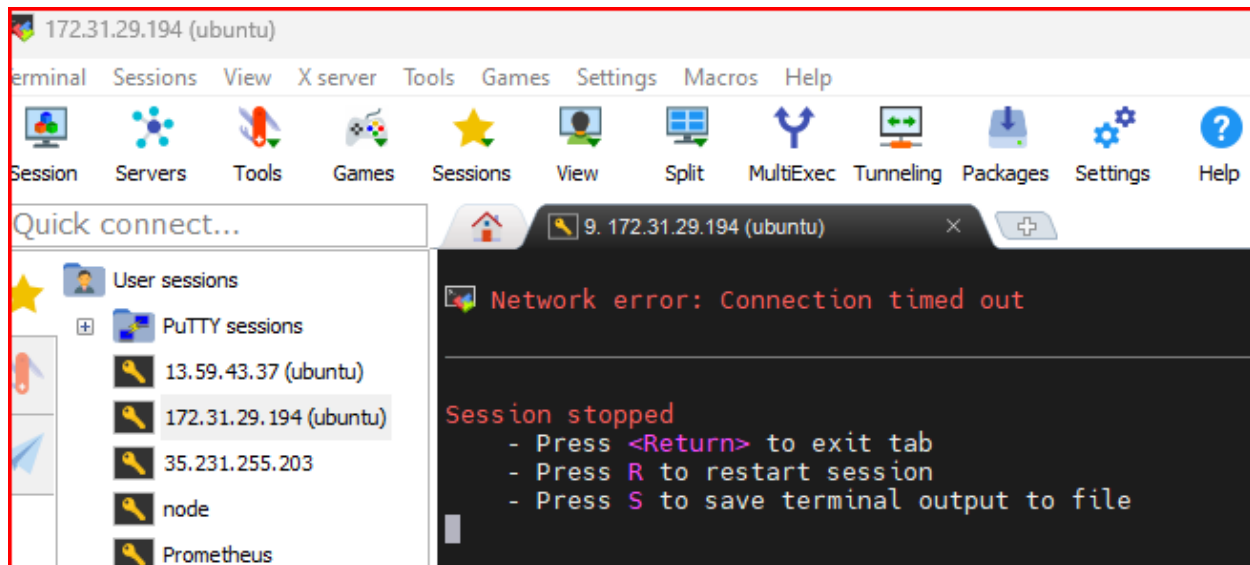
SSH-browser type: SFTP protocol  ☐ Follow SSH path (experimental)

☒ Use private key C:\Users\user\key:  

Execute macro at session start: <none>

OK Cancel

Connect aws instance using private ip address getting error



To connect Private IP addresses in aws we having two methods:

- 1- Bastion Host or Jump Server
- 2- EIC (EC2 Instance connect).

## 1- Bastion Host or Jump Server:

There is no public Ip for pvt-inst so only private ip address

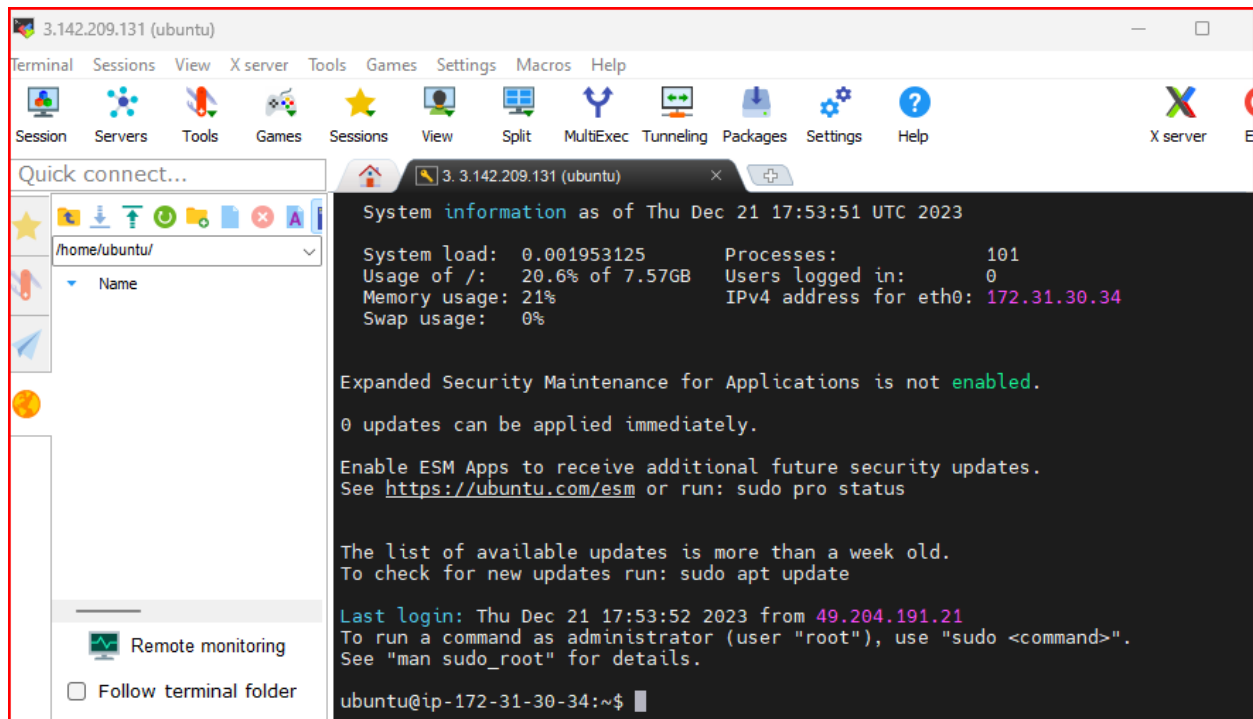
Instances (3) Info								
<input type="text" value="Find Instance by attribute or tag (case-sensitive)"/>								
<input type="button" value="running"/> <input type="button" value="Clear filters"/>								
<input type="checkbox"/>	Name	Instance ID	Instance state	Instanc...	Status check	Availabi...	Public IPv4 ...	Private IP ad
<input type="checkbox"/>	Pvt-Inst	i-016f05bd86a443f53	Running	t2.micro	2/2 checks p...	us-east-2a	-	172.31.14.22
<input type="checkbox"/>	Test-Pvt	i-0a8b962883bd3c7...	Running	t2.micro	2/2 checks p...	us-east-2b	18.191.133.26	172.31.29.19
<input type="checkbox"/>	bastion	i-0cae0ad7142e5237c	Running	t2.micro	2/2 checks p...	us-east-2b	3.142.209.131	172.31.30.34

Here we need to connect the Pvt-Inst using a bastion server.

First copy the bastion server ip and ssh into any client.

Name	Instance ID	Instance state	Instanc...	Status check	Availabi...	Public IPv4 ...	Private IP ad...
Pvt-Inst	i-016f05bd86a443f53	Running	t2.micro	2/2 checks p...	us-east-2a	-	172.31.14.220
Test-Pvt	i-0a8b962883bd3c7...	Running	t2.micro	2/2 checks p...	us-east-2b	18.191.133.26	172.31.29.194
bastion	i-0cae0ad7142e5237c	Running	t2.micro	2/2 checks p...	us-east-2b	3.142.209.131	172.31.30.34

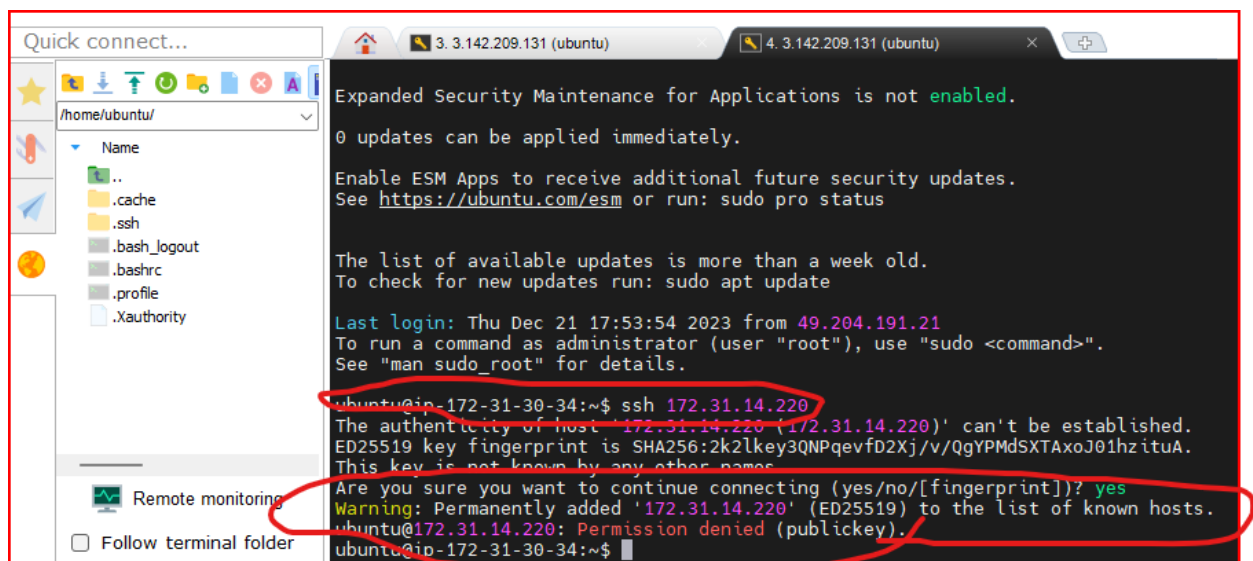
This is **bastion server** connectivity check private ip



The screenshot shows a terminal window titled '3. 3.142.209.131 (ubuntu)'. The left sidebar contains a 'Quick connect...' section with a file manager view showing the directory '/home/ubuntu/'. The main terminal area displays system information as of Thursday, December 21, 2023, at 17:53:51 UTC. It lists system load, memory usage, and processes. A warning message states that Expanded Security Maintenance for Applications is not enabled and that 0 updates can be applied immediately. It also shows the last login time and the user's IP address (49.204.191.21). The terminal prompt is 'ubuntu@ip-172-31-30-34:~\$'.

Now connect Pvt-inst server in bastion server

But I am getting following error because in bastion server there is no .pem or .ppk file of pvt-inst server so copy that in bastion machine server.

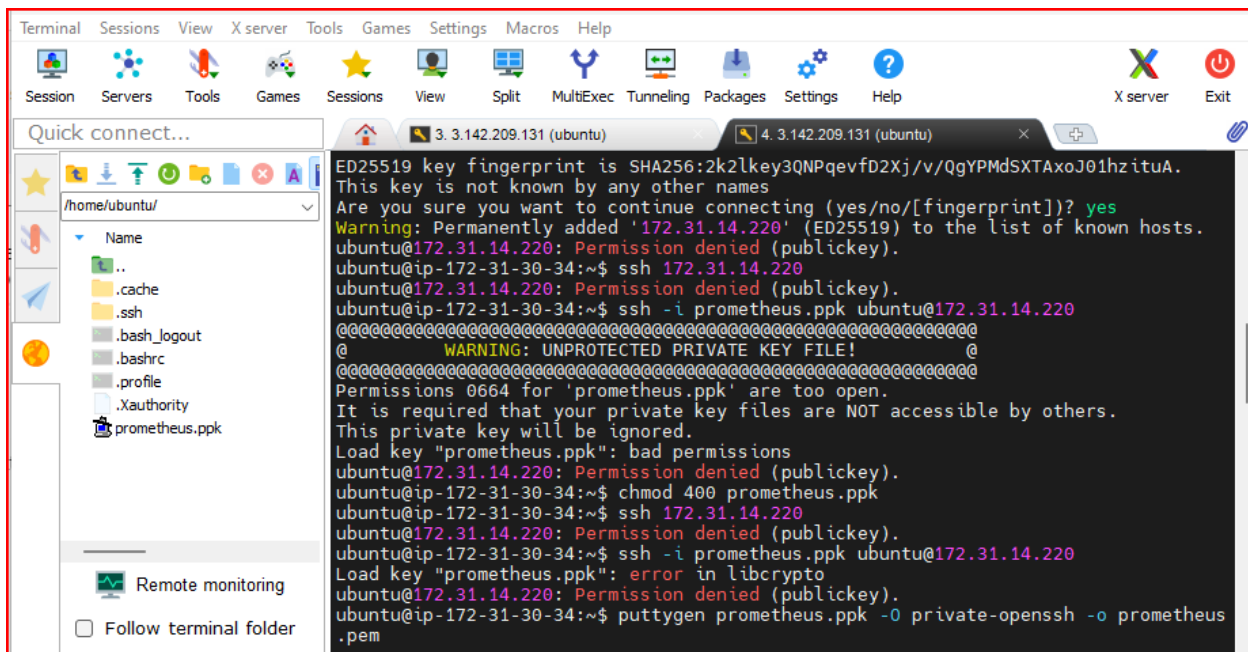
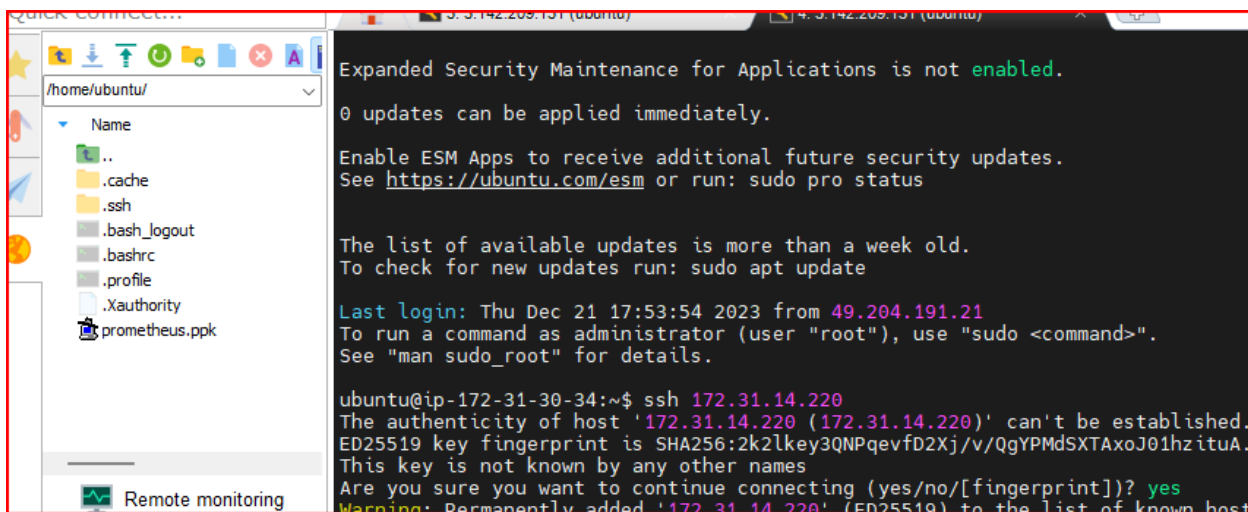
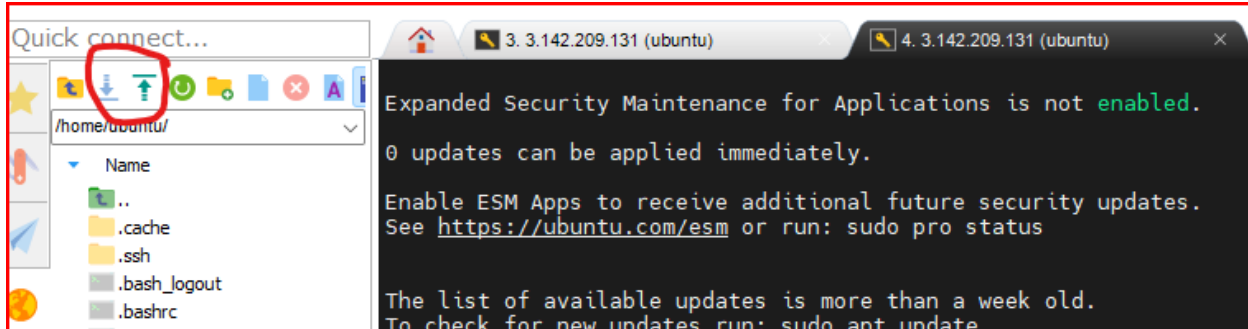


The screenshot shows a terminal window with two tabs. The active tab is titled '3. 3.142.209.131 (ubuntu)'. The left sidebar shows a file manager view of '/home/ubuntu/'. The main terminal area displays the same system information as the previous screenshot. A red circle highlights the command 'ssh 172.31.14.220' entered at the prompt. Below the command, the terminal shows an error message: 'The authenticity of host '172.31.14.220' (172.31.14.220) can't be established. ED25519 key fingerprint is SHA256:2k2lkey3QNPqevfD2Xj/v/QgYPMdSXTaxoJ01hzitUA. This key is not known by any other names.' Another red circle highlights the response 'yes' to the prompt 'Are you sure you want to continue connecting (yes/no/[fingerprint])?'. The terminal then shows a warning: 'Warning: Permanently added '172.31.14.220' (ED25519) to the list of known hosts.' Finally, the terminal shows the error 'Permission denied (publickey)' and the prompt 'ubuntu@ip-172-31-30-34:~\$'.

First copy the pem file two ways

1. Direct upload the file into client like mobaXterm
2. Using SCP Command to copy the local pem file into bastion machine.

```
~/Downloads$ sudo scp -i public_instance.pem instance_key_pair.pem ubuntu@3.142.113.73:/home/ubuntu/private instance_key.pem
instance_key_pair.pem 100% 1678 9.1KB/s 00:00
~/Downloads$
```



I am getting error here so

### **Putty:**

The error "Load key 'prometheus.ppk': error in libcrypto" indicates a problem with loading or processing the private key file due to a cryptographic library issue. To address this, you can try the following steps:

#### **Use OpenSSH Private Key:**

- **Convert the PuTTY private key** (prometheus.ppk) to OpenSSH format using the puttygen tool. Run the following command in your local terminal:

```
puttygen prometheus.ppk -O private-openssh -o prometheus.pem
```

- Use the converted key (prometheus.pem) in your SSH command:

```
ssh -i prometheus.pem ubuntu@172.31.14.220
```

#### **Check Key Permissions:**

- Ensure that the permissions for the private key file (prometheus.pem) are set correctly:

```
chmod 600 prometheus.pem
```

#### **Verify Key Format:**

- Double-check that the private key file is in the correct format (OpenSSH format) after the conversion.

#### **Update SSH Client:**

- Ensure that you are using an up-to-date version of the OpenSSH client on your local machine. You can update it using your package manager:  
For Ubuntu/Debian:

```
sudo apt-get update
```

```
sudo apt-get install openssh-client
```

- For CentOS/RHEL:

```
sudo yum update
```

```
sudo yum install openssh-clients
```

#### **Check SSH Agent:**

- If you have an SSH agent running, try restarting it or clearing loaded keys:

```
eval "$(ssh-agent -s)"
```

```
ssh-add -D # Clears all identities from the agent
```

```
ssh-add prometheus.pem
```



#### Check Crypto Libraries:

- Ensure that the cryptographic libraries on your system are up to date. Perform a system update and upgrade:

For Ubuntu/Debian:

```
sudo apt-get update
```

```
sudo apt-get upgrade
```

- For CentOS/RHEL:

```
sudo yum update
```

#### Check Key Passphrase:

- If the private key has a passphrase, make sure you are entering it correctly when prompted.

#### Generate a New Key Pair (Optional):

- If the issue persists, consider generating a new key pair and updating the public key on the remote server.

### **Mobaxterm:**

The error "Load key 'prometheus.ppk': error in libcrypto" suggests an issue with the private key file or its compatibility with the SSH client. Since you are using MobaXterm, you might want to ensure that the key file is correctly loaded and that MobaXterm is handling the key conversion properly.

Here are steps you can take to resolve the issue:

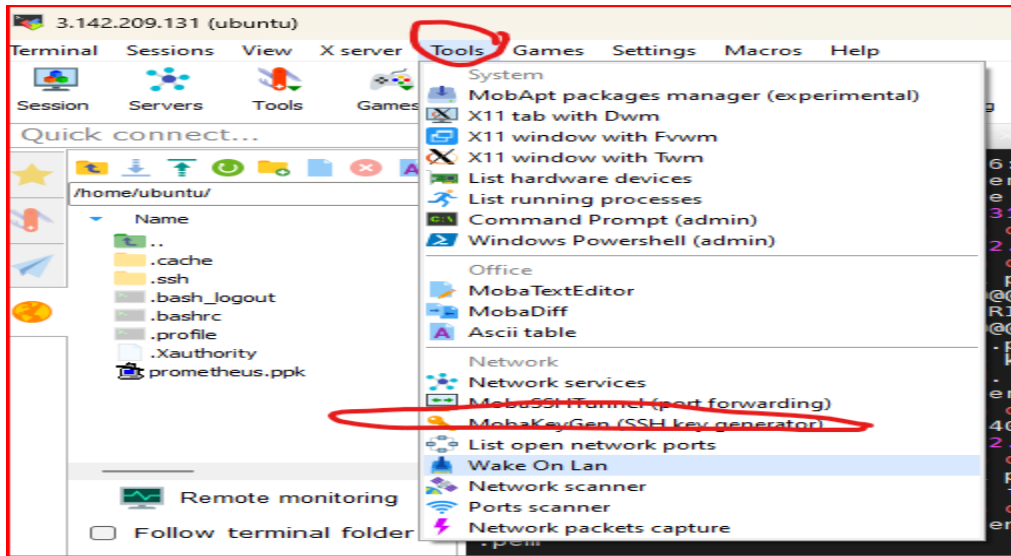
#### Check Key Format:

- Ensure that the private key file (prometheus.ppk) is in the correct format. MobaXterm uses its own private key format, so it's important to make sure the key is in the right format for OpenSSH.

#### Convert Key to OpenSSH Format:

- Use MobaXterm itself to convert the key to OpenSSH format:
  - Open MobaXterm.
  - Go to the "Tools" menu.
  - Select "MobaKeyGen."
  - Load your private key (prometheus.ppk).
  - In the "Conversions" menu, choose "Export OpenSSH key" and save the key with a .pem extension.

```
chmod 600 prometheus.pem
```

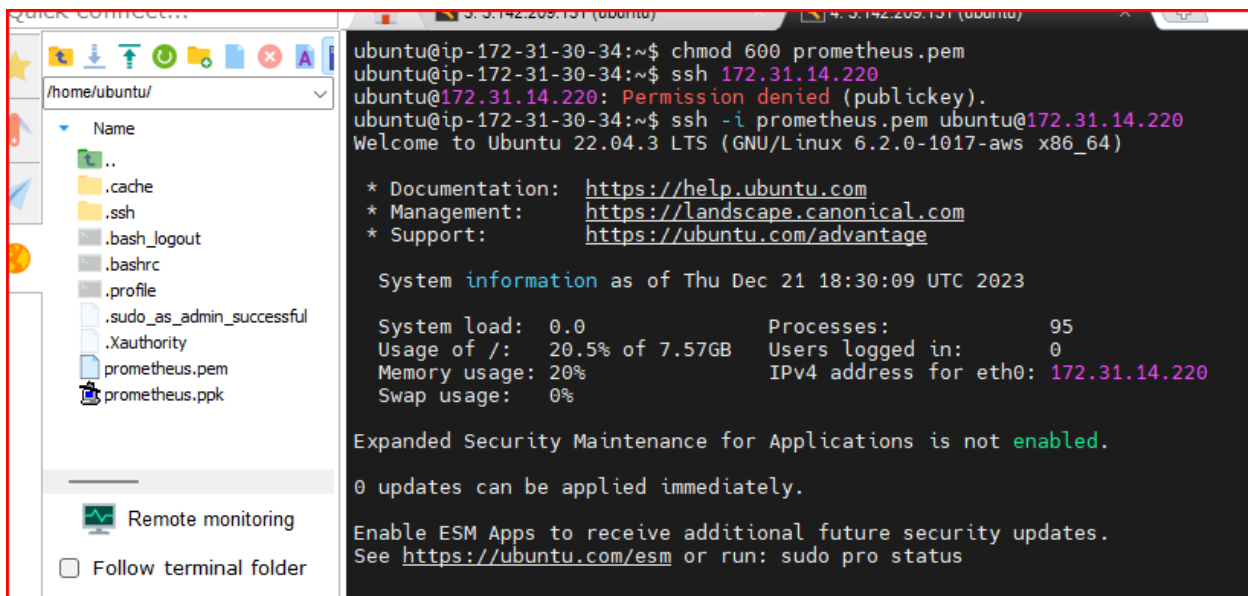


Use the Converted Key:

- After converting the key, use the new OpenSSH key (prometheus.pem) in your SSH command:

**ssh -i prometheus.pem ubuntu@172.31.14.220**

**Successfully connected pvt ip address in bastion host server if doubt check the ip addresses. 172.31.30.34 172.31.14.220**



Ensure Key is Loaded in MobaXterm:

- Open MobaXterm.
- In the terminal, check if the private key is loaded using the following command:

**ssh-add -l**

- If the key is not listed, add it using:

```
ssh-add /path/to/prometheus.pem
```

Verify Permissions:

- Ensure that the permissions for the private key file are set correctly:

```
chmod 600 prometheus.pem
```

Check MobaXterm Settings:

- In MobaXterm, go to "Settings" > "Configuration."
- Under the "SSH" tab, make sure that the "Use internal SSH agent" option is selected.

Restart MobaXterm:

- Sometimes, restarting MobaXterm can resolve certain issues. Close and reopen the application.

Check MobaXterm Logs:

- MobaXterm may log information about key loading and authentication attempts. Check the logs for any relevant error messages.

Update MobaXterm:

- Ensure that you are using the latest version of MobaXterm. If not, consider updating to the latest release.

## 2- EIC (EC2 Instance connect):

**On June 13th, AWS launched a new service called EC2 Instance Connect Endpoint (EIC Endpoint). Which Allows to have secure SSH and RDP connectivity to private EC2 instances without using public IP addresses.**

**This Article discusses working of EIC Endpoint and demonstrates how to create and use it to SSH/RDP to an instance from the Internet.**

**EC2 Instance Endpoint Connect any resources:**

★ Use "EC2 instance Connect" to connect to RDS and other VPC resources — no VPN required, no EC2 Bastion instance needed 🔥

① Upgrading the AWS CLI to version 2.12+

② Create (if you haven't already) an EC2 Instance Connect Endpoint

```
• aws ec2 create-instance-connect-endpoint --region us-east-1 --subnet-id  
subnet-0123456789abcdef
```

⚠ Change "region" and "subnet-id" to your values.

After creation you use "InstanceConnectEndpointId".

### ③ Connecting to EC2 Instance Connect Endpoint

The EC2 User Guide so far only lists connection to an EC2 instance by "instance-id". However, the AWS CLI v2 lists others for "ec2-instance-connect open-tunnel", in particular "private-ip-address" and "remote-port".

So we use this command:

```
• aws ec2-instance-connect open-tunnel --private-ip-address <your-private-IP-here>
--instance-connect-endpoint-id eice-0123456789abcdef12 --remote-port 5432 --local-port
5432
```

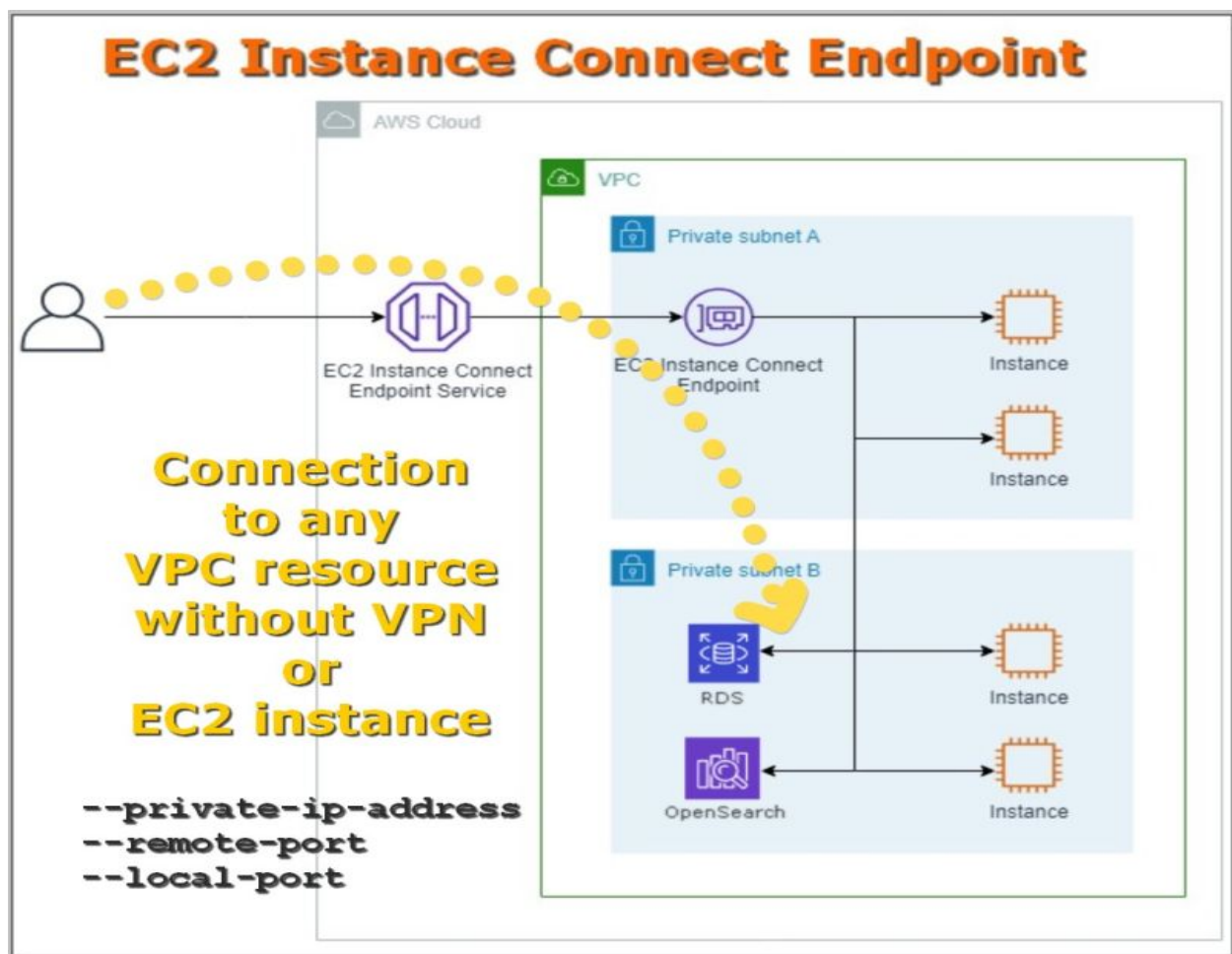
⚠ Change "private-ip-address", "instance-connect-endpoint-id" (obtained during creation), "remote-port" and "local-port" to your values.

The result will be a tunnel:

- Listening for connections on port 5432.
- [1] Accepted new tcp connection, opening websocket tunnel.

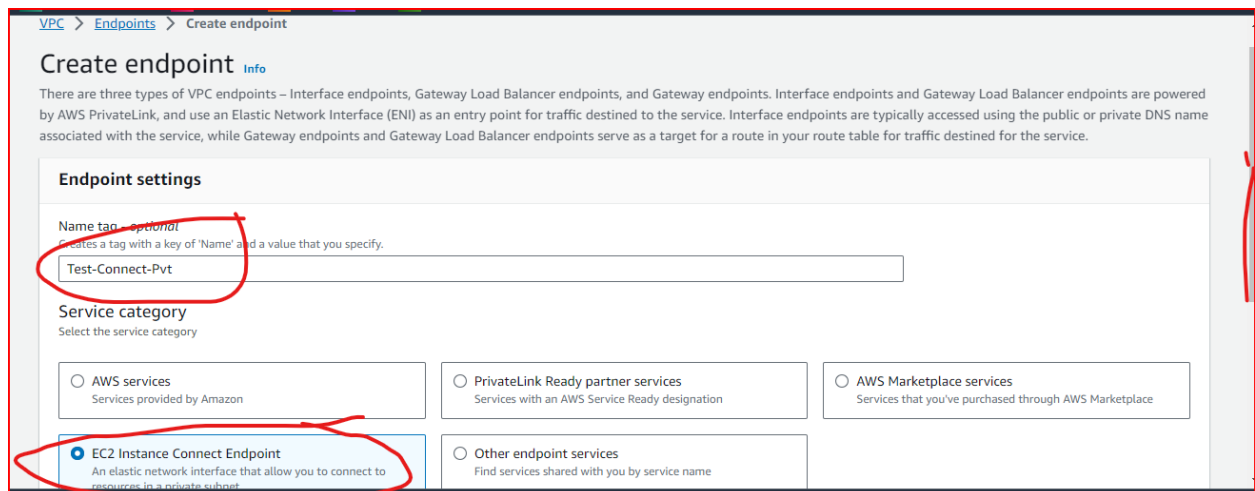
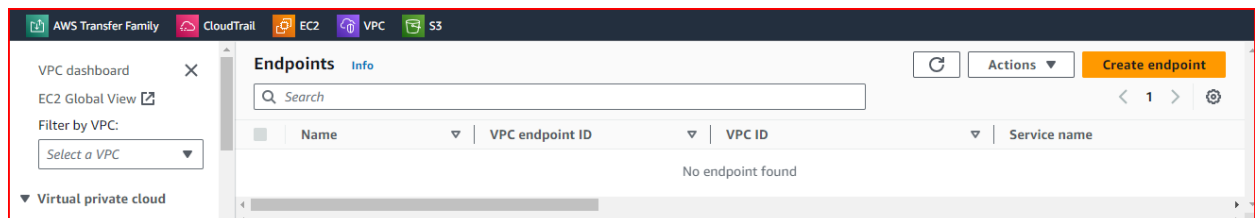
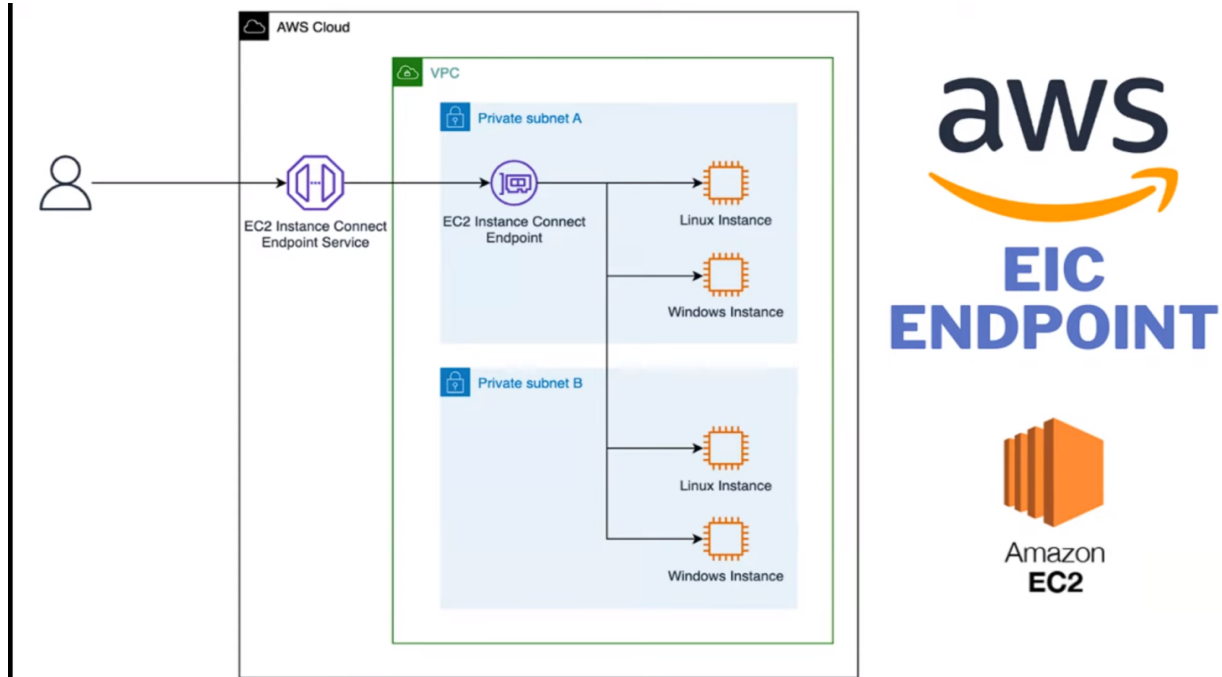
### ④ Connect to the local port (localhost:5432 from the example above) and that's it! 👍

It definitely works for IPs from other VPCs connected via VPC Peering. I haven't tried it for another — let me know if it doesn't work.



## Creation of the Endpoint Under VPC Dashboard:

### EIC EndPoint:



**VPC**

Select the VPC in which to create the endpoint

VPC

The VPC in which to create your endpoint.

vpc-074e7529444273a39

▼ Additional settings

Preserve Client IP

☐ EC2 Instance Connect Endpoint supports client IP preservation. You can configure the EC2 Instance Connect Endpoint to use your client's IP address as the source (preserveClientIp parameter is true) when connecting to a resource.

Security groups (1/3) Info

Search

< 1 > ⚙

	Group ID	Group name	VPC ID	Description
<input checked="" type="checkbox"/>	sg-0f9a098d3a9cdae40	default	vpc-074e7529444273a39	default VPC security group
<input type="checkbox"/>	sg-031f1ea56a01a4e44	launch-wizard-1	vpc-074e7529444273a39	launch-wizard-1 created 2023-12-12T...
<input type="checkbox"/>	sg-0d77779fefb86448c	launch-wizard-2	vpc-074e7529444273a39	launch-wizard-2 created 2023-12-12T...

sg-0f9a098d3a9cdae40 X

**Subnet**

Select the Subnet in which to create the endpoint

Subnet

Select the subnets in which to create the endpoint.

subnet-08f3852a6c22eb5e8

**Tags**

Endpoints (1/1) Info

Search

< 1 > ⚙

Actions

Create endpoint

	Endpoint type	Status	Creation time
	EC2 Instance Connect Endpoint	Pending	Thursday, December 21, 2023

Endpoints (1/1) Info

Search

< 1 > ⚙

Actions

Create endpoint

	Service name	Endpoint type	Status
vpc-074e7529444273a39	eice-0cdcd4db3e069304.03732eb8.ec2-instance-conn...	EC2 Instance Connect Endpoint	Available

IAM Inline Policy is created Under the specific User:

IAM > Users > Raju-IndCog > Create policy

Step 1  
Specify permissions

Step 2  
Review and create

## Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

VisualJSONActions

▼ Select a service

Specify what actions can be performed on specific resources in a service.

Service

Choose a service

+ Add more permissions

CancelNext

Step 2  
Review and create

Policy editor

VisualJSONActions

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "Statement1",
6       "Effect": "Allow",
7       "Action": [],
8       "Resource": []
9     }
10  ]
11 }
```

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

+ Add new statement

Step 2  
Review and save

Policy editor

VisualJSONActions

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "AllowAllEC2Actions",
6       "Effect": "Allow",
7       "Action": [
8         "ec2:DescribeInstances",
9         "ec2:DescribeInstanceConnectEndpoints"
10      ],
11       "Resource": "*"
12     },
13     {
14       "Sid": "AllowSpecificActionsForUserAMN",
15       "Effect": "Allow",
16       "Action": [
17         "ec2-instance-connect:OpenTunnel",
18         "ec2-instance-connect:SendSSHPublicKey"
19       ],
20       "Resource": [
21         "arn:aws:ec2:us-east-2:02351-1-1:instance-connect-endpoint/eice-8cdca4db3e069304",
22         "arn:aws:ec2:us-east-2:02351-1-1:instance/i-0a8b962883bd3c729"
23       ]
24     }
25  ]
26 }
```

Edit statement

AllowAllEC2Actions Remove

Add actions

Choose a service

Filter services

Included

EC2

Available

AMP

API Gateway

API Gateway V2

ASC

Access Analyzer

Account

Activate

Add a resource

Add

Add a condition (optional)

Add

Step 1

[Modify permissions in eice-policy](#)

Step 2

**Review and save**

## Review and save [Info](#)

Review the permissions, specify details, and tags.

**Permissions defined in this policy** [Info](#)

Edit

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

**Allow (2 of 402 services)** ☐ Show remaining 400 services

Service	Access level	Resource	Request condition
<a href="#">EC2</a>	Limited: List	All resources	None
<a href="#">EC2 Instance Connect</a>	Limited: Write	Multiple	None

Cancel

Previous


Save changes

This is the policy of eice-policy inline policy created under the user





```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAllEC2Actions",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceConnectEndpoints"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowSpecificActionsForUserARN",
      "Effect": "Allow",
      "Action": [
        "ec2-instance-connect:OpenTunnel",
        "ec2-instance-connect:SendSSHPublicKey"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-2:AccountNumber:instance-connect-endpoint/eice-0cdcd4db3e069304",
        "arn:aws:ec2:us-east-2:Account Number
        :instance/i-0a8b962883bd3c729"
      ]
    }
  ]
}
```




Connect Private IP Address Testing :

**Instances (1/1)** [Info](#)  [Connect](#) ☐

[running](#) ☒ [Clear filters](#)


<input checked="" type="checkbox"/>	Name 	Instance ID	Instance state	Insta
<input checked="" type="checkbox"/>	Test-Pvt	i-0a8b962883bd3c729	 Running  	t2.m

Instance ID  
 [i-0a8b962883bd3c729](#) (Test-Pvt)

Connection Type


☐ Connect using EC2 Instance Connect  
Connect using the EC2 Instance Connect browser-based client, with a public IPv4 address.

☒ Connect using EC2 Instance Connect Endpoint  
Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

Private IP address  
 172.31.29.194

Enter the user name defined in the AMI used to launch the instance.  
ubuntu

Max tunnel duration (seconds)  
The maximum allowed duration of the SSH connection. Must be at least 1 second and no more than 3600 seconds (1 hour).  
3600  
Min 1 second. Max 3600 seconds (1 hour).

EC2 Instance Connect Endpoint  
Only endpoints that have completed the creation process can be selected.  
 [Select an endpoint](#)

Using Endpoint Successfully connect Pvt Ip Address :

```
aws | Services | Search [Alt+S]
AWS Transfer Family CloudTrail EC2 VPC S3

* Ubuntu Pro delivers the most comprehensive open source security and
  compliance features.

  https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

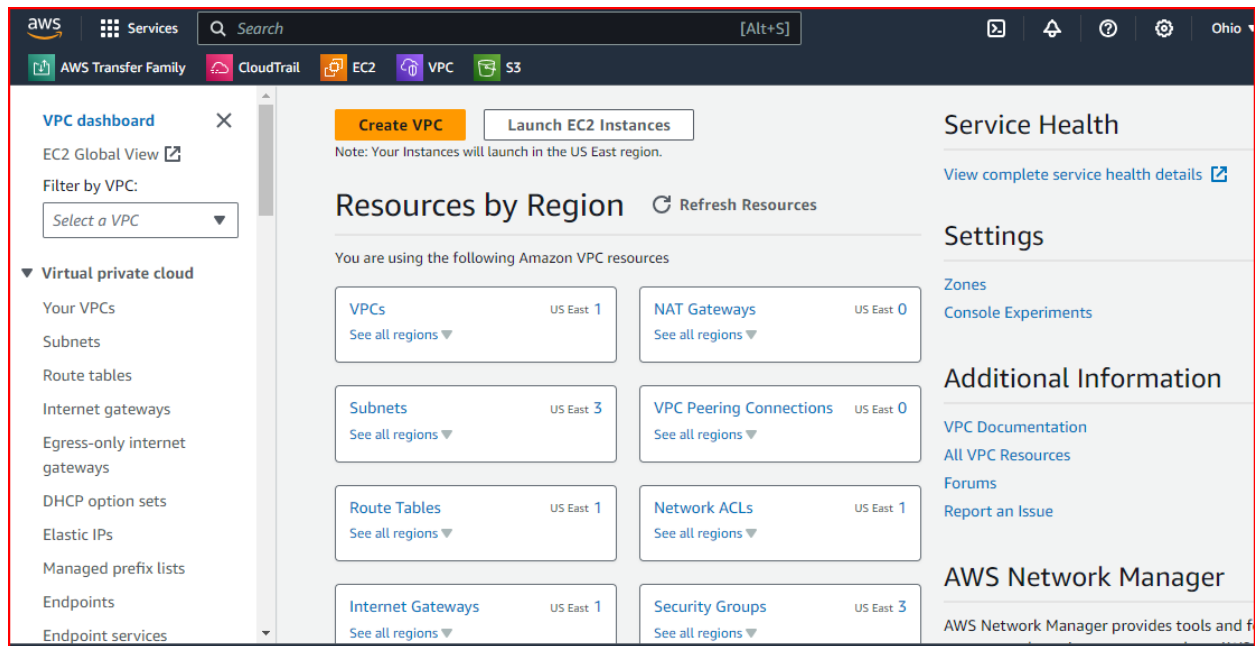
The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Wed Dec 20 22:35:13 2023 from 172.31.21.161
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

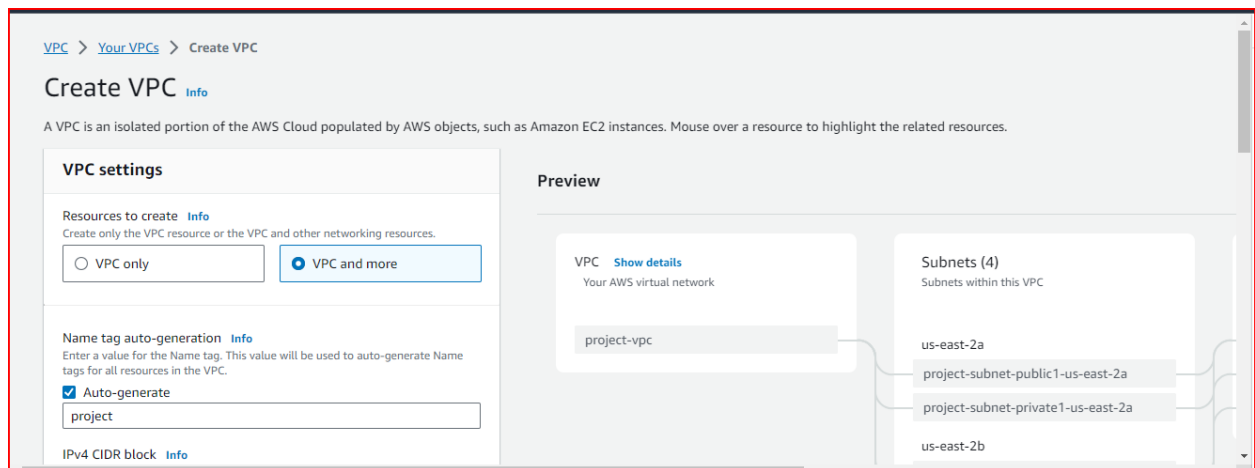
ubuntu@ip-172-31-29-194:~$
```

# VPC Launch :

Step1: Goto AWS Console and search vpc and open vpc dashboard.



Click on Create VPC then enter the name of vpc



Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

☒ Auto-generate

IPv4 CIDR block [Info](#)

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

65,536 IPs

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

IPv6 CIDR block [Info](#)

☒ No IPv6 CIDR block

☐ Amazon-provided IPv6 CIDR block

Tenancy [Info](#)

Default

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

Preview

VPC [Show details](#)

Your AWS virtual network

stage-vpc

Subnets (4)

Subnets within this VPC

us-east-2a

stage-subnet-public1-us-east-2a

stage-subnet-private1-us-east-2a

us-east-2b

stage-subnet-public2-us-east-2b

stage-subnet-private2-us-east-2b

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

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

Preview

VPC [Show details](#)

Your AWS virtual network

stage-vpc

Subnets (4)

Subnets within this VPC

us-east-2a

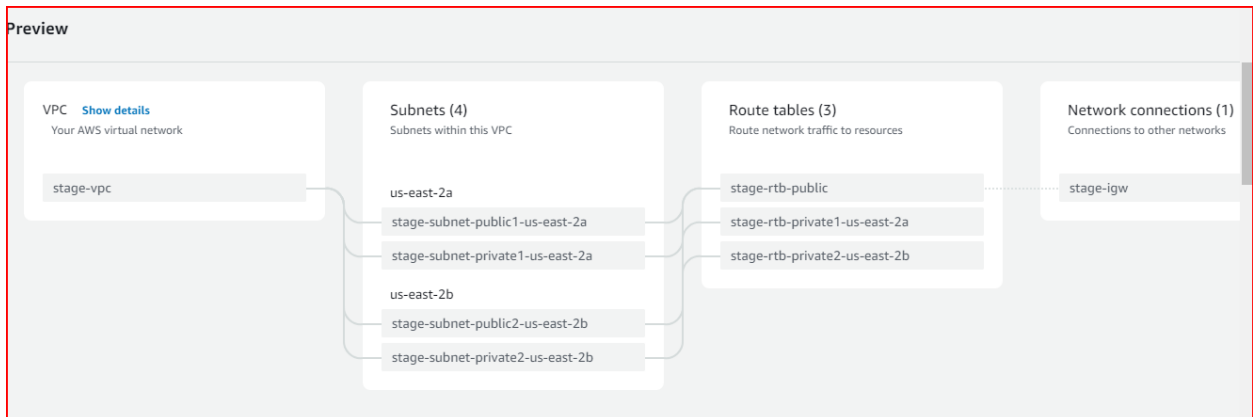
stage-subnet-public1-us-east-2a

stage-subnet-private1-us-east-2a

us-east-2b

stage-subnet-public2-us-east-2b

stage-subnet-private2-us-east-2b



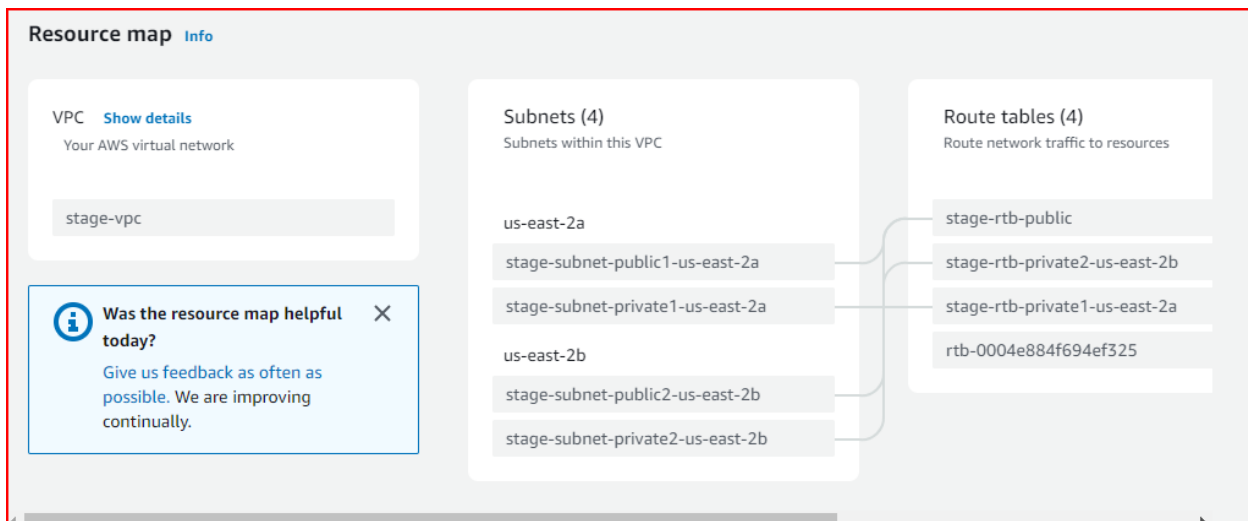
VPC > Your VPCs > Create VPC > Create VPC resources

## Create VPC workflow

✓ Success

▼ Details

- ✓ Create VPC: [vpc-04daedf59e25c0641](#)
- ✓ Enable DNS hostnames
- ✓ Enable DNS resolution
- ✓ Verifying VPC creation: [vpc-04daedf59e25c0641](#)
- ✓ Create subnet: [subnet-0ebada16fbbc3b0eb](#)
- ✓ Create subnet: [subnet-0733539e3ebe6e6c4](#)
- ✓ Create subnet: [subnet-081c501c5e9cdc506](#)
- ✓ Create subnet: [subnet-0d6c505cb65f1b928](#)
- ✓ Create internet gateway: [igw-00ff5086c2d44f88e](#)
- ✓ Attach internet gateway to the VPC
- ✓ Create route table: [rtb-05518d9a0de4b3d08](#)
- ✓ Create route
- ✓ Associate route table
- ✓ Associate route table
- ✓ Create route table: [rtb-05fa5ac2d5cdae66](#)
- ✓ Associate route table
- ✓ Create route table: [rtb-057280ecc2a34d151](#)
- ✓ Associate route table
- ✓ Verifying route table creation



Step2: Checking IGW is added in vpc if not attach the vpc

Why this? – Internet connectivity i.e public

VPC > Internet gateways > igw-00ff5086c2d44f88e

## igw-00ff5086c2d44f88e / stage-igw

Actions

**Details** Info

Internet gateway ID igw-00ff5086c2d44f88e	State Attached	VPC ID vpc-04daedf59e25c0641   stage-vpc	Owner 023516359556
--	-------------------	---	-----------------------

**Tags** Manage tags

Search tags

Key	Value
Name	stage-igw

## Step3: Subnets

Create 2 Public and 2 Private Subnets in 2 AZs

Subnets (7) Info

Find resources by attribute or tag

Actions Create subnet

Name	Subnet ID	State	VPC	IPv4 CIDR
stage-subnet-public2-us-east-2b	subnet-0733539e3ebe6e6c4	Available	vpc-04daedf59e25c0641   stag...	10.0.16.0/20
stage-subnet-private2-us-east-2b	subnet-0d6c505cb65f1b928	Available	vpc-04daedf59e25c0641   stag...	10.0.144.0/20
stage-subnet-private1-us-east-2a	subnet-081c501c5e9cdc506	Available	vpc-04daedf59e25c0641   stag...	10.0.128.0/20
stage-subnet-public1-us-east-2a	subnet-0ebada16fbbc3b0eb	Available	vpc-04daedf59e25c0641   stag...	10.0.0.0/20

## Step4: Route Tables

Default Route Table is Public one then create pvt rt

Route tables (5) Info

Find resources by attribute or tag

Actions Create route table

	Name	Route table ID	Explicit subnet associati...	Edge associations	Main
<input type="checkbox"/>	stage-rtb-public	rtb-05518d9a0de4b3d08	2 subnets	-	No
<input type="checkbox"/>	stage-rtb-private2-us-east-2b	rtb-057280ecc2a34d151	subnet-0d6c505cb65f1b...	-	No
<input type="checkbox"/>	stage-rtb-private1-us-east-2a	rtb-05fa5ac2d5ccaae66	subnet-081c501c5e9cdc5...	-	No
<input type="checkbox"/>	-	rtb-02807e1bfb6400b69	subnet-08f3852a6c22eb...	-	Yes

## Step5: Route Table Subnets association

Adding public subnets into public route table

Virtual private cloud

Route table ID: **rtb-05518d9a0de4b3d06**

Main: No

Owner ID: 023516359556

Explicit subnet associations: 2 subnets

Edge associations: -

Subnet associations

Explicit subnet associations (2)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
stage-subnet-public2-us-east-2b	<a href="#">subnet-0733539e3e6e6e6c4</a>	10.0.16.0/20	-
stage-subnet-public1-us-east-2a	<a href="#">subnet-0ebada16fbbc3b0eb</a>	10.0.0.0/20	-

Subnets without explicit associations (0)

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

Adding private subnets into private route table

Virtual private cloud

Route table ID: **rtb-057280ecc2a34d151**

Main: No

Owner ID: 023516359556

Explicit subnet associations: [subnet-0d6c505cb65f1b928](#) / [stage-subnet-private2-us-east-2b](#)

Edge associations: -

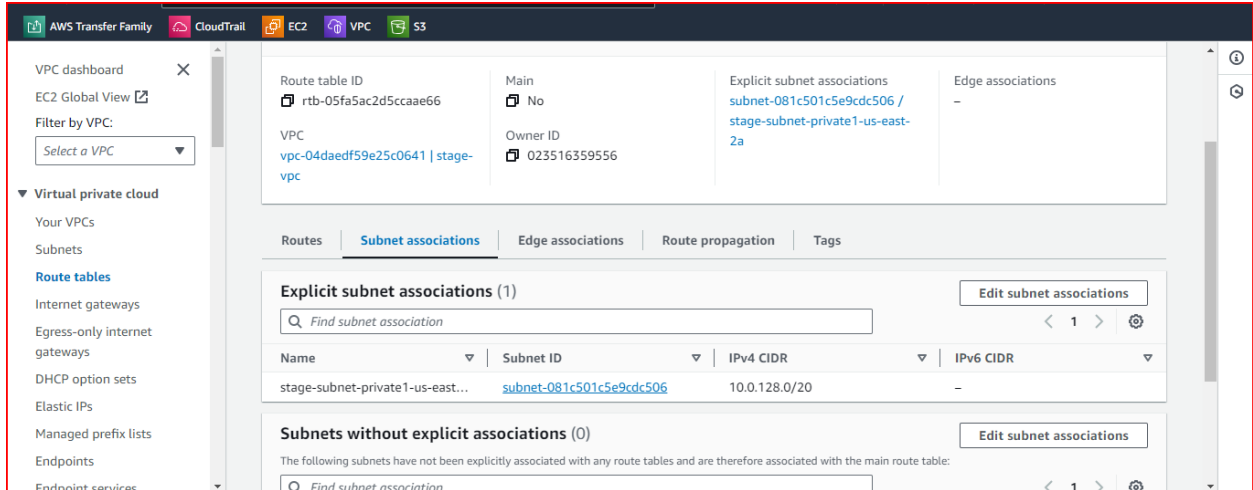
Subnet associations

Explicit subnet associations (1)

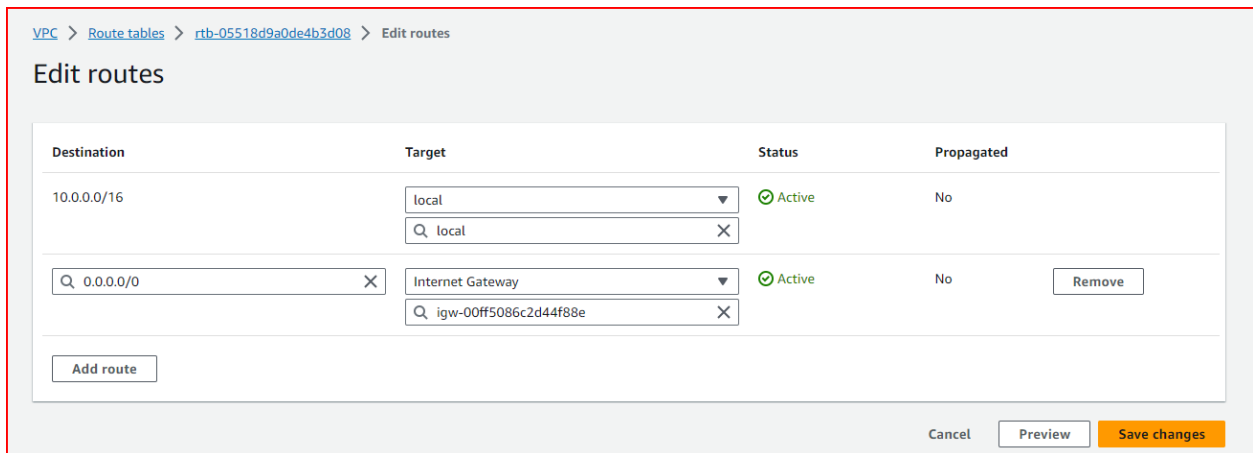
Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
stage-subnet-private2-us-east-2b	<a href="#">subnet-0d6c505cb65f1b928</a>	10.0.144.0/20	-

Subnets without explicit associations (0)

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



Step6: adding the Internet gateway to the public route table to explore the subnet to access from internet



## Step7: Creating NAT Gateway

Creating NAT for private route table to provide internet to them  
Here choose any pub subnet to access internet to the NAT gateway



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

**nat\_stage**

The name can be up to 256 characters long.

**Subnet**  
Select a subnet in which to create the NAT gateway.

**subnet-0733539e3ebe6e6c4 (stage-subnet-public2-us-east-2b)**

**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-06f03fd05fc7241a7**

**Allocate Elastic IP**

[▶ Additional settings](#) [Info](#)

✔ Elastic IP address 18.221.161.26 (eipalloc-06f03fd05fc7241a7) allocated.

**NAT gateway nat-0865b2308932c1586 | nat\_stage was created successfully.**

**NAT gateways (1/1)** [Info](#)

Name	NAT gateway ID	Connectivit...	State	State message	Primary public
<input checked="" type="radio"/> nat_stage	nat-0865b2308932c1586	Public	✔ Available	–	18.221.161.26

## Step8: Add the nat gateway into pvt route table under routes

Then Choose any pvt route table to attach the nat gateway to serve internet

**Route tables (5)** [Info](#)

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associati...	Edge associations	Main
<input type="checkbox"/>	stage-rtb-public	rtb-05518d9a0de4b3d08	2 subnets	–	No
<input type="checkbox"/>	stage-rtb-private2-us-east-2b	rtb-057280ecc2a34d151	subnet-0d6c505cb65f1b...	–	No
<input type="checkbox"/>	stage-rtb-private1-us-east-2a	rtb-05fa5ac2d5ccea66	subnet-081c501c5e9cdc5...	–	No
<input type="checkbox"/>	–	rtb-02807e1bfb6400b69	subnet-08f3852a6c22eb...	–	Yes

[VPC](#) > [Route tables](#) > [rtb-057280ecc2a34d151](#) > Edit routes

### Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	<div>local</div> <div>Q local X</div>	Active	No
<div>Q 0.0.0.0/0 X</div>	<div>NAT Gateway</div> <div>Q nat- X</div>	-	No

Add route

CancelPreviewSave changes

Successfully configured vpc setup if any other services under the vpc we can add based on the requirements.