

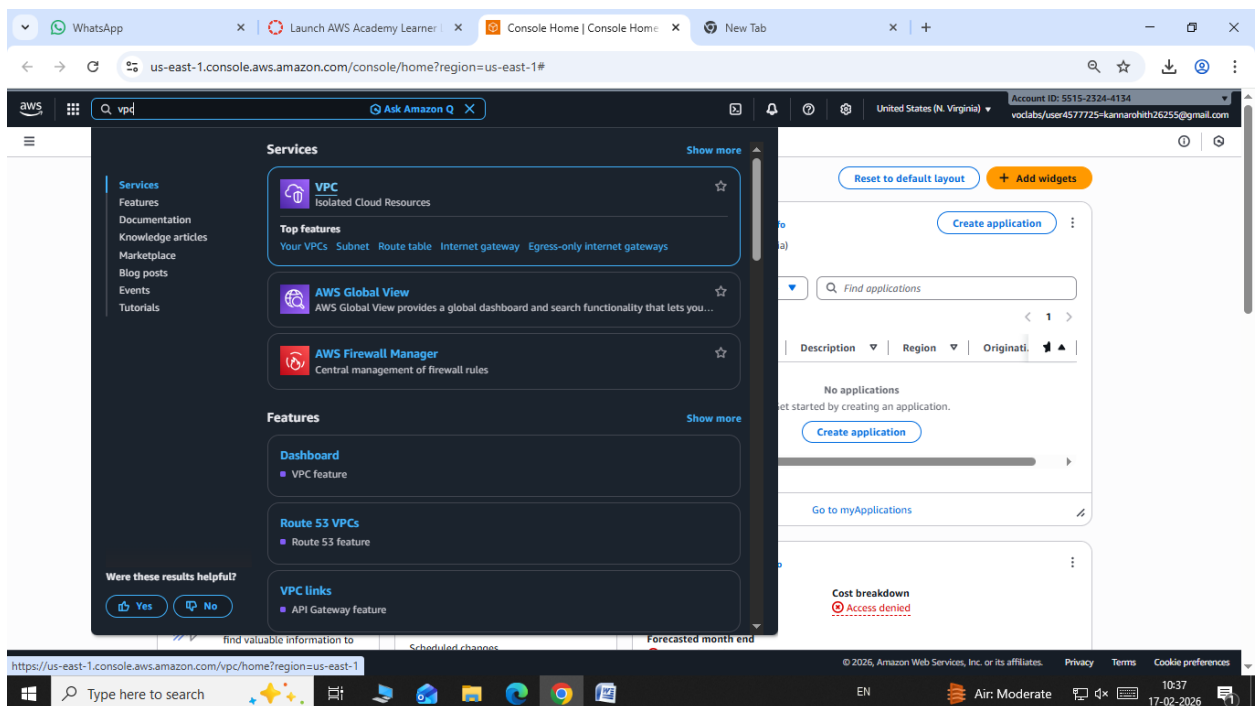
Name: k.Rohith

Rollno.: 23bd1a1291

Week 5: VPC Creation and Ec2 Instance Connection

◆Step 1: Create the VPC

1. Go to **AWS Management Console** → **VPC**
2. Click **Create VPC**
3. Choose **VPC only**
4. Enter:
 - **Name:** Custom-VPC
 - **IPv4 CIDR block:** e.g. 10.0.0.0/16
5. Click **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 info
Creates a tag with a key of 'Name' and a value that you specify.

custom-VPC

IPv4 CIDR block info
☒ 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 info
☒ No IPv6 CIDR block
☐ IPAM-allocated IPv6 CIDR block
☐ Amazon-provided IPv6 CIDR block
☐ IPv6 CIDR owned by me

Tenancy info
Default

VPC encryption control (\$) info
Monitor mode provides visibility into encryption status without blocking traffic. Enforce mode prevents unencrypted traffic. Additional charges apply.

☒ None ☐ Monitor mode
See which resources in your VPC are unencrypted but allow the creation of unencrypted resources. ☐ Enforce mode
Requires all resources, except exclusions, in your VPC to be encryption-capable and blocks creation of unencrypted resources.

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

Key	Value - optional	
Name	custom-VPC	Remove tag

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

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

◆ Step 2: Create Subnets (Public & Private)

Create subnets in same **Availability Zones** for high availability.

Example:

- **Public Subnet:** 10.0.1.0/24 (AZ-A)
- **Private Subnet:** 10.0.2.0/24 (AZ-A)

Steps:

1. Go to **Subnets** → **Create subnet**
2. Select your VPC
3. Choose AZ
4. Enter CIDR
5. Create subnet

The screenshot shows the AWS Management Console interface for the 'us-east-1' region. The main content area displays the 'Subnets (6)' page. A table lists the following subnets:

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	IPv6 CIDR
-	subnet-0dc9b8d069b931153	Available	vpc-08e6f3ebe3f57f6d6	Off	172.31.80.0/20	-
-	subnet-0ca26ba5d3fb87451	Available	vpc-08e6f3ebe3f57f6d6	Off	172.31.32.0/20	-
-	subnet-0d7a03052448b6930	Available	vpc-08e6f3ebe3f57f6d6	Off	172.31.0.0/20	-
-	subnet-0050e2917f24e87fa	Available	vpc-08e6f3ebe3f57f6d6	Off	172.31.16.0/20	-
-	subnet-028f5b647ba46c845	Available	vpc-08e6f3ebe3f57f6d6	Off	172.31.64.0/20	-
-	subnet-07386b3fcaa765066	Available	vpc-08e6f3ebe3f57f6d6	Off	172.31.48.0/20	-

The left sidebar shows the 'Virtual private cloud' section expanded, with 'Subnets' selected. The bottom of the screen shows the Windows taskbar with the search bar and various application icons.

WhatsApp Launch AWS Academy Learner VPC | us-east-1 New Tab

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateSubnet

Search [Alt+S]

United States (N. Virginia) Account ID: 5515-2324-4134 vodabs/user4577725-kannaroth26255@gmail.com

Create subnet

VPC

VPC ID
Create subnets in this VPC.
vpc-0a9d577c85b87e742 (custom-VPC)

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.
cc_vpc_subnet1
The name can be up to 256 characters long.

Availability Zone
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
United States (N. Virginia) / use1-az6 (us-east-1a)

IPv4 VPC CIDR block
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

CloudShell Feedback

© 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

EN 23°C Sunny 10:50 17-02-2026

(1) WhatsApp Launch AWS Academy Learner VPC | us-east-1

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateSubnet

Search [Alt+S]

United States (N. Virginia) Account ID: 5515-2324-4134 vodabs/user4577725-kannaroth26255@gmail.com

Create subnet

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

Availability Zone
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
United States (N. Virginia) / use1-az6 (us-east-1a)

IPv4 VPC CIDR block
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

Tags - optional

Key	Value - optional
Name	public_subnet

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

[Remove](#)

[Add new subnet](#)

[Cancel](#) [Create subnet](#)

CloudShell Feedback

© 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

EN 23°C Sunny 11:02 17-02-2026

Private:

Create subnet [Info](#)

VPC
VPC ID
Create subnets in this VPC.
vpc-0a9d577c85b87e742 (custom-VPC)

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.
cc_vpc_subnet2
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.
United States (N. Virginia) / use1-az6 (us-east-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

Create subnet [Info](#)

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
private_subnet
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.
United States (N. Virginia) / use1-az6 (us-east-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

Tags - optional

Key	Value - optional	
Name	private_subnet	Remove

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

[Remove](#)

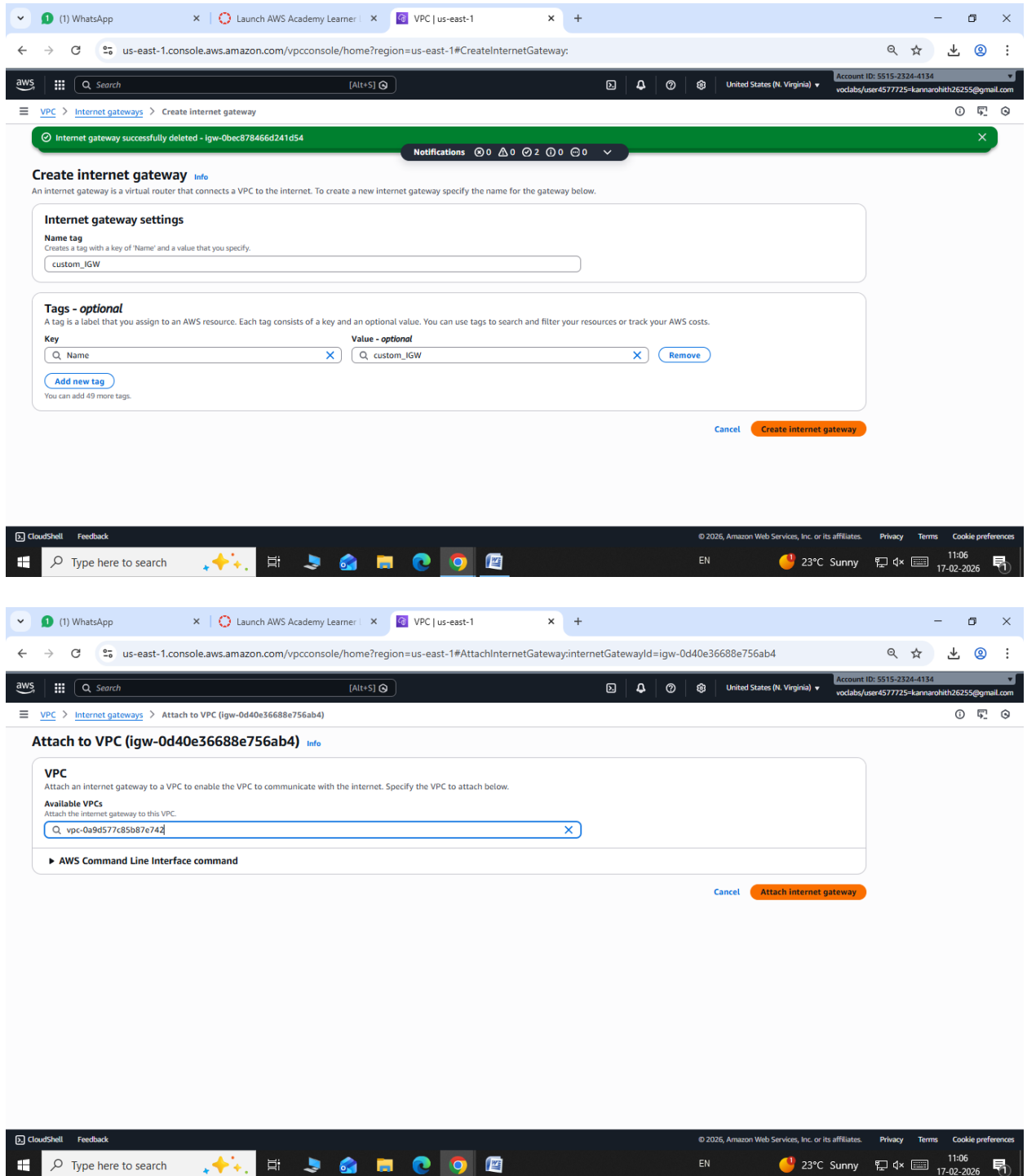
[Add new subnet](#)

[Cancel](#) [Create subnet](#)

◆ Step 3: Create an Internet Gateway (IGW)

1. Go to **Internet Gateways**
2. Click **Create internet gateway**

3. Name it `Custom-IGW`
4. **Attach** it to your VPC



◆ Step 4: Create Route Tables

You need **separate route tables** for public and private subnets.

Public Route Table

1. Go to **Route Tables** → **Create route table**
2. Select VPC
3. Add route:
 - Destination: 0.0.0.0/0
 - Target: **Internet Gateway**
4. Associate with **public subnet**

The screenshot shows the AWS Management Console interface for creating a new route table. The browser tabs include 'WhatsApp', 'Launch AWS Academy Learner', and 'VPC | us-east-1'. The address bar shows the URL: `us-east-1.console.aws.amazon.com/vpconsole/home?region=us-east-1#CreateRouteTable:`. The console header displays the AWS logo, a search bar, and account information for 'United States (N. Virginia)' with account ID '5515-2324-4134'.

The main content area is titled 'Create route table' with a sub-header 'Route table settings'. Below this, there is a section for 'Name - optional' with a text input field containing 'public_route_table'. A note indicates that the name is optional and should be unique. Below the name field is a dropdown menu for 'VPC', which is currently set to 'vpc-0a9d577c85b87e742 (custom-VPC)'. A note explains that the VPC is used for this route table.

Below the VPC selection is a 'Tags' section. It includes a 'Key' input field with 'Name' and a 'Value - optional' input field with 'public_route_table'. There is a 'Remove' button next to the value field and an 'Add new tag' button. A note states that you can add up to 49 more tags.

At the bottom right of the form, there are two buttons: 'Cancel' and 'Create route table'.

The bottom of the image shows a Windows taskbar with the search bar, task view button, and several application icons. The system tray on the right shows the date and time as '11:08 17-02-2026' and the weather as '23°C Sunny'.

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#RouteTableDetails:RouteTableId=rtb-098657d0c8f22f82b

VPC > Route tables > rtb-098657d0c8f22f82b

rtb-098657d0c8f22f82b / public_route_table

VPC dashboard

Filter by VPC

Virtual private cloud

- Your VPCs
- Subnets
- Route tables
- Internet gateways
- Egress-only internet gateways
- Carrier gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- NAT gateways
- Peering connections
- Route servers

Security

- Network ACLs
- Security groups

PrivateLink and Lattice

Details

Route table ID: rtb-098657d0c8f22f82b

VPC: vpc-0a9d577c85b87e742 | custom-VPC

Main: No

Owner ID: 551523244134

Explicit subnet associations: -

Edge associations: -

Routes (1)

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	Create Route Table

Actions

- Set main route table
- Edit subnet associations
- Edit edge associations
- Edit route propagation
- Edit routes
- Manage tags
- Delete

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

EN 23°C Sunny 11:09 17-02-2025

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#EditRoutes:RouteTableId=rtb-098657d0c8f22f82b

VPC > Route tables > rtb-098657d0c8f22f82b > Edit routes

Edit routes

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

Add route

Cancel Preview Save changes

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

EN 23°C Sunny 11:09 17-02-2025

rtb-098657d0c8f22f82b / public_route_table

Details

- Route table ID: rtb-098657d0c8f22f82b
- VPC: vpc-0a9d577c85b87e742 | custom-VPC
- Main: No
- Owner ID: 551523244134

Routes (2)

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-0d40c36688e756ab4	Active	No	Create Route
10.0.0.0/16	local	Active	No	Create Route Table

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
<input checked="" type="checkbox"/> public_subnet	subnet-062d708d1e84c0504	10.0.1.0/24	-	Main (rtb-0a9cc5f45a9894086)
<input type="checkbox"/> private_subnet	subnet-0ea466f88c8c81453	10.0.2.0/24	-	Main (rtb-0a9cc5f45a9894086)

Selected subnets

subnet-062d708d1e84c0504 / public_subnet

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

Private Route Table

- Keep default local route only (no IGW)
- Associate with **private subnet**

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateRouteTable:

Account ID: 5515-2324-4134
vodafone/user4577725-kannanroth26255@gmail.com

United States (N. Virginia)

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

private_route_table

VPC
The VPC to use for this route table.

vpc-0a9d577c85b87e742 (custom-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

Q Name

Value - optional

Q private_route_table

Remove

Add new tag

You can add 49 more tags.

Cancel Create route table

CloudShell Feedback

Type here to search

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

EN 23°C Sunny 11:12 17-02-2025

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#RouteTableDetails:RouteTableId=rtb-0e211c732d711dc87

Account ID: 5515-2324-4134
vodafone/user4577725-kannanroth26255@gmail.com

United States (N. Virginia)

Route tables > rtb-0e211c732d711dc87

Route table rtb-0e211c732d711dc87 | private_route_table was created successfully.

rtb-0e211c732d711dc87 / private_route_table

Set main route table
Edit subnet associations
Edit edge associations
Edit route propagation
Edit routes
Manage tags
Delete

Details

Route table ID
rtb-0e211c732d711dc87

Main
No

Explicit subnet associations
-

Edge associations
-

VPC
vpc-0a9d577c85b87e742 | custom-VPC

Owner ID
551523244134

Routes Subnet associations Edge associations Route propagation Tags

Routes (1)

Filter routes

Destination	Target	Status	Propagated	Route Origin
10.0.0/16	local	Active	No	Create Route Table

Both Edit routes

Virtual private cloud

Filter by VPC

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

NAT gateways

Peering connections

Route servers

Security

Network ACLs

Security groups

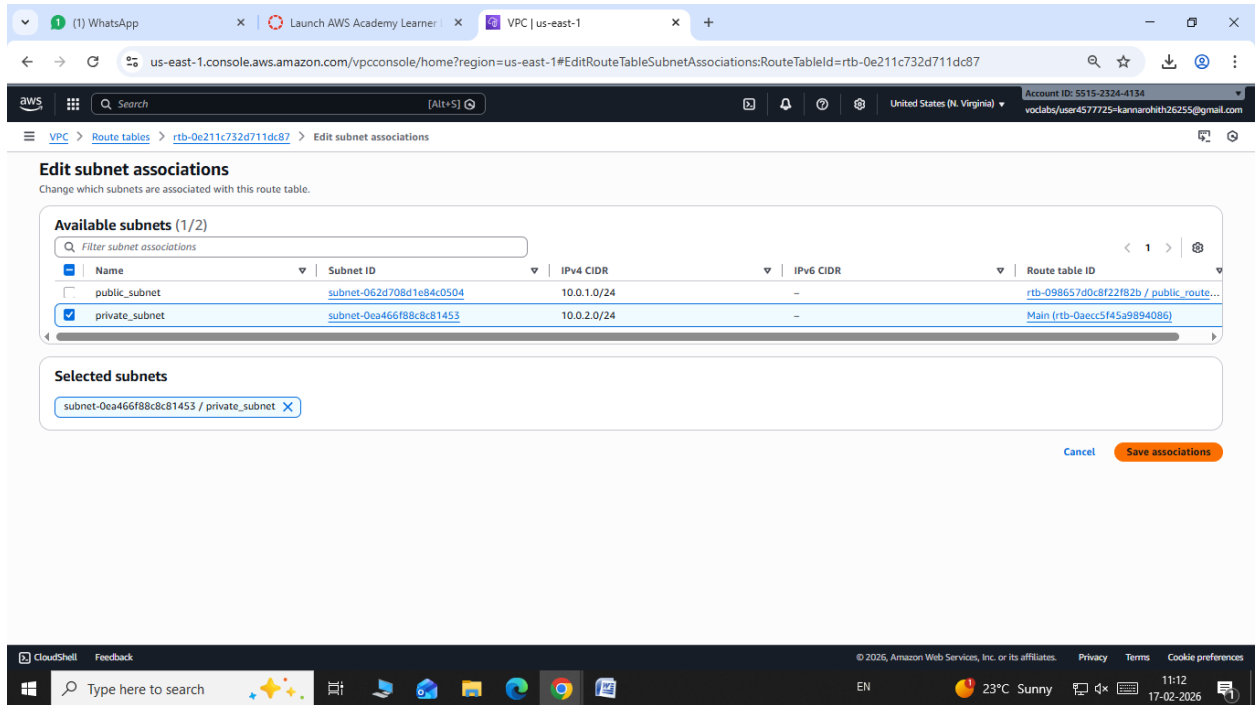
PrivateLink and Lattice

CloudShell Feedback

Type here to search

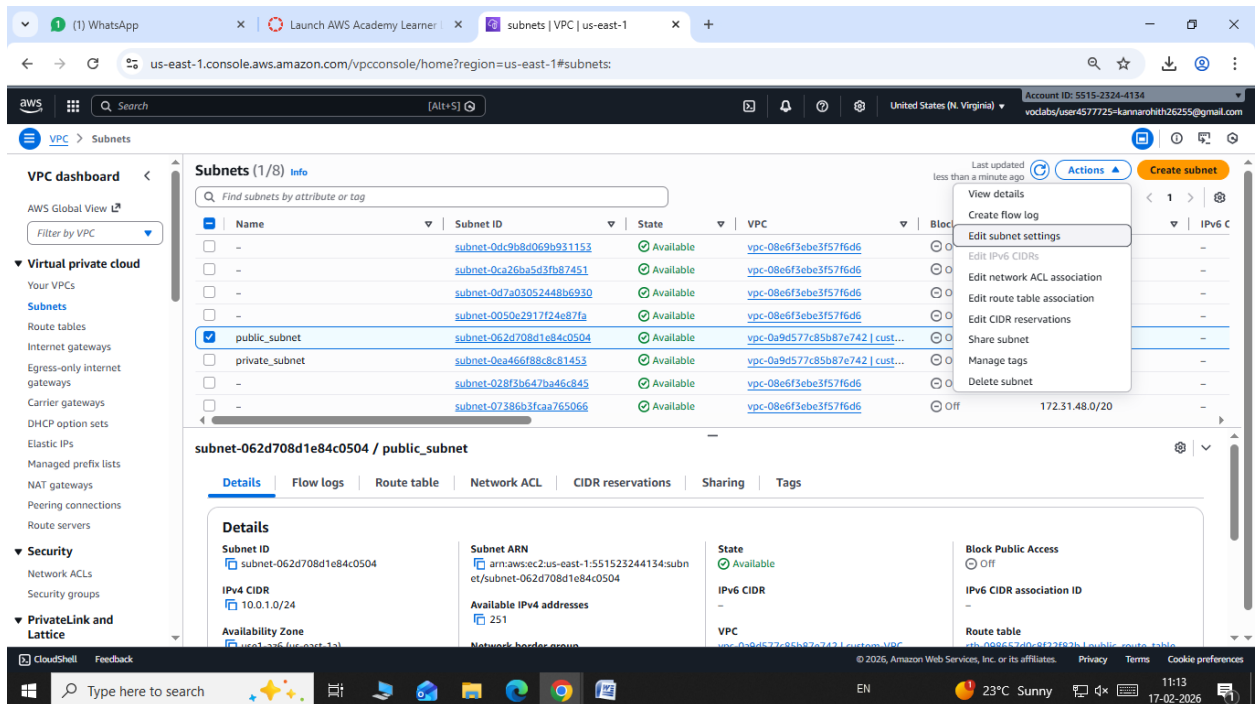
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

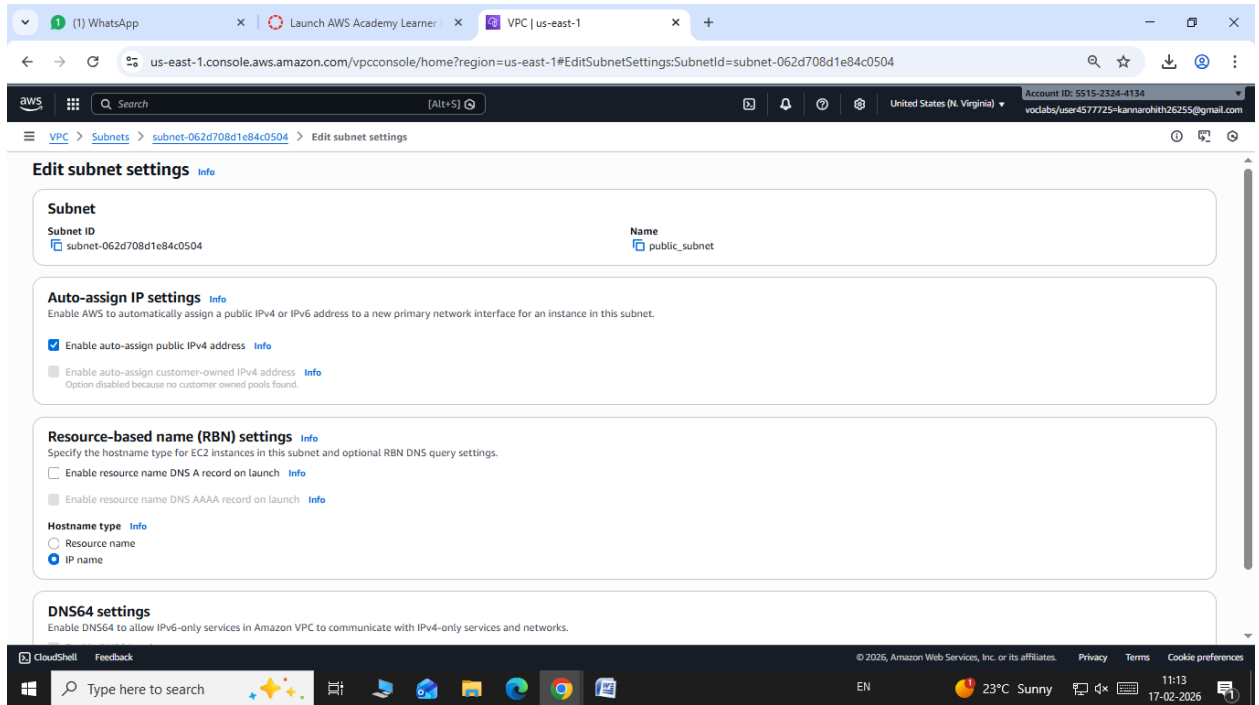
EN 23°C Sunny 11:12 17-02-2025



◆ Step 5: Enable Auto-Assign Public IP (Public Subnet)

1. Select **Public Subnet**
2. Go to **Edit subnet settings**
3. Enable **Auto-assign public IPv4 address**





◆ Step 6: Configure Security Groups

1. Create a **Security Group**
2. Add inbound rules:
 - HTTP (80) / HTTPS (443)
 - SSH (22) from trusted IP
3. Attach to EC2 instances

Edit inbound rules

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

Inbound rules

Security group rule ID: sgr-02013558c59eb2344

Type	Protocol	Port range	Source	Description - optional	Action
All traffic	All	All	Custom		Delete
HTTP	TCP	80	Anywhere...	sg-0cace6efd85bd484f	Delete
HTTPS	TCP	443	Anywhere...	0.0.0.0/0	Delete
SSH	TCP	22	Anywhere...	0.0.0.0/0	Delete

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.

Buttons: Add rule, Cancel, Preview changes, Save rules

Security Groups (1/14)

Name	Security group ID	Security group name	VPC ID	Description
-	sg-0cace6efd85bd484f	default	vpc-0a9d577c85b87e742	default VPC security group
-	sg-06ecde1b22bcad940	launch-wizard-8	vpc-08e6f3e3e3f57f6d6	launch-wizard-8 created 2026-01-27T0...
-	sg-0ba190d05106abea6	launch-wizard-7	vpc-08e6f3e3e3f57f6d6	launch-wizard-7 created 2026-01-20T0...
-	sg-0864d174d476641ff	launch-wizard-1	vpc-08e6f3e3e3f57f6d6	launch-wizard-1 created 2026-01-08T0...

sg-0cace6efd85bd484f - default

Details | **Inbound rules** | Outbound rules | Sharing | VPC associations | Related resources - new | Tags

Inbound rules (1)

Name	Security group rule ID	IP version	Type	Protocol	Port range	Source
-	sgr-02013558c59eb2344	-	All traffic	All	All	sg-0cace6efd85bd484f

◆ Step 7: Launch EC2 Instances

- Public EC2 → Public subnet

WhatsAppLaunch AWS Academy LearnerLaunch an instance | EC2 | us-east-1SecurityGroups | VPC Console

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:

Search[Alt+F5]Ask Amazon QUnited States (N. Virginia)Account ID: 5515-2324-4134vodafone/user4577725-kannanroth26255@gmail.com

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

pubic_EC2

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-0c1fe732b5494dc14 (64-bit (x86), uefi-preferred) / ami-02b86da1e539b4dd0 (64-bit (Arm), uefi)

Free tier eligible

Summary

Number of instances | Info

1

Software image (AMI)

Amazon Linux 2023 AMI 2023.10...[read more](#)

ami-0c1fe732b5494dc14

Virtual server type (instance type)

t2.micro

Firewall (security group)

default

Storage (volumes)

1 volume(s) - 8 GiB

Cancel

Launch instance

[Preview code](#)

CloudShellFeedback

Type here to search

© 2026, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

EN23°C Sunny11:4317-02-2026

WhatsAppLaunch AWS Academy LearnerLaunch an instance | EC2 | us-east-1SecurityGroups | VPC Console

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:

Search[Alt+F5]Ask Amazon QUnited States (N. Virginia)Account ID: 5515-2324-4134vodafone/user4577725-kannanroth26255@gmail.com

EC2>Instances>Launch an instance

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-0c1fe732b5494dc14 (64-bit (x86), uefi-preferred) / ami-02b86da1e539b4dd0 (64-bit (Arm), uefi)

Free tier eligible

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 2023.10.20260202.2 x86_64 HVM kernel-6.1

Architecture

64-bit (x86)

Boot mode

uefi-preferred

AMI ID

ami-0c1fe732b5494dc14

Publish Date

2026-02-03

Username

ec2-user

Verified provider

Instance type

Info | Get advice

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory Current generation: true On-Demand Linux base pricing: 0.0116 USD per Hour

On-Demand Windows base pricing: 0.0162 USD per Hour On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour

On-Demand SUSE base pricing: 0.0116 USD per Hour On-Demand RHEL base pricing: 0.026 USD per Hour

All generations

[Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

Summary

Number of instances | Info

1

Software image (AMI)

Amazon Linux 2023 AMI 2023.10...[read more](#)

ami-0c1fe732b5494dc14

Virtual server type (instance type)

t2.micro

Firewall (security group)

default

Storage (volumes)

1 volume(s) - 8 GiB

Cancel

Launch instance

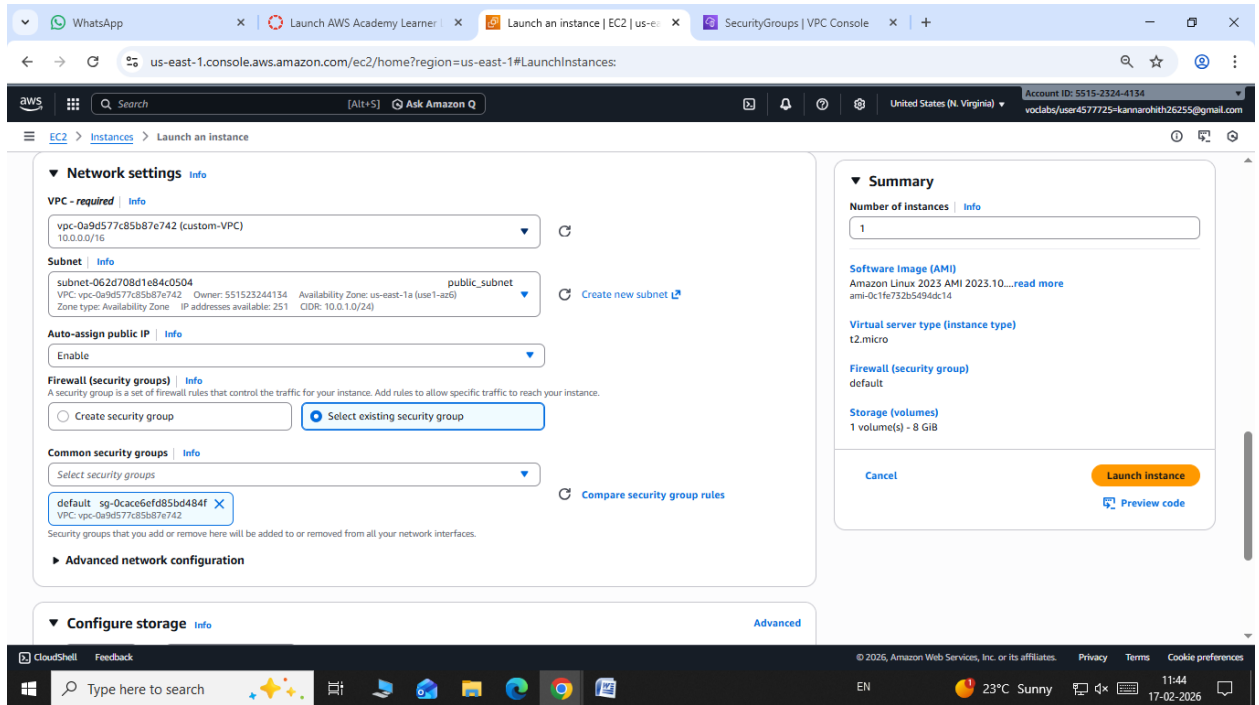
[Preview code](#)

CloudShellFeedback

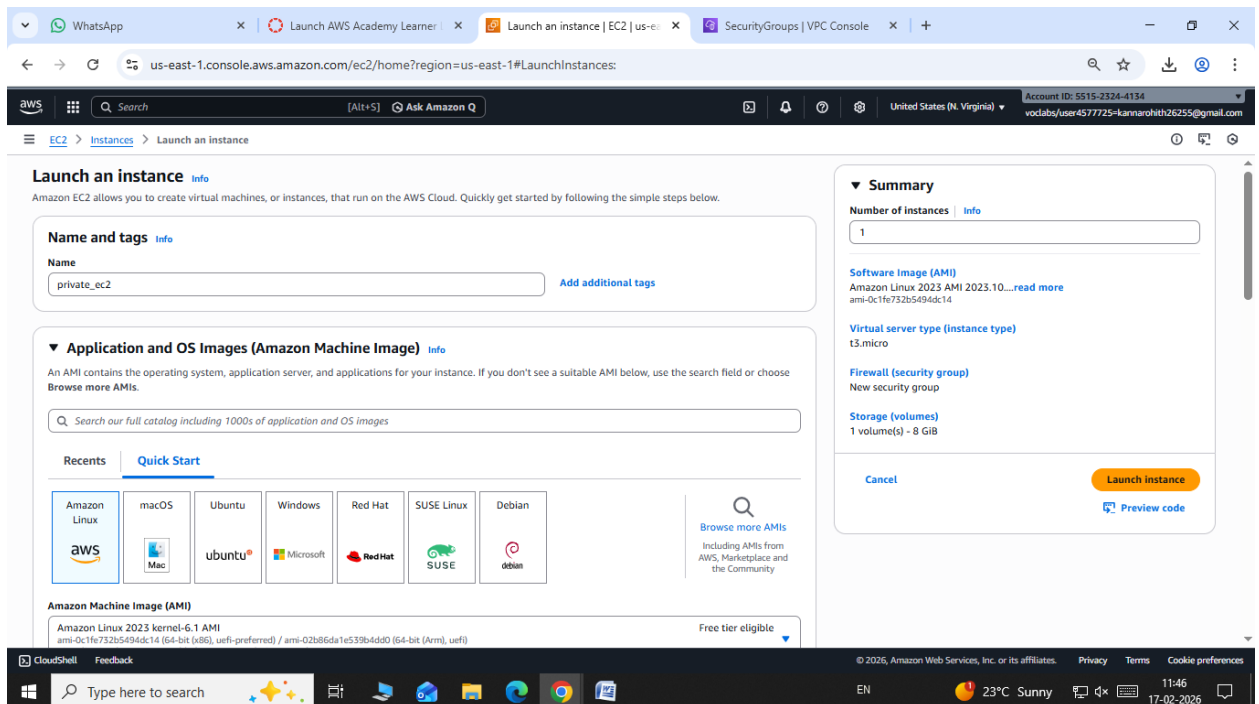
Type here to search

© 2026, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

EN23°C Sunny11:4317-02-2026



- Private EC2 → Private subnet
Attach correct security groups.



us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:

EC2 > Instances > Launch an instance

Recents Quick Start

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Linux Debian

Amazon Machine Image (AMI)

Amazon Linux 2023 kernel-6.1 AMI
ami-0c1fe732b5494dc14 (64-bit (x86), uefi-preferred) / ami-02b86da1e539b4dd0 (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 2023.10.20260202 2 x86_64 HVM kernel-6.1

Architecture Boot mode AMI ID Publish Date Username

64-bit (x86) uefi-preferred ami-0c1fe732b5494dc14 2026-02-03 ec2-user

Free tier eligible

Verified provider

Instance type Info | Get advice

Instance type

Summary

Number of instances | Info

1

Software image (AMI)
Amazon Linux 2023 AMI 2023.10...read more
ami-0c1fe732b5494dc14

Virtual server type (instance type)
t3.micro

Firewall (security group)
New security group

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

Cancel Launch instance Preview code

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:

EC2 > Instances > Launch an instance

Instance type

t3.micro
Family: t3 2 vCPU 1 GiB Memory Current generation: true On-Demand Linux base pricing: 0.0104 USD per Hour
On-Demand Windows base pricing: 0.0196 USD per Hour On-Demand Ubuntu Pro base pricing: 0.0139 USD per Hour
On-Demand SUSE base pricing: 0.0104 USD per Hour On-Demand RHEL base pricing: 0.0392 USD per Hour

Free tier eligible

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

exp5 Create new key pair

Network settings Info

Network | Info
vpc-08e6f3ebe3f57f6d6

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 new security group Select existing security group

Summary

Number of instances | Info

1

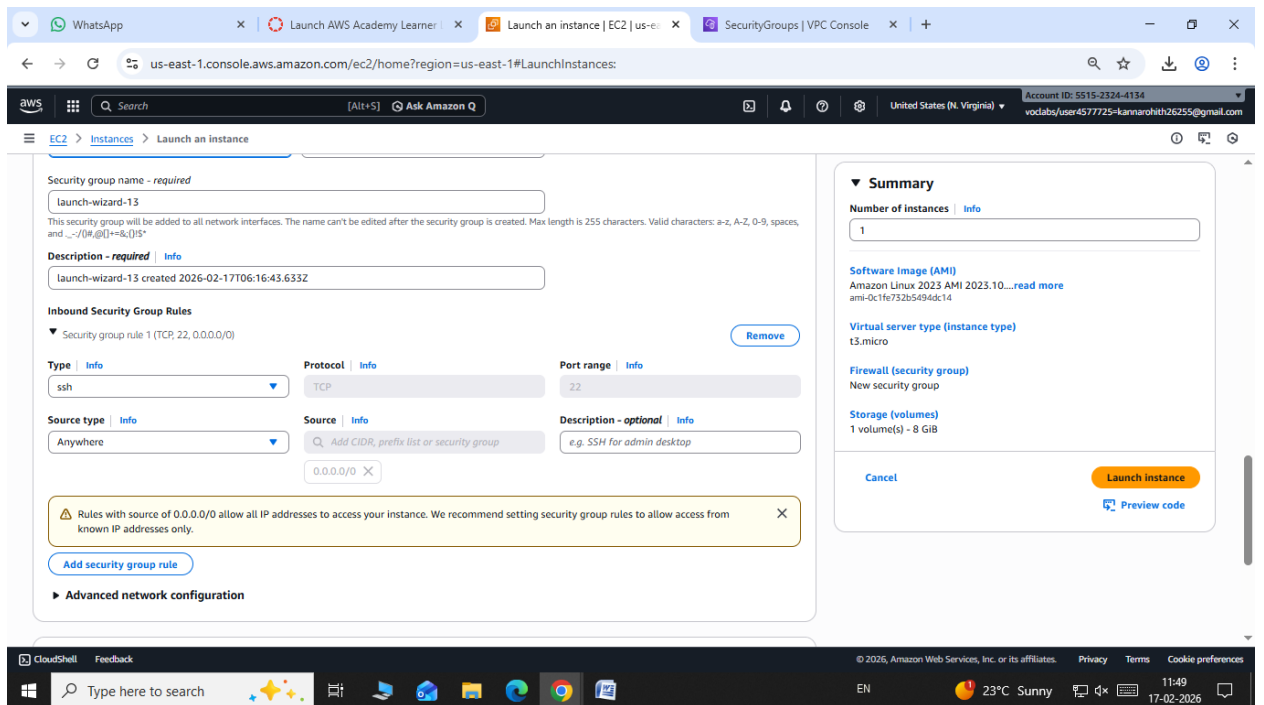
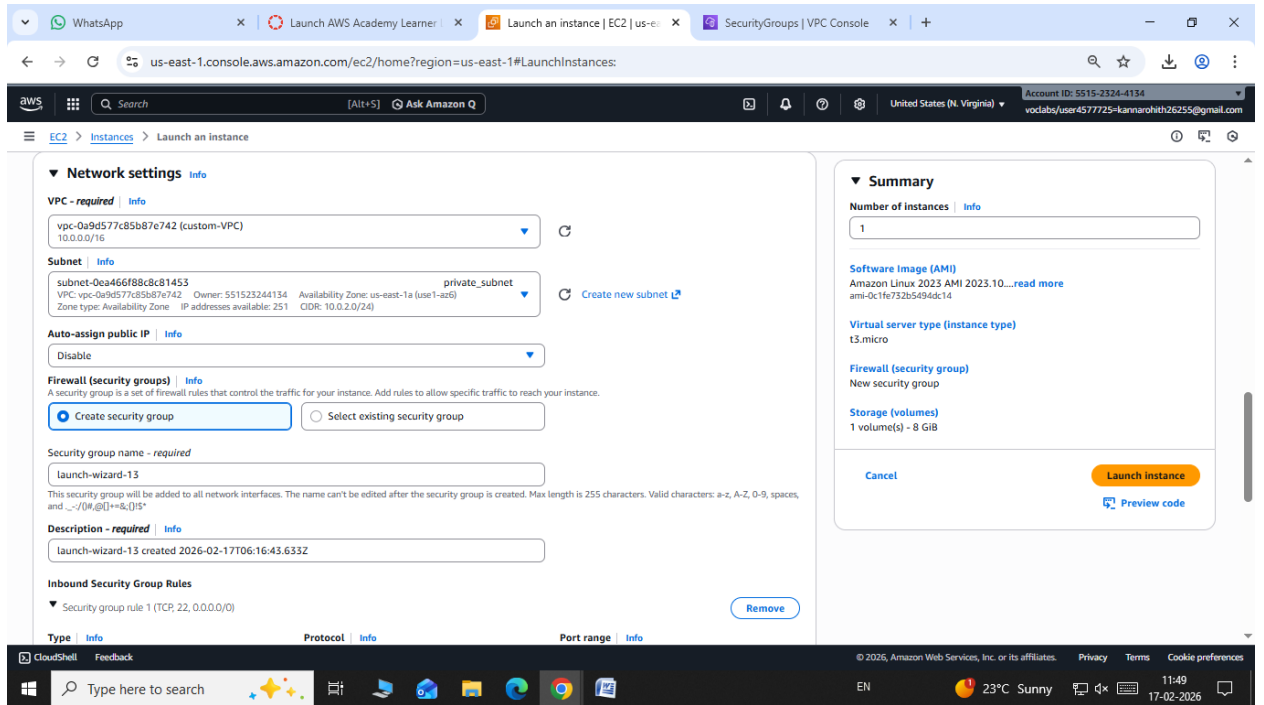
Software image (AMI)
Amazon Linux 2023 AMI 2023.10...read more
ami-0c1fe732b5494dc14

Virtual server type (instance type)
t3.micro

Firewall (security group)
New security group

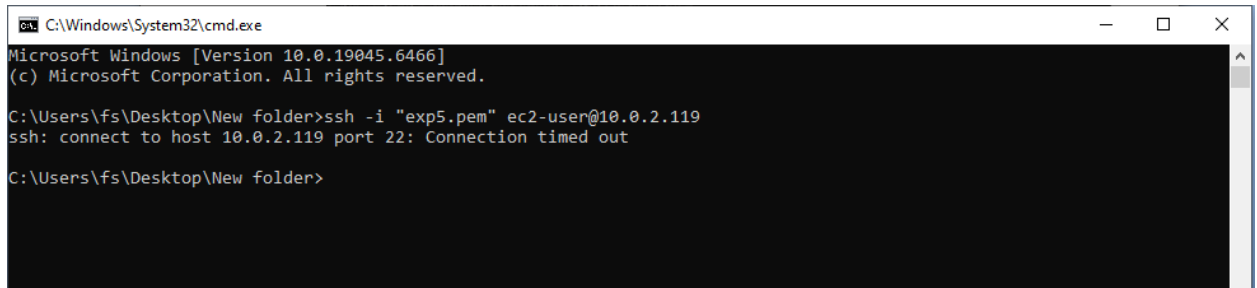
Storage (volumes)
1 volume(s) - 8 GiB

Cancel Launch instance Preview code



◆ Step 8: Test the Setup

- Public EC2 → Internet access ✓



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.6466]
(c) Microsoft Corporation. All rights reserved.

C:\Users\fs\Desktop\New folder>ssh -i "exp5.pem" ec2-user@10.0.2.119
ssh: connect to host 10.0.2.119 port 22: Connection timed out

C:\Users\fs\Desktop\New folder>
```

Scenario Based Questions:

1. You have a web application where users access a website, but the database should not be exposed to the internet. How would you design the VPC? Which resources go into public and private subnets?

Answer: Place ALB/Web servers in public subnets and the database in private subnets; allow DB access only from the application security group.

2. An EC2 instance in a public subnet cannot access the internet. What VPC components would you check and why?

Answer: Check Internet Gateway attachment, route table (0.0.0.0/0 → IGW), public IP assignment, and Security Group/NACL rules.

3. Your application server needs to connect to an RDS database securely. How would you configure security groups and subnets?

Answer: Deploy RDS in a private subnet and allow inbound DB port access only from the application server's security group.

4. You are asked to design a VPC for 500 servers today, but it should scale to 2,000 servers in the future. How would you choose the CIDR block?

Answer: Choose a larger CIDR block (e.g., /20) to accommodate future scaling without IP exhaustion.

5. A company wants secure connectivity between its on-premises data center and AWS VPC. Which AWS services would you choose and why (VPN vs Direct Connect)?

Answer: Use VPN for quick, cost-effective setup; choose Direct Connect for dedicated, high-bandwidth, low-latency connectivity.

6. You need to connect two VPCs, but both use the same CIDR range. How would you solve this problem?

Answer: Modify one VPC's CIDR range or use NAT/PrivateLink to handle overlapping IP addresses.

7. Multiple microservices running in different subnets need to communicate securely. How would you design routing and security groups?

Answer: Use private subnets with proper route tables and configure security groups referencing each other for controlled access.

8. Design a VPC for a 3-tier application (Web, App, DB) with high security and scalability. Explain subnets, route tables, gateways, and security groups.

Answer: Use public subnets for ALB, private subnets for App, isolated private subnets for DB; attach IGW/NAT appropriately and restrict access via security groups.

9. You suspect unusual traffic inside your VPC. How would you monitor and analyze network traffic?

Answer: Enable VPC Flow Logs and analyze using CloudWatch, GuardDuty, or Traffic Mirroring.

10. Why can't a private subnet have an Internet Gateway directly attached?

Answer: An Internet Gateway attaches to the VPC, not to individual subnets; private subnets simply lack a route to it.

11. What happens if route tables are misconfigured in a VPC?

Answer: Traffic will fail to reach intended destinations, causing connectivity issues or outages.

12. What happens if a route table has no local route?

Answer: Instances within the VPC will not be able to communicate with each other.

13. An EC2 instance allows traffic on port 80 in the security group, but traffic is still blocked. What could be the reason?

Answer: Possible causes include NACL blocking, OS firewall rules, missing public IP, incorrect routing, or the web service not running.

14. You need to create a VPC that will host 1,000+ EC2 instances across multiple AZs. How do you decide the CIDR block?

Answer: Select a sufficiently large CIDR (e.g., /21 or /20) and divide it into multiple subnets across AZs for scalability.

15. Only a company's corporate IP should be able to SSH into EC2 instances. How would you implement this securely in AWS VPC?

Answer: Configure the security group to allow port 22 access only from the corporate public IP address (/32).

16. An EC2 instance can send traffic out but cannot receive responses. Which VPC component might be misconfigured and why?

Answer: Likely a Network ACL blocking inbound return traffic (ephemeral ports) or asymmetric routing issue.

