

## AWS Task-2

### Task Description:

Set up a VPC with an Internet gateway, create a public subnet with 256 IP addresses, a private subnet with 256 IP addresses, make a route table connecting the Internet gateway and the subnets, and launch a Linux EC2 instance by using the above VPC and public subnet.

### Part A: Base VPC & Public EC2 Setup

**Step 1:** Create a VPC

**Step 2:** Create public and private subnets (256 IPs each)

**Step 3:** Create and attach an Internet Gateway

**Step 4:** Public Route Table configuration and Internet Gateway association

**Step 5:** Create a Security Group

**Step 6:** Verify Network ACLs

**Step 7:** Launch a Linux EC2 Instance in the Public Subnet

**Step 8:** Verify EC2 Instance and Web Access

### Part B: DMZ Setup & Private Subnet Access

**Step 9:** Create a security group for private subnet

**Step 10:** Launch an EC2 instance in the private subnet

**Step 11:** Connect to the private server via the public server (bastion host)

### Part C: Public Subnet Internet Access using NAT Gateway

**Step 12:** Create a NAT Gateway and allocate an Elastic IP

**Step 13:** Create a private route table and associate the NAT Gateway with it

**Step 14:** Verify private subnet access to the internet

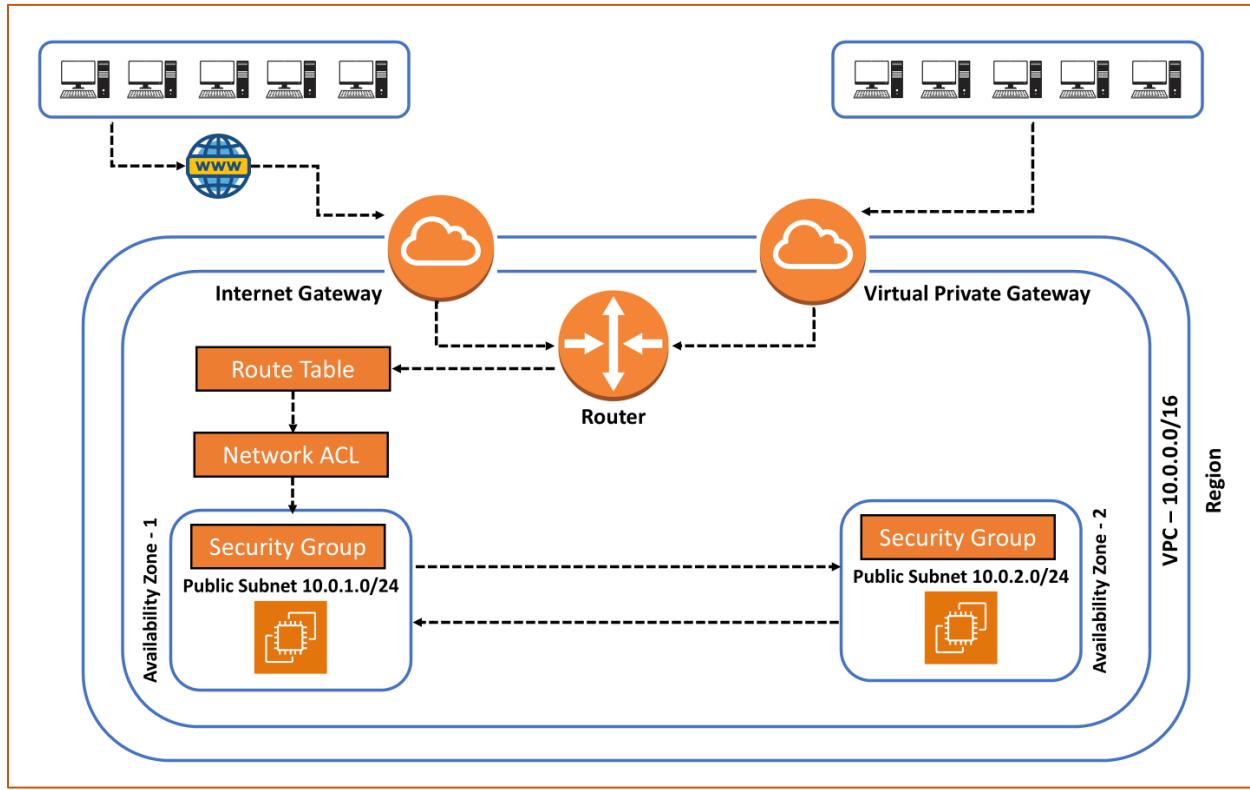
**Step 15:** Restrict direct internet access for the private subnet

### Part D : Clean up

Delete all created AWS resources

- NAT Gateway
- Elastic IP
- EC2 Instances
- Custom VPC and associated components

## VPC Architecture:



This architecture showcases a standard AWS network design using a VPC, public and private subnets, bastion host access, and NAT Gateway–based internet connectivity. The following steps outline the AWS networking and EC2 setup implemented as part of this task.

- Created a VPC with CIDR block **10.0.0.0/16**.
- Created a **public subnet (10.0.1.0/24)** and a **private subnet (10.0.2.0/24)**, each supporting 256 IP addresses.
- Created an **Internet Gateway (IGW)** and attached it to the VPC.
- **Modified the default route table** by adding the route **0.0.0.0/0 → Internet Gateway** and associated it with the public subnet.
- Created a **security group** allowing **SSH (22)** and **HTTP (80)** access from the internet.
- Verified that **Network ACLs** allow the required inbound and outbound traffic.
- Launched a **Linux EC2 instance** in the public subnet.
- Verified EC2 instance connectivity and web access from the internet.
- Created a **security group for the private subnet** allowing SSH access only from the public subnet security group.
- Launched a **Linux EC2 instance** in the private subnet with no public IP assigned.
- Connected to the private EC2 instance via the public EC2 instance (**bastion host**) using SSH.

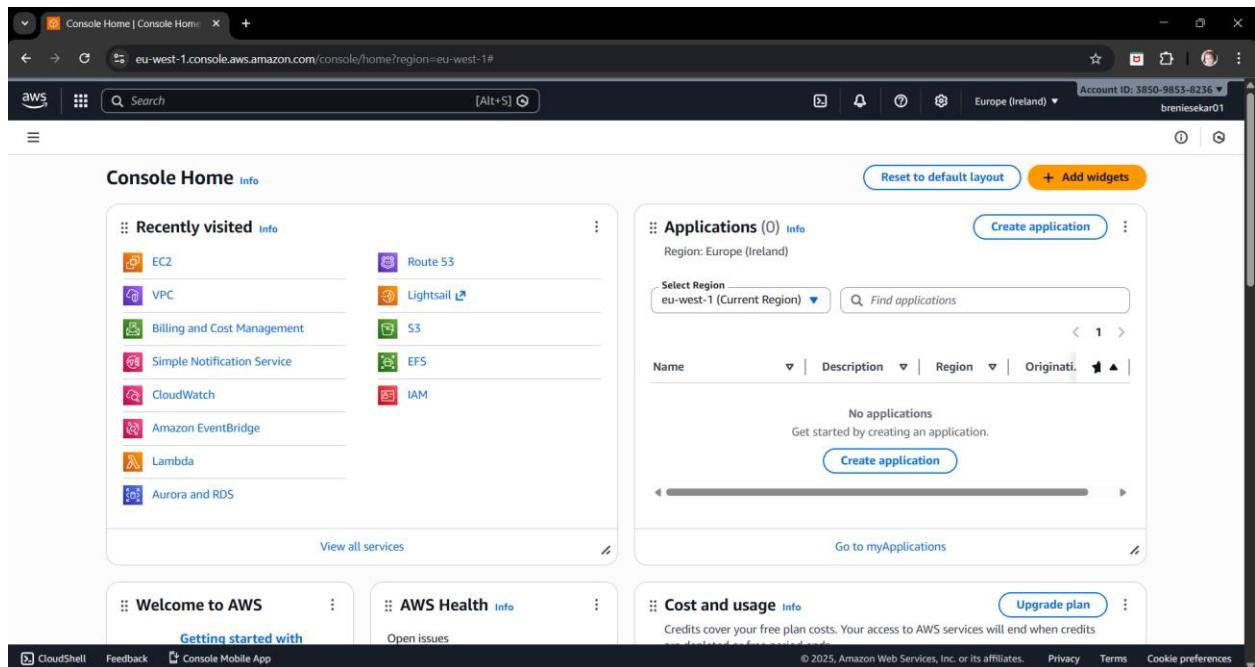
- Created a **NAT Gateway** in the public subnet and allocated an **Elastic IP address**.
- Created a **private route table** with route **0.0.0.0/0 → NAT Gateway** and associated it with the private subnet.
- Verified that the private EC2 instance can access the internet (e.g., software updates).
- Ensured that no direct Internet Gateway route exists for the private subnet.
- Terminated both public and private EC2 instances.
- Deleted the NAT Gateway and released the Elastic IP address.
- Deleted route tables, security groups, subnets, Internet Gateway, and finally the custom VPC.

## Part A : Base VPC & Public EC2 Setup

### Step 1: Create a VPC

A VPC is a logically isolated network in AWS used to deploy and manage cloud resources securely.

- A custom VPC named **custVPC01** was created in the **eu-west-1 (Ireland) region** using the AWS Management Console.
- The VPC was assigned an IPv4 CIDR block of **10.0.0.0/16**, providing sufficient IP addresses for public and private subnets.
- AWS automatically created a default route table and network ACL for the VPC.
- The VPC was successfully created and is in the **Available** state.



The screenshot shows the AWS VPC dashboard for the eu-west-1 region. On the left, there's a sidebar with navigation links for VPCs, Subnets, Route tables, Internet gateways, Egress-only internet gateways, DHCP option sets, Elastic IPs, Managed prefix lists, NAT gateways, Peering connections, Route servers, Security groups, and AWS Network Manager. The main content area displays 'Resources by Region' with sections for VPCs, Subnets, Route Tables, Internet Gateways, and Egress-only Internet Gateways, each showing counts for Ireland 1 and Ireland 3. There are also sections for Endpoint Services, NAT Gateways, VPC Peering Connections, Network ACLs, and Security Groups. A 'Create VPC' button and a 'Launch EC2 Instances' button are at the top. On the right, there are boxes for Service Health, Settings (including Block Public Access and Zones), Additional Information (VPC Documentation, All VPC Resources, Forums, Report an Issue), and AWS Network Manager. The bottom of the page includes CloudShell, Feedback, and Console Mobile App links, along with copyright and legal information.

The screenshot shows the 'Create VPC' configuration page. At the top, it says 'Create VPC' and 'Info'. Below that, it says 'A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.' Under 'VPC settings', there's a section for 'Resources to create' with 'VPC only' selected. There's also a 'Name tag - optional' field containing 'custVPC01'. The 'IPv4 CIDR block' section has 'IPv4 CIDR manual input' selected and contains the value '10.0.0.0/16'. The 'IPv6 CIDR block' section has 'No IPv6 CIDR block' selected. At the bottom, there are CloudShell, Feedback, and Console Mobile App links, along with copyright and legal information.

CreateVpc | VPC | eu-west-1

eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#CreateVpc:createMode=vpcOnly

aws Search [Alt+S]

Account ID: 3850-9853-8236 Europe (Ireland) breniesekar01

VPC > Your VPCs > Create VPC

No IPv6 CIDR block (selected)

- 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 (\$)

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: Name Value - optional: custVPC01

Add tag

You can add 49 more tags

Cancel Preview code Create VPC

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

VPC | eu-west-1

eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#VpcDetails:VpcId=vpc-037f0d5b144ffe537

aws Search [Alt+S]

Account ID: 3850-9853-8236 Europe (Ireland) breniesekar01

VPC > Your VPCs > vpc-037f0d5b144ffe537

You successfully created vpc-037f0d5b144ffe537 / custVPC01

Actions

VPC dashboard AWS Global View Filter by VPC

Virtual private cloud Your VPCs Subnets Route tables Internet gateways Egress-only internet gateways DHCP option sets Elastic IPs Managed prefix lists NAT gateways Peering connections Route servers Security Network ACLs Security groups

Details Info

VPC ID: vpc-037f0d5b144ffe537	State: Available	Block Public Access: Off	DNS hostnames: Disabled
DNS resolution: Enabled	Tenancy: default	DHCP option set: dopt-08eb5d48179324311	Main route table: rtb-0c89db1ccb8ea859
Main network ACL: acl-08e6f0687979e13e8	Default VPC: No	IPv4 CIDR: 10.0.0.0/16	IPv6 pool: -
IPv6 CIDR: -	Network Address Usage metrics: Disabled	Route 53 Resolver DNS Firewall rule groups: -	Owner ID: 385098538236
Encryption control ID: -	Encryption control mode: -	Show all details	

Resource map

Resource map Info

VPC	Subnets (0)	Route tables (1)
-----	-------------	------------------

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

Your VPCs

VPCs | VPC encryption controls

Your VPCs (1/2) Info

Name	VPC ID	State	Encryption c...	Encryption control ...	Block Public...	IPv...
<input checked="" type="checkbox"/> defaultVPC	vpc-Of015a10b4b968d24	Available	-	-	Off	172
<input type="checkbox"/> custVPC01	vpc-037f0d5b144ffe537	Available	-	-	Off	10.0

vpc-Of015a10b4b968d24 / defaultVPC

Details | Resource map | CIDRs | Flow logs | Tags | Integrations

**Details**

VPC ID vpc-Of015a10b4b968d24	State Available	Block Public Access Off	DNS hostnames Enabled
DNS resolution Enabled	Tenancy default	DHCP option set dopt-08eb5d48179324311	Main route table rtb-08cf603592fec862f
Main network ACL lambda-Of015a10b4b968d24	Default VPC VPC	IPv4 CIDR 172.31.0.0/16	IPv6 pool

## Step 2: Create public and private subnets (256 IPs each)

A subnet is a logical subdivision of a VPC that defines a range of IP addresses where AWS resources such as EC2 instances can be launched.

- Two subnets were created within the custom VPC **custVPC01**.
- A **public subnet** named **sn01-pub** was created with the CIDR block **10.0.1.0/24**, providing 256 IP addresses.
- A **private subnet** named **sn02-priv** was created with the CIDR block **10.0.2.0/24**, also providing 256 IP addresses.
- Both subnets were created within the VPC CIDR range **10.0.0.0/16**.
- The subnets were successfully created and are in the **Available** state.

Screenshot of the AWS VPC Subnets page in the eu-west-1 region.

The left sidebar shows the VPC dashboard and various cloud services like Route tables, Internet gateways, and Security groups.

The main content area displays a table of existing subnets:

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
-	subnet-02606b7a6d79b98a5	Available	vpc-0f015a10b4b968d24   defa...	Off	172.31.0.0/20
-	subnet-04c62c45c4abc99f6	Available	vpc-0f015a10b4b968d24   defa...	Off	172.31.32.0/20
-	subnet-0600722a47f09067c	Available	vpc-0f015a10b4b968d24   defa...	Off	172.31.16.0/20

A "Create subnet" button is located at the top right of the table.

Screenshot of the "Create subnet" wizard in the eu-west-1 region.

The top navigation bar shows the current step: "Create subnet".

The left sidebar shows the VPC dashboard and various cloud services.

The main content area is divided into sections:

- VPC**: Shows the selected VPC ID: `vpc-037f0d5b144ffe557 (custVPC01)`.
- Associated VPC CIDRs**: Shows the IPv4 CIDR: `10.0.0.0/16`.
- Subnet settings**: A summary section stating: "Specify the CIDR blocks and Availability Zone for the subnet." It includes a note: "The name can be up to 256 characters long."
- Subnet 1 of 1**:
  - Subnet name**: Input field containing `my-subnet-01`. A note says: "Create a tag with a key of 'Name' and a value that you specify." Another note says: "The name can be up to 256 characters long."
  - Availability Zone**: A dropdown menu showing "us-east-1a" and "us-east-1b".

At the bottom, standard AWS footer links are visible: CloudShell, Feedback, Console Mobile App, Privacy, Terms, and Cookie preferences.

VPC | eu-west-1

eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#CreateSubnet

aws Search [Alt+S]

Subnets Create subnet

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

**Availability Zone** Europe (Ireland) / euw1-az2 (eu-west-1a)

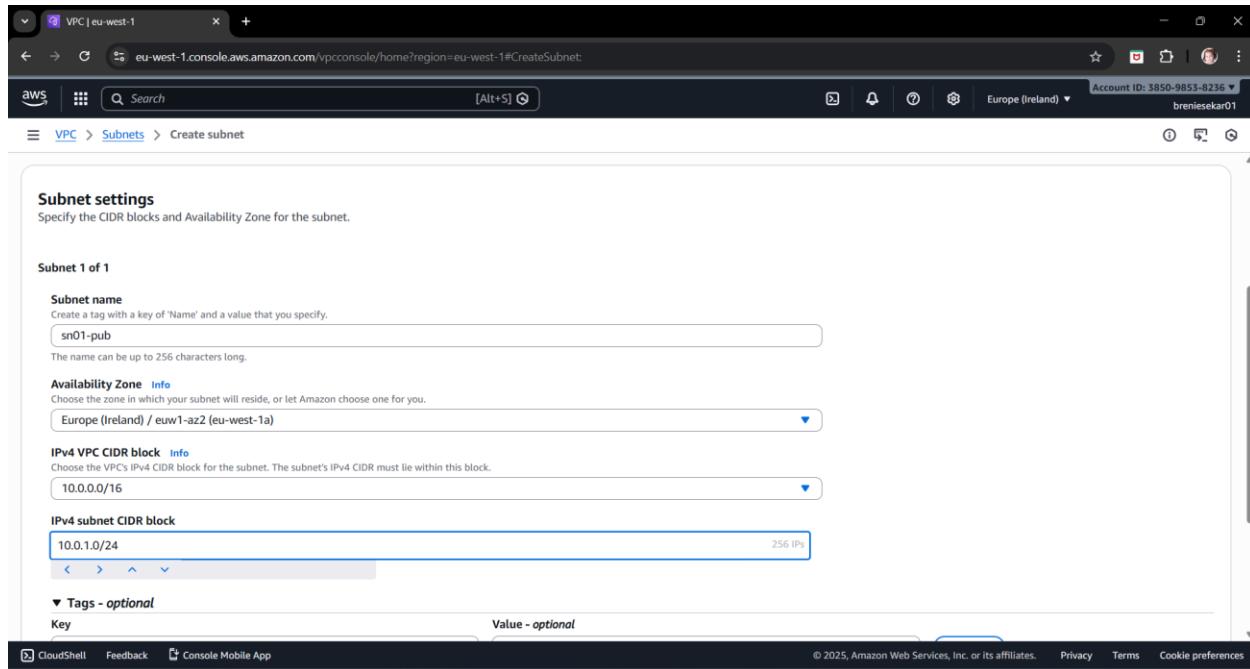
**IPv4 VPC CIDR block** 10.0.0.0/16

**IPv4 subnet CIDR block** 10.0.1.0/24 (256 IPs)

**Tags - optional**

Key	Value - optional
Q Name	sn01-pub

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



VPC | eu-west-1

eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#CreateSubnet

aws Search [Alt+S]

Subnets Create subnet

**Availability Zone** Europe (Ireland) / euw1-az2 (eu-west-1a)

**IPv4 VPC CIDR block** 10.0.0.0/16

**IPv4 subnet CIDR block** 10.0.1.0/24 (256 IPs)

**Tags - optional**

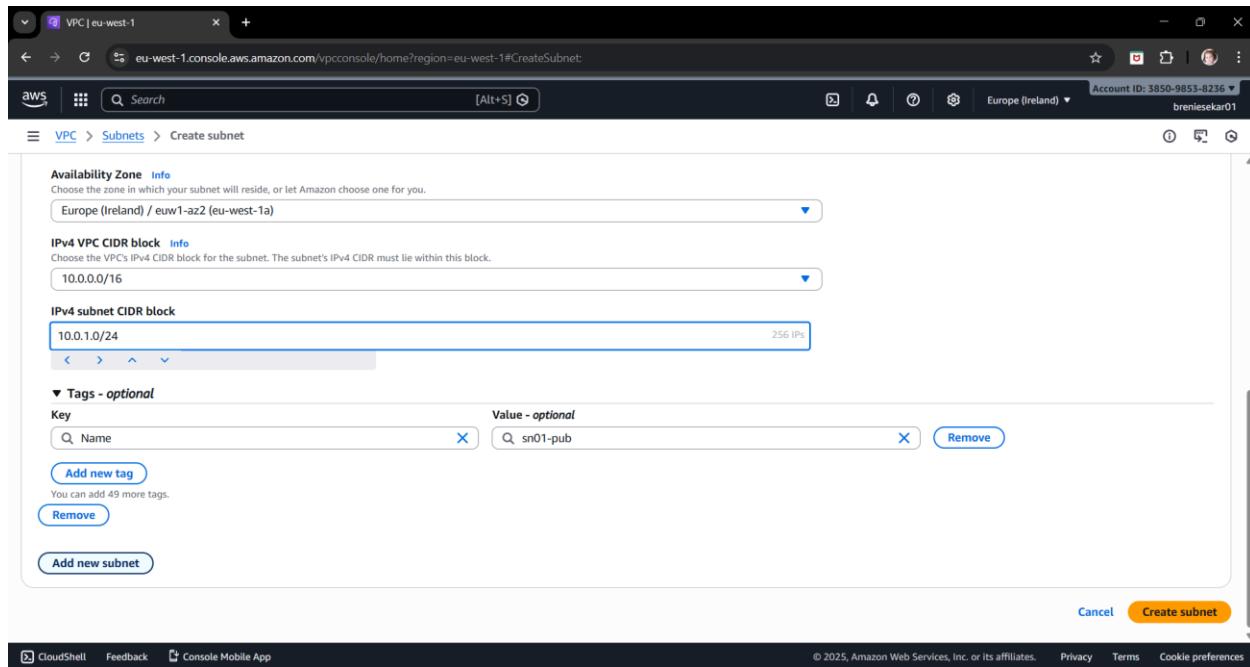
Key	Value - optional
Q Name	sn01-pub

Add new tag Remove  
You can add 49 more tags.

Add new subnet

Cancel Create subnet

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



VPC | eu-west-1

eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#CreateSubnet:

Subnet 2 of 2

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

**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.

**IPv4 subnet CIDR block**  
 256 IPs

**Tags - optional**

Key	Value - optional
<input type="text" value="Name"/> <input type="button" value="X"/>	<input type="text" value="sn02-priv"/> <input type="button" value="Remove"/>

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

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

VPC | eu-west-1

eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#CreateSubnet:

Subnet 2 of 2

**Availability Zone** [Info](#)  
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

**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.

**IPv4 subnet CIDR block**  
 256 IPs

**Tags - optional**

Key	Value - optional
<input type="text" value="Name"/> <input type="button" value="X"/>	<input type="text" value="sn02-priv"/> <input type="button" value="Remove"/>

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

[Add new subnet](#)

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

You have successfully created 2 subnets: subnet-0b75b67eee6db0a7c, subnet-0051699bf17ab344a

Last updated less than a minute ago

Subnets (2) Info

Subnet ID : subnet-0b75b67eee6db0a7c Subnet ID : subnet-0051699bf17ab344a Clear filters

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
sn02-priv	subnet-0051699bf17ab344a	Available	vpc-037f0d5b144ffe537   custV...	Off	10.0.2.0/24
sn01-pub	subnet-0b75b67eee6db0a7c	Available	vpc-037f0d5b144ffe537   custV...	Off	10.0.1.0/24

Select a subnet

You have successfully created 2 subnets: subnet-0b75b67eee6db0a7c, subnet-0051699bf17ab344a

Last updated 1 minute ago

Subnets (5) Info

Subnet ID : subnet-02606b7a6d79b98a3 Subnet ID : subnet-04c62c45c4abc99f6 Subnet ID : subnet-0600722a47f09067c Subnet ID : subnet-0051699bf17ab344a Subnet ID : subnet-0b75b67eee6db0a7c Clear filters

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
-	subnet-02606b7a6d79b98a3	Available	vpc-0f015a10b4b968d24   defa...	Off	172.31.0.0/20
-	subnet-04c62c45c4abc99f6	Available	vpc-0f015a10b4b968d24   defa...	Off	172.31.32.0/20
-	subnet-0600722a47f09067c	Available	vpc-0f015a10b4b968d24   defa...	Off	172.31.16.0/20
sn02-priv	subnet-0051699bf17ab344a	Available	vpc-037f0d5b144ffe537   custV...	Off	10.0.2.0/24
sn01-pub	subnet-0b75b67eee6db0a7c	Available	vpc-037f0d5b144ffe537   custV...	Off	10.0.1.0/24

Select a subnet

### Step 3: Create and attach an Internet Gateway

An Internet Gateway is an AWS-managed component that allows resources inside a VPC to communicate with the public internet. The Internet Gateway was **not automatically created** when the custom VPC **custVPC01** was created.

- An Internet Gateway was created to enable communication between the VPC and the public internet.

- The Internet Gateway was attached to the custom VPC **custVPC01**.
- This allows resources in the public subnet to send and receive internet traffic.
- The Internet Gateway was named **custvpc01-igw** with the ID **igw-014b5331fc12c0826**.
- The Internet Gateway state is **Attached**, confirming it is actively associated with the VPC.

The screenshot shows two browser windows side-by-side. The top window displays the 'Internet gateways' list for the 'eu-west-1' region. It shows one entry: 'igw-090ac2ce5ff21c1cf' (Name), 'Attached' (State), and 'vpc-0f015a10b4b968d24 | defaultVPC' (VPC ID). The bottom window shows the 'Create internet gateway' wizard. In the 'Internet gateway settings' step, a 'Name tag' is being added with the value 'custvpc01-igw'. Below this, under 'Tags - optional', a single tag 'Name: custvpc01-igw' is listed. At the bottom right of the wizard are 'Cancel' and 'Create Internet gateway' buttons.

**Internet gateways (1) Info**

Name	Internet gateway ID	State	VPC ID	Owner
-	igw-090ac2ce5ff21c1cf	Attached	vpc-0f015a10b4b968d24   defaultVPC	385098538236

Select an internet gateway above

**Create internet gateway** Info

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

**Internet gateway settings**

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

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

Key	Value - optional	Remove
<input type="text" value="Name"/>	<input type="text" value="custvpc01-igw"/>	<input type="button" value="Remove"/>

You can add 49 more tags.

VPC | eu-west-1

eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#InternetGateway:InternetGatewayId=igw-014b5331fc12c0826

AWS Search [Alt+S]

Europe (Ireland) Account ID: 3850-9853-8236 brenieskar01

VPC > Internet gateways > igw-014b5331fc12c0826

The following internet gateway was created: igw-014b5331fc12c0826 - custvc01-igw. You can now attach to a VPC to enable the VPC to communicate with the internet.

igw-014b5331fc12c0826 / custvc01-igw

Attach to a VPC Actions

**Details**

Internet gateway ID igw-014b5331fc12c0826	State Detached	VPC ID -	Owner 385098538236
--	-------------------	-------------	-----------------------

**Tags (1)**

Key	Value
Name	custvc01-igw

Manage tags

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

VPC | eu-west-1

eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#AttachInternetGateway:InternetGatewayId=igw-014b5331fc12c0826

AWS Search [Alt+S]

Europe (Ireland) Account ID: 3850-9853-8236 brenieskar01

VPC > Internet gateways > Attach to VPC (igw-014b5331fc12c0826)

The following internet gateway was created: igw-014b5331fc12c0826 - custvc01-igw. You can now attach to a VPC to enable the VPC to communicate with the internet.

Attach to a VPC

**Attach to VPC (igw-014b5331fc12c0826)**

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

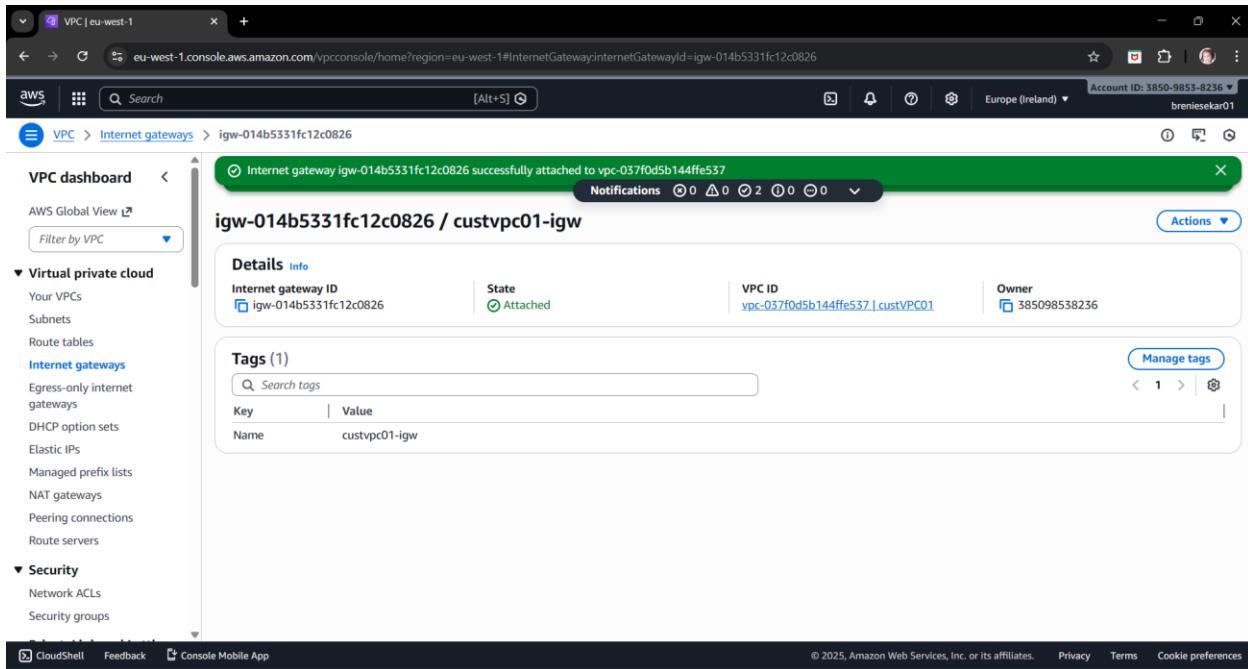
**Available VPCs**  
Attach the internet gateway to this VPC.

vpc-037f0d5b144ffe537

AWS Command Line Interface command

Cancel Attach internet gateway

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



## Step 4: Public Route Table configuration and Internet Gateway association

A routing table controls how network traffic is directed within a VPC.

- When the custom VPC was created, AWS automatically created a default route table.
- The default route table contained a local route that allowed communication within the VPC CIDR range.
- By default, the route table did not provide internet access.
- The renamed route table **custVPC-PubRt01** was used to enable internet connectivity for the public subnet.
- A new route was added with the destination set to **0.0.0.0/0**.
- The target for this route was the Internet Gateway **igw-014b5331fc12c0826**.
- The public subnet was associated with the default route table.
- This configuration enabled resources in the public subnet to communicate with the outside world through the Internet Gateway.

RouteTables | VPC | eu-west-1

eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#RouteTables:

VPC dashboard < Route tables

Route tables (1/2) Info

Last updated 1 minute ago Actions Create route table

Name	Route table ID	Explicit subnet assoc...	Edge associations	Main	VPC
rtb-08cf603592fec862f	-	-	-	Yes	vpc-0f015a10b4b968d24   defa.
Edit Name custVPC-PubRt01	0c89d0b1ccb8ea859	-	-	Yes	vpc-037f0d5b144ffe537   custV.

rtb-0c89d0b1ccb8ea859

Details Routes Subnet associations Edge associations Route propagation Tags

Details

Route table ID rtb-0c89d0b1ccb8ea859	Main <input checked="" type="checkbox"/> Yes	Explicit subnet associations -	Edge associations -
---	---	-----------------------------------	------------------------

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

CloudShell Feedback Console Mobile App

VPC | eu-west-1

eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#RouteTableDetails:RouteTableId=rtb-0c89d0b1ccb8ea859

VPC dashboard < Route tables > rtb-0c89d0b1ccb8ea859

rtb-0c89d0b1ccb8ea859 / custVPC-PubRt01 Actions

Details Info

Route table ID rtb-0c89d0b1ccb8ea859	Main <input checked="" type="checkbox"/> Yes	Explicit subnet associations -	Edge associations -
VPC vpc-037f0d5b144ffe537   custVPC01	Owner ID 385098538236		

Routes Subnet associations Edge associations Route propagation Tags

Routes (1)

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

Both Edit routes

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

CloudShell Feedback Console Mobile App

**Edit routes**

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	CreateRouteTable
Q 0.0.0.0/0	Internet Gateway	-	No	CreateRoute
	Q igw-014b5331fc12c0826	-		

Add route Remove Cancel Preview Save changes

Updated routes for rtb-0c89d0b1ccb8ea859 / custVPC-PubRt01 successfully

rtb-0c89d0b1ccb8ea859 / custVPC-PubRt01

**Details** Info

Route table ID rtb-0c89d0b1ccb8ea859	Main Yes	Explicit subnet associations -	Edge associations -
VPC vpc-037f0d5b144ffe537   custVPC01	Owner ID 385098538236		

**Routes** (2)

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-014b5331fc12c0826	Active	No	Create Route
10.0.0.0/16	local	Active	No	Create Route Table

## Step 5: Create a Security Group

A Security Group is a virtual firewall in AWS that controls inbound and outbound network traffic for resources such as EC2 instances within a VPC. It is a **stateful firewall** and supports only allow rules—there are no explicit deny rules.

- Navigate to **VPC → Security Groups → Create security group**

- A public subnet security group named **pubsg01-pubsn01** was created to control inbound and outbound traffic for public-facing resources.
- The security group was created by navigating to **VPC → Security Groups → Create security group**.
- The custom VPC **custVPC01** was selected while creating this security group.
- This security group is associated with resources launched in the **public subnet (sn01-pub)**.
- **Inbound Rules:**
  - SSH access is allowed on port 22 from any IPv4 (0.0.0.0/0) and any IPv6 (::/0) address.
  - HTTP access is allowed on port 80 from any IPv4 (0.0.0.0/0) and any IPv6 (::/0) address.
- **Outbound Rules:**

All outbound traffic is allowed by default.

The screenshot shows the AWS VPC Security Groups page. The left sidebar includes links for Gateways, DHCP option sets, Elastic IPs, Managed prefix lists, NAT gateways, Peering connections, Route servers, Security (Network ACLs, Security groups), PrivateLink and Lattice (Getting started, Endpoints, Endpoint services, Service networks, Lattice services, Resource configurations, Resource gateways, Target groups, Domain verifications), and DNS firewall. The main content area displays a table titled "Security Groups (2)" with the following data:

Name	Security group ID	Security group name	VPC ID	Description
-	sg-04f71b34a105af264	default	vpc-0f015a10b4b968d24	default VPC security
-	sg-0cd7d98ce19757ea9	default	vpc-037f0d5b144ffe537	default VPC security

Below the table, a section titled "Select a security group" is visible.

VPC | eu-west-1

eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#CreateSecurityGroup:

aws Search [Alt+S] Europe (Ireland) Account ID: 3850-9853-8236 breniesekar01

**Create security group** Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

**Basic details**

Security group name Info  
pubsg01-pubsn01  
Name cannot be edited after creation.

Description Info  
pubsg01-pubsn01

VPC Info  
vpc-037f0d5b144ffe537 (custVPC01)

**Inbound rules** Info

This security group has no inbound rules.

[Add rule](#)

**Outbound rules** Info

Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Destination <small>Info</small>	Description - optional <small>Info</small>
CloudShell	Feedback	Console Mobile App		© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

VPC | eu-west-1

eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#CreateSecurityGroup:

aws Search [Alt+S] Europe (Ireland) Account ID: 3850-9853-8236 breniesekar01

**Create security group**

vpc-037f0d5b144ffe537 (custVPC01)

**Inbound rules** Info

Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Source <small>Info</small>	Description - optional <small>Info</small>
SSH	TCP	22	Anywhere <input type="button" value="Delete"/>	0.0.0.0/0 <input type="button" value="Delete"/>
SSH	TCP	22	Anywhere <input type="button" value="Delete"/>	::/0 <input type="button" value="Delete"/>
HTTP	TCP	80	Anywhere <input type="button" value="Delete"/>	0.0.0.0/0 <input type="button" value="Delete"/>
HTTP	TCP	80	Anywhere <input type="button" value="Delete"/>	::/0 <input type="button" value="Delete"/>

[Add rule](#)

⚠ 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.

**Outbound rules** Info

Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Destination <small>Info</small>	Description - optional <small>Info</small>
CloudShell	Feedback	Console Mobile App		© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

VPC | eu-west-1

eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#CreateSecurityGroup:

aws Search [Alt+S] Europe (Ireland) Account ID: 3850-9853-8236 brenilesekar01

VPC > Security Groups > Create security group

⚠ 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.

**Outbound rules - Info**

Type	Info	Protocol	Info	Port range	Info	Destination	Info	Description - optional	Info
All traffic	▼	All	All	Custom	▼	0.0.0.0/0	X	Delete	Add rule

⚠ Rules with destination of 0.0.0.0/0 or ::/0 allow your instances to send traffic to any IPv4 or IPv6 address. We recommend setting security group rules to be more restrictive and to only allow traffic to specific known IP addresses.

**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 tags

Create security group

VPC | eu-west-1

eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#SecurityGroup:groupId=sg-0395edf245b3c525a

aws Search [Alt+S] Europe (Ireland) Account ID: 3850-9853-8236 brenilesekar01

VPC > Security Groups > sg-0395edf245b3c525a - pubsg01-pubsn01

Security group (sg-0395edf245b3c525a | pubsg01-pubsn01) was created successfully

Details

Security group name	sg-0395edf245b3c525a	Security group ID	sg-0395edf245b3c525a	Description	pubsg01-pubsn01	VPC ID	vpc-037f0d5b14ffe537
Owner	385098538236	Inbound rules count	4 Permission entries	Outbound rules count	1 Permission entry		

Inbound rules | Outbound rules | Sharing | VPC associations | Tags

Inbound rules (4)

Name	Security group rule ID	IP version	Type	Protocol	Port range
-	sgr-03e506b1db9f01534	IPv6	SSH	TCP	22
-	sgr-0c57285ed8dc9bdfd	IPv6	HTTP	TCP	80
-	sgr-096e32f14a7824f26	IPv4	HTTP	TCP	80
-	sgr-01d73ffb2b1bd4ba9	IPv4	SSH	TCP	22

Manage tags | Edit inbound rules

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the AWS VPC Security Groups console in the eu-west-1 region. A success message at the top indicates "Security group (sg-0395edf245b3c525a | pubsg01-pubsn01) was created successfully". The main table displays three security groups: "sg-04f71b34a105af264" (Name: pubsg01-pubsn01, Security group ID: sg-04f71b34a105af264, VPC ID: vpc-0f015a10b4b968d24), "pubsg01-pubsn01" (Name: pubsg01-pubsn01, Security group ID: sg-0395edf245b3c525a, VPC ID: vpc-037f0d5b144ffe537), and "sg-0395edf245b3c525a" (Name: default, Security group ID: sg-0395edf245b3c525a, VPC ID: vpc-037f0d5b144ffe537). The "Details" tab is selected for the first group. The "Edit Name" field contains "pubsg01-pubsn01". The "Save" button is highlighted in orange.

This screenshot is identical to the one above, showing the AWS VPC Security Groups console with the same success message and table of security groups. The "sg-0395edf245b3c525a" row is now expanded, revealing its details. The "Edit Name" field now contains "sg-0395edf245b3c525a - pubsg01-pubsn01". The "Save" button is still highlighted in orange.

## Step 6: Verify Network ACLs

Network ACL (NACL) is a **stateless, subnet-level** firewall that controls inbound and outbound traffic for subnets in a VPC.

- Verified that the **default Network ACL** is associated with the required subnets.
- Confirmed that **Rule 100** allows **all inbound traffic** from 0.0.0.0/0.

- Ensured that the **default deny rule (\*)** is present at the end of the rule list.
- This confirms that required inbound traffic is explicitly allowed, while all other traffic is denied by default.

Screenshot of the AWS VPC Network ACLs page (eu-west-1 console.aws.amazon.com/vpcconsole/home?region=eu-west-1#acl:).

The left sidebar shows navigation links for VPC, Security, PrivateLink and Lattice, and DNS firewall.

The main content displays a table of Network ACLs:

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound
-	acl-0e90e0154153341e6	3 Subnets	Yes	vpc-0f015a10b4b968d24 / defaultVPC	2 Inbou
-	acl-08e6f0687979e13e8	2 Subnets	Yes	vpc-037f0d5b144ffe537 / custVPC01	2 Inbou

Below the table, a section titled "Select a network ACL" lists "acl-08e6f0687979e13e8".

Screenshot of the AWS VPC Network ACL details page (eu-west-1 console.aws.amazon.com/vpcconsole/home?region=eu-west-1#NetworkAclDetails:networkAclId=acl-08e6f0687979e13e8).

The left sidebar shows navigation links for VPC, Security, PrivateLink and Lattice, and DNS firewall.

The main content displays the details for Network ACL ID "acl-08e6f0687979e13e8".

Network ACL ID	Associated with	Default	VPC ID
acl-08e6f0687979e13e8	2 Subnets	Yes	vpc-037f0d5b144ffe537 / custVPC01

The "Inbound rules" tab is selected, showing two rules:

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

## Step 7: Launch a Linux EC2 Instance in the Public Subnet

- A new **EC2 instance** was launched.
- The instance was named **pubWebServer01**.
- The **Ubuntu Server 24.04 LTS (HVM), SSD Volume Type** AMI was selected.
- The instance type **t3.micro** was chosen.
- The instance was launched in the **CustVPC01** network.
- The **public subnet sn01-pub** was selected.
- **Auto-assign Public IP** was enabled.
- The security group **pubsg01-pubsn01** was associated with the instance.
- The root storage size was configured as **10 GB**.
- A **user data (bootstrap) script** was added to install Apache and deploy web content.

```
#!/bin/bash
apt install wget unzip apache2 -y
cd /tmp
wget https://www.tooplate.com/zip-templates/2139_neural_portfolio.zip
unzip 2139_neural_portfolio.zip
mv /tmp/2139_neural_portfolio/* /var/www/html/
```

- The instance configuration was reviewed and the instance was successfully launched.

### Script Explanation:

Line	Command	Explanation
1	#!/bin/bash	Specifies the script should run using the Bash shell
2	apt install wget unzip apache2 -y	Installs <b>Apache web server</b> , <b>wget</b> , and <b>unzip</b> packages
3	cd /tmp	Changes directory to /tmp
4	wget https://www.tooplate.com/zip-templates/2139_neural_portfolio.zip	Downloads the website template ZIP file
5	unzip 2139_neural_portfolio.zip	Extracts the downloaded ZIP file
6	mv /tmp/2139_neural_portfolio/* /var/www/html/	Moves website files to Apache's web root directory

The screenshot shows the AWS EC2 Home page. On the left, a sidebar menu for 'EC2' includes 'Dashboard', 'AWS Global View', 'Events', 'Instances' (selected), 'Images', and 'Elastic Block Store'. The main content area features a large heading 'Amazon Elastic Compute Cloud (EC2)' and sub-headings 'Create, manage, and monitor virtual servers in the cloud.' Below this is a brief description of EC2's capabilities and a 'Launch a virtual server' button.

**Benefits and features**

**EC2 offers ultimate scalability and control**

Fully resizable compute capacity to support virtually any workload. This service is best if you want:

- Highest level of control of the entire technology stack, allowing full integration with all AWS services
- Widest variety of server size options
- Widest availability of operating systems to choose from including Linux, Windows, and macOS
- Global scalability

**Additional actions**

[View running instances](#)  
[Migrate a server](#)

**Pricing (US)**

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

The screenshot shows the 'Launch an instance' wizard. Step 1: Set instance details. It includes fields for 'Name and tags', 'Application and OS Images (Amazon Machine Image)', and 'Summary'. A message at the top says 'It seems like you may be new to launching instances in EC2. Take a walkthrough to learn about EC2, how to launch instances and about best practices.' Buttons for 'Take a walkthrough' and 'Do not show me this message again.' are present. The 'Summary' section shows 1 instance and provides options for 'Software Image (AMI)', 'Virtual server type (instance type)', 'Firewall (security group)', and 'Storage (volumes)'. Buttons for 'Cancel', 'Launch instance', and 'Preview code' are at the bottom.

Launch an instance | EC2 | eu-west-1

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

Search [Alt+S]

EC2 Instances Launch an instance

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)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type Canonical, Ubuntu, 24.04, amd64 noble image

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type Canonical, Ubuntu, 24.04, amd64 noble image

Description

Ubuntu Server 24.04 LTS (HVM) EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Canonical, Ubuntu, 24.04, amd64 noble image

CloudShell Feedback Console Mobile App

Number of instances [Info](#)

1

Software Image (AMI)

Canonical, Ubuntu, 24.04, amd64... [read more](#)

ami-0d9442a6cf8319180

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](#)

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

Launch an instance | EC2 | eu-west-1

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

Search [Alt+S]

EC2 Instances Launch an instance

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

Instance type

t3.micro

Family: t3 2 vCPU 1 GiB Memory Current generation: true

On-Demand RHEL base pricing: 0.0402 USD per Hour

On-Demand Ubuntu Pro base pricing: 0.0149 USD per Hour

On-Demand SUSE base pricing: 0.0114 USD per Hour

On-Demand Wind

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

Key pair name - required

Select

Network [Info](#)

vpc-0f015a10b4b968d24 | defaultVPC

Subnet [Info](#)

Create key pair

Key pair name [Info](#)

Key pairs allow you to connect to your instance securely.

aws-vpc-pem-kp-ireland

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](#)

Summary

Number of instances [Info](#)

1

Software Image (AMI)

Canonical, Ubuntu, 24.04, amd64... [read more](#)

ami-0d9442a6cf8319180

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](#)

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

Launch an instance | EC2 | eu-west-1

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

aws Search [Alt+S]

EC2 Instances Launch an instance

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

**Instance type**

t3.micro Free tier eligible

Family: t3 2 vCPU 1 GiB Memory Current generation: true

On-Demand RHEL base pricing: 0.0402 USD per Hour On-Demand Linux base pricing: 0.0114 USD per Hour

On-Demand Ubuntu Pro base pricing: 0.0149 USD per Hour

On-Demand SUSE base pricing: 0.0114 USD per Hour On-Demand Windows base pricing: 0.0206 USD per Hour

**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**

aws-vpc-pem-kp-ireland [Create new key pair](#)

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

**Network** [Info](#)

vpc-0f015a10b4b968d24 | defaultVPC

**Subnet** [Info](#)

CloudShell Feedback Console Mobile App

Recent download history

aws-vpc-pem-kp-ireland.pem 1.678 B • Done

Transformer Curriculum Brochure.pdf 13.7 MB • 1 day ago

Number of instances: 1

Software Image (AMI) Canonical, Ubuntu, 24.04, amd6... [read more](#)

ami-049442a6cf8319180

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](#)

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

Launch an instance | EC2 | eu-west-1

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

aws Search [Alt+S]

EC2 Instances Launch an instance

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

**VPC - required** [Info](#)

vpc-037fd5b144ffe537 (custVPC01) 10.0.0.0/16

**Subnet** [Info](#)

subnet-0b75b67eee6db0a7c sn01-pub

VPC: vpc-037fd5b144ffe537 Owner: 385098538236 Availability Zone: eu-west-1a (euw1-az2) Zone type: Availability Zone IP addresses available: 251 CIDR: 10.0.1.0/24

**Create new subnet**

**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

pubsg01-pubsn01 sg-0395edf245b3c525a [X](#)

VPC: vpc-037fd5b144ffe537

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

**Advanced network configuration**

CloudShell Feedback Console Mobile App

Recent download history

aws-vpc-pem-kp-ireland.pem 1.678 B • Done

Transformer Curriculum Brochure.pdf 13.7 MB • 1 day ago

Number of instances: 1

Software Image (AMI) Canonical, Ubuntu, 24.04, amd6... [read more](#)

ami-049442a6cf8319180

Virtual server type (instance type) t3.micro

Firewall (security group) pubsg01-pubsn01

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

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

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

Launch instance | EC2 | eu-west-1

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

EC2 > Instances > Launch an instance

VPC: vpc-037f0d5b144ff6537  
Security groups that you add or remove here will be added to or removed from all your network interfaces.

Advanced network configuration

Configure storage Info

1x 10 GiB gp3 Root volume, 3000 IOPS, Not encrypted

Add new volume

The selected AMI contains instance store volumes, however the instance does not allow any instance store volumes. None of the 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

Advanced details Info

Summary

Number of instances Info

1

Software Image (AMI)  
Canonical, Ubuntu, 24.04, amd64... [read more](#)  
ami-049442a6cf8319180

Virtual server type (instance type)  
t3.micro

Firewall (security group)  
pubsg01-pubsn01

Storage (volumes)  
1 volume(s) - 10 GiB

Cancel Launch instance Preview code

CloudShell Feedback Console Mobile App

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

Launch instance | EC2 | eu-west-1

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

EC2 > Instances > Launch an instance

Configure storage Info

1x 10 GiB gp3 Root volume, 3000 IOPS, Not encrypted

Add new volume

The selected AMI contains instance store volumes, however the instance does not allow any instance store volumes. None of the 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

Advanced details Info

Domain join directory Info

Select Create new directory

IAM instance profile Info

Select Create new IAM profile

Hostname type Info

Summary

Number of instances Info

1

Software Image (AMI)  
Canonical, Ubuntu, 24.04, amd64... [read more](#)  
ami-049442a6cf8319180

Virtual server type (instance type)  
t3.micro

Firewall (security group)  
pubsg01-pubsn01

Storage (volumes)  
1 volume(s) - 10 GiB

Cancel Launch instance Preview code

CloudShell Feedback Console Mobile App

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

The screenshot shows the 'Launch an instance' wizard in the AWS Management Console. On the left, there's a large text area for 'User data - optional' containing a base64-encoded shell script. On the right, the 'Summary' section shows the configuration: 1 instance, Canonical, Ubuntu 24.04 AMI, t3.micro instance type, and 1 volume (10 GiB). Buttons for 'Launch instance' and 'Preview code' are at the bottom.

```
#!/bin/bash
apt install wget unzip apache2 -y
cd /tmp
wget https://www.tooplate.com/zip-templates/2139_neural_portfolio.zip
unzip 2139_neural_portfolio.zip
mv /tmp/2139_neural_portfolio/* /var/www/html/
```

The screenshot shows the 'Launch an instance' wizard after a successful launch. A green success bar indicates 'Successfully initiated launch of instance (i-0428462c80b3c63b7)'. Below it, a 'Next Steps' section lists several options: Create billing usage alerts, Connect to your instance, Connect an RDS database, Create EBS snapshot policy, Manage detailed monitoring, Create Load Balancer, Create AWS budget, and Manage CloudWatch alarms. Each option has a corresponding button or link.

## Step 8: Verify EC2 Instance and Web Access

- The EC2 instance **pubWebServer01** was successfully launched and is in the **Running** state.
- The instance was assigned the public IPv4 address **108.130.74.208**.

- The Apache web server was installed and started using the **bootstrap script**.
- The public IP address 108.130.74.208 was accessed through a web browser.
- The **Neural Network Portfolio webpage** loaded successfully.
- This verified that the **public subnet, route table, Internet Gateway, security group, and Network ACLs** were correctly configured.

The screenshot shows the AWS EC2 Instances page. The left sidebar is collapsed, and the main area displays the following information:

**Instances (1/1) Info**

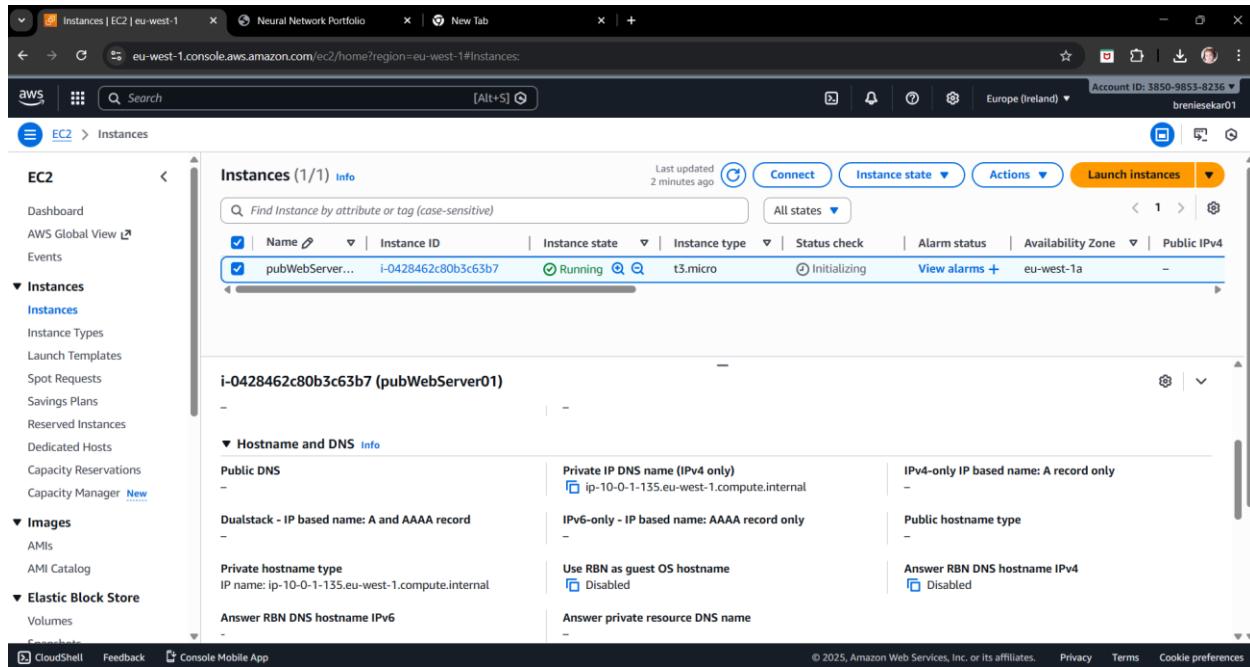
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
pubWebServer01	i-0428462c80b3c63b7	Running	t3.micro	Initializing		eu-west-1a	-

**i-0428462c80b3c63b7 (pubWebServer01)**

Availability zone ID euw1-az2	Outpost ID -
<b>IP addresses</b> <small>Info</small>	
Public IPv4 address 108.130.74.208   <a href="#">open address</a>	Private IPv4 addresses 10.0.1.135
Secondary private IPv4 addresses -	Carrier IP addresses (ephemeral) -

At the bottom of the page, there are links for CloudShell, Feedback, and Console Mobile App, along with copyright and legal information.

The screenshot shows a web browser window with the URL [108.130.74.208](http://108.130.74.208). The page has a dark background with a network-like pattern of green dots and lines. At the top, there's a navigation bar with links for HOME, ABOUT, PROJECTS, SKILLS, and CONTACT. The main title "NEURAL NETWORK" is prominently displayed in large white letters. Below it, the text "WEB DEVELOPER & DIGITAL ARCHITECT" is visible. In the top left corner, there's a logo consisting of three colored circles (blue, yellow, red) followed by the word "NEURAL".



## Part B: DMZ Setup & Private Subnet Access

A DMZ (Demilitarized Zone) setup is used to securely access private resources through a public-facing instance. In this architecture, the public subnet EC2 instance acts as a bastion/DMZ host. Private subnet instances are not directly accessible from the internet.

### Step 9 : Create a security group for private subnet

The purpose of the **private security group** is to allow secure SSH access from the **public subnet (DMZ host)** to the **private subnet**, enable basic connectivity testing using **ICMP**, and prevent direct internet access to private instances by following the **DMZ security architecture**.

- A new security group named **privsg01-privsn01** was created.
- The custom VPC **custVPC01** was selected while creating the security group.
- This security group is associated with instances launched in the **private subnet (sn02-priv)**.
- **Inbound Rules:**  
SSH access was allowed using **TCP port 22** from the **public subnet CIDR 10.0.1.0/24**. ICMP (IPv4) traffic was allowed from **10.0.1.0/24** for basic connectivity testing.
- **Outbound Rules:**  
All outbound traffic was allowed to **0.0.0.0/0**.

Screenshot of the AWS EC2 Security Groups page (eu-west-1.console.aws.amazon.com/ec2/home?region=eu-west-1#SecurityGroups):

The page shows a list of three security groups:

Name	Security group ID	Security group name	VPC ID	Description
-	sg-04f71b34a105af264	default	vpc-0f015a10b4b968d24	default VPC security
pubsg01-pubsn01	sg-0395edf245b3c525a	pubsg01-pubsn01	vpc-037f0d5b144ffe537	pubsg01-pubsn01
-	sg-0cd7d98ce19757ea9	default	vpc-037f0d5b144ffe537	default VPC security

Select a security group:

Screenshot of the Create security group page (eu-west-1.console.aws.amazon.com/ec2/home?region=eu-west-1#CreateSecurityGroup):

**Create security group**

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

**Basic details**

**Security group name**  Name cannot be edited after creation.

**Description**

**VPC**

**Inbound rules** Info

This security group has no inbound rules.

**Add rule**

**Outbound rules** Info

Type	Protocol	Port range	Destination	Description - optional
------	----------	------------	-------------	------------------------

Screenshot of the AWS EC2 Security Groups creation interface showing Inbound and Outbound rules.

**Inbound rules:**

- Type: SSH
- Protocol: TCP
- Port range: 22
- Source: Custom (10.0.1.0/24)
- Description: optional

**Outbound rules:**

- Type: All traffic
- Protocol: All
- Port range: All
- Destination: Custom (0.0.0.0/0)
- Description: optional

Message: **⚠️** Rules with destination of 0.0.0.0/0 or ::/0 allow your instances to send traffic to any IPv4 or IPv6 address. We recommend setting security group rules to be more restrictive and to only allow traffic to specific known IP addresses.

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Screenshot of the AWS EC2 Security Groups creation interface showing Outbound rules and Tags.

**Outbound rules:**

- Type: All traffic
- Protocol: All
- Port range: All
- Destination: Custom (0.0.0.0/0)
- Description: optional

Message: **⚠️** Rules with destination of 0.0.0.0/0 or ::/0 allow your instances to send traffic to any IPv4 or IPv6 address. We recommend setting security group rules to be more restrictive and to only allow traffic to specific known IP addresses.

**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 Create security group

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

**Security group (sg-018b30375f354a3f6 | privsg01-privsn01) was created successfully**

**sg-018b30375f354a3f6 - privsg01-privsn01**

**Details**

Security group name privsg01-privsn01	Security group ID sg-018b30375f354a3f6	Description privsg01-privsn01	VPC ID vpc-037f0d5b144ffe537
Owner 385098538236	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	

**Inbound rules**   **Outbound rules**   **Sharing**   **VPC associations**   **Tags**

**Inbound rules (2)**

Name	Security group rule ID	IP version	Type	Protocol	Port range
-	sgr-0afab506ecb22657	IPv4	SSH	TCP	22
-	sgr-0bf0c1dafcd8713ef	IPv4	All ICMP - IPv4	ICMP	All

## Step 10 : Launch an EC2 in the Private Subnet

This step launches an **EC2 instance in the private subnet** with **no direct internet access**, ensuring secure access only through the **DMZ (public subnet)** host.

- A new EC2 instance was launched.
- A name **dbServerPrivSn01** was assigned to the instance.
- An appropriate **Ubuntu Server AMI** was selected.
- The instance type **t3.micro** was chosen.
- The instance was launched in the **CustVPC01** network.
- The **private subnet (sn02-priv)** was selected.
- **Auto-assign Public IP** was set to **Disable**.
- The security group **privsg01-privsn01** was associated with the instance.
- Storage was configured using the **default settings**.
- The configuration was reviewed and the instance was successfully launched.

The screenshot shows the AWS EC2 home page in a web browser. The left sidebar contains a navigation menu with sections like EC2, Instances, Images, and Elastic Block Store. The main content area features a large banner for 'Amazon Elastic Compute Cloud (EC2)' with the subtext 'Create, manage, and monitor virtual servers in the cloud.' Below the banner, there's a section titled 'Benefits and features' with a sub-section 'EC2 offers ultimate scalability and control'. A call-to-action button 'Launch instance' is prominently displayed, along with other options like 'View dashboard' and 'Get started walkthroughs'. The bottom of the page includes a footer with copyright information and links to Privacy, Terms, and Cookie preferences.

The screenshot shows the 'Launch an instance' wizard, step 1: Set instance details. The top bar indicates the user is on the 'Instances' tab and has selected 'Launch an instance'. A blue header bar at the top says 'It seems like you may be new to launching instances in EC2. Take a walkthrough to learn about EC2, how to launch instances and about best practices' with buttons for 'Take a walkthrough' and 'Do not show me this message again.' The main form area starts with 'Name and tags' where the name 'dbServerPrivSn01' is entered. Below it is a section for 'Application and OS Images (Amazon Machine Image)' with a search bar and a list of recent AMIs: Amazon Linux, macOS, Ubuntu, Windows, Red Hat, SUSE Linux, and Debian. To the right, there are summary sections for 'Number of instances' (set to 1), 'Software Image (AMI)' (Amazon Linux 2023.9.2...), 'Virtual server type (instance type)' (t3.micro), 'Firewall (security group)' (New security group), and 'Storage (volumes)' (1 volume(s) - 8 GiB). At the bottom right are 'Cancel', 'Launch instance' (highlighted in orange), and 'Preview code' buttons.

Screenshot of the AWS EC2 Launch an instance page.

The left sidebar shows the navigation path: EC2 > Instances > Launch an instance.

The main content area has a heading "Application and OS Images (Amazon Machine Image) [Info](#)". It includes a search bar and a "Quick Start" tab selected. Below are recent AMI icons: Amazon Linux, macOS, Ubuntu, Windows, Red Hat, SUSE Linux, and Debian. A "Browse more AMIs" link is available.

A specific AMI is selected: "Ubuntu Server 24.04 LTS (HVM), SSD Volume Type". The details show it's "Free tier eligible".

The "Description" section states: "Ubuntu Server 24.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>)."

The "Summary" panel on the right shows 1 instance, the selected AMI, the instance type t3.micro, and the "Launch instance" button.

Screenshot of the AWS EC2 Launch an instance page, showing configuration steps.

The left sidebar shows the navigation path: EC2 > Instances > Launch an instance.

The main content area starts with the "Instance type" section, which lists the selected t3.micro instance type. It includes details like family, vCPU, memory, and current generation status, along with pricing information for On-Demand and On-Demand Windows usage.

The "Key pair (login)" section requires a key pair name, with "aws-vpc-pem-kp-ireland" selected and a "Create new key pair" button.

The "Network settings" section shows the selected network and subnet: "vpc-0f015a10b4b968d24 | defaultVPC" and "Subnet | [Info](#)". An "Edit" button is present.

The "Summary" panel on the right shows 1 instance, the selected AMI, the instance type t3.micro, and the "Launch instance" button.

Launch an instance | EC2 | eu-west-1 | Neural Network Portfolio | New Tab

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

aws Search [Alt+S]

EC2 Instances Launch an instance

**Network settings**

VPC - required: Info  
vpc-037f0d5b144ffe537 (custVPC01)  
10.0.0.0/16

Subnet - Info  
subnet-0051699bf17ab344a  
VPC: vpc-037f0d5b144ffe537 Owner: 385098538236 Availability Zone: eu-west-1b (euw1-az3) Zone type: Availability Zone IP addresses available: 251 CIDR: 10.0.2.0/24

Auto-assign public IP - Info  
Disable

Firewall (security groups) - Info  
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.  
 Create security group  Select existing security group  
privsg01-privsn01

Common security groups - Info  
Select security groups  
privsg01-privsn01 sg-018b3037f354a3f6 X  
VPC: vpc-037f0d5b144ffe537

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

Advanced network configuration

**Summary**

Number of instances: Info  
1

Software Image (AMI)  
Canonical, Ubuntu, 24.04, amd6...read more  
ami-049442a6cf8319180

Virtual server type (instance type)  
t3.micro

Firewall (security group)  
privsg01-privsn01

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

Cancel Launch instance Preview code

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Launch an instance | EC2 | eu-west-1 | Neural Network Portfolio | New Tab

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

aws Search [Alt+S]

EC2 Instances Launch an instance

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

Advanced network configuration

**Configure storage**

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

Add new volume

The selected AMI contains instance store volumes, however the instance does not allow any instance store volumes. None of the 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

Advanced details

**Summary**

Number of instances: Info  
1

Software Image (AMI)  
Canonical, Ubuntu, 24.04, amd6...read more  
ami-049442a6cf8319180

Virtual server type (instance type)  
t3.micro

Firewall (security group)  
privsg01-privsn01

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

Cancel Launch instance Preview code

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the AWS EC2 Instances page. The left sidebar is collapsed. The main area displays a table titled "Instances (2) Info" with the following data:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
dbServerPrivS...	i-08967f7dadf2d226e	Running	t3.micro	Initializing	<a href="#">View alarms +</a>	eu-west-1b	-
pubWebServer...	i-0428462c80b3c65b7	Running	t3.micro	3/3 checks passed	<a href="#">View alarms +</a>	eu-west-1a	-

Below the table, a section titled "Select an instance" is visible.

## Step 11 : Connecting the Private server via the public server (bastion host)

This step verifies that the **private subnet** is securely accessible only through the **public server**, following best practices for network isolation and security.

- The **public EC2 instance** acts as a **DMZ / bastion host**.
- Direct internet access to the **private EC2 instance** is not allowed.
- An SSH connection was first established to the **public EC2 instance**.
- From the public instance, an **SSH connection** was initiated to the private EC2 instance.
- The private EC2 instance was accessed using its **private IP address 10.0.2.59**, and successful ICMP ping responses confirmed network connectivity between the public (DMZ) instance and the private subnet instance.
- SSH access was permitted because the **private security group allows SSH traffic from the public security group**.
- This confirmed secure access to the private server through the **DMZ architecture**.

Screenshot of the AWS Cloud Console showing the EC2 Instances page. The left sidebar shows navigation for EC2, Instances, Images, and Elastic Block Store. The main area displays two instances: dbServerPrivS... (running, t3.micro, initializing) and pubWebServer01 (running, t3.micro, 3/3 checks passed). The pubWebServer01 details page is open, showing networking information including VPC ID (vpc-037f0d5b144ffe537), Subnet ID (subnet-0b75b67eee6db0a7c), Availability zone (eu-west-1a), and IP addresses (Public IPv4 address 108.130.74.208, Private IPv4 address 10.0.1.135).

Screenshot of the MobaXterm application window. The interface includes a toolbar with icons for Terminal, Sessions, View, X server, Tools, Games, Settings, Macros, Help, and session buttons for Session, Servers, Tools, Games, Sessions, View, Split, MultiExec, Tunneling, Packages, Settings, and Help. A 'Quick connect...' sidebar lists user sessions: 192.168.1.5 (brenieskar), 35.161.56.238 (ubuntu), 35.91.214.131 (ubuntu), 54.74.240.50 (Administrator), awsCloud, gitServer01, gitServer02, and gitServer03. The main window shows the 'Session settings' dialog for an SSH connection to host 108.130.74.208, port 22, with options for X11-Forwarding, Compression, Execute command, SSH-browser type (SFTP protocol), Use private key (C:\Users\del\Downloads\aws-vp), and OK/Cancel buttons.

```

10.8.130.74.208 (ubuntu)
Terminal Sessions View Xserver Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunnelling Packages Settings Help
Quick connect...
Name /home/ubuntu/
ssh cache profile .bashrc .bash_logout
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-1015-aws x86_64)

* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro

System information as of Tue Dec 30 03:55:08 UTC 2025
System load: 0.08 Temperature: -273.1 C
Usage of /: 20.5% of 8.65GB Processes: 119
Memory usage: 24% Users logged in: 0
Swap usage: 0% IPv4 address for ens: 10.0.1.135

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 programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

/usr/bin/xauth: file /home/ubuntu/.Xauthority does not exist
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-1-135:~$ 

```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

Instances | EC2 | eu-west-1 | Neural Network Portfolio | New Tab | +

eu-west-1.console.aws.amazon.com/ec2/home?region=eu-west-1#Instancesv3;\$case=true%5C;client=false;\$regex=tags:false%5C;client=false

aws Search [Alt+5] Account ID: 5850-885-8236 Europe (Ireland) brendesekar01

**EC2 > Instances**

**Instances (1/2) Info**

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
dbServerPrivS...	i-08967f7dadf2d226e	Running	t3.micro	Initializing	<a href="#">View alarms +</a>	eu-west-1b	-
pubWebServer...	i-0428462c80b3c63b7	Running	t3.micro	3/3 checks passed	<a href="#">View alarms +</a>	eu-west-1a	-

**i-08967f7dadf2d226e (dbServerPrivSn01)**

Details	Status and alarms	Monitoring	Security	Networking	Storage	Tags
VPC ID <a href="#">vpc-037fd5b144ffe537 (custVPC01)</a>	Subnet ID <a href="#">subnet-0051699bf17ab344a (sn02-priv)</a>	Availability zone eu-west-1b				
Availability zone ID <a href="#">euw1-az3</a>	Outpost ID -					
IP addresses <a href="#">Info</a>	Private IPv4 addresses <a href="#">10.0.2.59</a>	IPv6 addresses -				
Public IPv4 address -	Carrier IP addresses (ephemeral) -					
Secondary private IPv4 addresses -						

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

```

108.130.74.208 (ubuntu)
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
2 108.130.74.208 (ubuntu)
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 programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

/usr/bin/xauth:  file /home/ubuntu/.Xauthority does not exist
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

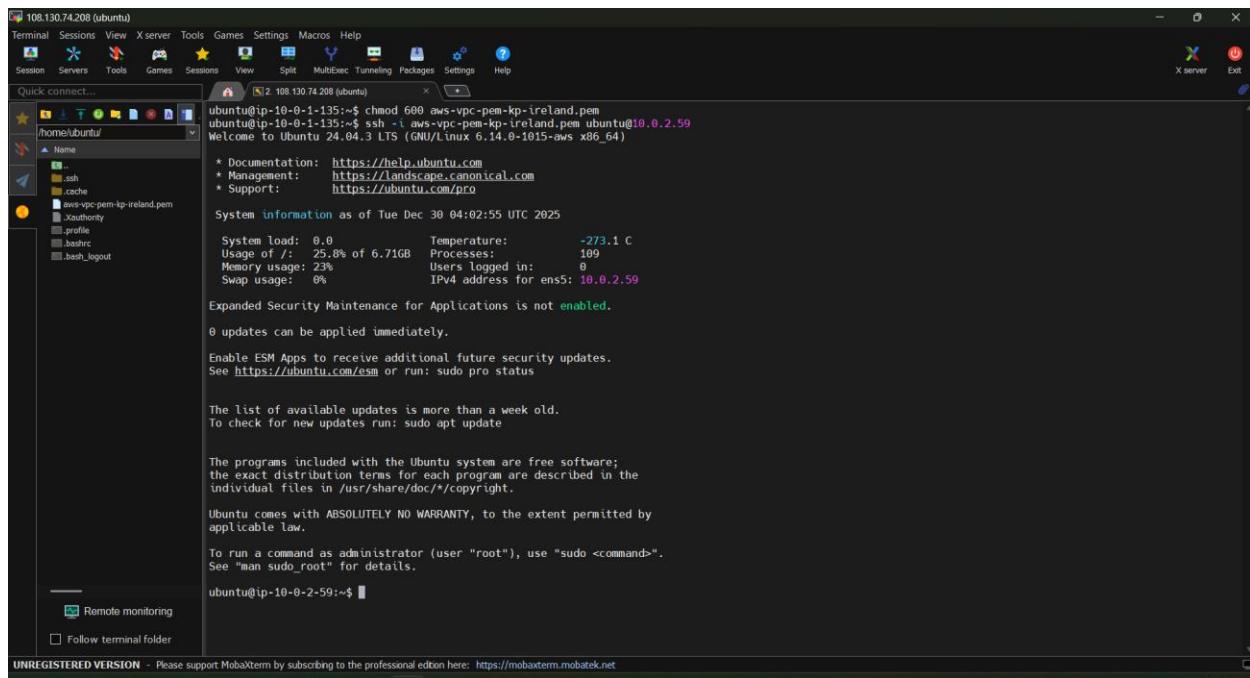
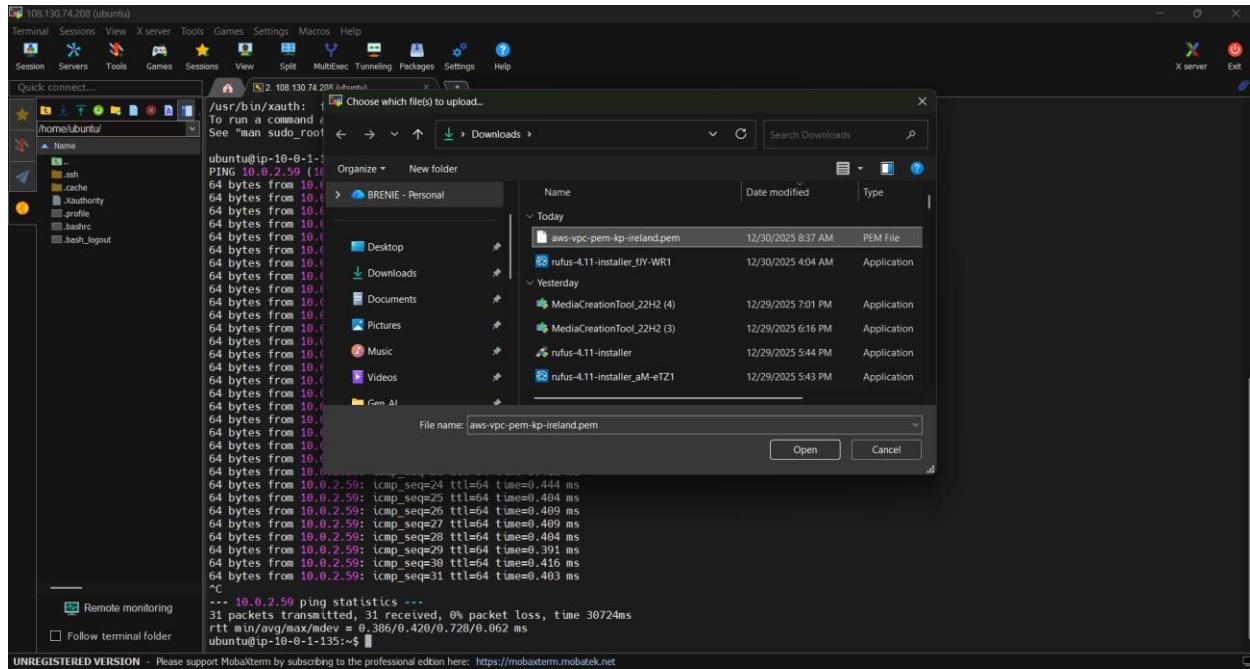
ubuntu@ip-10-0-1-135:~$ ping 10.0.2.59
PING 10.0.2.59 (10.0.2.59) 56(84) bytes of data.
64 bytes from 10.0.2.59: icmp_seq=1 ttl=64 time=0.728 ms
64 bytes from 10.0.2.59: icmp_seq=2 ttl=64 time=0.402 ms
64 bytes from 10.0.2.59: icmp_seq=3 ttl=64 time=0.403 ms
64 bytes from 10.0.2.59: icmp_seq=4 ttl=64 time=0.405 ms
64 bytes from 10.0.2.59: icmp_seq=5 ttl=64 time=0.405 ms
64 bytes from 10.0.2.59: icmp_seq=6 ttl=64 time=0.396 ms
64 bytes from 10.0.2.59: icmp_seq=7 ttl=64 time=0.405 ms
64 bytes from 10.0.2.59: icmp_seq=8 ttl=64 time=0.391 ms
64 bytes from 10.0.2.59: icmp_seq=9 ttl=64 time=0.410 ms
64 bytes from 10.0.2.59: icmp_seq=10 ttl=64 time=0.533 ms
64 bytes from 10.0.2.59: icmp_seq=11 ttl=64 time=0.400 ms
64 bytes from 10.0.2.59: icmp_seq=12 ttl=64 time=0.397 ms
64 bytes from 10.0.2.59: icmp_seq=13 ttl=64 time=0.405 ms
64 bytes from 10.0.2.59: icmp_seq=14 ttl=64 time=0.407 ms
64 bytes from 10.0.2.59: icmp_seq=15 ttl=64 time=0.401 ms
64 bytes from 10.0.2.59: icmp_seq=16 ttl=64 time=0.398 ms
64 bytes from 10.0.2.59: icmp_seq=17 ttl=64 time=0.422 ms
64 bytes from 10.0.2.59: icmp_seq=18 ttl=64 time=0.398 ms
64 bytes from 10.0.2.59: icmp_seq=19 ttl=64 time=0.455 ms

```

UNREGISTERED VERSION - Please support Mobaxterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

The **public EC2 instance** was used as a **DMZ / bastion host** to access the private subnet.

- **Direct internet access** to the private EC2 instance is **not permitted**.
- **SSH access** was first established to the **public EC2 instance** using its **public IP address**.
- The **private key pair** was securely **uploaded to the public server** and proper **file permissions** were applied.
- From the public instance, an **SSH connection** was initiated to the **private EC2 instance** using its **private IP address 10.0.2.59**.
- SSH access was allowed because the **private security group** permits **SSH traffic from the public subnet**.
- Successful login to the private instance **confirms secure access through the DMZ architecture**.



```
10.130.74.208 (ubuntu)
Terminal Sessions View Xserver Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultExec Tunneling Packages Settings Help
Quick connect...
[home/ubuntu/]
Name
ssh
cache
aws-vpc.pem-kp-ireland.pem
Xauthority
.profile
.bashrc
.bash_logout

Memory usage: 23% Users logged in: 0
Swap usage: 0% IPv4 address for ens5: 10.0.2.59

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

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-2-59:~$ uptime
04:04:20 up 12 min, 1 user, load average: 0.02, 0.01, 0.00
ubuntu@ip-10-0-2-59:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 brd 0委 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: ens5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group default qlen 1000
    link/ether 0a:75:a6:2b:15 brd ff:ff:ff:ff:ff:ff
        altname enp0s5
        inet 10.0.2.59/24 metric 100 brd 10.0.2.255 scope global dynamic ens5
            valid_lft 2841sec preferred_lft 2841sec
            inet6 fe00::1:1aff:fe00:2b15/64 scope link
                valid_lft forever preferred_lft forever
ubuntu@ip-10-0-2-59:~$ ping google.com
PING google.com (74.125.193.138) 56(84) bytes of data.
```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

```
10.130.74.208 (ubuntu)
Terminal Sessions View Xserver Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultExec Tunneling Packages Settings Help
Quick connect...
[home/ubuntu/]
Name
ssh
cache
aws-vpc.pem-kp-ireland.pem
Xauthority
.profile
.bashrc
.bash_logout

Memory usage: 23% Users logged in: 0
Swap usage: 0% IPv4 address for ens5: 10.0.2.59

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

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-2-59:~$ uptime
04:04:20 up 12 min, 1 user, load average: 0.02, 0.01, 0.00
ubuntu@ip-10-0-2-59:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 brd 0委 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: ens5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group default qlen 1000
    link/ether 0a:75:a6:2b:15 brd ff:ff:ff:ff:ff:ff
        altname enp0s5
        inet 10.0.2.59/24 metric 100 brd 10.0.2.255 scope global dynamic ens5
            valid_lft 2841sec preferred_lft 2841sec
            inet6 fe00::1:1aff:fe00:2b15/64 scope link
                valid_lft forever preferred_lft forever
ubuntu@ip-10-0-2-59:~$ ping google.com
PING google.com (74.125.193.138) 56(84) bytes of data.
```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

```
10.04.2 LTS (ubuntu)
Terminal Sessions View Xserver Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
/home/ubuntu/
Name
ssh cache
aws-vpc.pem-kg-ireland.pem
Xauthority .profile .bashrc .bash_logout
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-2-59:~$ uptime
04:04:28 up 12 min, 1 user, load average: 0.02, 0.01, 0.00
ubuntu@ip-10-0-2-59:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 00:00:00:00:00:00 scope host
        valid_lft forever preferred_lft forever
        inet6 ::1/128 brd :: scope host
            valid_lft forever preferred_lft forever
2: ens: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9000 qdisc mq state UP group default qlen 1000
    link/ether 0a:75:fa:a6:2b:15 brd ff:ff:ff:ff:ff:ff
    altname enp0s5
    inet 10.0.2.59/24 brd 10.0.2.255 scope global dynamic ens5
        valid_lft 2841sec preferred_lft 2841sec
        inet6 fe80::8e0:2b15:64 scope link
            valid_lft forever preferred_lft forever
ubuntu@ip-10-0-2-59:~$ ping google.com
PING google.com (74.125.193.138) 56(84) bytes of data.
^C
--- google.com ping statistics ---
38 packets transmitted, 0 received, 100% packet loss, time 37887ms
ubuntu@ip-10-0-2-59:~$
```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

```
10.04.2 LTS (ubuntu)
Terminal Sessions View Xserver Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
/home/ubuntu/
Name
ssh cache
aws-vpc.pem-kg-ireland.pem
Xauthority .profile .bashrc .bash_logout
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-2-59:~$ uptime
04:04:28 up 12 min, 1 user, load average: 0.02, 0.01, 0.00
ubuntu@ip-10-0-2-59:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 00:00:00:00:00:00 scope host
        valid_lft forever preferred_lft forever
        inet6 ::1/128 brd :: scope host
            valid_lft forever preferred_lft forever
2: ens: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9000 qdisc mq state UP group default qlen 1000
    link/ether 0a:75:fa:a6:2b:15 brd ff:ff:ff:ff:ff:ff
    altname enp0s5
    inet 10.0.2.59/24 brd 10.0.2.255 scope global dynamic ens5
        valid_lft 2841sec preferred_lft 2841sec
        inet6 fe80::8e0:2b15:64 scope link
            valid_lft forever preferred_lft forever
ubuntu@ip-10-0-2-59:~$ ping google.com
PING google.com (74.125.193.138) 56(84) bytes of data.
^C
--- google.com ping statistics ---
38 packets transmitted, 0 received, 100% packet loss, time 37887ms
ubuntu@ip-10-0-2-59:~$ sudo apt update
0% [Connecting to eu-west-1.ec2.archive.ubuntu.com (2a05:d018:fd:f302:b1a0:e9fe:fb7e:b575)] [Connecting to security.ubuntu.com (2620:2d:4000:1::101)]
```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

## Private Subnet Internet Access Verification

- The EC2 instance launched in the **private subnet** was accessed successfully through the **public EC2 instance (DMZ host)** using SSH.
  - The private instance was confirmed to have the **private IP address 10.0.2.59**.
  - Network interface details were verified using the ip a command.
  - An **attempt to reach the internet** using *ping google.com* failed, indicating no outbound internet connectivity.
  - Running *sudo apt update* also failed with “**Network is unreachable**” errors.
  - This confirms that the **private subnet does not have direct internet access**.
  - The behavior is **expected**, as no **NAT Gateway and private route table** were yet configured at this stage.
  - This validates proper **network isolation of the private subnet** as per security best practices.

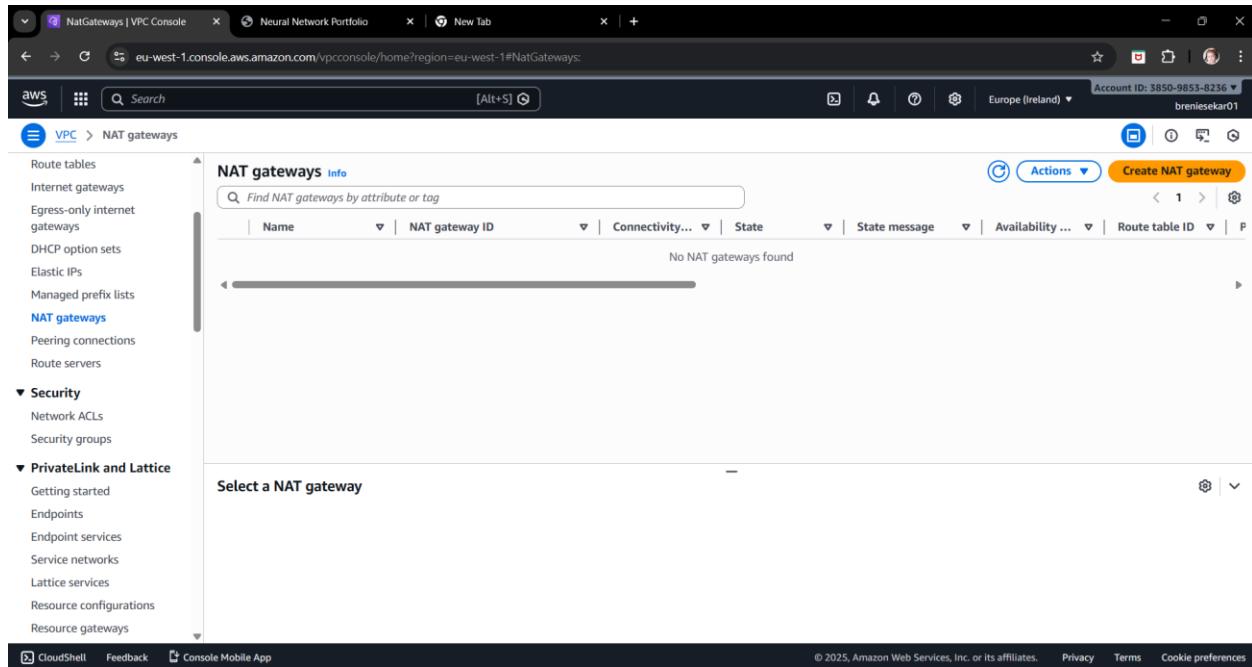
## Part C: Private Subnet Internet Access Using NAT Gateway

This step enables **instances in the private subnet** to access the **internet for outbound traffic** while preventing any **direct inbound access** from the internet. This is achieved by routing private subnet traffic through a **NAT Gateway placed in the public subnet**, ensuring secure and controlled internet connectivity.

## Step 12 : Create a NAT Gateway and allocate an Elastic IP

The purpose of a NAT Gateway is to allow instances in a **private subnet to access the internet for outbound traffic** (such as updates or downloads) while preventing inbound internet access, thereby **maintaining security and isolation**. A NAT Gateway enables private subnet instances to initiate outbound connections to the internet without being directly reachable from it.

- During the NAT Gateway creation process, AWS **automatically allocates and associates an Elastic IP (EIP)** to provide a stable public IP address.
- The NAT Gateway was created by navigating to **VPC → NAT Gateways → Create NAT Gateway**.
- The public subnet **sn01-pub** was selected to host the NAT Gateway.
- An Elastic IP was allocated and associated with the NAT Gateway as part of the creation process.
- The NAT Gateway was successfully created, and its state changed to **Available**.
- The NAT Gateway is now ready to provide secure internet access to instances in the private subnet.



VPC | eu-west-1 Neural Network Portfolio New Tab

eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#CreateNatGateway.

aws Search [Alt+S] Europe (Ireland) Account ID: 3850-9853-8236 brenieskar01

VPC > NAT gateways > Create NAT gateway

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

**Availability mode Info**  
Choose whether to deploy across all zones in the region or restrict to a single availability zone.  
 Regional - new  
Scales automatically across all regional AZs, simplifying management for multi AZ deployments.  
 Zonal  
Provides granular control within a specific availability zone, adhering to subnet level settings.

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

**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.

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

VPC | eu-west-1 Neural Network Portfolio New Tab

eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#CreateNatGateway.

aws Search [Alt+S] Europe (Ireland) Account ID: 3850-9853-8236 brenieskar01

VPC > NAT gateways > Create NAT gateway

Elastic IP address 54.73.76.157 (eipalloc-0c31b655e64091727) allocated.

subnet-0b75b67eee6db0a7c (sn01-pub)

**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.

**Additional settings Info**

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

**Key**  **Value - optional**     
You can add 49 more tags.

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

NAT gateway nat-045e6d922bd951855 | ngw-custVPC01 was created successfully.

**nat-045e6d922bd951855 / ngw-custVPC01**

**Details**

NAT gateway ID <a href="#">nat-045e6d922bd951855</a>	Connectivity type Public	State <a href="#">Pending</a>	State message Info –
NAT gateway ARN <a href="#">arn:aws:ec2:eu-west-1:385098538236:natgateway/nat-045e6d922bd951855</a>	Primary public IPv4 address –	Primary private IPv4 address –	Primary network interface ID –
VPC <a href="#">vpc-037f0d5b144ffe537 / custVPC01</a>	Subnet <a href="#">subnet-0b75b67eee6db0a7c / sn01-pub</a>	Created <a href="#">Tuesday, December 30, 2025 at 09:50:10 GMT+5:30</a>	Deleted –

**Secondary IPv4 addresses** | Monitoring | Tags

**Secondary IPv4 addresses**

Secondary IPv4 addresses are not available for this nat gateway.

### Step 13 : Create a private route table and associate the NAT Gateway with it

The purpose of the private route table is to allow instances in the private subnet to access the internet only for outbound traffic through the NAT Gateway, while preventing direct inbound internet access.

- A private route table named **custVPC-PrivRt01** was created in the custom VPC to manage outbound internet access for instances in the private subnet while preserving network isolation.
- A default route was added with destination **0.0.0.0/0**, targeting the **NAT Gateway**.
- The private route table was explicitly associated with the private subnet **sn02-priv (10.0.2.0/24)**.
- This configuration allows private subnet instances to access the internet only for outbound traffic while preventing any direct inbound internet access.

Screenshot of the AWS VPC Console showing the RouteTables page and the Create route table wizard.

**RouteTables Page:**

Name	Route table ID	Explicit subnet associations	Main	VPC
-	rtb-08cf603592fec862f	-	Yes	vpc-0f015a10b4b968d24   defa.
custVPC-PubRt01	rtb-0c89d0b1cb8bea859	-	Yes	vpc-037f0d5b144ffe537   custV.

**Create route table wizard - Step 1: Select a route table**

The wizard is titled "Create route table" and shows the following steps:

- Route table settings**: Fields include "Name - optional" (custVPC-PrivRt01) and "VPC" (vpc-037f0d5b144ffe537 (custVPC01)).
- Tags**: A table with one row: "Key" (Q Name) and "Value - optional" (Q custVPC-PrivRt01). Buttons include "Add new tag" and "Remove".
- Next Step**: Buttons for "Cancel" and "Create route table".

VPC | eu-west-1 Neural Network Portfolio New Tab

eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#RouteTableDetails:RouteTableId=rtb-06087655fc410d4e7

AWS Search [Alt+S]

Account ID: 3850-9853-8236 Europe (Ireland) brenieskar01

VPC > Route tables > rtb-06087655fc410d4e7

Route table rtb-06087655fc410d4e7 | custVPC-PrivRt01 was created successfully.

rtb-06087655fc410d4e7 / custVPC-PrivRt01

Details info

Route table ID rtb-06087655fc410d4e7	Main No	Explicit subnet associations -	Edge associations -
VPC vpc-037f0d5b144ffe537   custVPC01	Owner ID 385098538236		

Actions

Routes Subnet associations Edge associations Route propagation Tags

Routes (1)

Filter routes		Both	Edit routes	
Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	Create Route Table

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

VPC | eu-west-1 Neural Network Portfolio New Tab

eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#RouteTableDetails:RouteTableId=rtb-06087655fc410d4e7

AWS Search [Alt+S]

Account ID: 3850-9853-8236 Europe (Ireland) brenieskar01

VPC > Route tables > rtb-06087655fc410d4e7

rtb-06087655fc410d4e7 / custVPC-PrivRt01

Details info

Route table ID rtb-06087655fc410d4e7	Main No	Explicit subnet associations -	Edge associations -
VPC vpc-037f0d5b144ffe537   custVPC01	Owner ID 385098538236		

Actions

Routes Subnet associations Edge associations Route propagation Tags

Routes (1)

Filter routes		Both	Edit routes	
Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	Create Route Table

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

VPC | eu-west-1 Neural Network Portfolio New Tab

eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#EditRoutes:RouteTableId=rtb-06087655fc410d4e7

aws Search [Alt+S]

Europe (Ireland) Account ID: 3850-9853-8236 brenieskar01

VPC > Route tables > rtb-06087655fc410d4e7 > Edit routes

### Edit routes

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	CreateRouteTable
Q 0.0.0.0/0	NAT Gateway	-	No	CreateRoute
Q nat-045e6d922bd951855				

Add route Remove

Cancel Preview Save changes

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

VPC | eu-west-1 Neural Network Portfolio New Tab

eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#RouteTableDetails:RouteTableId=rtb-06087655fc410d4e7

aws Search [Alt+S]

Europe (Ireland) Account ID: 3850-9853-8236 brenieskar01

VPC > Route tables > rtb-06087655fc410d4e7

Updated routes for rtb-06087655fc410d4e7 / custVPC-PrivRt01 successfully  
► Details

### rtb-06087655fc410d4e7 / custVPC-PrivRt01

Actions

VPC dashboard AWS Global View Filter by VPC

Virtual private cloud Your VPCs Subnets

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

Security Network ACLs Security groups

Details Info

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-06087655fc410d4e7	No	-	-
VPC	Owner ID		
vpc-037f0d5b144ffe537   custVPC01	385098538236		

Routes Subnet associations Edge associations Route propagation Tags

Routes (2)

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	nat-045e6d922bd951855	Active	No	Create Route
10.0.0.0/16	local	Active	No	Create Route Table

Both Edit routes

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

VPC | eu-west-1 Neural Network Portfolio New Tab

eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#RouteTableDetails:RouteTableId=rtb-06087655fc410d4e7

aws Search [Alt+5]

VPC > Route tables > rtb-06087655fc410d4e7

Updated routes for rtb-06087655fc410d4e7 / custVPC-PrivRT01 successfully

VPC dashboard AWS Global View Filter by VPC

Virtual private cloud Your VPCs Subnets Route tables Internet gateways Egress-only internet gateways DHCP option sets Elastic IPs Managed prefix lists NAT gateways Peering connections Route servers Security Network ACLs Security groups

CloudShell Feedback Console Mobile App

No subnet associations You do not have any subnet associations.

No subnet associations

Subnets without explicit associations (2)

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
sn02-priv	subnet-0051699bf17ab344a	10.0.2.0/24	-
sn01-pub	subnet-0b75b67eee6db0a7c	10.0.1.0/24	-

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

VPC | eu-west-1 Neural Network Portfolio New Tab

eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#EditRouteTableSubnetAssociations:RouteTableId=rtb-06087655fc410d4e7

aws Search [Alt+5]

VPC > Route tables > rtb-06087655fc410d4e7 > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/2)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input checked="" type="checkbox"/> sn02-priv	subnet-0051699bf17ab344a	10.0.2.0/24	-	Main (rtb-0c89d0b1ccb8ea859 / custV...)
<input type="checkbox"/> sn01-pub	subnet-0b75b67eee6db0a7c	10.0.1.0/24	-	Main (rtb-0c89d0b1ccb8ea859 / custV...)

Selected subnets

subnet-0051699bf17ab344a / sn02-priv X

Cancel Save associations

CloudShell Feedback Console Mobile App

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

The screenshot shows the AWS VPC Route Tables page. The URL is eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#RouteTableDetails:RouteTableId=rtb-06087655fc410d4e7. The page displays a success message: "You have successfully updated subnet associations for rtb-06087655fc410d4e7 / custVPC-PrivRt01." Below this, the route table ID is shown as "rtb-06087655fc410d4e7 / custVPC-PrivRt01". The "Details" section shows the route table ID, which is "rtb-06087655fc410d4e7", and the owner ID, which is "385098538236". The "Main" checkbox is checked. The "Explicit subnet associations" section lists one association: "subnet-0051699bf17ab344a / sn02-priv". The "Edge associations" section is empty. The "Subnet associations" tab is selected. The "Explicit subnet associations" table has one row:

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
sn02-priv	subnet-0051699bf17ab344a	10.0.2.0/24	-

The "Subnets without explicit associations" section shows one subnet: "Find subnet association". The footer includes links for CloudShell, Feedback, Console Mobile App, and navigation icons.

## Step 14: Verify Internet Access from Private Subnet

The purpose of this step is to ensure that the **private EC2 instance can access the internet only through the NAT Gateway**, confirming proper routing and maintaining security by preventing direct inbound access.

```
108.130.74.208 (ubuntu)
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split Multibet Tunneling Packages Settings Help
Quick connect...
[ 2 108.130.74.208 (ubuntu) x ]
Name
64 bytes from ig-in-f102.1e100.net (74.125.193.102): icmp_seq=4 ttl=106 time=1.01 ms
64 bytes from ig-in-f102.1e100.net (74.125.193.102): icmp_seq=5 ttl=106 time=1.02 ms
64 bytes from ig-in-f102.1e100.net (74.125.193.102): icmp_seq=6 ttl=106 time=1.01 ms
64 bytes from ig-in-f102.1e100.net (74.125.193.102): icmp_seq=7 ttl=106 time=1.02 ms
64 bytes from ig-in-f102.1e100.net (74.125.193.102): icmp_seq=8 ttl=106 time=1.09 ms
64 bytes from ig-in-f102.1e100.net (74.125.193.102): icmp_seq=9 ttl=106 time=0.996 ms
64 bytes from ig-in-f102.1e100.net (74.125.193.102): icmp_seq=10 ttl=106 time=1.04 ms
64 bytes from ig-in-f102.1e100.net (74.125.193.102): icmp_seq=11 ttl=106 time=1.02 ms
64 bytes from ig-in-f102.1e100.net (74.125.193.102): icmp_seq=12 ttl=106 time=1.02 ms
64 bytes from ig-in-f102.1e100.net (74.125.193.102): icmp_seq=13 ttl=106 time=1.02 ms
64 bytes from ig-in-f102.1e100.net (74.125.193.102): icmp_seq=14 ttl=106 time=0.996 ms
64 bytes from ig-in-f102.1e100.net (74.125.193.102): icmp_seq=15 ttl=106 time=1.01 ms
64 bytes from ig-in-f102.1e100.net (74.125.193.102): icmp_seq=16 ttl=106 time=1.00 ms
64 bytes from ig-in-f102.1e100.net (74.125.193.102): icmp_seq=17 ttl=106 time=1.01 ms
64 bytes from ig-in-f102.1e100.net (74.125.193.102): icmp_seq=18 ttl=106 time=1.00 ms
64 bytes from ig-in-f102.1e100.net (74.125.193.102): icmp_seq=19 ttl=106 time=1.00 ms
64 bytes from ig-in-f102.1e100.net (74.125.193.102): icmp_seq=20 ttl=106 time=0.992 ms
64 bytes from ig-in-f102.1e100.net (74.125.193.102): icmp_seq=21 ttl=106 time=0.996 ms
64 bytes from ig-in-f102.1e100.net (74.125.193.102): icmp_seq=22 ttl=106 time=1.02 ms
^C
--- google.com ping statistics ---
22 packets transmitted, 22 received, 0% packet loss, time 21025ms
rtt min/avg/max/mdev = 0.992/1.030/1.386/0.080 ms
ubuntut@ip-10-0-2-59:~$ sudo apt update
Hit:1 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu - universe amd64 Packages [126 kB]
Get:3 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu - universe Translation-en [5982 kB]
Get:4 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu - universe amd64 Components [15.0 MB]
Get:5 http://security.ubuntu.com/ubuntu noble - security InRelease [126 kB]
Get:6 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu - universe Translation-en [5982 kB]
Get:7 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu - universe amd64 Components [3871 kB]
Get:8 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu - universe amd64 c-n-f Metadata [301 kB]
Get:9 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu - multiverse amd64 Packages [269 kB]
Get:10 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu - multiverse Translation-en [118 kB]
Get:11 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu - multiverse amd64 Components [35.0 kB]
Get:12 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu - multiverse amd64 c-n-f Metadata [8326 kB]
Get:13 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu - universe main amd64 Packages [1684 kB]
Get:14 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu - universe main Translation-en [311 kB]
Get:15 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu - universe main amd64 Components [175 kB]
Get:16 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu - universe main amd64 c-n-f Metadata [15.8 kB]
Get:17 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu - universe main Translation-en [1566 kB]
Get:18 http://eu-west-1.ec2.archive.ubuntu.com/ubuntu - universe Translation-en [386 kB]
Remote monitoring
Follow terminal folder
UNREGISTERED VERSION - Please support Mobatek by subscribing to the professional edition here: https://mobatext.mobatek.net
```

- After completing the NAT Gateway and private route table configuration, outbound internet connectivity was **tested from the private EC2 instance**.
  - The private instance was able to **successfully reach external destinations** (for example, using *ping google.com*).
  - The command *sudo apt update* executed successfully, confirming access to external package repositories.
  - This verifies that **internet-bound traffic from the private subnet is correctly routed through the NAT Gateway**.
  - The private subnet **remains secure**, with no direct inbound internet access allowed.

## **Step 15 : Restrict direct internet access for the private subnet**

The purpose of this step is to ensure that instances in the private subnet do not have direct internet access, enforcing secure network isolation once the update is completed.

- The **NAT Gateway was removed** from the private route table.
  - The associated **Elastic IP was automatically released** by AWS.
  - The private route table **no longer contained a 0.0.0.0/0 route** to the NAT Gateway.
  - **Outbound internet access was tested** from the private subnet.
  - **Ping and package update commands failed**, confirming no external connectivity.
  - This **verified complete network isolation** of the private subnet.

RouteTableDetails | VPC Console

Neural Network Portfolio

New Tab

eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#RouteTableDetails:RouteTableId=rtb-06087655fc410d4e7

AWS Search [Alt+S]

Europe (Ireland) Account ID: 3850-9853-8236 brenieskar01

VPC > Route tables > rtb-06087655fc410d4e7

VPC dashboard

AWS Global View Filter by VPC

Virtual private cloud Your VPCs Subnets Route tables Internet gateways Egress-only internet gateways DHCP option sets Elastic IPs Managed prefix lists NAT gateways Peering connections Route servers Security Network ACLs Security groups

rtb-06087655fc410d4e7 / custVPC-PrivRt01

Details Info

Main No Owner ID 385098538236

Explicit subnet associations subnet-0051699bf17ab344a / sn02-priv

Edge associations -

Actions

Routes Subnet associations Edge associations Route propagation Tags

Routes (2)

Filter routes

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	nat-045e6d922bd951855	Active	No	Create Route
10.0.0.0/16	local	Active	No	Create Route Table

Both Edit routes

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

VPC | eu-west-1

Neural Network Portfolio

New Tab

eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#EditRoutes:RouteTableId=rtb-06087655fc410d4e7

AWS Search [Alt+S]

Europe (Ireland) Account ID: 3850-9853-8236 brenieskar01

VPC > Route tables > rtb-06087655fc410d4e7 > Edit routes

Edit routes

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

Add route Remove

Cancel Preview Save changes

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

**Edit routes**

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

Add route

Cancel   Preview   Save changes

```

ping -c 50 google.com
PING google.com (74.125.193.108) 56(84) bytes of data.
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=1 ttl=106 time=1.03 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=19 ttl=106 time=1.05 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=20 ttl=106 time=1.02 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=21 ttl=106 time=1.01 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=22 ttl=106 time=1.02 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=23 ttl=106 time=1.04 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=24 ttl=106 time=1.03 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=25 ttl=106 time=1.05 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=26 ttl=106 time=1.01 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=27 ttl=106 time=1.01 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=28 ttl=106 time=1.01 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=29 ttl=106 time=1.02 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=30 ttl=106 time=1.05 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=31 ttl=106 time=1.03 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=32 ttl=106 time=1.03 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=33 ttl=106 time=1.04 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=34 ttl=106 time=1.01 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=35 ttl=106 time=1.03 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=36 ttl=106 time=1.03 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=37 ttl=106 time=1.00 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=38 ttl=106 time=1.03 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=39 ttl=106 time=1.02 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=40 ttl=106 time=1.04 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=41 ttl=106 time=1.02 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=42 ttl=106 time=1.03 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=43 ttl=106 time=1.04 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=44 ttl=106 time=1.02 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=45 ttl=106 time=1.01 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=46 ttl=106 time=1.14 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=47 ttl=106 time=1.02 ms
64 bytes from ig-in-f100.1e100.net (74.125.193.108): icmp_seq=48 ttl=106 time=1.03 ms
```


-- google.com ping statistics --  
52 packets transmitted, 48 received, 7.6923% packet loss, time 5114ms  
rtt min/avg/max/mdev = 0.996/1.043/1.415/0.063 ms  
ubuntu@ip-10-0-2-59:~$ ping google.com  
PING google.com (74.125.193.108) 56(84) bytes of data.  
^C  
-- google.com ping statistics --  
13 packets transmitted, 0 received, 100% packet loss, time 1229ms  
ubuntu@ip-10-0-2-59:~$



UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net


```

## Part D: Clean Up

This step involves removing all resources created during the VPC setup to ensure no residual configurations remain.

- The **NAT Gateway was deleted** to remove outbound internet access for the private subnet.
- The **associated Elastic IP was released** as part of the NAT Gateway deletion.

- All **EC2 instances** created during the setup **were terminated**, including public and private instances.
- The **custom VPC was deleted** after removing dependent resources.
- Deleting the custom VPC automatically removed all associated components, such as subnets, route tables, security groups, and network ACLs.

## 1. Deleting the NAT Gateway

NAT gateways (1/1) Info

| Name          | NAT gateway ID        | Connectivity type | State     |
|---------------|-----------------------|-------------------|-----------|
| ngw-custVPC01 | nat-045e6d922bd951855 | Public            | Available |

**Actions**

View details  
Edit secondary IPv4 address associations  
Manage tags  
**Delete NAT gateway**

**nat-045e6d922bd951855 / ngw-custVPC01**

**Details** Secondary IPv4 addresses Monitoring Tags

**Details**

|                                         |                             |                              |                               |
|-----------------------------------------|-----------------------------|------------------------------|-------------------------------|
| NAT gateway ID<br>nat-045e6d922bd951855 | Connectivity type<br>Public | State<br>Available           | State message                 |
| NAT gateway ARN                         |                             | Primary public IP or address | Primary private IP or address |
|                                         |                             | Primary network interface ID | Primary network interface ID  |

**Delete NAT gateway**

**Will be deleted**  
The following NAT gateway will be deleted permanently and can't be recovered later.

|               |                       |           |
|---------------|-----------------------|-----------|
| Name          | NAT gateway ID        | State     |
| ngw-custVPC01 | nat-045e6d922bd951855 | Available |

To confirm deletion, type **delete** in the field:  
**delete**

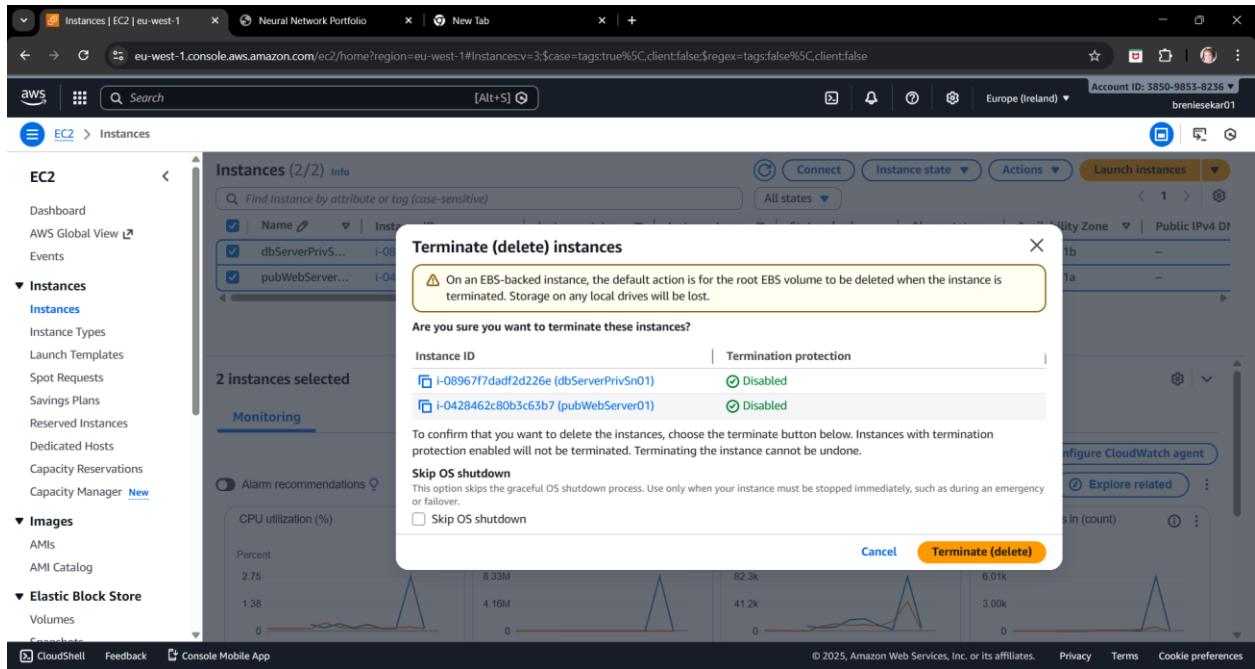
**Delete**

## 2. Deleting the Elastic IP

The screenshot shows the AWS VPC Console with the URL [eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#Addresses](https://eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#Addresses). The left sidebar is expanded to show 'Virtual private cloud' and 'Elastic IPs'. In the main area, it shows 'Elastic IP addresses (1/1) Info' for a single entry: Name - 52.30.138.131, Type - Public IP, Allocation ID - eipalloc-052b104a89a5fb5e6. A modal window titled 'Release Elastic IP addresses' is open, containing a table with one row: Name - 52.30.138.131, IPv4 address - 52.30.138.131, Allocation ID - eipalloc-052b104a89a5fb5e6. Below the table are 'Cancel' and 'Release' buttons.

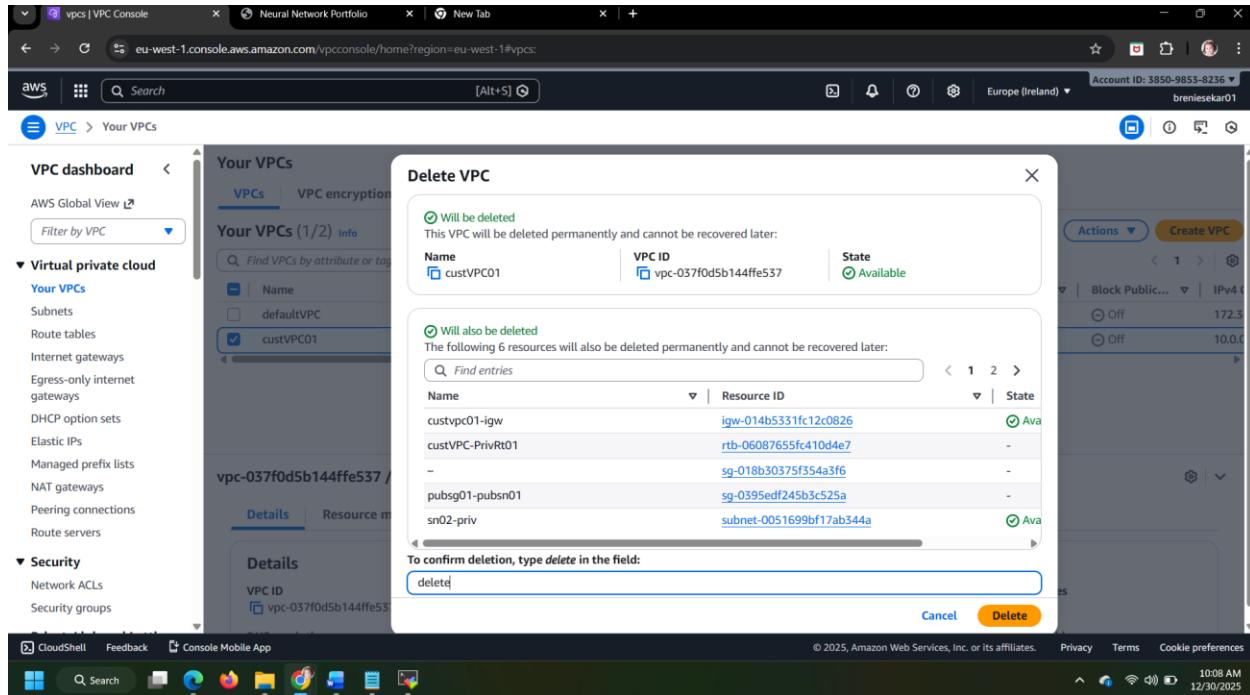
## 3. Deleting the created EC2 Instances

The screenshot shows the AWS EC2 Instances page with the URL [eu-west-1.console.aws.amazon.com/ec2/home?region=eu-west-1#Instancesv3;case=true%5C.clientfalse\\$regex=false%5C.clientfalse](https://eu-west-1.console.aws.amazon.com/ec2/home?region=eu-west-1#Instancesv3;case=true%5C.clientfalse$regex=false%5C.clientfalse). The left sidebar is expanded to show 'Instances' and 'Launch Templates'. The main area shows 'Instances (2/2) Info' with two instances listed: dbServerPriv5... (i-08967f7dadf2d226e, Running, t3.micro, 3/3 checks) and pubWebServer... (i-0428462c80b3c63b7, Running, t3.micro, 3/3 checks). A context menu is open over the second instance, showing options: Stop instance, Start instance, Reboot instance, Hibernate instance, and Terminate (delete) instance. The 'Terminate (delete) instance' option is highlighted.



## 4. Deleting the custom VPC

| Name             | VPC ID                       | State            | Encryption |
|------------------|------------------------------|------------------|------------|
| defaultVPC       | vpc-0f015a10b4b968d24        | Available        | -          |
| <b>custVPC01</b> | <b>vpc-037f0d5b144ffe537</b> | <b>Available</b> | <b>-</b>   |



## Task Summary :

- Created a **custom VPC** to host the network infrastructure.
- Configured an **Internet Gateway** and attached it to the VPC.
- Created a **public subnet (256 IPs)** and a **private subnet (256 IPs)** within the VPC.
- Configured a **route table** to connect the public subnet to the Internet Gateway.
- Launched a **Linux EC2 instance configured as a web server** in the public subnet and **successfully accessed the web server using its public IP address**.
- Extended the setup by implementing a **DMZ architecture** for secure private subnet access.
- Further enhanced the design using a **NAT Gateway** for controlled private subnet internet access.
- Cleaned up all created AWS resources after verification.