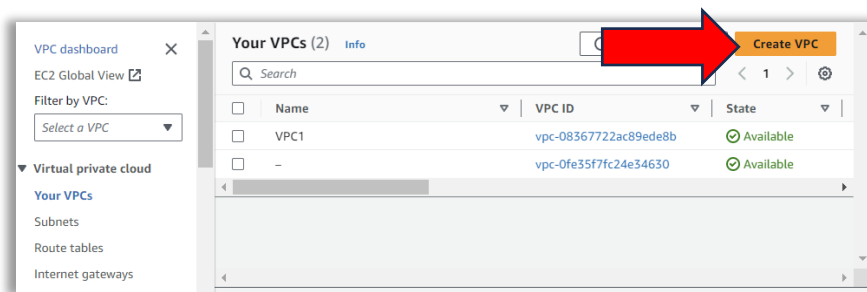


AWS Elastic Compute Cloud Lab (EC2)

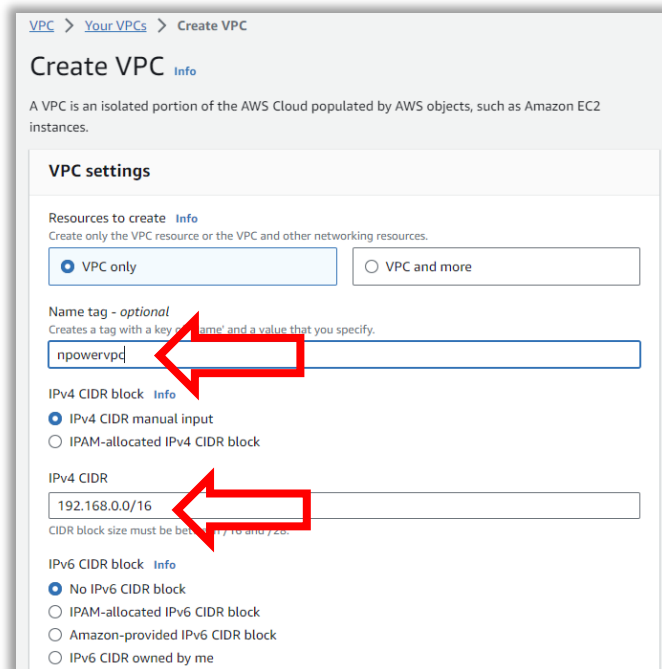
In this lab, you are going to learn about the EC2 Instance which is the virtual server in the AWS cloud. Amazon Elastic Compute Cloud (Amazon EC2) provides on-demand, scalable computing capacity in the Amazon Web Services (AWS) Cloud. Using Amazon EC2 reduces hardware costs so you can develop and deploy applications faster. You can use Amazon EC2 to launch as many or as few virtual servers as you need, configure security and networking, and manage storage.

Virtual Private Cloud (VPC) is a logically isolated virtual network. You can launch AWS resources in a logically isolated virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

Step 1. Create a VPC.



Step 1a. Name the VPC, and give an IPv4 CIDR block of **192.168.0.0/16**

A screenshot of the 'Create VPC' form in the AWS console. The form is titled 'Create VPC' and includes a description: 'A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.' Under 'VPC settings', there are two radio buttons: 'VPC only' (selected) and 'VPC and more'. Below this, there's a section for 'Name tag - optional' with a text input field containing 'npowervpc'. Further down, there's a section for 'IPv4 CIDR block' with two radio buttons: 'IPv4 CIDR manual input' (selected) and 'IPAM-allocated IPv4 CIDR block'. Below this, there's a text input field for 'IPv4 CIDR' containing '192.168.0.0/16'. At the bottom, there's a section for 'IPv6 CIDR block' with four radio buttons: 'No IPv6 CIDR block' (selected), 'IPAM-allocated IPv6 CIDR block', 'Amazon-provided IPv6 CIDR block', and 'IPv6 CIDR owned by me'. Two red arrows point to the 'Name tag' and 'IPv4 CIDR' input fields respectively.

Tenancy Info
Default

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

Key Value - optional

Q Name X Q npowervpc X

Remove tag

Add tag

You can add 49 more tags

Cancel Create VPC

Step 2. An Internet Gateway is a VPC component that allows communication between your VPC and the internet. It supports IPv4 and IPv6 traffic. An internet gateway enables resources in your public subnets (such as EC2 instances) to connect to the internet if the resource has a public IPv4 address or an IPv6 address. Similarly, resources on the internet can initiate a connection to resources in your subnet using the public IPv4 address or IPv6 address.

- Create an Internet Gateway
- Name the Internet gateway (npowerigw) and click create.

VPC dashboard

EC2 Global View

Filter by VPC:
Select a VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Internet gateway (1) Info

Actions Create internet gateway

Search

Name Internet gateway ID

Select an internet gateway above

VPC > Internet gateways > Create internet gateway

Create internet gateway Info

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

Internet gateway settings

Name tag

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

npowerigw

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

Q Name X Q npowerigw X

Remove

Add new tag

You can add 49 more tags.

Cancel Create internet gateway

Step 3. Attach the Internet Gateway to the VPC that was just created.

VPC > Internet gateways > igw-023ad4588b43528a5

✓ The following internet gateway was created: igw-023ad4588b43528a5 - npowerigw. You can now attach to a VPC to enable the VPC to communicate with the internet.

Attach to a VPC

igw-023ad4588b43528a5 / npowerigw

Actions ▲

- Attach to VPC
- Detach from VPC
- Manage tags
- Delete

Details Info

Internet gateway ID	State
igw-023ad4588b43528a5	Detached
VPC ID	Owner
—	979845650489

VPC > Internet gateways > Attach to VPC (igw-023ad4588b43528a5)

Attach to VPC (igw-023ad4588b43528a5) Info

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.

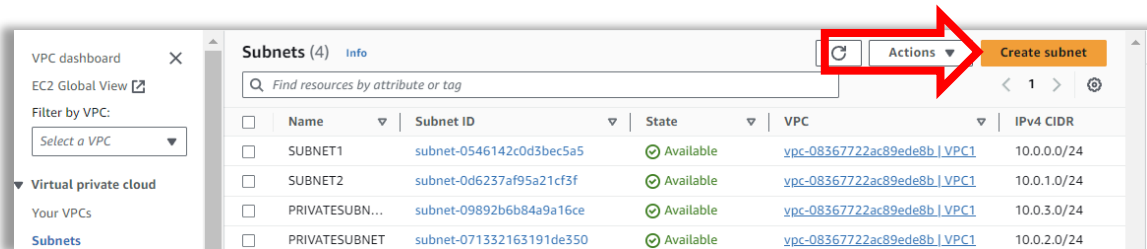
Q Select a VPC

- vpc-013248384c7875035 - npowervpc
- vpc-0fe35f7fc24e34630

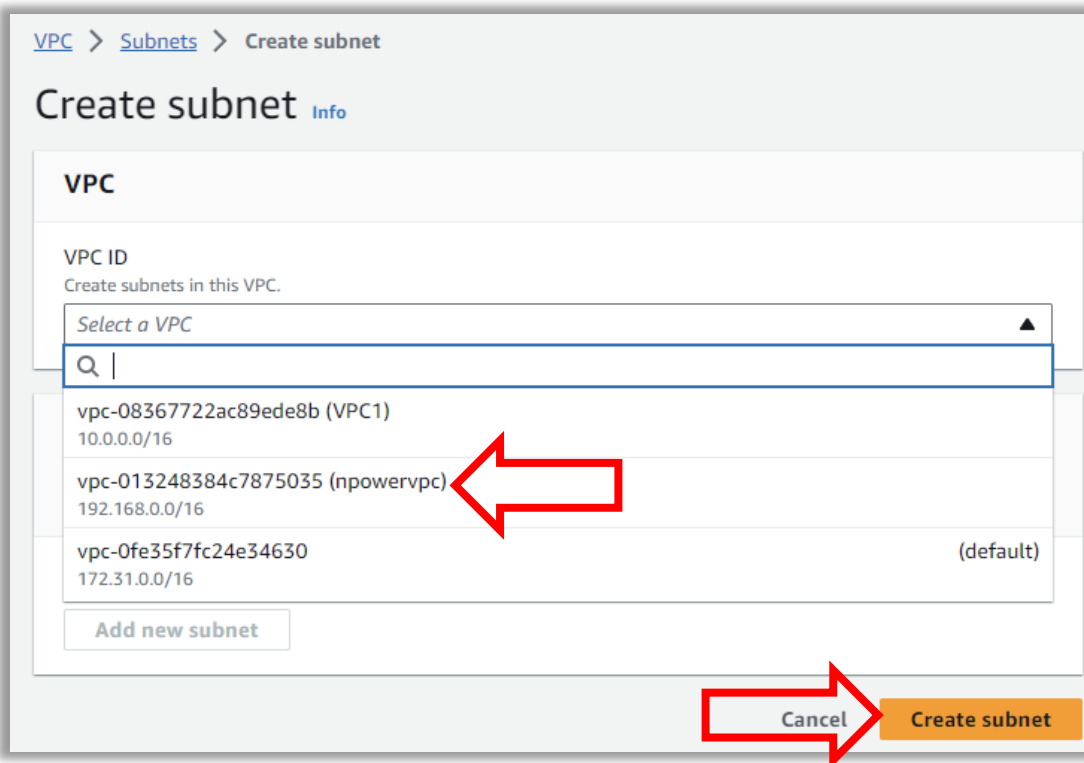
Cancel Attach internet gateway

Step 4. A *subnet* is a range of IP addresses in your VPC. You can create AWS resources, such as EC2 instances, in specific subnets. Each subnet must reside entirely within one Availability Zone and cannot span zones. By launching AWS resources in separate Availability Zones, you can protect your applications from the failure of a single Availability Zone.

- Create two subnets Named (PublicData, SecureData), and attach to your VPC. Give each one a different Availability Zone (1a, 1b) with CIDR Blocks (192.168.1.0/24, & 192.168.2.0/24) respectively.



- Choose the VPC created in step 1.



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

IPv4 VPC CIDR block [Info](#)
Choose the IPv4 VPC CIDR block to create a subnet in.

IPv4 subnet CIDR block
 256 IPs

Tags - optional

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

You can add 49 more tags.

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 IPv4 VPC CIDR block to create a subnet in.

IPv4 subnet CIDR block
 256 IPs

Tags - optional

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

You can add 49 more tags.

Step 5. A *route table* contains a set of rules, called *routes*, that determine where network traffic from your subnet or gateway is directed. The **Main route table**—The route table that automatically comes with your VPC.

- Select your VPC and click on the Main route table

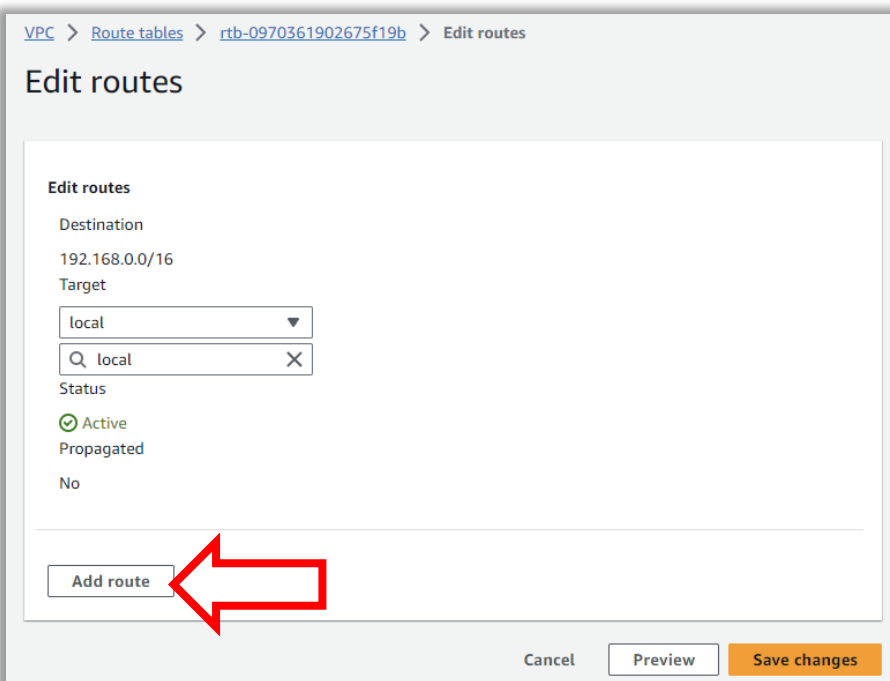
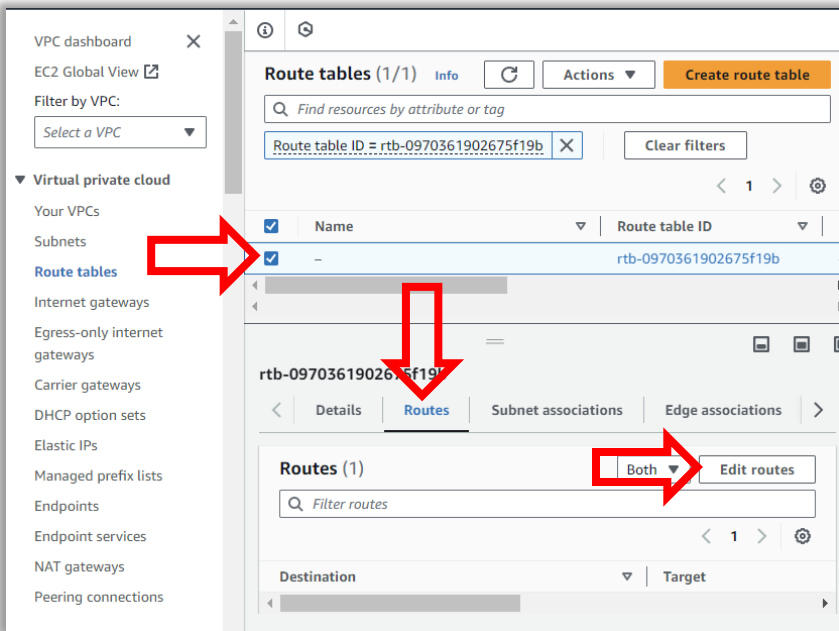
The screenshot shows the AWS Management Console interface for VPCs. On the left is a navigation sidebar with categories like 'Virtual private cloud' and 'Security'. The main area is titled 'Your VPCs (1/3)' and contains a table of VPCs. The VPC 'npowervpc' is selected, and its details are shown below. A red arrow points to the 'npowervpc' row in the table, and another red arrow points to the 'Main route table' link in the 'Details' section.

Name	VPC ID	State	IPv4 CIDR
VPC1	vpc-08367722ac89ede8b	Available	10.0.0.0/16
npowervpc	vpc-013248384c7875035	Available	192.168.0.0/16

vpc-013248384c7875035 / npowervpc			
Details			
VPC ID vpc-013248384c7875035	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-0da889e6b485f28c	Main route table rtb-0970361902675f19b	Main network ACL acl-018bd0e0cc0a0c918
Default VPC No	IPv4 CIDR 192.168.0.0/16	IPv6 pool -	IPv6 CIDR (Network border group) -
Network Address Usage metrics	Route 53 Resolver DNS Firewall rule groups -	Owner ID 979845650489	

Step 6. Each route in a table specifies a destination and a target. For example, to enable your subnet to access the internet through an internet gateway, add the following route to your subnet route table. The destination for the route is 0.0.0.0/0, which represents all IPv4 addresses. The target is the internet gateway that's attached to your VPC.

- Edit routes, add universal IP address 0.0.0.0/0, with target set with the Internet Gateway we created from Step 2.



Edit routes

Destination
0.0.0.0/0

Target
Internet Gateway

igw-
Use: "igw-"
igw-023ad4588b43528a5 (npowerigw)

No

Remove

Add route

Cancel Preview Save changes

Step 7. Each subnet in your VPC must be associated with a route table. A subnet can be explicitly associated with custom route table, or implicitly or explicitly associated with the main route table.

- Edit subnet associations of the route table.

VPC > Route tables > rtb-0970361902675f19b

rtb-0970361902675f19b

Actions

Details Info

Route table ID rtb-0970361902675f19b	Main Yes	Explicit subnet associations -	Edge associations -
VPC vpc-013248384c7875035 npowervpc	Owner ID 979845650489		

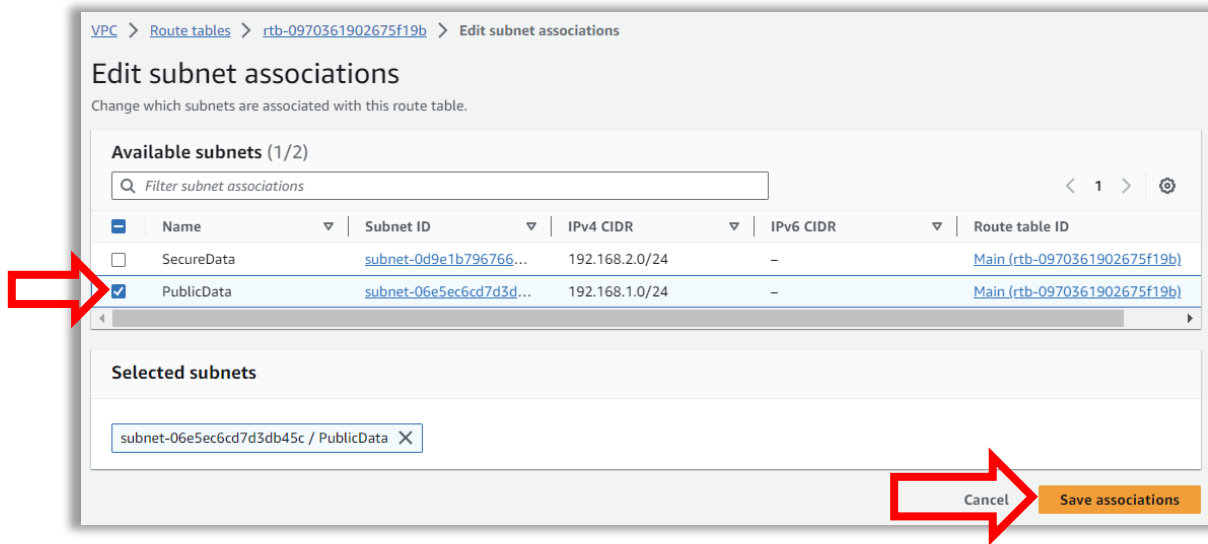
Routes Subnet associations Edge associations Route propagation Tags

Explicit subnet associations (0) Edit subnet associations

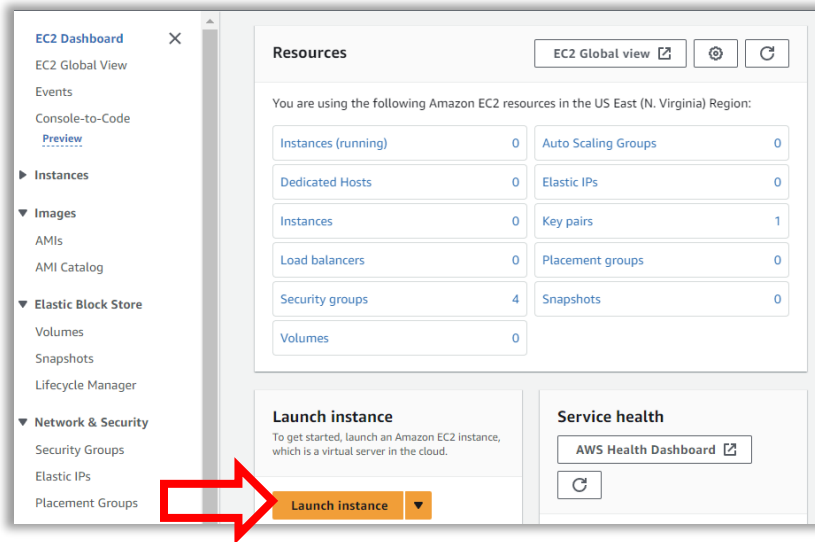
Find subnet association

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
No subnet associations			
You do not have any subnet associations.			

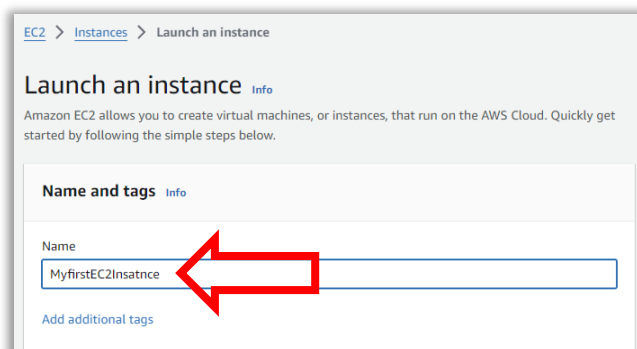
Step 7a. Associate Subnet: PublicData with the Rotatable and save.



Step 8. Launch an EC2 Instance



Step 8a. Name - MyFirstEC2Instance



- Choose the Amazon Linux 2 AMI (HVM), SSD Volume Type

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

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

Recents Quick Start

Amazon Linux
aws

macOS
Mac

Ubuntu
ubuntu

Windows
Microsoft

Red Hat
Red Hat

Sl

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

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI
ami-079db87dc4c10ac91 (64-bit (x86), uefi-preferred) / ami-02cd6549baea35b55 (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

Description

Amazon Linux 2023 AMI 2023.3.20231218.0 x86_64 HVM kernel-6.1

Architecture	Boot mode	AMI ID	
64-bit (x86)	uefi-preferred	ami-079db87dc4c10ac91	Verified provider

Step 8b. Leave instance type as default.

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

Instance type

t2.micro
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand RHEL base pricing: 0.0716 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour

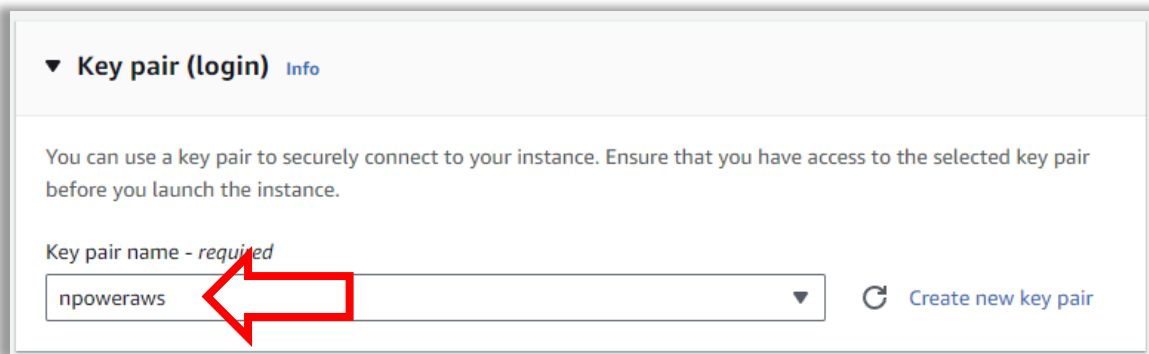
Free tier eligible

☐ All generations

[Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

Step 8c. Choose the existing Keypair created from Lab 1.



▼ **Key pair (login)** [Info](#)

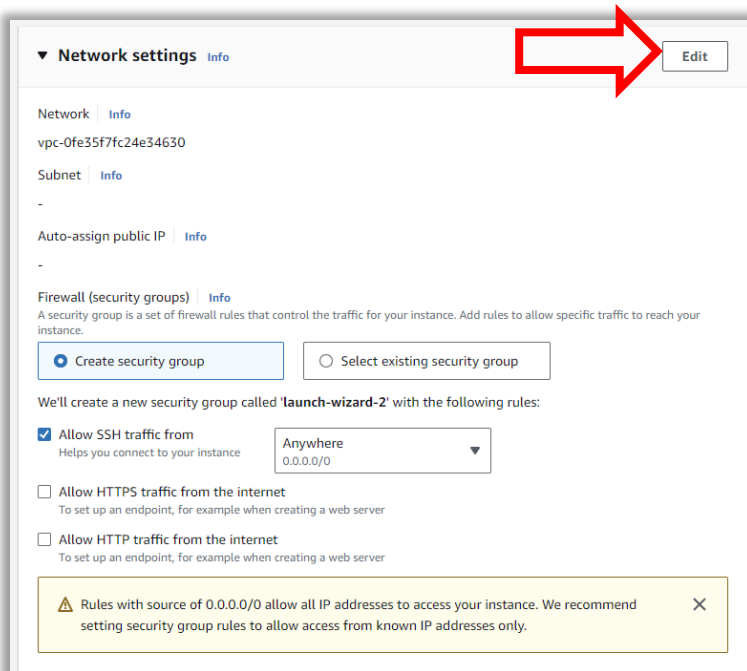
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

npoweraws ▼

↻ [Create new key pair](#)

Step 8d. Configure the Network Settings



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

Network [Info](#)

vpc-0fe35f7fc24e34630

Subnet [Info](#)

-

Auto-assign public IP [Info](#)

-

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group ☐ Select existing security group

We'll create a new security group called 'launch-wizard-2' with the following rules:

☒ Allow SSH traffic from [Info](#)
Helps you connect to your instance Anywhere
0.0.0.0/0

☐ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

☐ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

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

- VPC: **npowervpc** | Subnet: **PublicData** | Auto-assign public-IP: **Enabled**

▼ Network settings Info

VPC - required Info

vpc-013248384c7875035 (npowervpc)
192.168.0.0/16

Subnet Info

subnet-06e5ec6cd7d3db45c
PublicData
VPC: vpc-013248384c7875035 Owner: 979845650489
Availability Zone: us-east-1a IP addresses available: 251 CIDR: 192.168.1.0/24

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

Security group name - required

launch-wizard-2

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

Description - required Info

launch-wizard-2 created 2024-01-03T18:37:47.294Z

- Inbound Security Group rules leave as default.

Inbound Security Group Rules

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

Type Info

ssh

Protocol Info

TCP

Port range Info

22

Source type Info

Anywhere

Source Info

Q Add CIDR, prefix list or security
0.0.0.0/0 X

Description - optional Info

e.g. SSH for admin desktop

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

Add security group rule

► Advanced network configuration

- Configure storage leave it as default. Click **Launch instance**.

The screenshot shows the 'Configure storage' step of the AWS 'Launch instance' wizard. The 'Type' is 'ssh', 'Protocol' is 'TCP', and 'Port range' is '22'. The 'Source type' is 'Anywhere', 'Source' is '0.0.0.0/0', and 'Description' is 'e.g. SSH for admin desktop'. The 'Summary' panel on the right shows 'Number of instances' as 1, 'Software Image (AMI)' as 'Amazon Linux 2023 AMI 2023.3.2...', 'Virtual server type (instance type)' as 't2.micro', 'Firewall (security group)' as 'New security group', and 'Storage (volumes)' as '1 volume(s) - 8 GiB'. A red arrow points to the 'Launch instance' button in the 'Summary' panel.

Configure storage [Info](#) [Advanced](#)

1x 8 GiB gp3 Root volume (Not encrypted)

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

[Add new volume](#)

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](#) [Info](#)

Summary

Number of instances [Info](#)
1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.3.2...[read more](#)
ami-079db87dc4c10ac91

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

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

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

Step 9. Connect onto your EC2 Instance using SSH Client

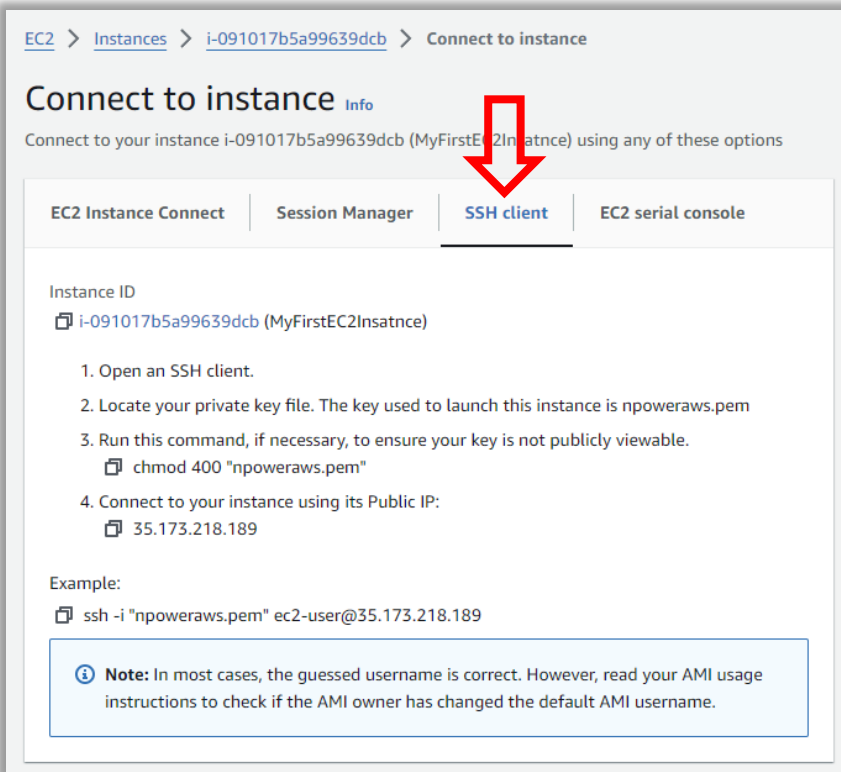
The screenshot shows the 'Instances' page in the AWS Management Console. It displays a table with one instance, 'MyFirstEC2Insatnce', which is in the 'Running' state. The table has columns for 'Name', 'Instance ID', and 'Instance state'. The 'Launch instances' button is visible at the top.

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

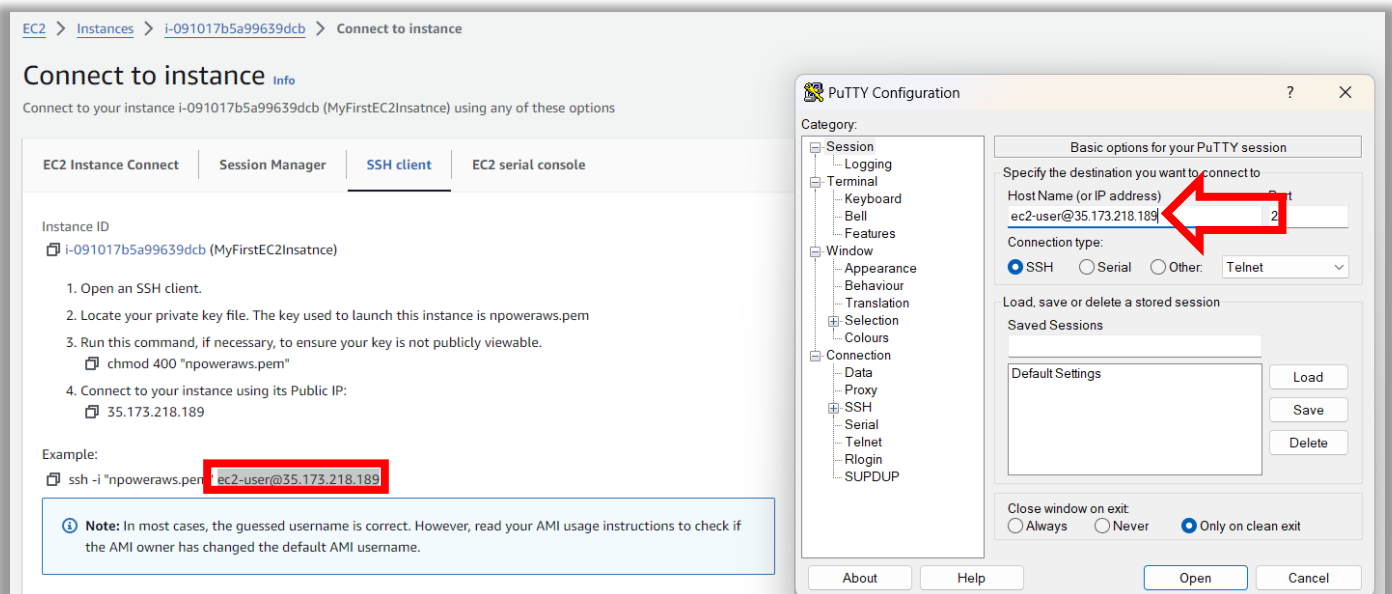
[Refresh](#) [Connect](#) [Instance state](#) [Actions](#)

[Launch instances](#)

<input checked="" type="checkbox"/>	Name ✎	Instance ID	Instance state
<input checked="" type="checkbox"/>	MyFirstEC2Insatnce	i-091017b5a99639dcb	Running 🔍

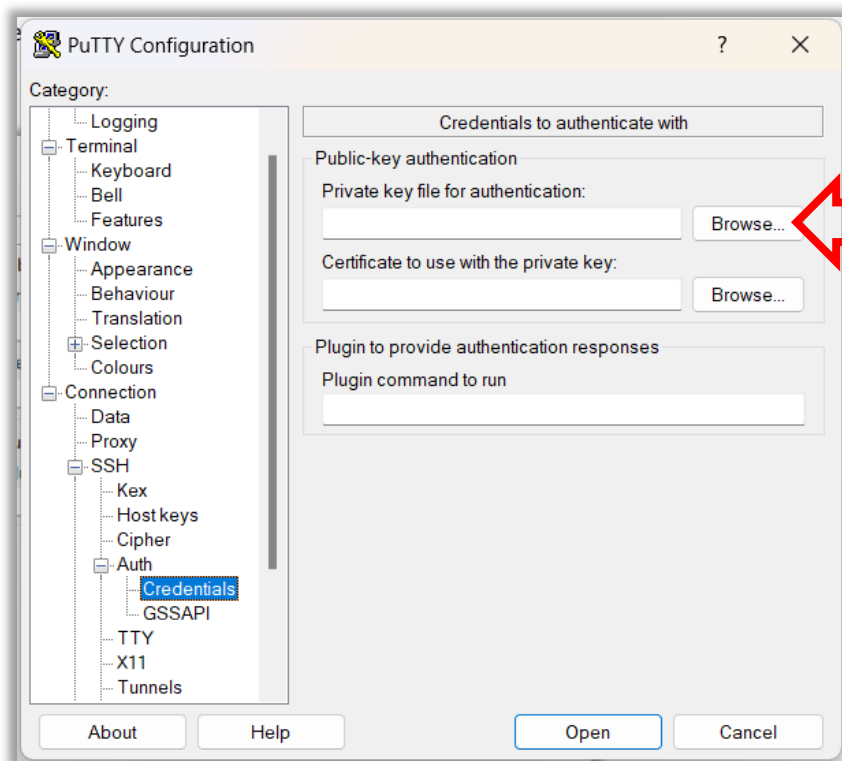


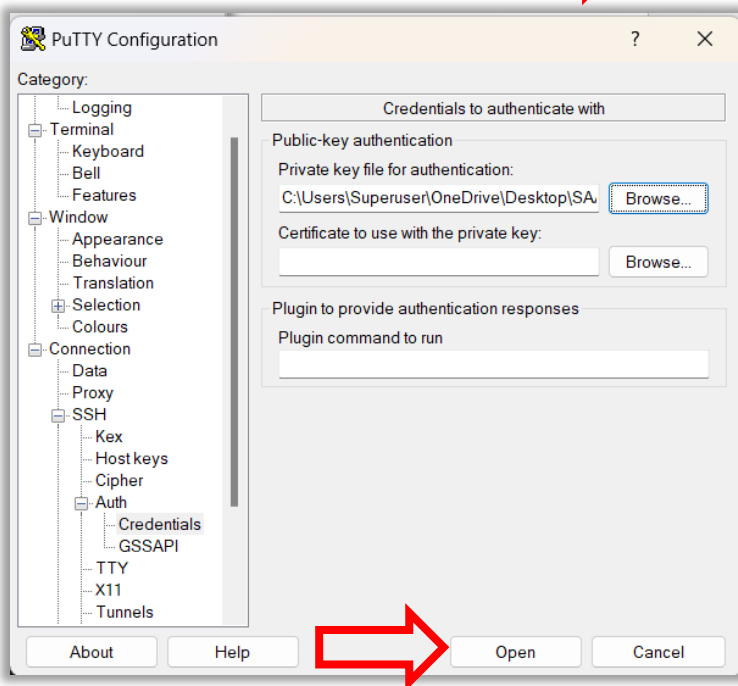
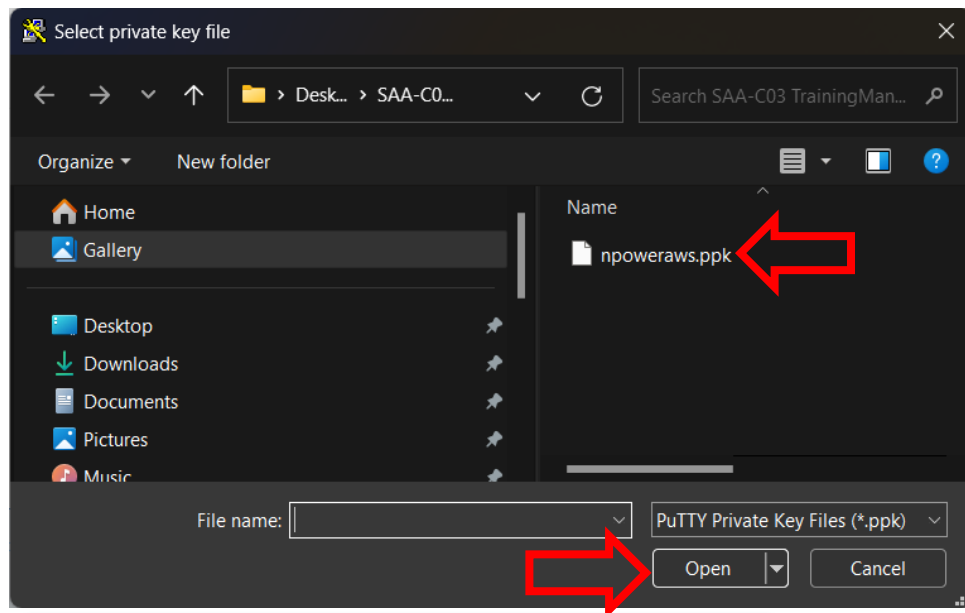
Step 9a. Open Putty, Copy the Host Name and paste it into Putty, under Host Name (or IP address)



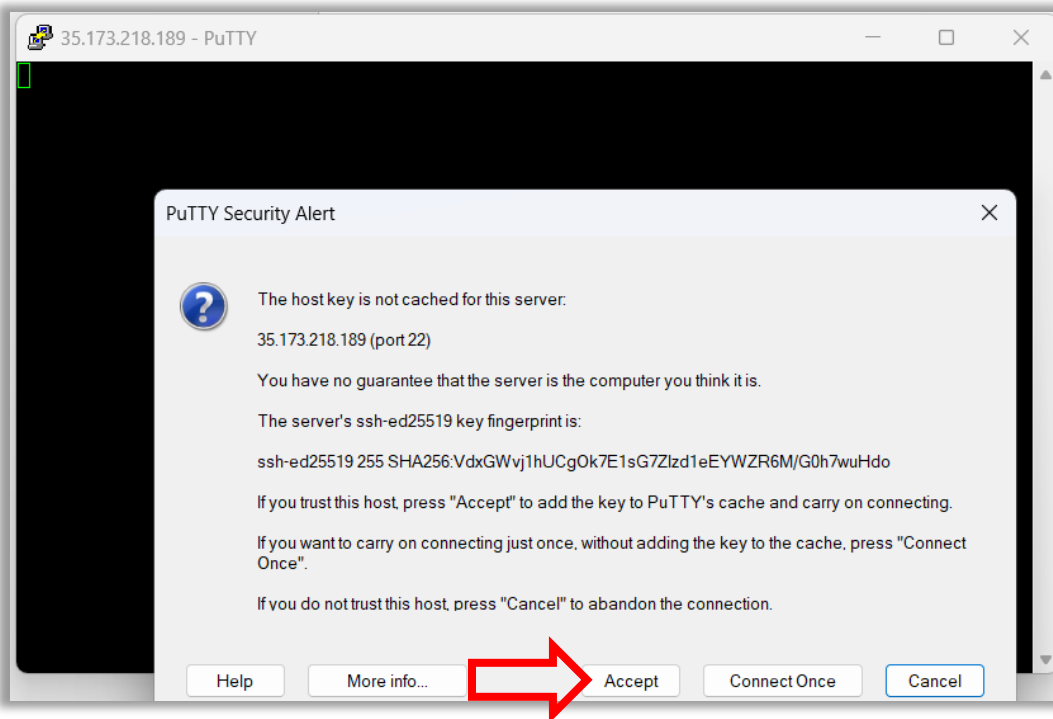
Step 9b. Authenticate your SSH Connection and Choose the Private Key that was selected with the EC2 instance.

- Expand the SSH tab by clicking on +
- Select the AUTH tab and click the +
- Choose **credentials**, click on Browse.



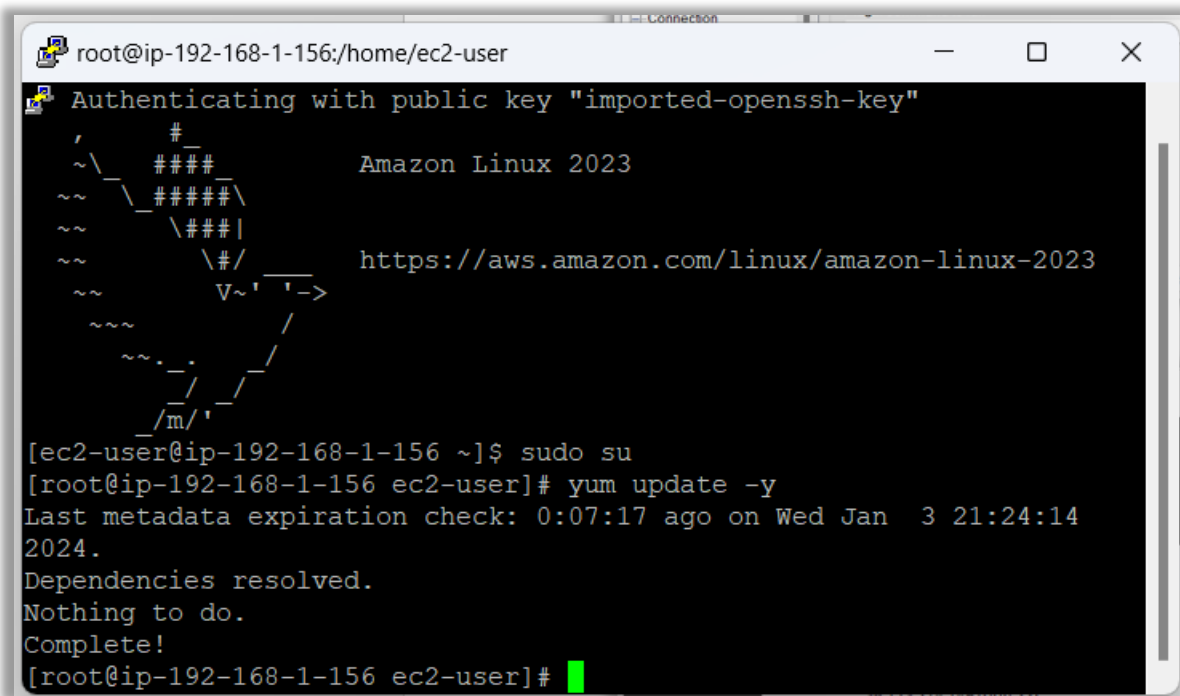


Step 9c. Click Accept



Step 10. Type following Linux commands.

- **sudo su** to become a root user | **yum update -y** to update the instance.



CONGRATULATIONS!! You have completed the EC2 Lab!