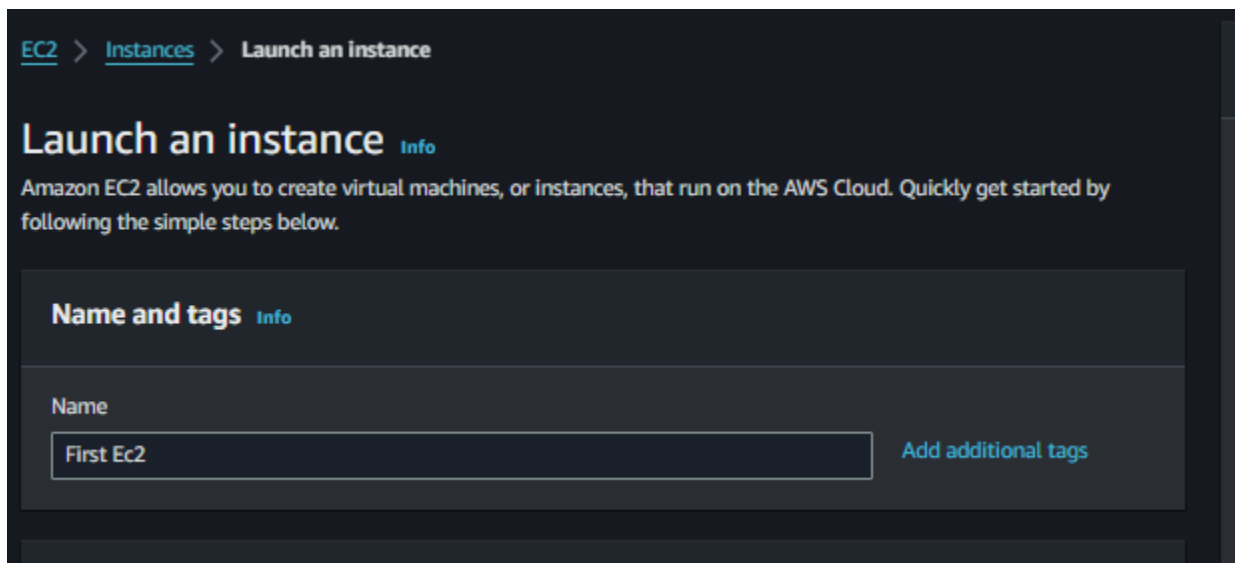


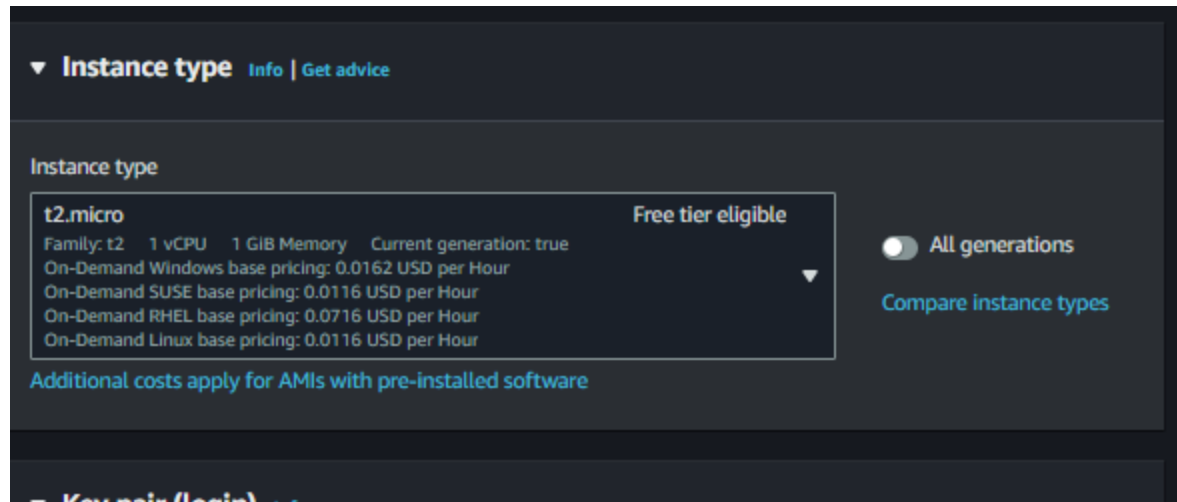
1. EC2 Basics Lab

- **Objective:** To understand the process of setting up and managing an Amazon EC2 instance.
- **Approach:** Students will start by launching a new EC2 instance, selecting an appropriate instance type and configuring the instance details. They will then create and configure a new Security Group, and allocate an Elastic IP address to the instance. The lab will also include connecting to the instance via SSH.
- **Goal:** By the end of this lab, students should be able to launch and manage an EC2 instance, understand instance types, security groups, and IP addressing in AWS.

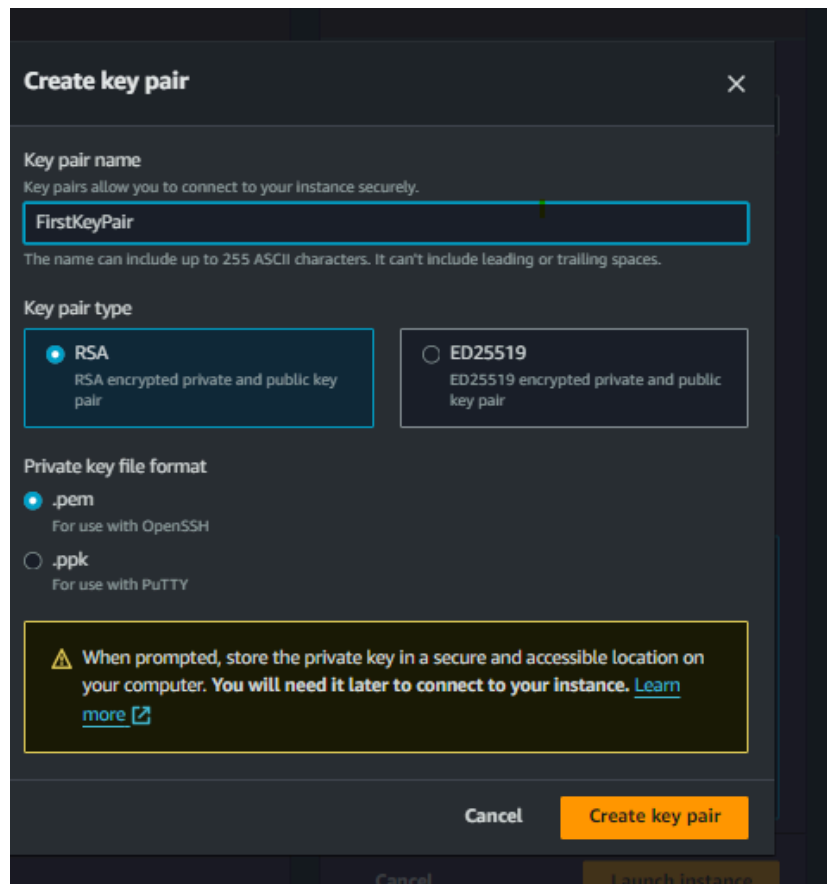
1. Open AWS Console ,select EC2 and Give the EC2 instance name
2. Select OS images and AMI



3. Select instance type as t2.micro



4. Create Key Pair:



5. Select create security group and edit the rules

▼ Network settings Info

Edit

Network Info

vpc-011240c3c27b5f129

Subnet Info

No preference (Default subnet in any availability zone)

Auto-assign public IP Info

Enable

Firewall (security groups) Info

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

☒ Create security group

☐ Select existing security group

We'll create a new security group called 'launch-wizard-1' with the following rules:

☒ Allow SSH traffic from
Helps you connect to your instance

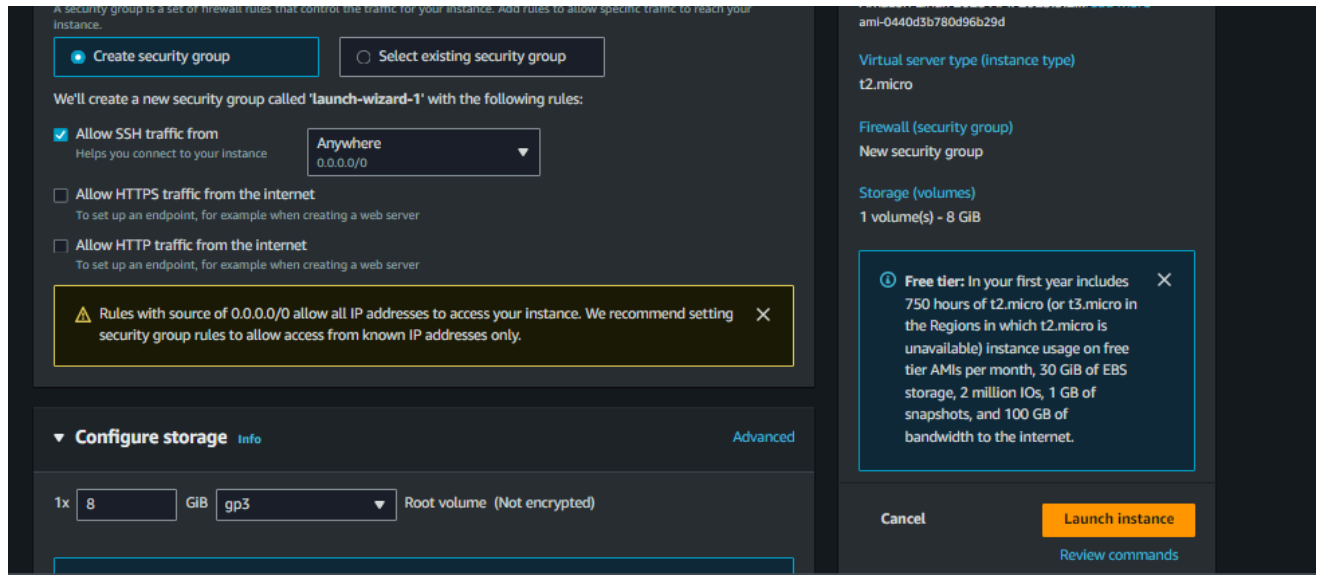
Anywhere
0.0.0.0/0 ▼

☐ Allow HTTPS traffic from the internet
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. ✕

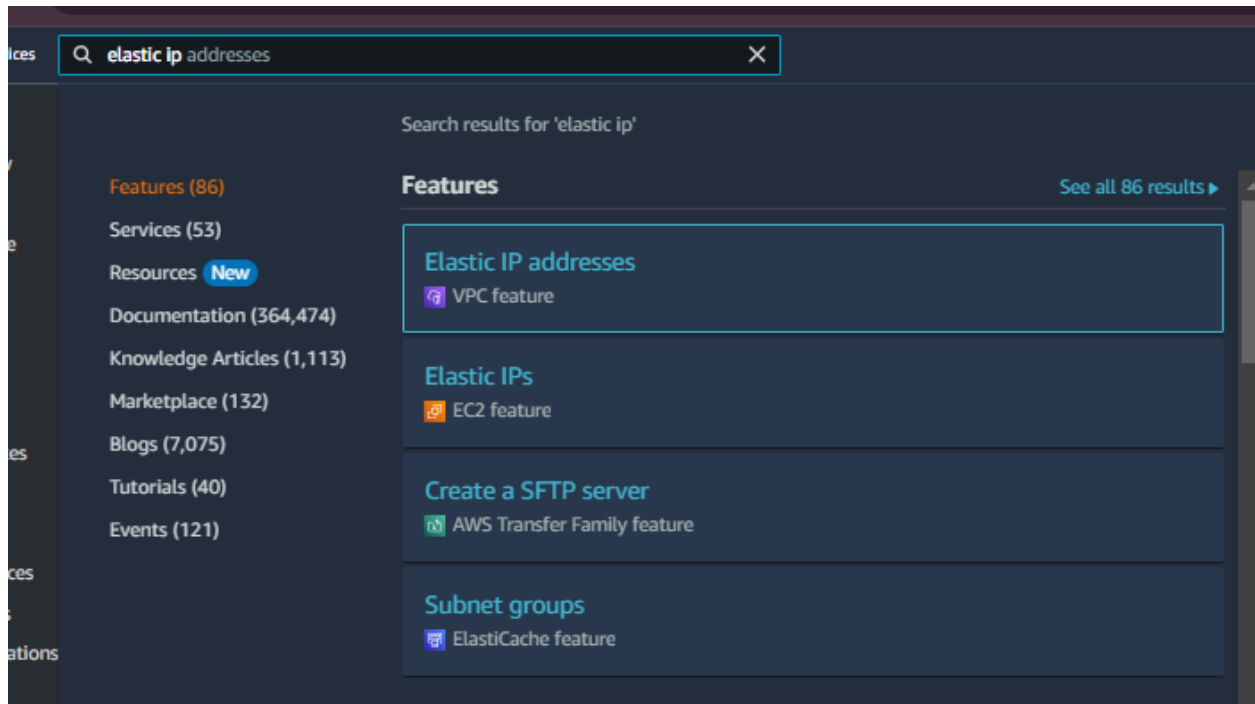
6.Lunch Instance:



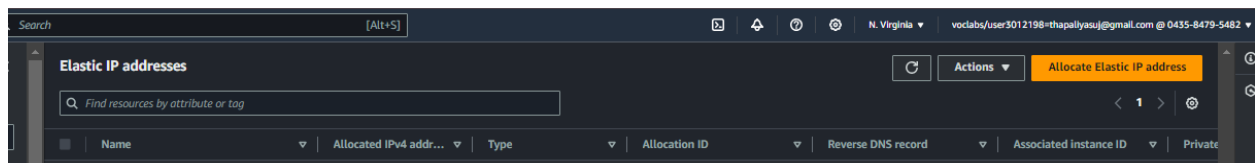
7. Now Instance has been successfully created.

Instances (1) Info										
Find Instance by attribute or tag (case-sensitive)										
Any state										
<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elast
<input type="checkbox"/>	First Ec2	i-04bd9eb1b757dcb1a	Running	t2.micro	Initializing	View alarms	us-east-1b	ec2-54-234-93-25.com...	54.234.93.25	-

8. Now we adding the Elastic IP address:



9. Allocate Elastic ip address



10. Select IPv4 to set IP address

Network border group [Info](#)

us-east-1

Public IPv4 address pool

- ☒ Amazon's pool of IPv4 addresses
- ☐ Public IPv4 address that you bring to your AWS account with BYOIP. (option disabled because no pools found) [Learn more](#)
- ☐ Customer-owned pool of IPv4 addresses created from your on-premises network for use with an Outpost. (option disabled because no customer owned pools found) [Learn more](#)

Global static IP addresses

AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. [Learn more](#)

Create accelerator

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 tag

Cancel Allocate

11.click action and select associate elastic ip address

Services Search [Alt+S]

N. Virginia

vocalabs/user3012198-thapaliyasuj@gmail.com @ 0435-8479-54

Elastic IP addresses (1/1)

Find resources by attribute or tag

Name	Allocated IPv4 address	Type	Allocation ID	Reverse DNS record
-	44.198.62.115	Public IP	eipalloc-0788fc18ed1aedf0f	-

Actions

- Allocate Elastic IP address
- View details
- Release Elastic IP address
- Associate Elastic IP address
- Disassociate Elastic IP address
- Update reverse DNS
- Enable transfers
- Disable transfers
- Accept transfers

12.Select the EC2 instance and click associate

aws

Services

Search

[Alt+S]

VPC > Elastic IP addresses > Associate Elastic IP address

Associate Elastic IP addressInfo

Choose the Instance or network interface to associate to this Elastic IP address (44.198.62.115)

Elastic IP address: 44.198.62.115

Resource type
Choose the type of resource with which to associate the Elastic IP address.

☒ Instance

☐ Network interface

⚠ If you associate an Elastic IP address with an instance that already has an Elastic IP address associated, the previously associated Elastic IP address will be disassociated, but the address will still be allocated to your account. [Learn more](#)

If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address.

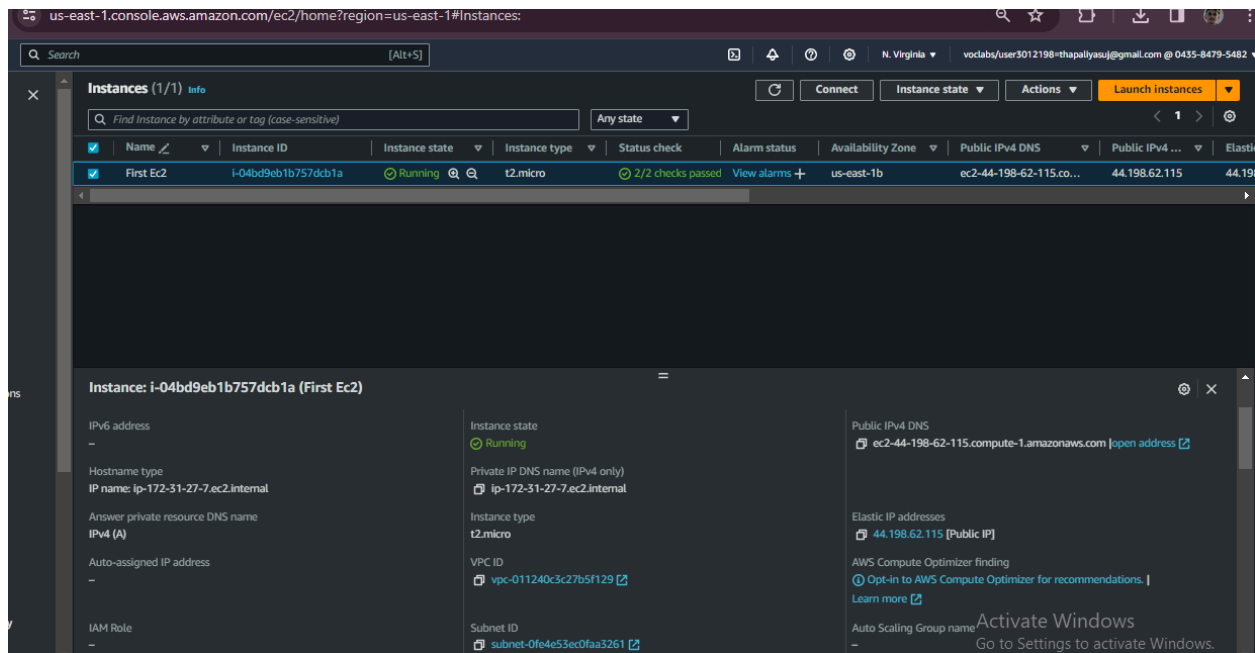
Instance

Private IP address
The private IP address with which to associate the Elastic IP address.

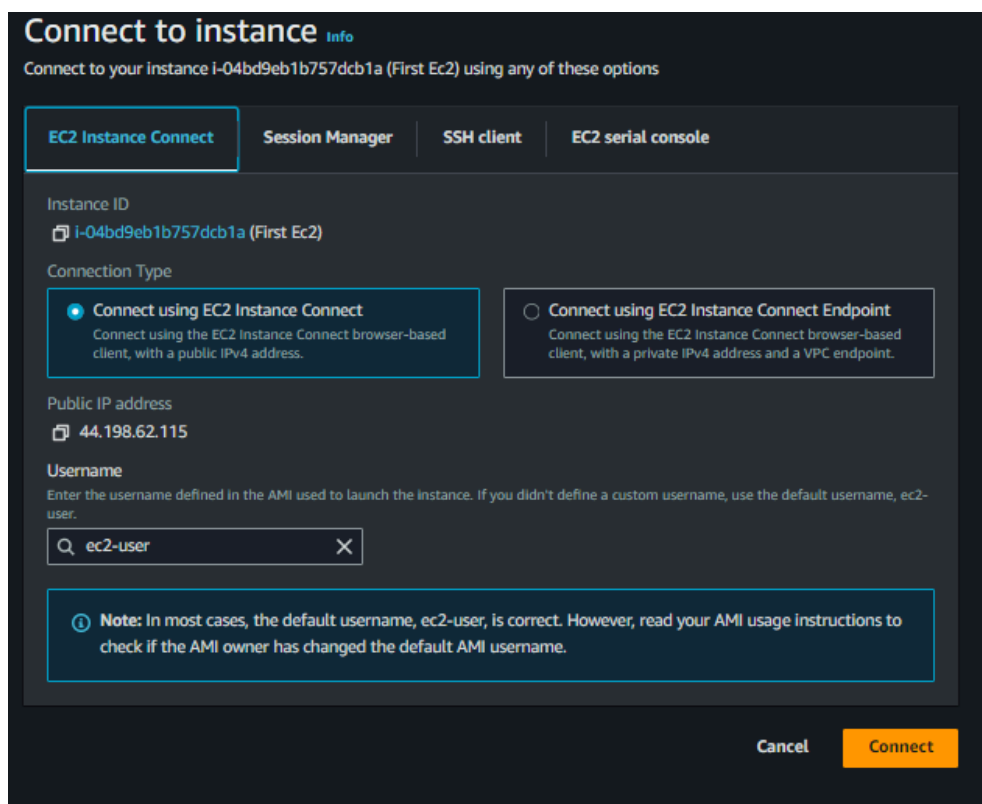
Reassociation
Specify whether the Elastic IP address can be reassociated with a different resource if it already associated with a resource.

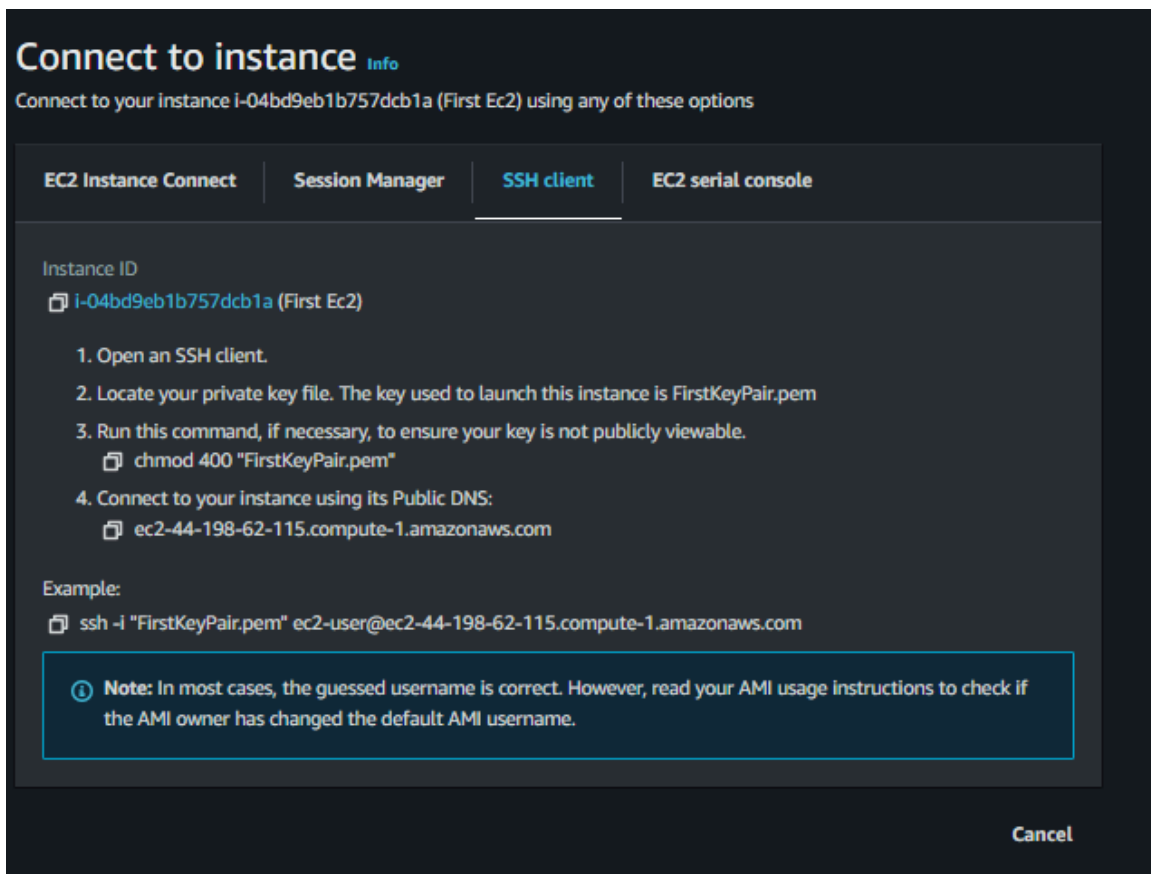
☐ Allow this Elastic IP address to be reassociated

13. Now we can see the ec2 is assigned an IP

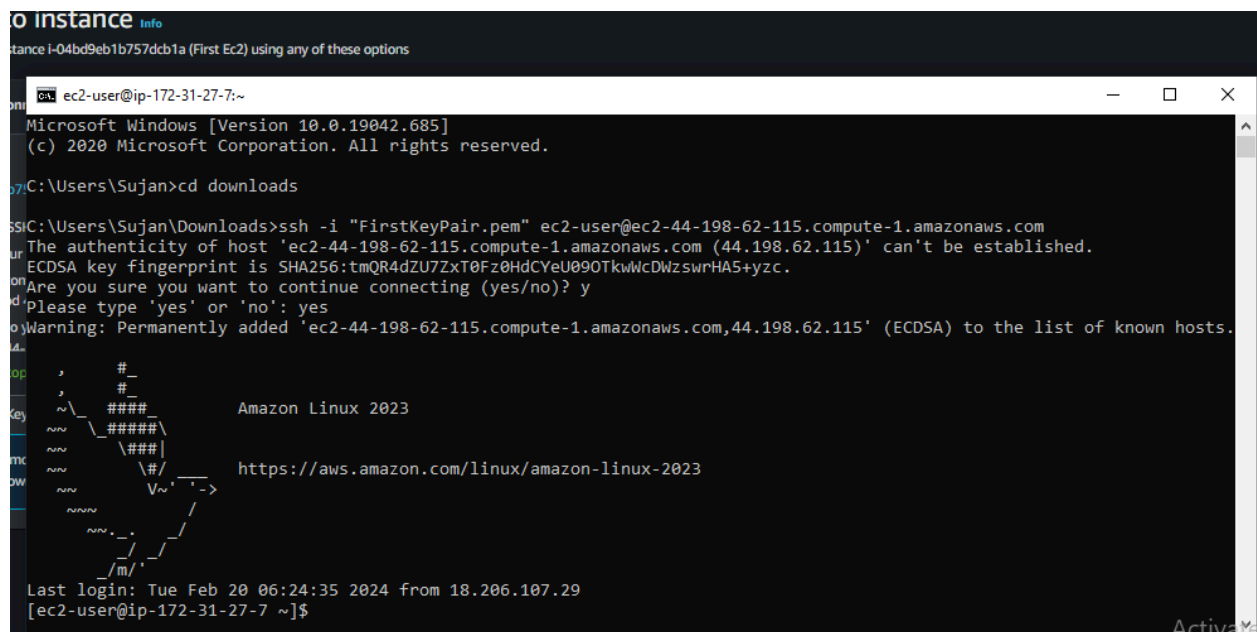


14. To connect to the ec2 instance via ssh with .pem file





15. EC2 Instance Connect loads in a new page



2. S3 Storage Fundamentals Lab

- **Objective:** To gain hands-on experience with Amazon S3 by performing basic storage operations.
- **Approach:** This lab involves creating an S3 bucket, uploading files to it, and setting up bucket policies for access control. Students will explore the S3 management console, learn about object storage, and understand the concepts of buckets and objects.
- **Goal:** Students will understand how to use S3 for storing and managing data, learn about S3 security and permissions, and become familiar with S3's user interface.

1. Go to the AWS Console and select S3 Click create bucket to create the S3 bucket and give unique bucket name:

The screenshot shows the 'Create bucket' page in the AWS Management Console. The 'General configuration' section is active, showing the 'AWS Region' set to 'US East (N. Virginia) us-east-1'. Under 'Bucket type', 'General purpose' is selected. The 'Bucket name' field contains 'basiclabbucket'. Below this, there is a 'Copy settings from existing bucket - optional' section with a 'Choose bucket' button. The 'Object Ownership' section at the bottom shows 'ACLs enabled' selected. The interface is dark-themed.

General configuration

AWS Region
US East (N. Virginia) us-east-1

Bucket type [Info](#)

- ☒ **General purpose**
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.
- ☐ **Directory - New**
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name [Info](#)
basiclabbucket
Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
[Choose bucket](#)
Format: s3://bucket/prefix

Object Ownership [Info](#)
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

- ☐ **ACLs disabled (recommended)**
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using...
- ☒ **ACLs enabled**
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be...

Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

☐ **ACLs disabled (recommended)**

All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

☒ **ACLs enabled**

Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

⚠ We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.


Object Ownership


☒ **Bucket owner preferred**

If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

☐ **Object writer**

The object writer remains the object owner.

i If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. [Learn more](#) 

applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#) 

☐ **Block all public access**

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☐ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

☐ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**

S3 will ignore all ACLs that grant public access to buckets and objects.

☐ **Block public access to buckets and objects granted through *new* public bucket or access point policies**

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

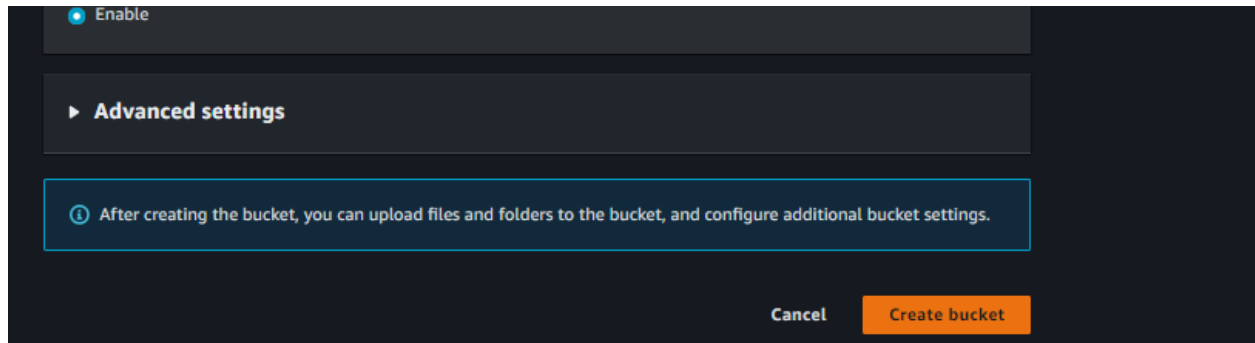
☐ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

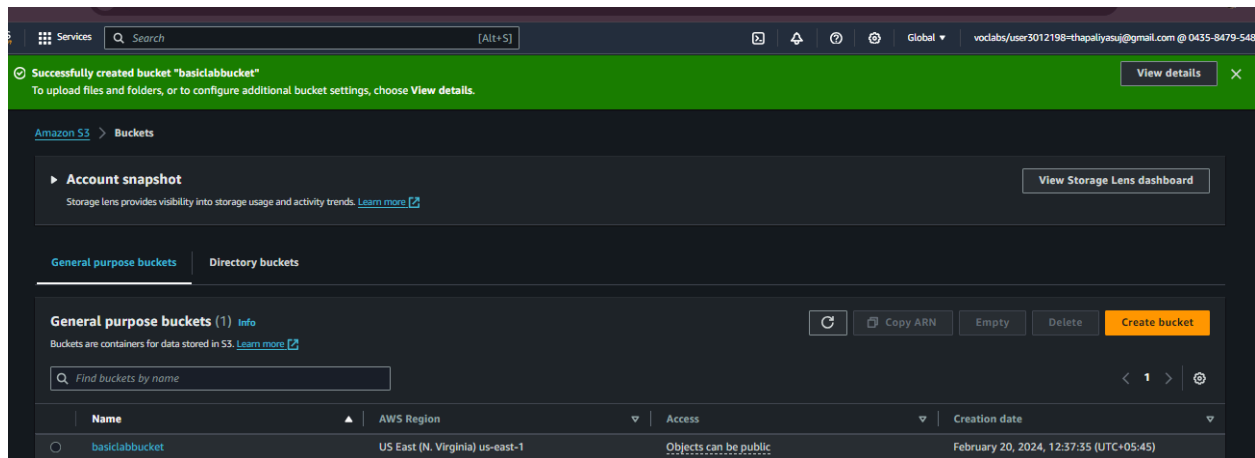
⚠ Turning off block all public access might result in this bucket and the objects within becoming public. AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☒ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

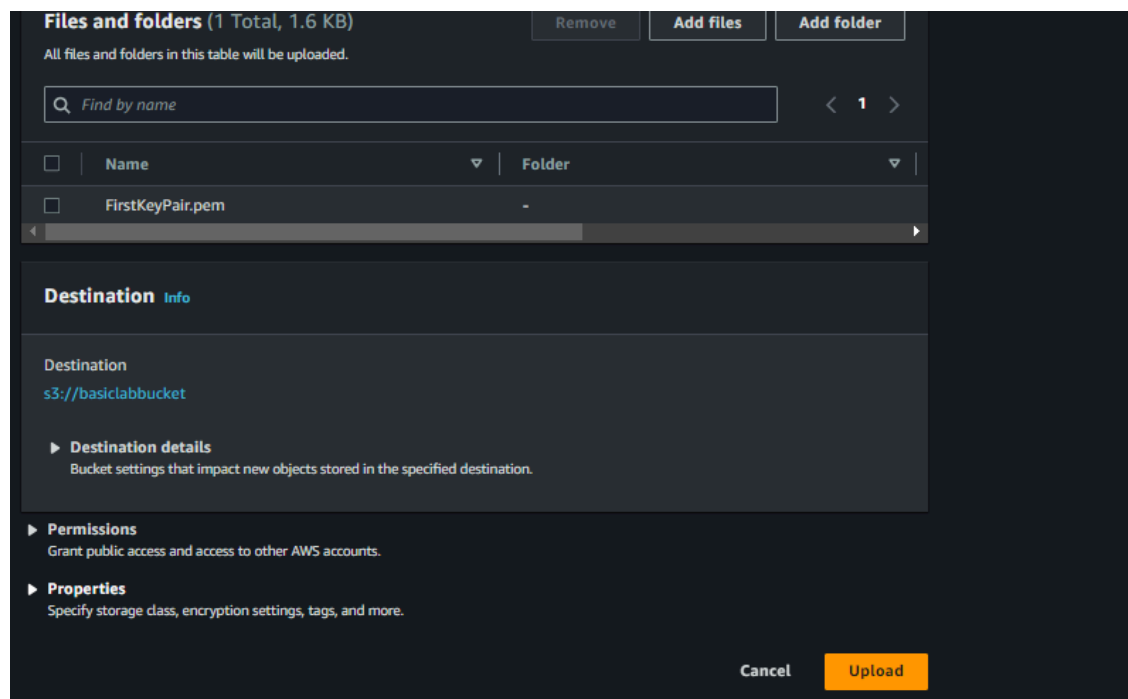
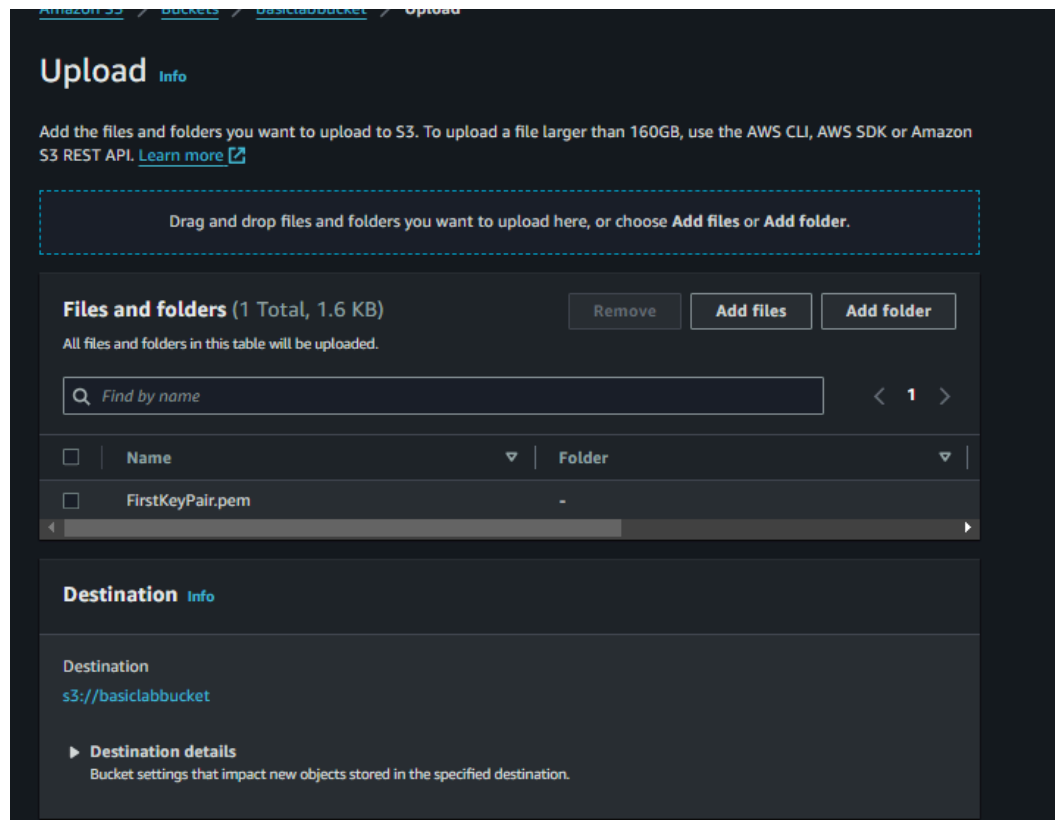
2. Click create bucket



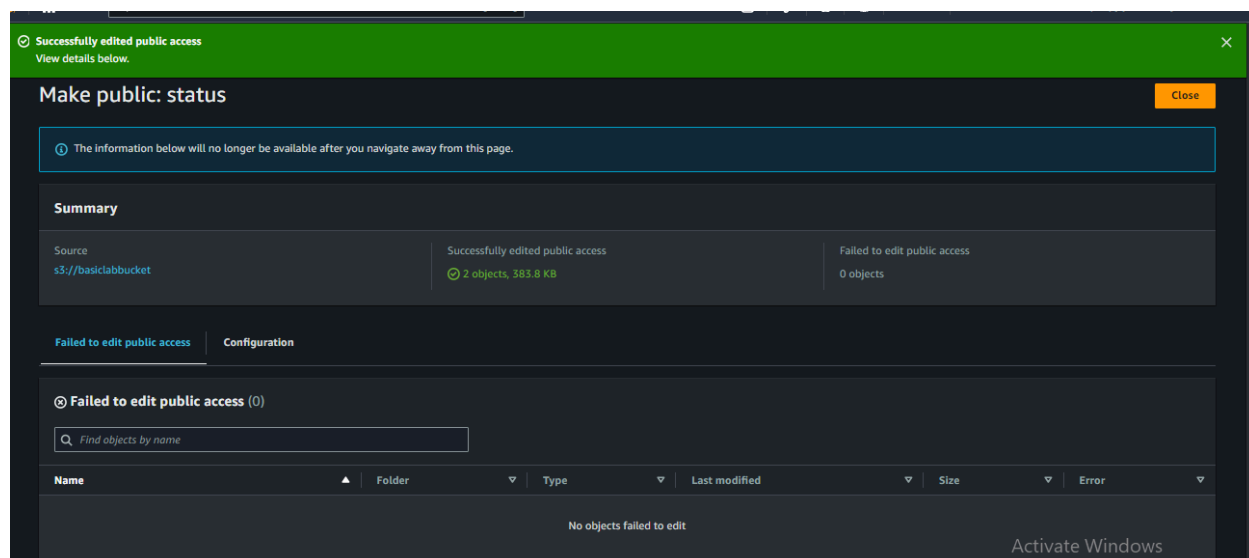
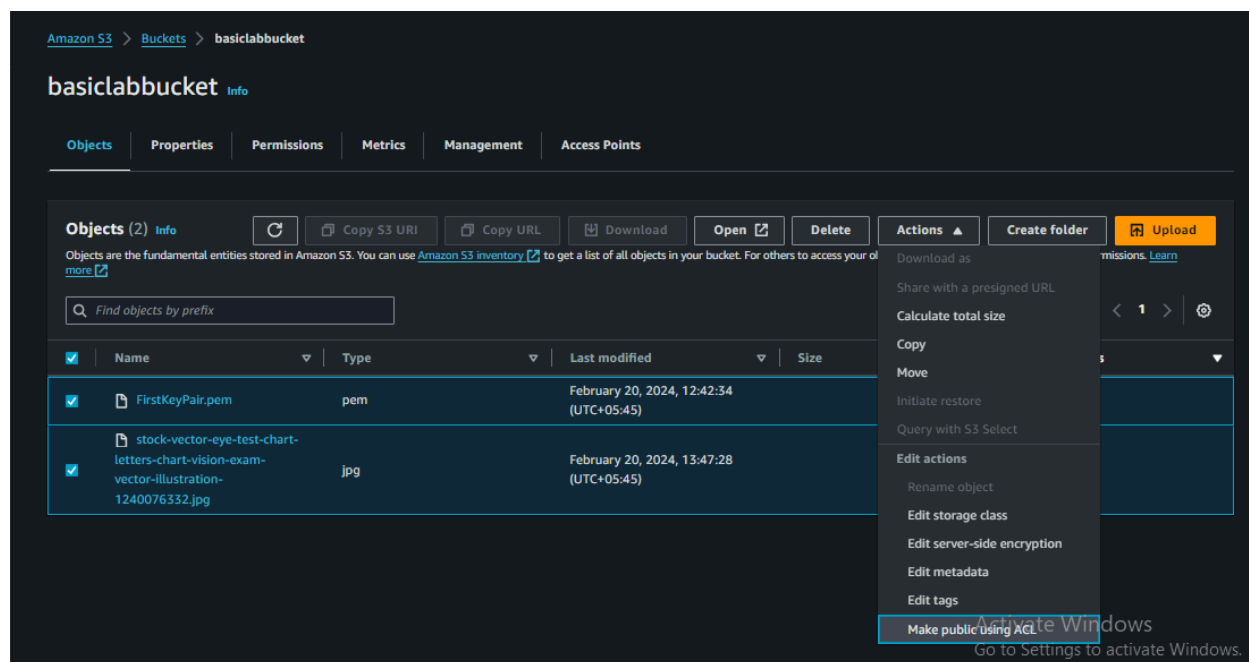
3. Bucket created successfully:



4. Click upload to upload the file



5. Make public using ACL: (Bucket Policy)



6. Now access the bucket through public URL

stock-vector-eye-test-chart-letters-chart-vision-exam-vector-illustration-1240076332.jpg

Copy S3 URI

Download

Open

Object actions

Properties

Permissions

Versions

Object overview

Owner

awslabsOw6979356t1703207674

AWS Region

US East (N. Virginia) us-east-1

Last modified

February 20, 2024, 13:47:28 (UTC+05:45)

Size

382.2 KB

Type

jpg

Key

stock-vector-eye-test-chart-letters-chart-vision-exam-vector-illustration-1240076332.jpg

S3 URI

s3://basiclabbucket/stock-vector-eye-test-chart-letters-chart-vision-exam-vector-illustration-1240076332.jpg

Amazon Resource Name (ARN)

arn:aws:s3:::basiclabbucket/stock-vector-eye-test-chart-letters-chart-vision-exam-vector-illustration-1240076332.jpg

Entity tag (Etag)

6612fb586a986670e754640f5ad8818a

Object URL

https://basiclabbucket.s3.amazonaws.com/stock-vector-eye-test-chart-letters-chart-vision-exam-vector-illustration-1240076332.jpg

Activate Windows

utterstock

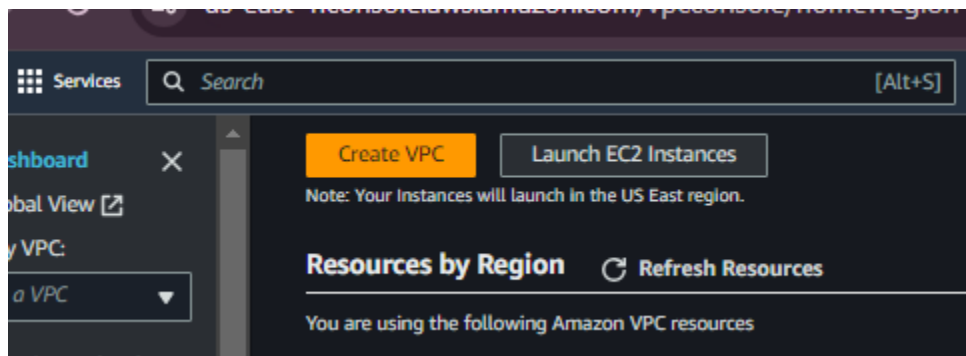
E	1	20/200
F P	2	20/100
T O Z	3	20/70
L P E D	4	20/50
P E C F D	5	20/40
E D F C Z P	6	20/30
D E F P O T E C	7	20/20

Activate Windows

3. VPC Configuration Lab

- **Objective:** To understand the fundamentals of AWS networking through the configuration of a Virtual Private Cloud (VPC).
- **Approach:** Students will create a new VPC, add subnets, set up an Internet Gateway, and configure route tables. The lab might also include setting up a simple EC2 instance within this VPC to demonstrate how resources are deployed in a custom network environment.
- **Goal:** By the end of this lab, students should be able to create and configure a VPC, understand subnetting, and the role of route tables and internet gateways in AWS.

1. Open AWS Console and search for VPC and click create VPC



Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such

VPC settings

Resources to create Info

Create only the VPC resource or the VPC and other networking resources.

☐ VPC only

☒ VPC and more

Name tag auto-generation Info

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

☒ Auto-generate

lab

IPv4 CIDR block Info

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

10.0.0.0/16

65,536 IPs

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

IPv6 CIDR block Info

☒ No IPv6 CIDR block

☐ Amazon-provided IPv6 CIDR block

Tenancy Info

Default

The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0

1

Number of private subnets Info

The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0

1

2

Customize subnets CIDR blocks

Public subnet CIDR block in us-east-1a

10.0.0.0/20

4,096 IPs

Private subnet CIDR block in us-east-1a

10.0.128.0/20

4,096 IPs

NAT gateways (\$) Info

Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway.

None

In 1 AZ

1 per AZ

VPC endpoints Info

Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

None

S3 Gateway

DNS options Info

☒ Enable DNS hostnames

☒ Enable DNS resolution

Additional tags

Cancel

Create VPC

2. Click create VPC and the VPC will be created in a while

VPC > Your VPCs > Create VPC > Create VPC resources

Create VPC workflow

✓ Success

▼ Details

- ✓ Create VPC: vpc-052995eb739249e11
- ✓ Enable DNS hostnames
- ✓ Enable DNS resolution
- ✓ Verifying VPC creation: vpc-052995eb739249e11
- ✓ Create subnet: subnet-062e711f0be9af119
- ✓ Create subnet: subnet-00e2c5a7ad3932bd0
- ✓ Create internet gateway: igw-03aa603b1184d7e56
- ✓ Attach internet gateway to the VPC
- ✓ Create route table: rtb-0ee2bcb089e1ed687
- ✓ Create route
- ✓ Associate route table
- ✓ Allocate elastic IP: elpallo-0b80869d66833061e
- ✓ Create NAT gateway: nat-092903cc42450bdd8
- ✓ Wait for NAT Gateways to activate
- ✓ Create route table: rtb-053875ede0f6b00e7
- ✓ Create route
- ✓ Associate route table
- ✓ Verifying route table creation

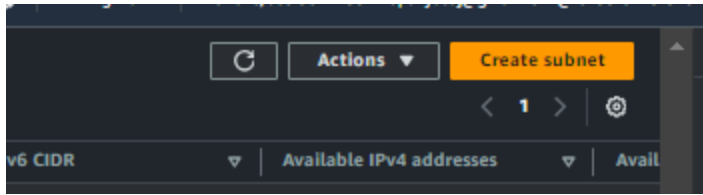
[View VPC](#)

vpc-052995eb739249e11 / project-vpc

Details info

VPC ID vpc-052995eb739249e11	State Available	DNS hostnames Enabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-009874bd5e947026b	Main route table rtb-043705d2b748e634	Main network ACL acl-0b6dc98479b04a71d
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool -	IPv6 CIDR (Network border group) -
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups Failed to load rule groups	Owner ID 043584795482	

3. To add Subnets, click Subnet and create :



8. Select the created VPC .Now give subnet name, availability zone, and add the IPv4-CIDR subnet

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.

vpc-052995eb739249e11 (lab-vpc) ▼

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 2

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

first-subnet

The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

US East (N. Virginia) / us-east-1a ▼

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

10.0.0.0/16 ▼

IPv4 subnet CIDR block

10.0.16.0/20 4,096 IPs

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
 4,096 IPs

▼ **Tags - optional**

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

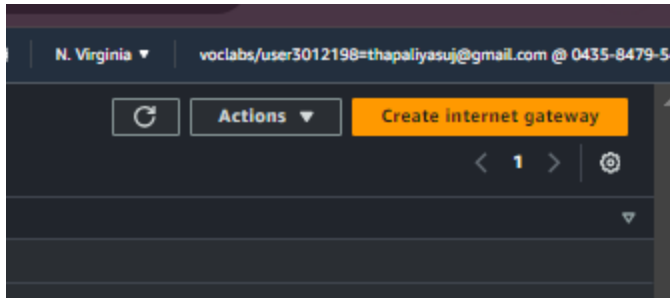
You can add 49 more tags.

9.Subnets created:

You have successfully created 2 subnets: subnet-049a7a9e94dc60881, subnet-08a43a0dc9d3959d

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses	Avail
first-subnet	subnet-049a7a9e94dc60881	Available	vpc-052995eb739249e11 lab-...	10.0.16.0/20	-	4091	us-ea
second-subnet	subnet-08a43a0dc9d3959d	Available	vpc-052995eb739249e11 lab-...	10.0.32.0/20	-	4091	us-ea

10.To set up the Internet Gateway, select Internet gateway from left-bar and select 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 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.

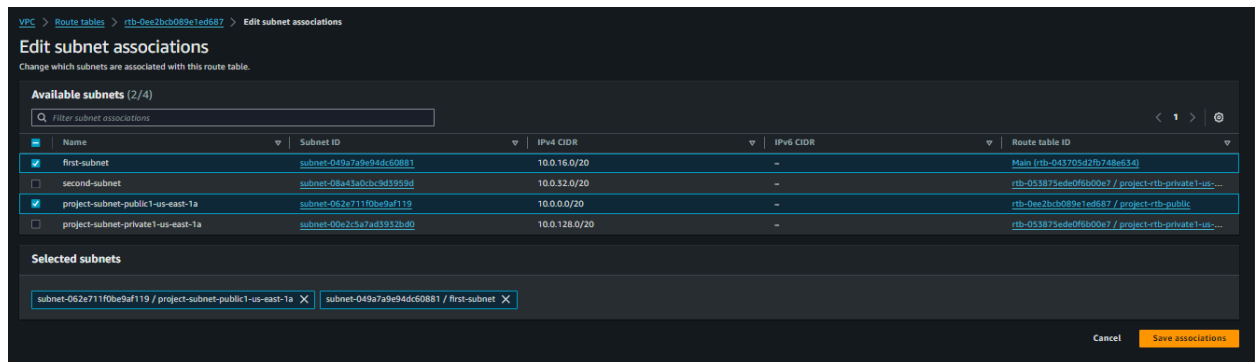
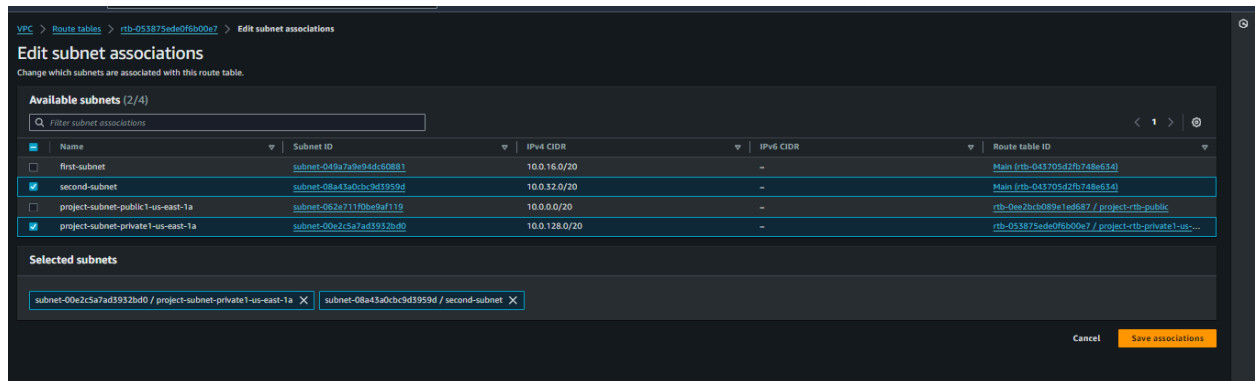
Key	Value - optional	
<input type="text" value="Name"/>	<input type="text" value="first-Internet-gateway"/>	<input type="button" value="Remove"/>

You can add 49 more tags.

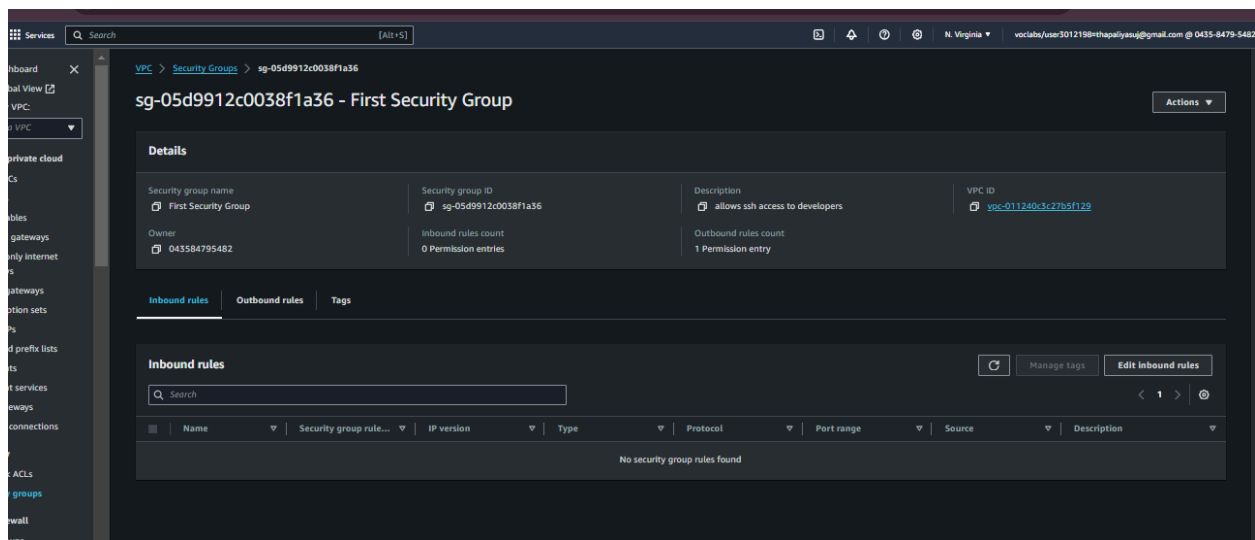
11. Internet gateway created:

	Name	Internet gateway ID	State	VPC ID	Owner
<input type="checkbox"/>	project-igw	igw-03ae603b1184d7e56	Attached	vpc-052995ab739249e11 lab-vpc	043584795482
<input type="checkbox"/>	-	igw-0686b22ce4ff63a9d	Attached	vpc-011240c3c27b5f129	043584795482
<input type="checkbox"/>	first-Internet-gateway	igw-0e57024ce6f70a326	Detached	-	043584795482

12. Configure the Route table by clicking on the Route Table and select the lab session.



13. Create Security Group with necessary rule for the VPC



14. Now create a EC2 instance with the created security group and the VPC And launch

[EC2](#) > [Instances](#) > Launch an instance

Launch an instance [Info](#)

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

Name and tags [Info](#)

Name

ec2 for vpc

Add additional tags

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

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

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

Recents

Quick Start

Amazon Linux

aws

macOS

Mae

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

SUSE Linux

SUSE Linux

Q

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI

ami-0440d3b780d96b29d (64-bit (x86), uefi-preferred) / ami-0f93c02efd1974b8b (64-bit (Arm), uefi)

Free tier eligible

▼ Network settings [Info](#)

Edit

Network [Info](#)

vpc-011240c3c27b5f129

Subnet [Info](#)

No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)

Enable

Firewall (security groups) [Info](#)

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

☐ Create security group

☒ Select existing security group

Common security groups [Info](#)

Select security groups

First Security Group sg-05d9912c0038f1a36 X

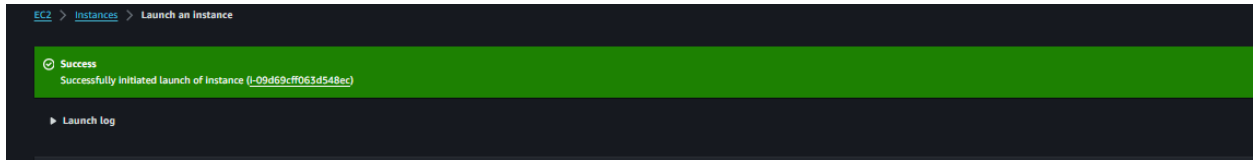
VPC: vpc-011240c3c27b5f129

Compare security group rules

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

▼ Configure storage [Info](#)

Advanced



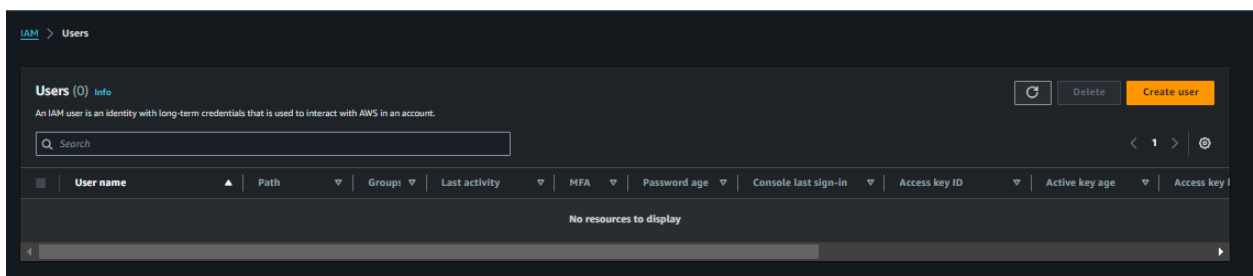
The screenshot shows the "Instances (2)" page in the AWS console. It displays a table with two instances. The table has columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, Public IPv4 DNS, Public IPv4 address, Elastic IP, and IPv6 IPs.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs
First Ec2	i-04bd9eb1b757dcb1a	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1b	ec2-44-198-62-115.co...	44.198.62.115	44.198.62.115	-
ec3 for vpc	i-09d69cf063d548ec	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1b	ec2-3-80-35-38.comput...	3.80.35.38	-	-

4. IAM Users and Roles Lab

- **Objective:** To understand AWS Identity and Access Management (IAM) by creating and managing users, groups, and roles.
- **Approach:** Students will create new IAM users, assign them to groups, and apply policies to manage permissions. The lab will also involve creating roles for AWS services and understanding the use of IAM roles for cross-service access.
- **Goal:** Students will learn about user and permission management in AWS, the importance of roles for security and best practices for IAM.

1. Create a IAM User first, to create this, open the AWS Console Management tab and search for IAM. Click the User on the left side and create IAM user with necessary attribute



Services IAM Users Create user

Step 1 Specify user details

Step 2 Set permissions

Step 3 Review and create

Specify user details

User details

User name
firstuser

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and +, =, @, _ (pgpshen)

☐ Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

Info If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Cancel Next

2. Attach the policy for that user, you have to select attach policies directly radio button to do so

Services IAM Users Create user

Step 1 Specify user details

Step 2 Set permissions

Step 3 Review and create

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

☐ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

☐ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access Analyzer
- External access
- Unused access
- Analyzer settings

Credential report

Organization activity

Service control policies (SCPs)

Related consoles

- IAM Identity Center
- AWS Organizations

Services IAM User groups Create user group

Create user group

Name the group

User group name
Enter a meaningful name to identify this group.
firstgroup
Maximum 128 characters. Use alphanumeric and "+, =, @, _" characters.

Add users to the group - Optional (0) [Info](#)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Search

1

Attach permissions policies - Optional (9/16) [Info](#)

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter by Type

Search

All types

<input type="checkbox"/>	Policy name	Type	Used as	Description
<input type="checkbox"/>	AdministratorAccess	AWS managed - job function	Permissions policy (1)	Provides full access to AWS services an...
<input type="checkbox"/>	AdministratorAccess-Ampify	AWS managed	None	Go to settings to activate window...

User group was not created.
 User: iam.amazonaws.com:assumed-role/voclabs/user3012198-thapalysas@gmail.com is not authorized to perform: iam:CreateGroup on resource: iam::awsiam:043584795482:group/* because no Identity-based policy allows the iam:CreateGroup action

Name	Type	Managed By	Permissions Summary	Description
AdministratorAccess-AWSelasticBeanstalk	Managed	AWS managed	None	Grants account administrative permissions...
AlexaForBusinessDeviceSetup	Managed	AWS managed	None	Provide device setup access to AlexaForBusiness...
AlexaForBusinessFullAccess	Managed	AWS managed	None	Grants full access to AlexaForBusiness...
AlexaForBusinessGatewayExecution	Managed	AWS managed	None	Provide gateway execution access to AlexaForBusiness...
AlexaForBusinessLifecycleDelegatedAccessPolicy	Managed	AWS managed	None	Provide access to Lifecycle AVS devices
AlexaForBusinessPolyDelegatedAccessPolicy	Managed	AWS managed	None	Provide access to Poly AVS devices
AlexaForBusinessReadOnlyAccess	Managed	AWS managed	None	Provide read only access to AlexaForBusiness...
AmazonAPIGatewayAdministrator	Managed	AWS managed	None	Provides full access to create/edit/delete API Gateway resources...
AmazonAPIGatewayInvokeFullAccess	Managed	AWS managed	None	Provides full access to invoke APIs in Amazon API Gateway...
AmazonAPIGatewayPushToCloudWatchLogs	Managed	AWS managed	None	Allows API Gateway to push logs to CloudWatch Logs...
AmazonAppFlowFullAccess	Managed	AWS managed	None	Provides full access to Amazon AppFlow...
AmazonAppFlowReadOnlyAccess	Managed	AWS managed	None	Provides read only access to Amazon AppFlow...
AmazonAppStreamFullAccess	Managed	AWS managed	None	Provides full access to Amazon AppStream...
AmazonAppStreamPCAAccess	Managed	AWS managed	None	Amazon AppStream 2.0 access to AWS IAM...
AmazonAppStreamReadOnlyAccess	Managed	AWS managed	None	Provides read only access to Amazon AppStream...
AmazonAppStreamServiceAccess	Managed	AWS managed	None	Default policy for Amazon AppStream...
AmazonAthenaFullAccess	Managed	AWS managed	None	Provide full access to Amazon Athena...
AmazonAugmentedAIRuntimeFullAccess	Managed	AWS managed	None	Provides access to perform all operations on Amazon Augmented AI Runtime...