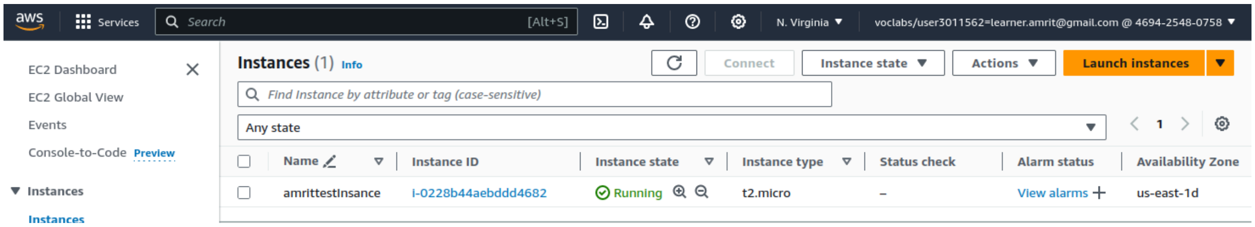
1. EC2 Basics Lab

- 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.

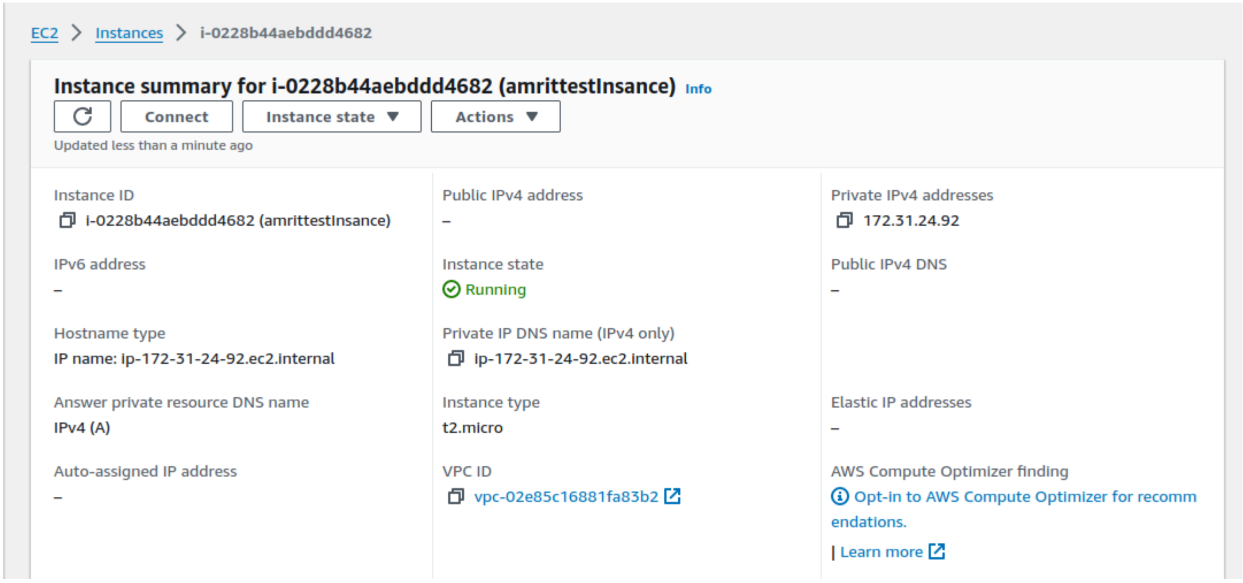
1. EC2 Instance Created



Instances (1) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
amrittestInsance	i-0228b44aebddd4682	✓ Running	t2.micro	–	View alarms +	us-east-1d

2.Instance Summary



Instance summary for i-0228b44aebddd4682 (amrittestInsance) Info

Updated less than a minute ago

Instance ID
i-0228b44aebddd4682 (amrittestInsance)

Public IPv4 address
–

Private IPv4 addresses
172.31.24.92

IPv6 address
–

Instance state
✓ Running

Public IPv4 DNS
–

Hostname type
IP name: ip-172-31-24-92.ec2.internal

Private IP DNS name (IPv4 only)
ip-172-31-24-92.ec2.internal

Answer private resource DNS name
IPv4 (A)

Instance type
t2.micro

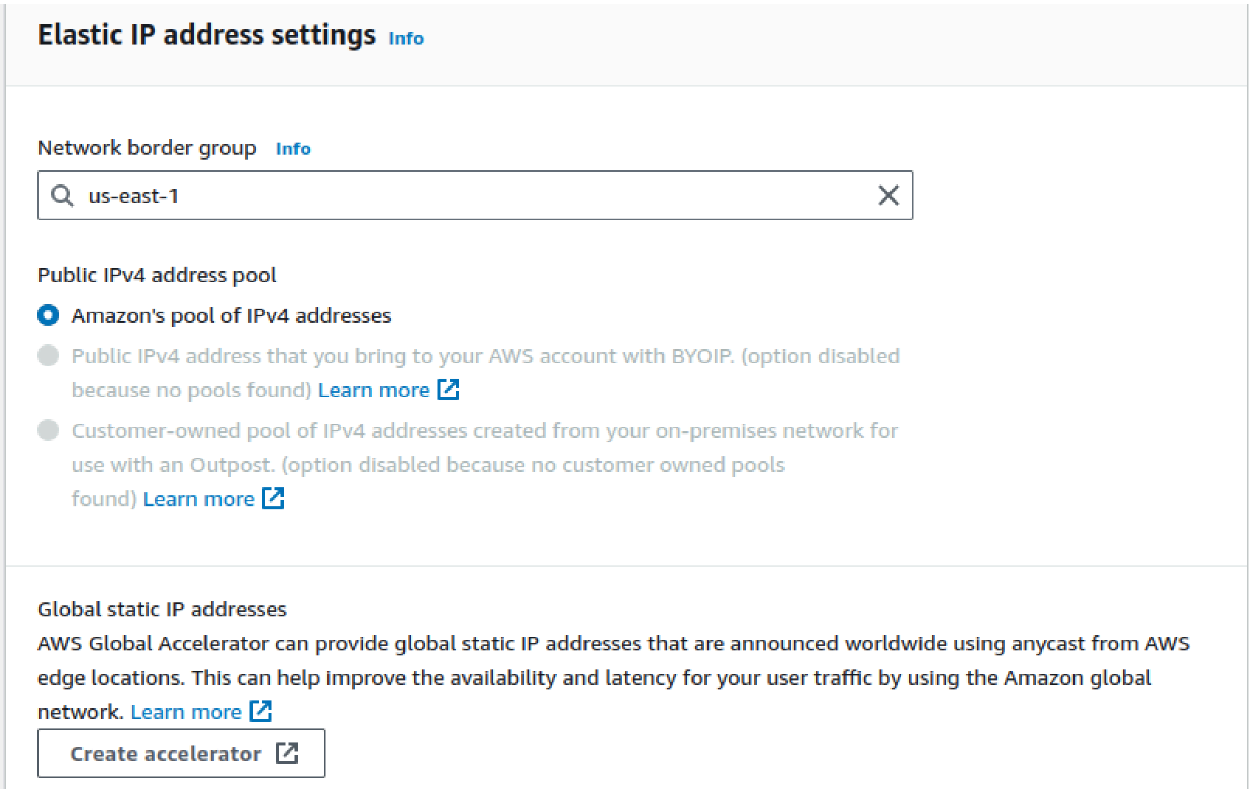
Elastic IP addresses
–

Auto-assigned IP address
–

VPC ID
vpc-02e85c16881fa83b2

AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations.
| Learn more

2.Adding the Elastic IP address



Elastic IP address settings Info

Network border group Info

us-east-1

Public IPv4 address pool

● Amazon's pool of IPv4 addresses

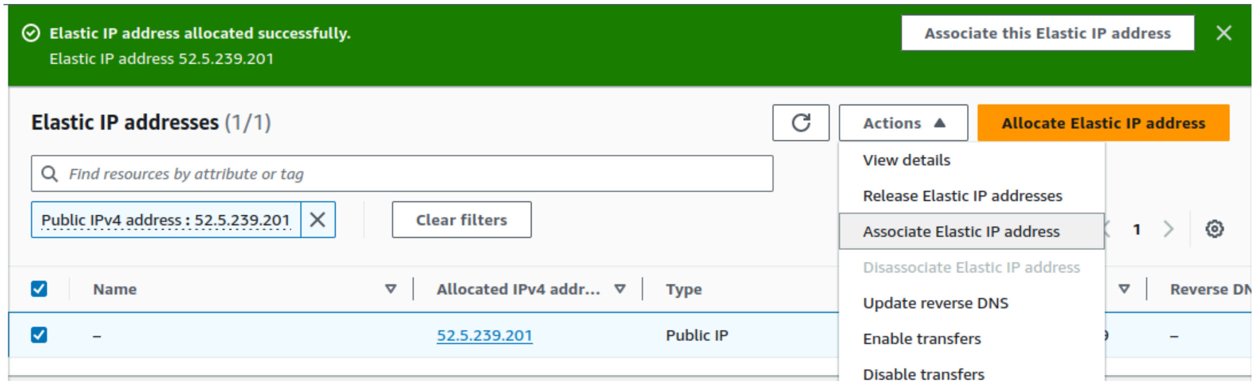
○ Public IPv4 address that you bring to your AWS account with BYOIP. (option disabled because no pools found) Learn more

○ 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

3.Allocate Elastic IP address



Elastic IP address allocated successfully.
Elastic IP address 52.5.239.201

Associate this Elastic IP address
Actions
Allocate Elastic IP address
View details
Release Elastic IP addresses
Associate Elastic IP address
Disassociate Elastic IP address
Update reverse DNS
Enable transfers
Disable transfers
Clear filters
1

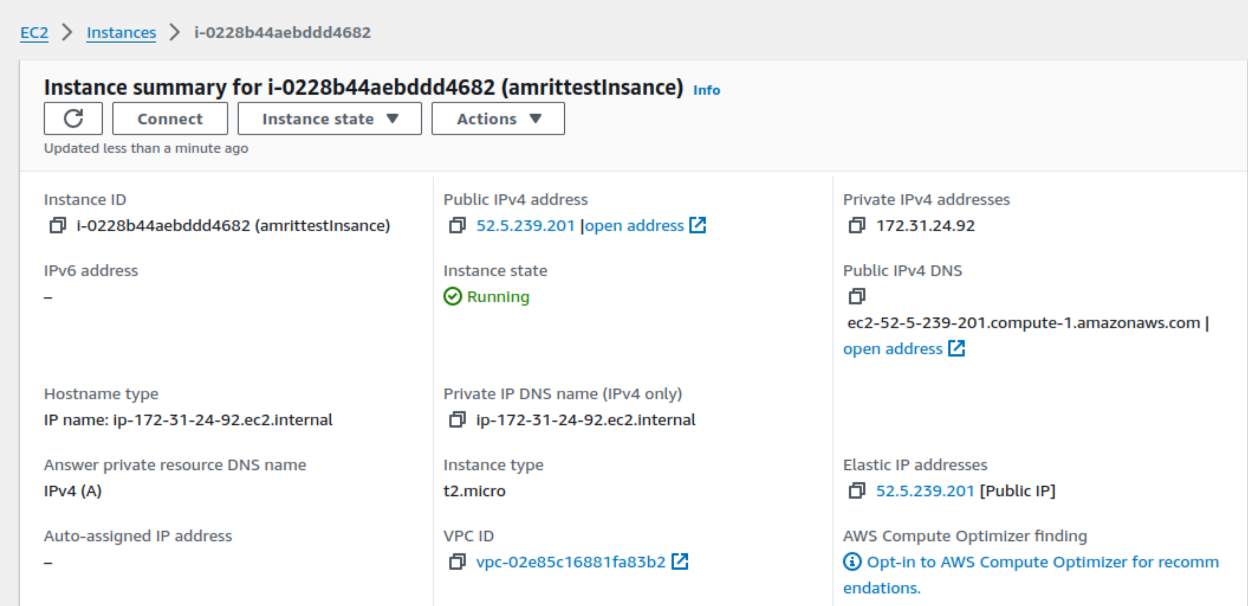
Elastic IP addresses (1/1)

Find resources by attribute or tag

Public IPv4 address : 52.5.239.201

☑	Name	Allocated IPv4 addr...	Type	Reverse DN
☑	–	52.5.239.201	Public IP	–

4.Elastic IP Assigned



Instance summary for i-0228b44aebddd4682 (amrittestInsance)

Updated less than a minute ago

Instance ID
i-0228b44aebddd4682 (amrittestInsance)

Public IPv4 address
52.5.239.201 |open address

Private IPv4 addresses
172.31.24.92

IPv6 address
–

Instance state
Running

Public IPv4 DNS
ec2-52-5-239-201.compute-1.amazonaws.com | open address

Hostname type
IP name: ip-172-31-24-92.ec2.internal

Private IP DNS name (IPv4 only)
ip-172-31-24-92.ec2.internal

Answer private resource DNS name
IPv4 (A)

Instance type
t2.micro

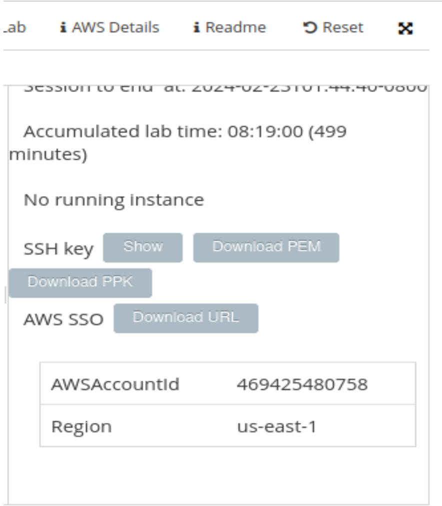
Elastic IP addresses
52.5.239.201 [Public IP]

Auto-assigned IP address
–

VPC ID
vpc-02e85c16881fa83b2

AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations.

5.Connect the EC2 instance via SSH, download the PEM file in AWS Details



Session to end at: 2024-02-23T01:44:40-0800

Accumulated lab time: 08:19:00 (499 minutes)

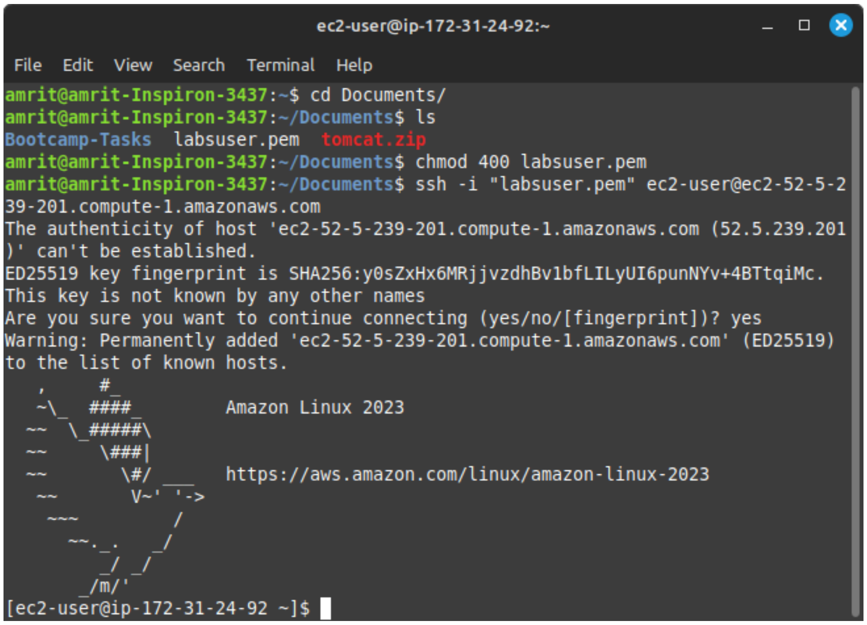
No running instance

SSH key

AWS SSO

AWSAccountId	469425480758
Region	us-east-1

6.Connected via SSH

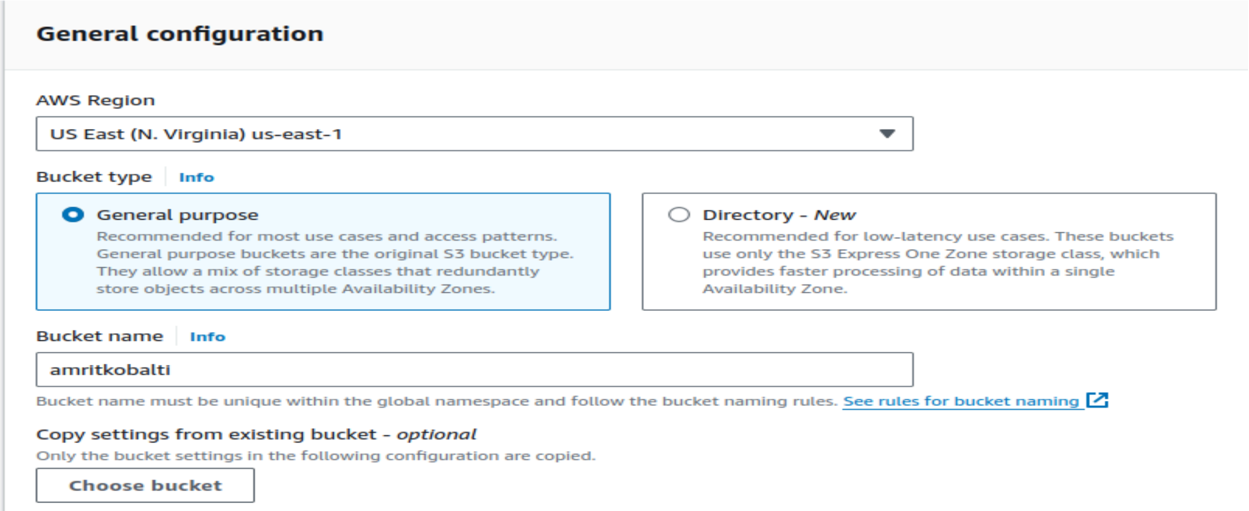


```
amrit@amrit-Inspiron-3437:~$ cd Documents/
amrit@amrit-Inspiron-3437:~/Documents$ ls
Bootcamp-Tasks  labsuser.pem  tomcat.zip
amrit@amrit-Inspiron-3437:~/Documents$ chmod 400 labsuser.pem
amrit@amrit-Inspiron-3437:~/Documents$ ssh -i "labsuser.pem" ec2-user@ec2-52-5-2
39-201.compute-1.amazonaws.com
The authenticity of host 'ec2-52-5-239-201.compute-1.amazonaws.com (52.5.239.201
)' can't be established.
ED25519 key fingerprint is SHA256:y0sZxHx6MRjjvzdhBv1bfLILyUI6punNYv+4BTtqiMc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-52-5-239-201.compute-1.amazonaws.com' (ED25519)
to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-172-31-24-92 ~]$ 
```

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.Create s3 bucket



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.

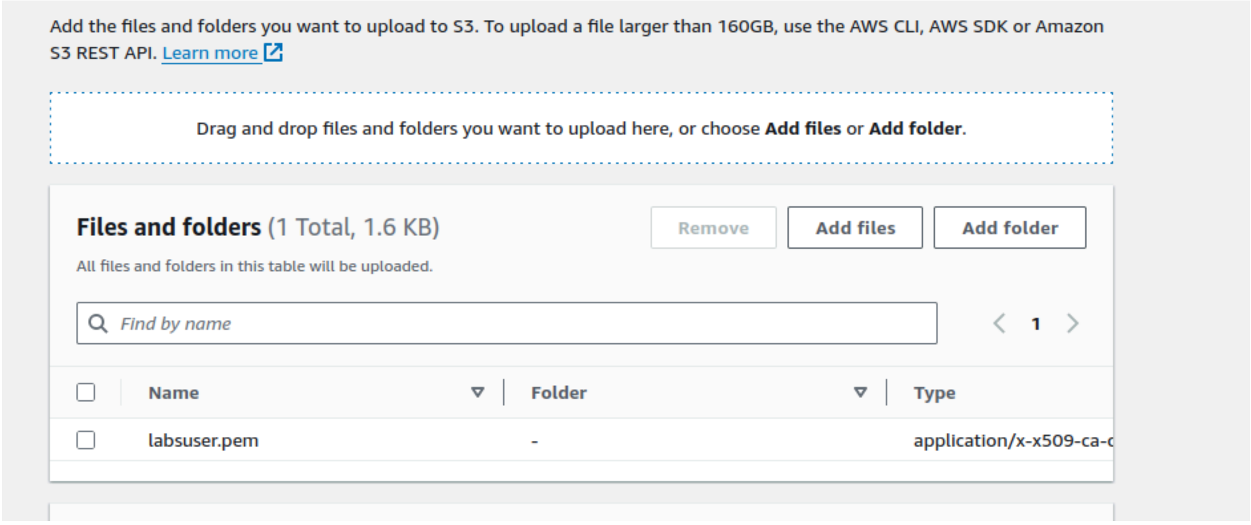
Bucket name Info

amritkobalti

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.

2. Upload file by drag and drop or chose Add files and Add folder



Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more

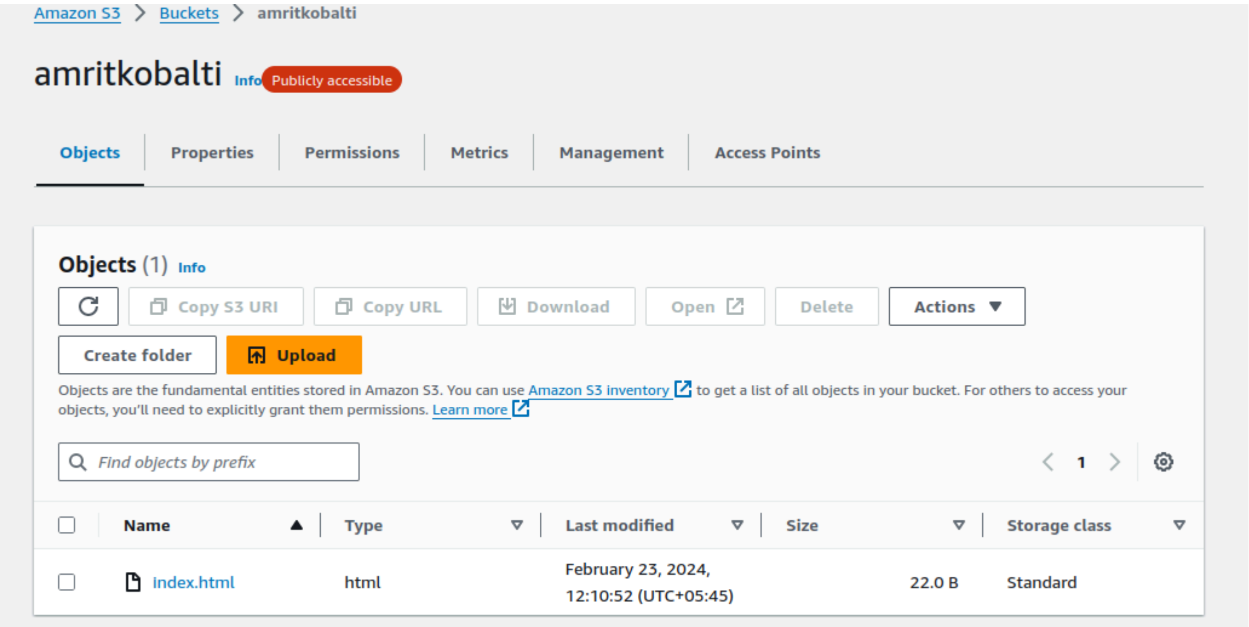
Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

Files and folders (1 Total, 1.6 KB)

All files and folders in this table will be uploaded.

□	Name	Folder	Type
□	labsuser.pem	-	application/x-x509-ca-c

3.File Uploaded



Amazon S3 > Buckets > amritkobalti

amritkobalti Info Publicly accessible

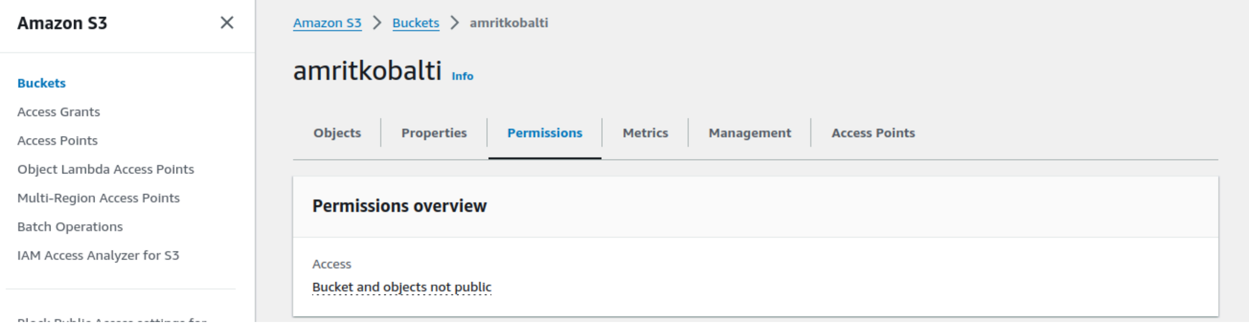
Objects (1) Info

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Find objects by prefix

□	Name	Type	Last modified	Size	Storage class
□	index.html	html	February 23, 2024, 12:10:52 (UTC+05:45)	22.0 B	Standard

4.Change Bucket Permission



Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3

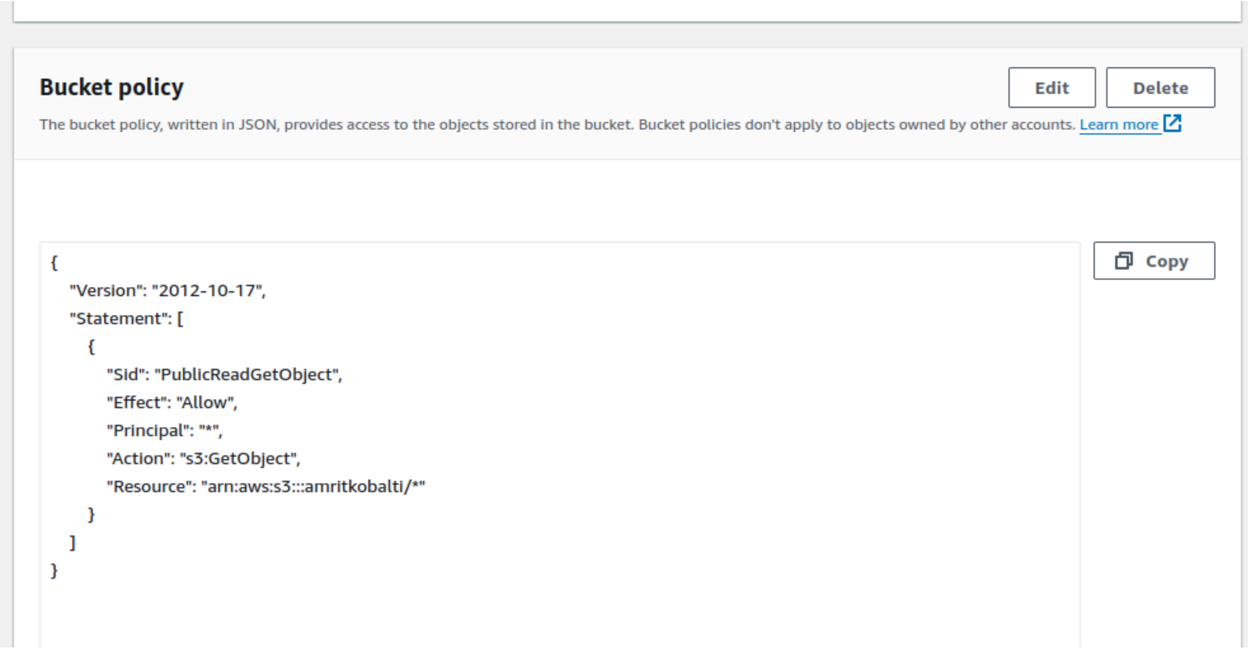
Amazon S3 > Buckets > amritkobalti

amritkobalti Info

Permissions overview

Access
Bucket and objects not public

5.Change Bucket Policy.

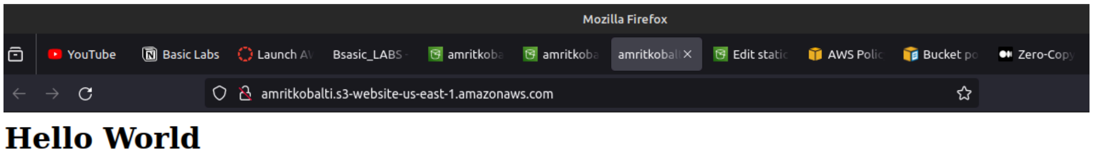


Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "PublicReadGetObject",
         "Effect": "Allow",
         "Principal": "*",
         "Action": "s3:GetObject",
         "Resource": "arn:aws:s3:::amritkobalti/*"
      }
   ]
}
```

6.Now we will access the Bucket through public URL.



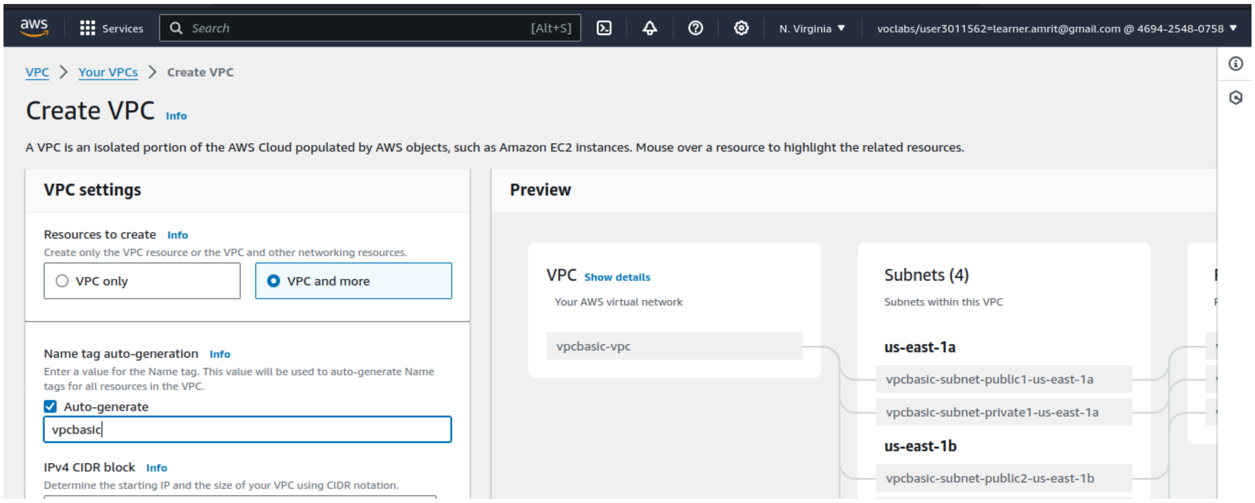
amritkobalti.s3-website-us-east-1.amazonaws.com

Hello World

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. Create VPC


aws
Services
Search [Alt+S]
N. Virginia ▼
voclabs/user3011562=learner.amrit@gmail.com @ 4694-2548-0758 ▼

VPC > Your VPCs > Create VPC

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. Mouse over a resource to highlight the related resources.

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
vpcbasic

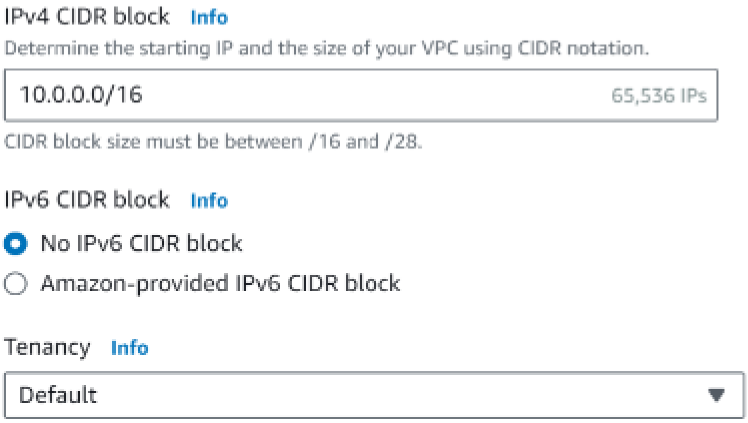
IPv4 CIDR block Info
Determine the starting IP and the size of your VPC using CIDR notation.

Preview

VPC Show details
Your AWS virtual network
vpcbasic-vpc

Subnets (4)
Subnets within this VPC
us-east-1a
vpcbasic-subnet-public1-us-east-1a
vpcbasic-subnet-private1-us-east-1a
us-east-1b
vpcbasic-subnet-public2-us-east-1b

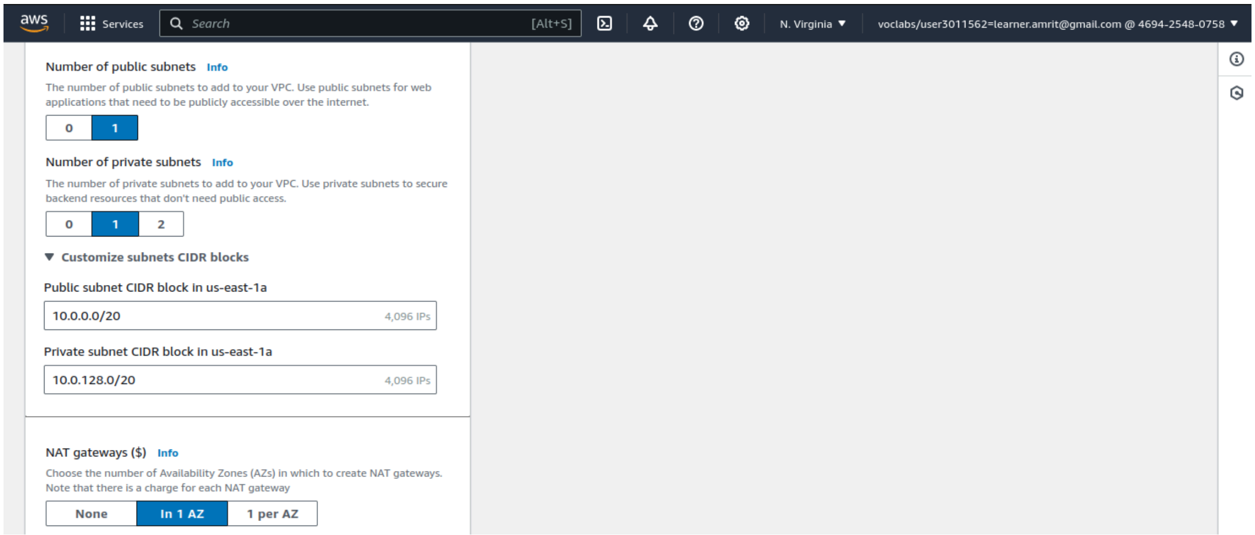
2. Maintain the IPv4 CIDR block as 10.0.0.0/16. Opt for 1 for the Number of Availability Zones.


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 ▼

3.Set Public subnet CIDR block to 10.0.0.0/24 and Private subnet CIDR block to 10.0.1.0/24.


aws
Services
Search [Alt+S]
N. Virginia
voclabs/user3011562=learner.amrit@gmail.com @ 4694-2548-0758

Number of public subnets Info

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

0 | **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

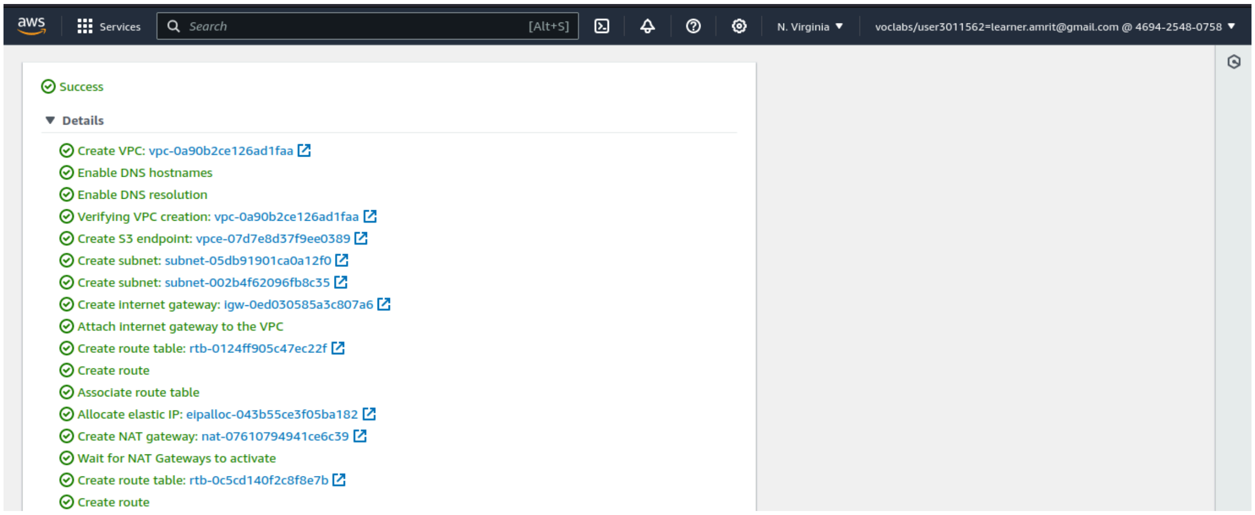
10.0.128.0/20 — 4,096 IPs

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

2.Created VPC and VPC Workflow

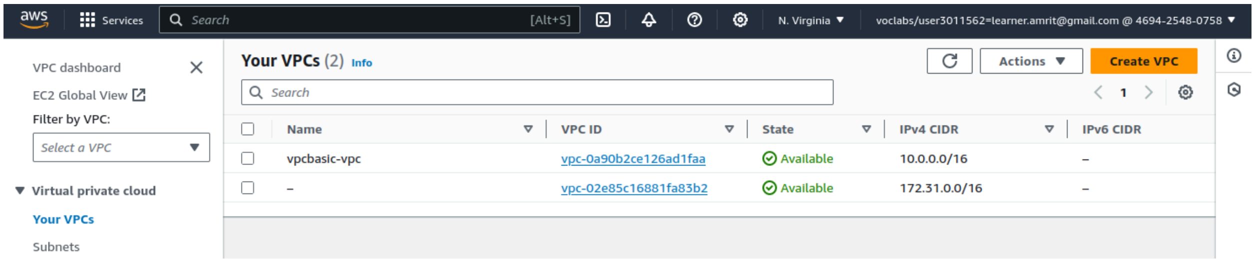

aws
Services
Search [Alt+S]
N. Virginia
voclabs/user3011562=learner.amrit@gmail.com @ 4694-2548-0758

✓ Success

▼ Details

- ✓ Create VPC: vpc-0a90b2ce126ad1faa
- ✓ Enable DNS hostnames
- ✓ Enable DNS resolution
- ✓ Verifying VPC creation: vpc-0a90b2ce126ad1faa
- ✓ Create S3 endpoint: vpce-07d7e8d37f9ee0389
- ✓ Create subnet: subnet-05db91901ca0a12f0
- ✓ Create subnet: subnet-002b4f62096fb8c35
- ✓ Create internet gateway: igw-0ed030585a3c807a6
- ✓ Attach internet gateway to the VPC
- ✓ Create route table: rtb-0124ff905c47ec22f
- ✓ Create route
- ✓ Associate route table
- ✓ Allocate elastic IP: eipalloc-043b55ce3f05ba182
- ✓ Create NAT gateway: nat-07610794941ce6c39
- ✓ Wait for NAT Gateways to activate
- ✓ Create route table: rtb-0c5cd140f2c8f8e7b
- ✓ Create route

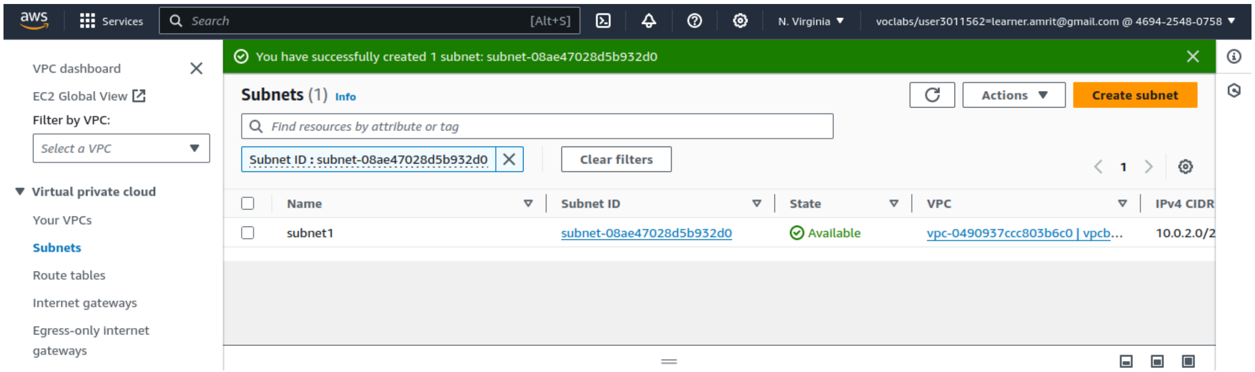
3.VPC created



Your VPCs (2) Info

□	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
□	vpcbasic-vpc	vpc-0a90b2ce126ad1faa	✓ Available	10.0.0.0/16	–
□	–	vpc-02e85c16881fa83b2	✓ Available	172.31.0.0/16	–

4. Subnet Created



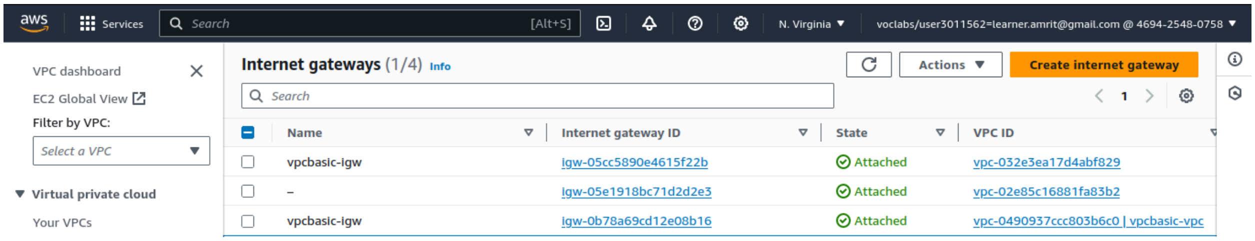
You have successfully created 1 subnet: subnet-08ae47028d5b932d0

Subnets (1) Info

Subnet ID : subnet-08ae47028d5b932d0

Name	Subnet ID	State	VPC	IPv4 CIDR
subnet1	subnet-08ae47028d5b932d0	Available	vpc-0490937ccc803b6c0 | vpcb...	10.0.2.0/2

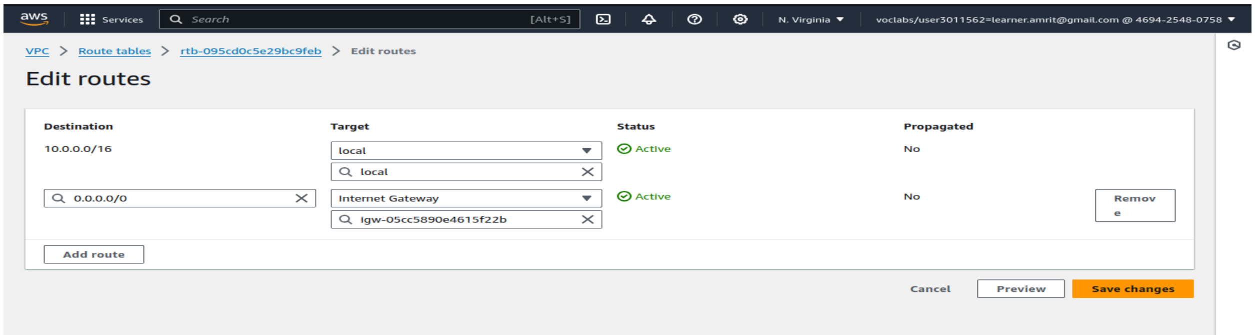
5. Create Internet Gateway



Internet gateways (1/4) Info

Name	Internet gateway ID	State	VPC ID
vpcbasic-igw	igw-05cc5890e4615f22b	Attached	vpc-032e3ea17d4abf829
–	igw-05e1918bc71d2d2e3	Attached	vpc-02e85c16881fa83b2
vpcbasic-igw	igw-0b78a69cd12e08b16	Attached	vpc-0490937ccc803b6c0 | vpcbasic-vpc

6.Configure the Route table and add Routes

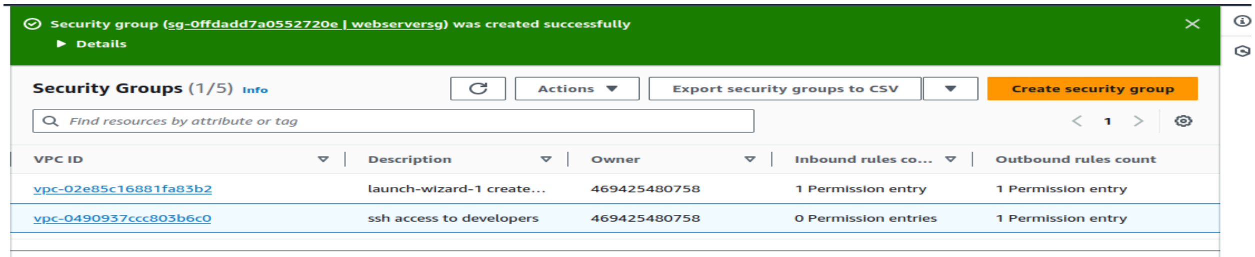


VPC > Route tables > rtb-095cd0c5e29bc9feb > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local local	Active	No
0.0.0.0/0	Internet Gateway igw-05cc5890e4615f22b	Active	No

7.create Security Group with rules for VPC



Security group (sg-0ffdadd7a0552720e | webserversg) was created successfully

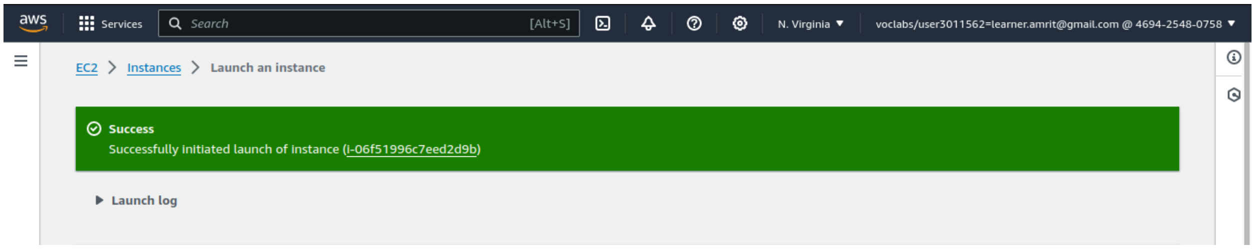
▶ Details

Security Groups (1/5) Info

VPC ID	Description	Owner	Inbound rules co...	Outbound rules count
vpc-02e85c16881fa83b2	launch-wizard-1 create...	469425480758	1 Permission entry	1 Permission entry
vpc-0490937ccc803b6c0	ssh access to developers	469425480758	0 Permission entries	1 Permission entry

Actions
Export security groups to CSV
Create security group
Find resources by attribute or tag
1

8.Set up and launch EC2 instance:


aws
Services
Search
[Alt+S]
N. Virginia ▼
voclabs/user3011562=learner.amrit@gmail.com @ 4694-2548-0758 ▼
EC2 > Instances > Launch an instance

Success

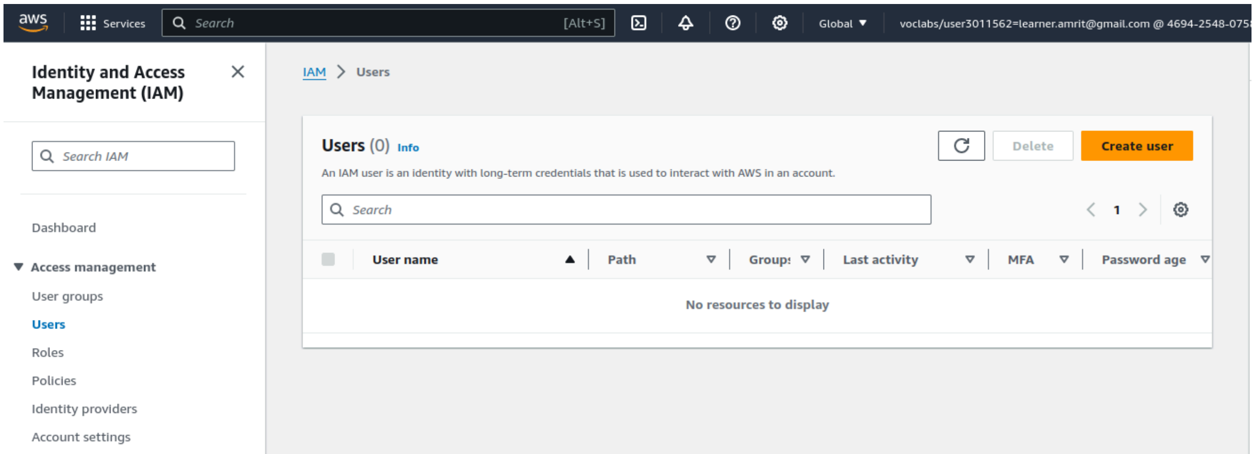
Successfully initiated launch of instance (i-06f51996c7eed2d9b)

Test using public IP address associated with the instance.

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 or 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. IAM User

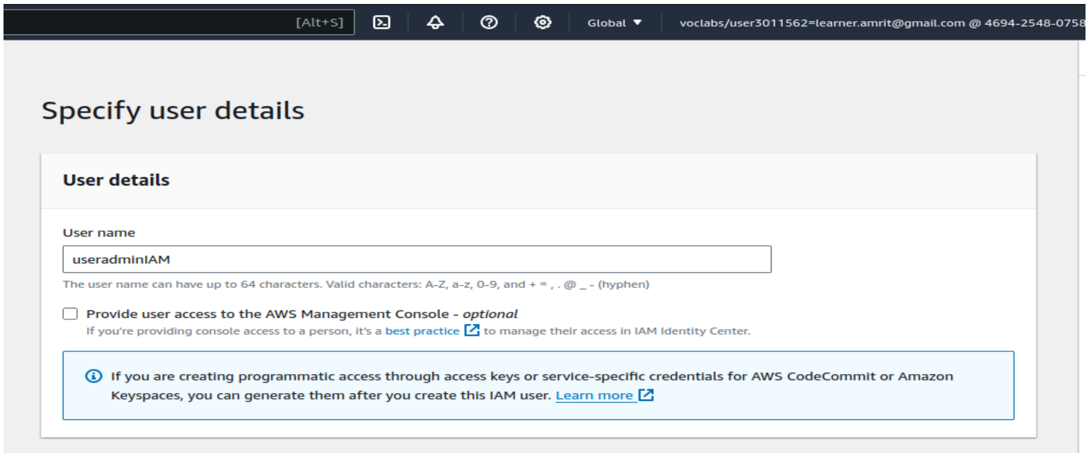


Users (0)

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

□	User name ▲	Path	Group:	Last activity	MFA	Password age
	No resources to display					

2.Create User


[Alt+S]
Global ▼
voclabs/user3011562=learner.amrit@gmail.com @ 4694-2548-0758

Specify user details

User details

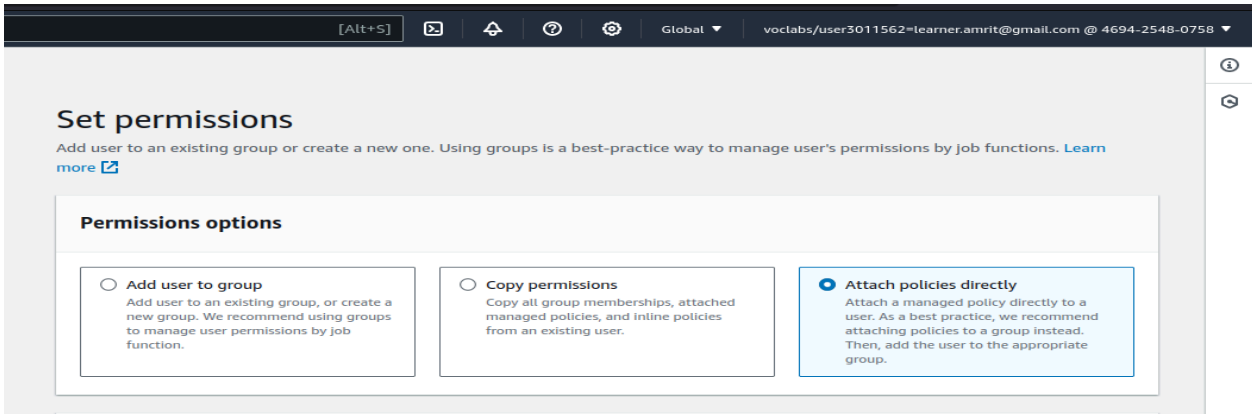
User name: useradminIAM

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

□ 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.

ⓘ 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

3.Set permission


[Alt+S]
Global
voclabs/user3011562=learner.amrit@gmail.com @ 4694-2548-0758

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

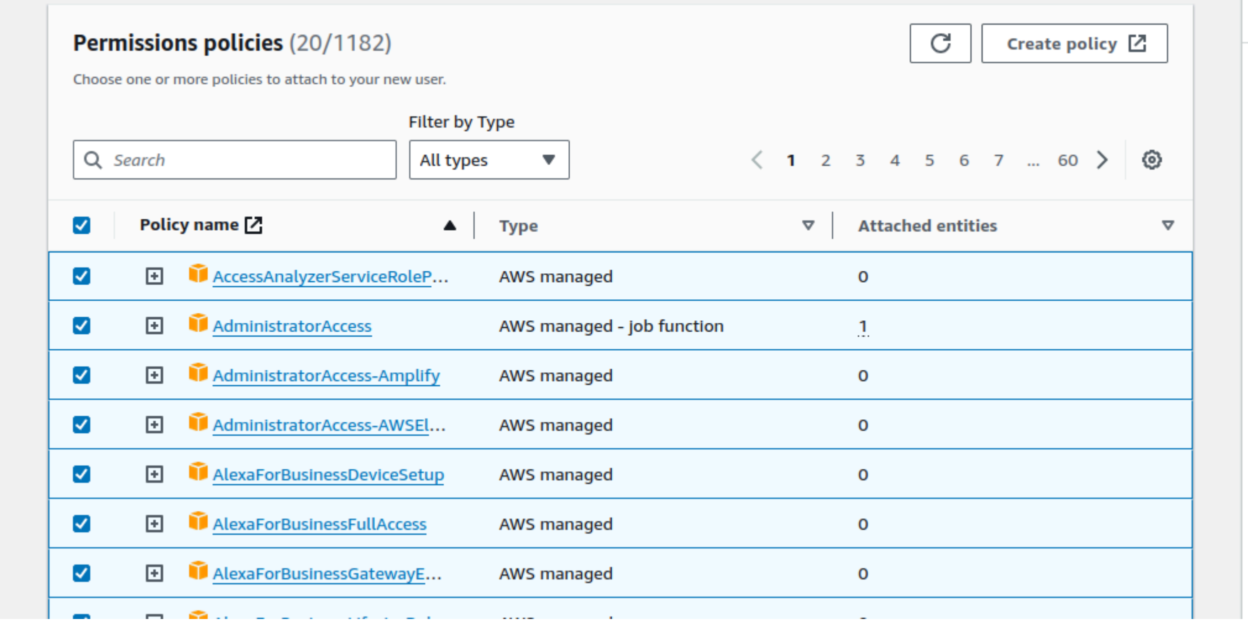
Permissions options

○ 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.

4.Select Permissions Policies



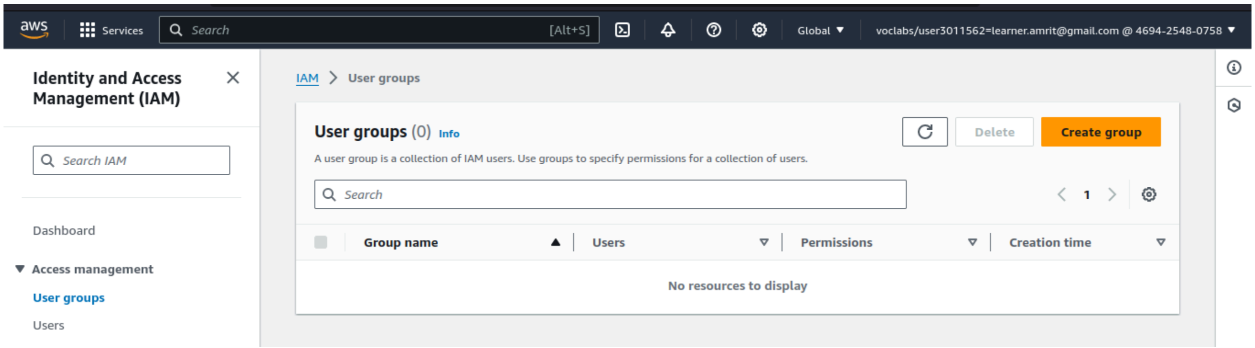
Permissions policies (20/1182)

Choose one or more policies to attach to your new user.

Filter by Type: All types

☑	Policy name	Type	Attached entities
☑	AccessAnalyzerServiceRoleP...	AWS managed	0
☑	AdministratorAccess	AWS managed - job function	1
☑	AdministratorAccess-Amplify	AWS managed	0
☑	AdministratorAccess-AWSEl...	AWS managed	0
☑	AlexaForBusinessDeviceSetup	AWS managed	0
☑	AlexaForBusinessFullAccess	AWS managed	0
☑	AlexaForBusinessGatewayE...	AWS managed	0

5.Create User Groups



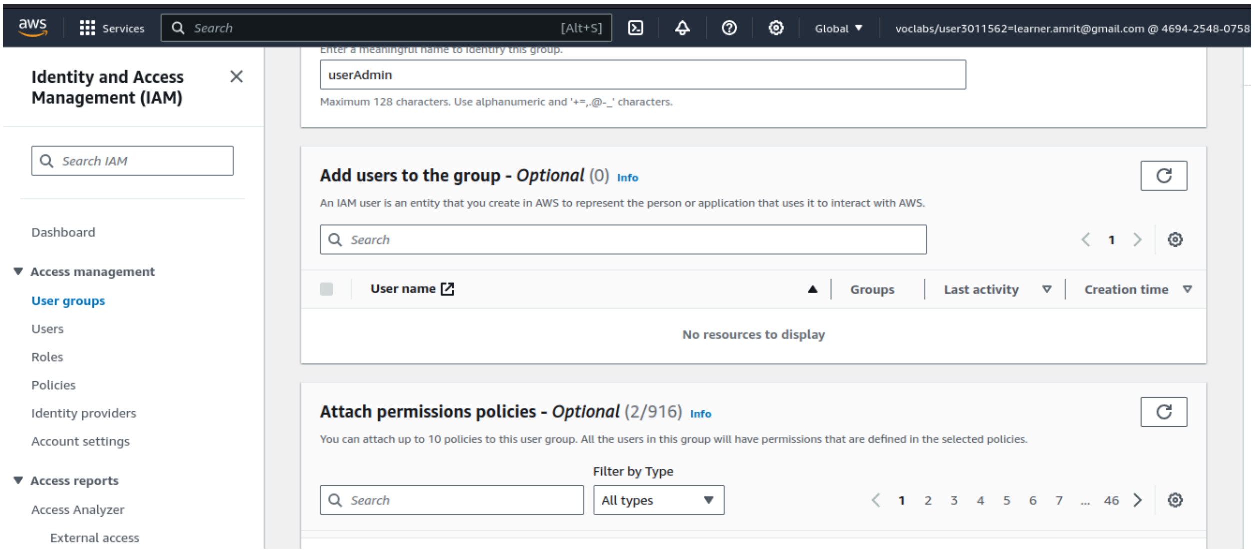
User groups (0) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

□	Group name	Users	Permissions	Creation time

No resources to display

6.Add users or attach permissions while creating user groups.



Enter a meaningful name to identify this group.

userAdmin

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.

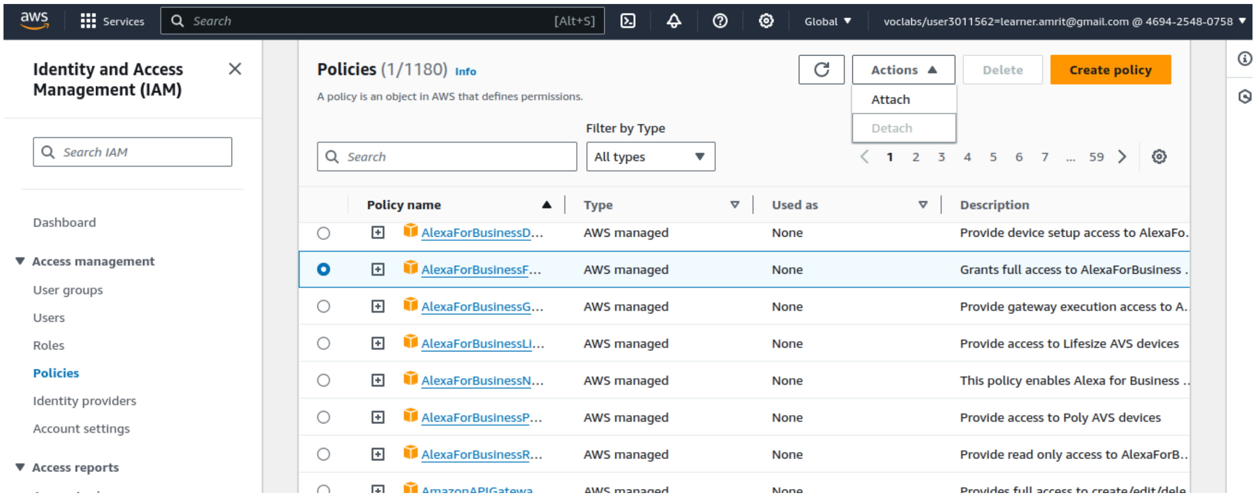
	User name	Groups	Last activity	Creation time
	No resources to display			

Attach permissions policies - *Optional* (2/916) 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: All types

7.Attach policies to User, User Groups



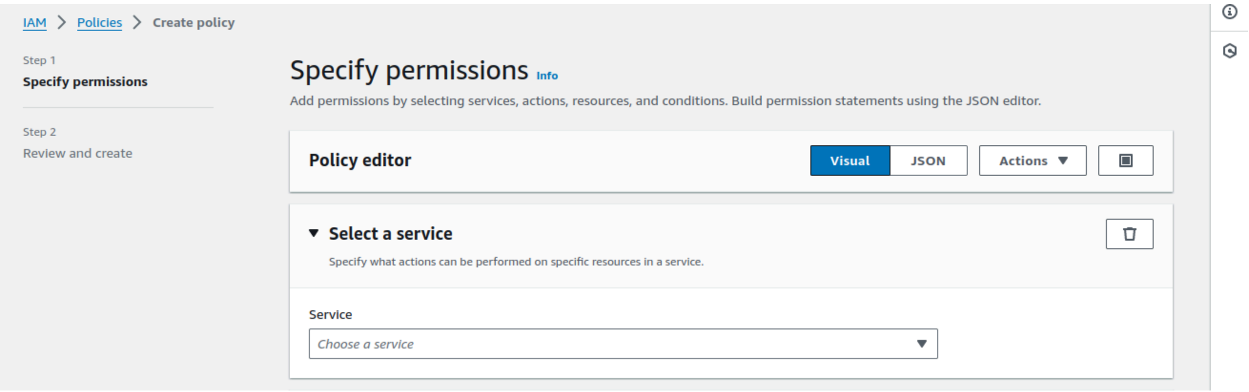
Policies (1/1180) Info

A policy is an object in AWS that defines permissions.

Filter by Type: All types

	Policy name	Type	Used as	Description
○	AlexaForBusinessD...	AWS managed	None	Provide device setup access to AlexaFo...
●	AlexaForBusinessF...	AWS managed	None	Grants full access to AlexaForBusiness ...
○	AlexaForBusinessG...	AWS managed	None	Provide gateway execution access to A...
○	AlexaForBusinessLi...	AWS managed	None	Provide access to Lifesize AVS devices
○	AlexaForBusinessN...	AWS managed	None	This policy enables Alexa for Business ...
○	AlexaForBusinessP...	AWS managed	None	Provide access to Poly AVS devices
○	AlexaForBusinessR...	AWS managed	None	Provide read only access to AlexaForB...
○	AmazonAPIGatewa...	AWS managed	None	Provides full access to create/edit/dele...

8. Also can create Policy



Specify permissions Info

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

Policy editor

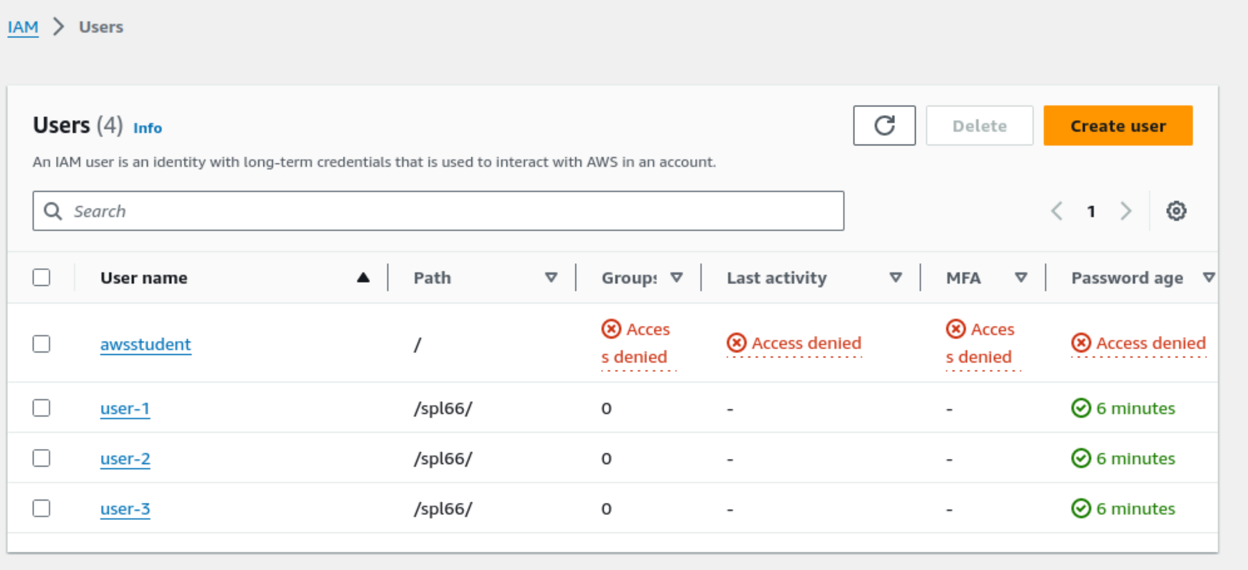
▼ Select a service

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

Service: Choose a service

Screenshots from Cloud foundation course as there is no access permitted to create IAM user, User Groups and policy:

- Create User

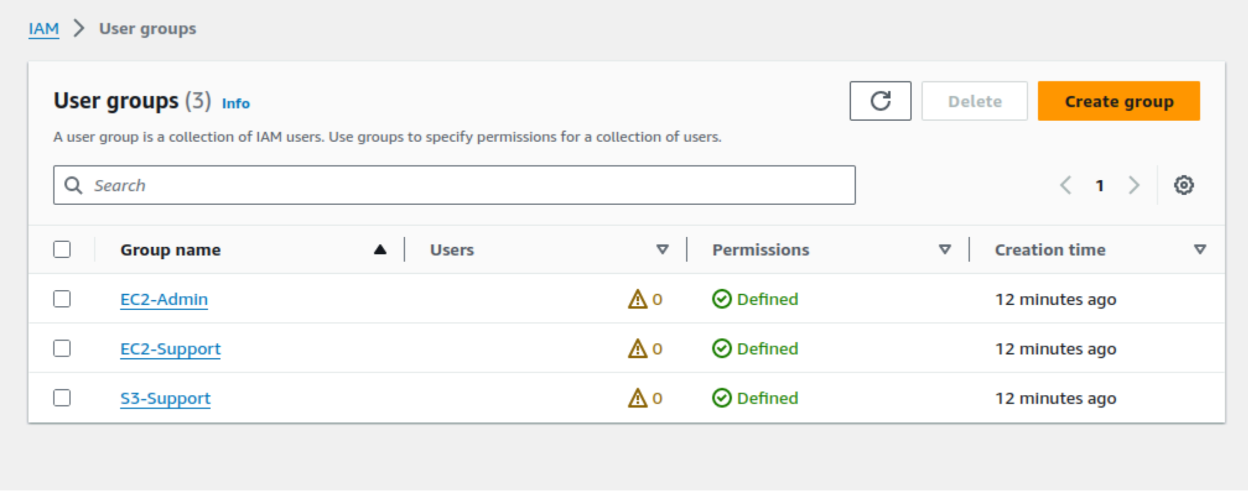


Users (4)

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

□	User name ▲	Path ▽	Group: ▽	Last activity ▽	MFA ▽	Password age ▽
□	awsstudent	/	⊗ Access denied	⊗ Access denied	⊗ Access denied	⊗ Access denied
□	user-1	/spl66/	0	-	-	✓ 6 minutes
□	user-2	/spl66/	0	-	-	✓ 6 minutes
□	user-3	/spl66/	0	-	-	✓ 6 minutes

- Create User Groups

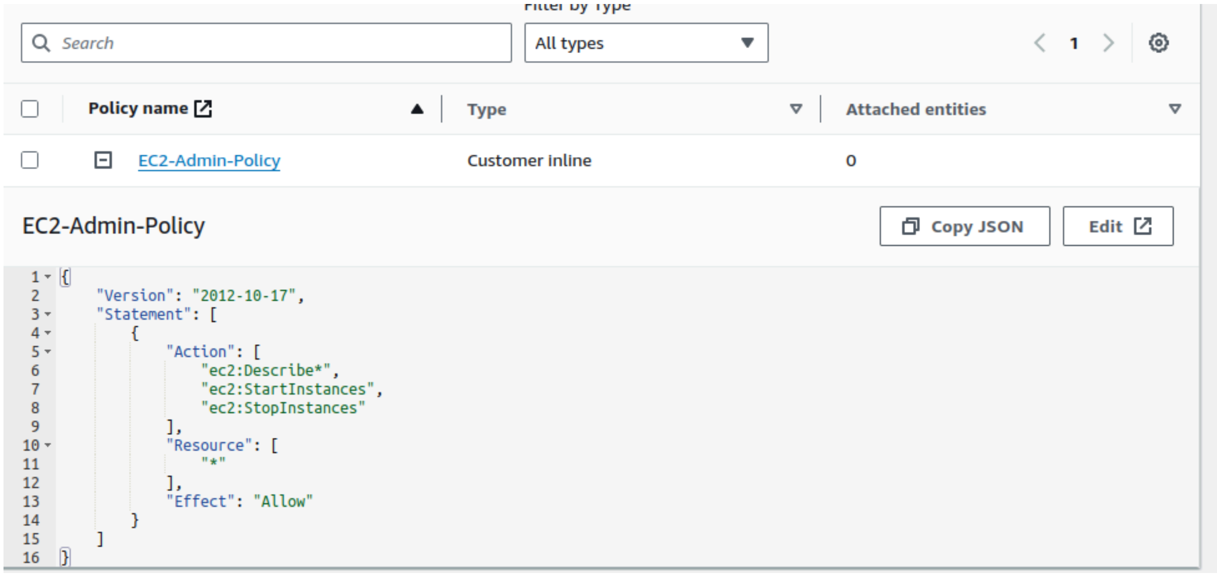


User groups (3)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

□	Group name ▲	Users ▽	Permissions ▽	Creation time ▽
□	EC2-Admin	⚠ 0	✓ Defined	12 minutes ago
□	EC2-Support	⚠ 0	✓ Defined	12 minutes ago
□	S3-Support	⚠ 0	✓ Defined	12 minutes ago

- Create Permissions/Policies

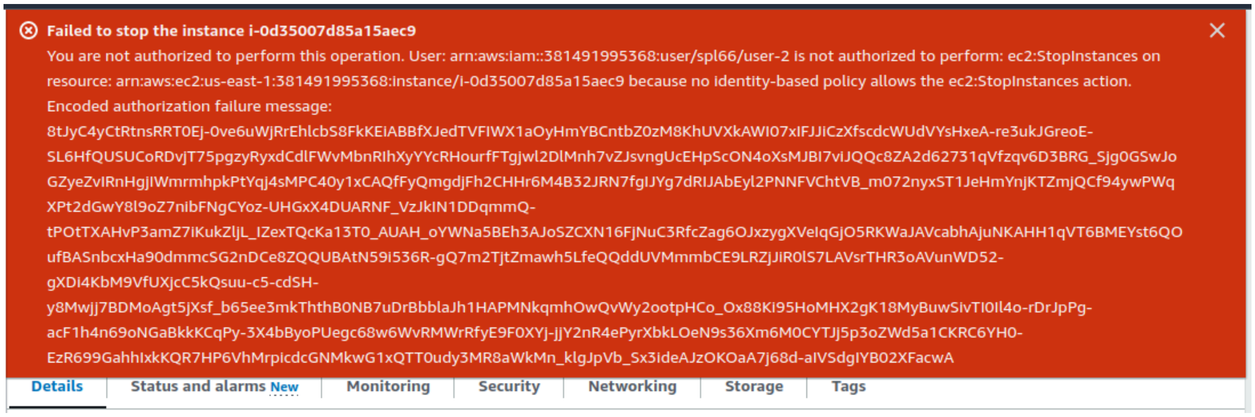


☐	Policy name	Type	Attached entities
☐	⊟ EC2-Admin-Policy	Customer inline	0

EC2-Admin-Policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:Describe*",
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

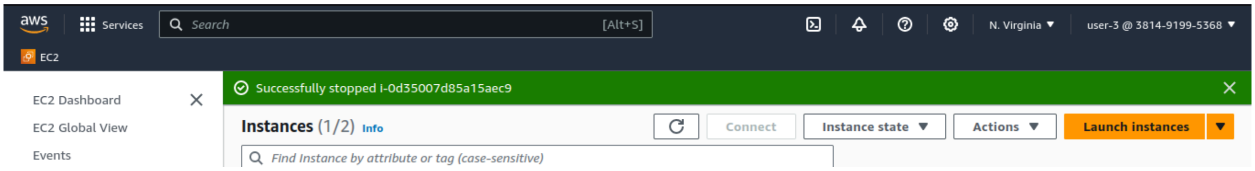
- Before Permission(EC2 Admin)



Failed to stop the instance i-0d35007d85a15aec9

```
You are not authorized to perform this operation. User: arn:aws:iam::381491995368:user/spl66/user-2 is not authorized to perform: ec2:StopInstances on
resource: arn:aws:ec2:us-east-1:381491995368:instance/i-0d35007d85a15aec9 because no identity-based policy allows the ec2:StopInstances action.
Encoded authorization failure message:
8tJyC4yCtRtnsRRT0Ej-0ve6uWjRrEhlcbS8FkKEiABBfXJedTVFIWX1aOyHmYBCntbZ0zM8KhUVXkAWI07xIFJJiCzXfscdcWUdVYsHxeA-re3ukJGreoE-
SL6HfQUSUCoRDvjT75pgzyRyxdCdlFWvMbnRIhXyYYcRHourfFTgjwl2DlMnh7vZJsvngUcEHpScON4oXsMJBI7viJQQc8ZA2d62731qVfzqv6D3BRG_Sjg0GSwJo
GZyeZvIRnHgjIWmrmhpkPtYqj4sMPC40y1xCAQfFyQmgdjFh2CHHr6M4B32JRN7fgIJYg7dRIJAbEyl2PNNFVChtVB_m072nyxST1JeHmYnjKTZmjQCf94ywPWq
XPt2dGwY8l9oZ7nibFNgCYoz-UHGxX4DUARNF_VzJkIN1DDqmmQ-
tPOtTXAHvP3amZ7iKukZljL_IZexTQcKa13T0_AUAH_oYWNa5BEh3AJoSZCXN16FjNuC3RfcZag6OJxzygXVelqGjO5RKWaJAVcabhAjuNKAHH1qVT6BMEYst6QO
ufBASnbcxHa90dmmcSG2nDCe8ZQQUBAtN59i536R-gQ7m2TjtZmawh5LfeQQddUVMmmbCE9LRZjJiR0lS7LAVsrTHR3oAVunWD52-
gXDi4KbM9VfUXjcC5kQsuu-c5-cdSH-
y8Mwjj7BDMoAgt5jXsf_b65ee3mkThthB0NB7uDrBbblaJh1HAPMNkqmhOwQvWy2ootpHCo_Ox88Ki95HoMHX2gK18MyBuwSivTI0Il4o-rDrJpPg-
acF1h4n69oNGaBkkKCqPy-3X4bByoPUegc68w6WvRMWrRfyE9F0XYj-jjY2nR4ePyrXbkLOeN9s36Xm6M0CYTJj5p3oZWd5a1CKRC6YH0-
EzR699GahhIxkKQR7HP6VhMrpicdcGNMkwG1xQTT0udy3MR8aWkMn_klgJpVb_Sx3ideAJzOKOaA7j68d-aIVSdgIYB02XFacwA
```

- After permission Granted(EC2 Admin)



Successfully stopped i-0d35007d85a15aec9

Instances (1/2) Info