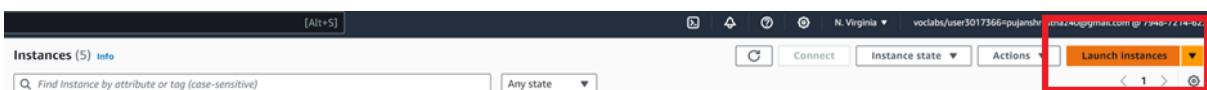
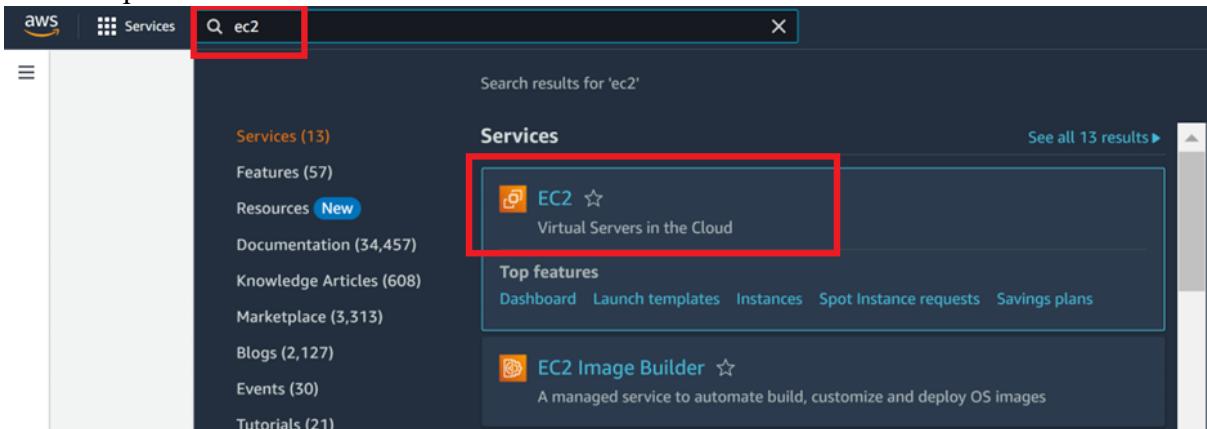


1. EC2 Basics Lab

- **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 and select EC2



2. Prompts to a new page, follow the steps below:

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.

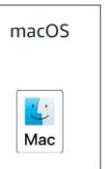
Name and tags Info

Name

[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

[Recents](#)[Quick Start](#)[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI

ami-0e731c8a588258d0d (64-bit (x86), uefi-preferred) / ami-0bbebc09f0a12d4d9 (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

[Free tier eligible](#)

Description

Amazon Linux 2023 AMI 2023.3.20240205.2 x86_64 HVM kernel-6.1

Architecture

Boot mode

uefi-preferred

AMI ID

ami-0e731c8a588258d0d

Verified provider

▼ 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

▼ 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*

▼
 [Create new key pair](#)

▼ Network settings [Info](#)

VPC - *required* [Info](#)

(default) ▼

Subnet [Info](#)

▼
 [Create new subnet](#)

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](#)

Security group name - *required*

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](#)

Inbound Security Group Rules

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

Type Info	Protocol Info	Port range Info
ssh	TCP	22

Source type [Info](#) Source [Info](#) Description - *optional* [Info](#)

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

▼ Summary

Number of instances [Info](#)

Software Image (AMI)

Amazon Linux 2023.3.2...[read more](#)
ami-0e731c8a588258d0d

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

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

Launching instance

Launch initiation

79%

3. Now our Instance has been successfully created.

The screenshot shows the AWS EC2 Instances page. At the top, there is a green success banner stating "Successfully initiated launch of instance (i-01a7673b374c1c5e7)". Below the banner, the instance list table shows one row for "bootcamp" with instance ID "i-01a7673b374c1c5e7", status "Running", type "t2.micro", and availability zone "us-east-1a".

8. Not any assign IP for the EC2 instance

The screenshot shows the Instance summary for instance "i-01a7673b374c1c5e7 (bootcamp)". The summary table includes fields such as Public IPv4 address (172.31.85.172), Instance state (Running), Private IP DNS name (ip-172-31-85-172.ec2.internal), Instance type (t2.micro), VPC ID (vpc-0106cbe3513a1507a), Subnet ID (subnet-0362a2e4a502fba72), and Auto Scaling Group name (None).

4. Now we adding the Elastic IP address

Select elastic IP

The screenshot shows the "Network & Security" section of the instance configuration. Under "Elastic IPs", there is a red box highlighting the "Allocate Elastic IP address" button. Other options shown include "Auto-assigned IP address" (None), "IAM Role" (None), and "IMDSv2" (Required).

5. Select allocate Elastic IP Address

The screenshot shows the "Elastic IP addresses" page. A red box highlights the "Allocate Elastic IP address" button. The table below shows no results: "No Elastic IP addresses found in this Region".

6. Select IPv4 to set IP Address

Allocate Elastic IP address [Info](#)

Elastic IP address settings [Info](#)

Network Border Group [Info](#)

us-east-1 X

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](#)

7. Keep the created IPv4 selected and click action and select associate elastic IP Address

Elastic IP addresses (1/1)

Name	Allocated IPv4 add...	Type	Allocation ID	Reverse DNS record
Elastic_IP	44.222.60.214	Public IP	eipalloc-020376cf95b3b14d9	-

Actions [Allocate Elastic IP address](#)

[View details](#) [Release Elastic IP addresses](#)

Associate Elastic IP address

[Update reverse DNS](#) [Enable transfers](#) [Disable transfers](#) [Accept transfers](#)

8. Select the EC2 instance and click Associate

Associate Elastic IP address [Info](#)

Choose the instance or network interface to associate to this Elastic IP address (44.222.60.214)

Elastic IP address: 44.222.60.214

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

i-01a7673b374c1c5e7 X

i-084ad51df8026f149 (MyWeb) - running
i-0e795a8f7009a6c3a (MyWeb) - running
i-0749fb686c3db234d - running

i-01a7673b374c1c5e7 (bootcamp) - running

Allow this Elastic IP address to be reassigned i-01a7673b374c1c5e7 (bootcamp) - running

[Cancel](#) [Associate](#)

9. Now we can see the ec2 is assign in IP

Instance: i-01a7673b374c1c5e7 (bootcamp)

IPv6 address	Instance state
-	Running
Hostname type	Private IP DNS name (IPv4 only)
IP name: ip-172-31-85-172.ec2.internal	ip-172-31-85-172.ec2.internal
Answer private resource DNS name	Instance type
IPv4 (A)	t2.micro
Auto-assigned IP address	VPC ID
-	vpc-0106cbe3513a1507a
IAM Role	Subnet ID
-	subnet-0362a2e4a502fba72

10. To connect the EC2 instance via SSH, download the PEM file in AWS Details

Instance summary for i-01a7673b374c1c5e7 (bootcamp) [Info](#)

Updated less than a minute ago

Instance ID	Public IPv4 address	Private IPv4 addresses
i-01a7673b374c1c5e7 (bootcamp)	44.222.60.214 (Elastic_IP) open address	172.31.85.172
IPv6 address	Instance state	Public IPv4 DNS
-	Running	ec2-44-222-60-214.compute-1.amazonaws.com open address
Hostname type	Private IP DNS name (IPv4 only)	Elastic IP addresses
IP name: ip-172-31-85-172.ec2.internal	ip-172-31-85-172.ec2.internal	44.222.60.214 (Elastic_IP) [Public IP]
Answer private resource DNS name	Instance type	AWS Compute Optimizer finding
IPv4 (A)	t2.micro	Opt-in to AWS Compute Optimizer for recommendations. Learn more
Auto-assigned IP address	VPC ID	Auto Scaling Group name
-	vpc-0106cbe3513a1507a	-
IAM Role	Subnet ID	
-	subnet-0362a2e4a502fba72	
IMDSv2		
Required		

Connect to instance [Info](#)

Connect to your instance i-01a7673b374c1c5e7 (bootcamp) using any of these options

[EC2 Instance Connect](#) [Session Manager](#) [SSH client](#) [EC2 serial console](#)

Instance ID
[i-01a7673b374c1c5e7 \(bootcamp\)](#)

Connection Type

[Connect using EC2 Instance Connect](#)
Connect using the EC2 Instance Connect browser-based client, with a public IPv4 address.

[Connect using EC2 Instance Connect Endpoint](#)
Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

Public IP address
[44.222.60.214](#)

Username
Enter the username defined in the AMI used to launch the instance. If you didn't define a custom username, use the default username, ec2-user.
 [X](#)

Note: In most cases, the default username, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

[Cancel](#) [Connect](#)

11. EC2 Instance Connect loads in a new page

A screenshot of an AWS Lambda function editor. The top navigation bar shows 'aws' and 'Services'. A search bar contains 'Search' and a keybinding '[Alt+S]'. The main area is a terminal window displaying a multi-line string of characters representing a URL. The URL is partially visible as 'https://aws.amazon.com/linux/amazon-linux-2023'. The terminal prompt at the bottom is '[ec2-user@ip-172-31-85-172 ~]\$'.

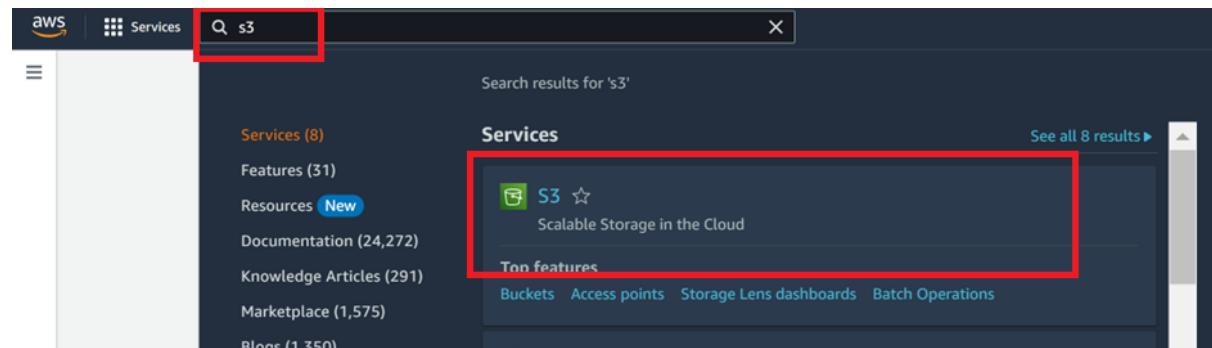
```
'~\_\#\#\#'
~~\_#\#\#\\
~~\#\#\#
~~\#/ \
~~V~'`->
~~`/`/
~~`/`/
~/`/`/
[ec2-user@ip-172-31-85-172 ~]$
```

-----Next Task in new page-----

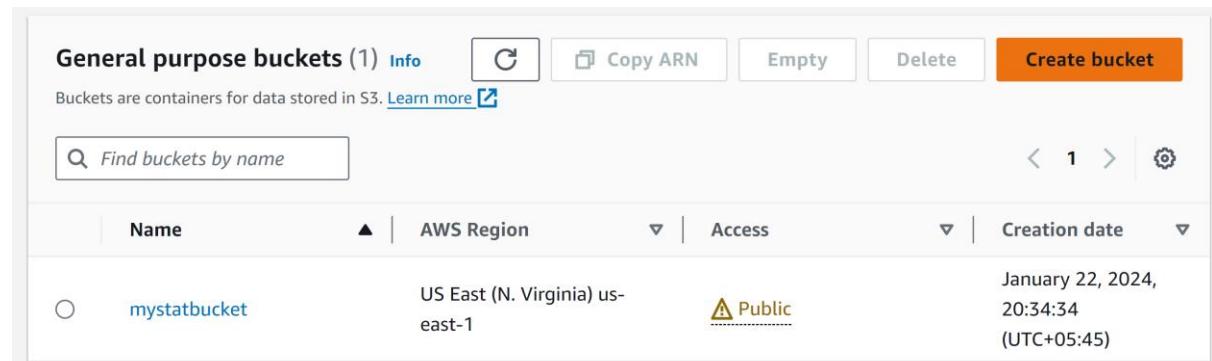
2. S3 Storage Fundamentals Lab

- **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.

i. Select S3 from Amazon Management Console and create an S3 Bucket



The screenshot shows the AWS Management Console search results for 's3'. The search bar at the top has 's3' typed into it. Below the search bar, there is a sidebar with links to 'Services (8)', 'Features (31)', 'Resources New', 'Documentation (24,272)', 'Knowledge Articles (291)', 'Marketplace (1,575)', and 'Blogs (1,350)'. The main area displays a list of services under 'Services'. The 'S3' service card is highlighted with a red box. It features a green icon of a cloud with a folder, the text 'S3 ☆', and the description 'Scalable Storage in the Cloud'. Below the service card, there are links for 'Top features', 'Buckets', 'Access points', 'Storage Lens dashboards', and 'Batch Operations'. At the bottom of the main area, there are buttons for 'See all 8 results ▶', 'Buckets', 'Access points', 'Storage Lens dashboards', and 'Batch Operations'.



The screenshot shows the 'General purpose buckets' list page. At the top, there is a header with 'General purpose buckets (1) Info' and a 'Create bucket' button. Below the header, there is a search bar with 'Find buckets by name' and a pagination indicator '1'. The main table lists one bucket: 'mystatbucket' (Name), 'US East (N. Virginia) us-east-1' (AWS Region), 'Public' (Access), and 'January 22, 2024, 20:34:34 (UTC+05:45)' (Creation date). The table has columns for Name, AWS Region, Access, and Creation date.

ii. Give a unique name to your 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](#)

awsplasticbucket

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

 After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

[Cancel](#)

[Create bucket](#)

iii. Bucket Created

Successfully created bucket "awsplasticbucket"

To upload files and folders, or to configure additional bucket settings, choose [View details](#).

General purpose buckets		Directory buckets
<p>General purpose buckets (2) Info</p> <p>Buckets are containers for data stored in S3. Learn more</p>		
<p>C Copy ARN Empty Delete Create bucket</p>		
<input type="text"/> Find buckets by name		< 1 > @
Name	AWS Region	Access
awsplasticbucket	US East (N. Virginia) us-east-1	Bucket and objects not public
		February 15, 2024, 22:06:27 (UTC+05:45)

iv. Click Upload to upload file to the bucket.

The screenshot shows the AWS S3 console interface for the bucket 'awsplasticbucket'. At the top, there are tabs for Objects, Properties, Permissions, Metrics, Management, and Access Points. The 'Objects' tab is selected. Below the tabs, there's a toolbar with actions like Copy S3 URI, Copy URL, Download, Open, Delete, Actions, Create folder, and Upload. A search bar says 'Find objects by prefix'. A table header includes columns for Name, Type, Last modified, Size, and Storage class. A message 'No objects' indicates there are no files in the bucket. An 'Upload' button is visible at the bottom right of the main area.

This screenshot shows the progress of an upload. The progress bar at the top is at 0%. Below it, a message says 'Total remaining: 1 file: 56.6 KB(100.00%)' and 'Estimated time remaining: calculating...'. Transfer rate is listed as '0 B/s'. Below this, a green success message says 'Upload succeeded' and 'View details below.'

The screenshot shows the AWS S3 console for the same bucket 'awsplasticbucket'. The interface is identical to the first one, with the 'Upload' button highlighted with a red box.

- v. To set the policies, click the bucket name and select permission tab and you can see the bucket policy. Now click edit to set the policies.

This screenshot shows the 'Permissions' tab selected for the 'awsplasticbucket' bucket. It displays the 'Permissions overview' section, which includes 'Access' and 'Bucket and objects not public' settings. Below this is the 'Block public access (bucket settings)' section, which is currently set to 'On'. An 'Edit' button is located next to the 'On' status. At the bottom, there's a 'Bucket policy' section with an 'Edit' and 'Delete' button.

- vi. Click policy generator to generate policy.

Edit bucket policy [Info](#)

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](#)

[Policy examples](#) [Policy generator](#) Policy generator



AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see [key concepts in Using AWS Identity and Access Management](#). Here are [sample policies](#).

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an [IAM Policy](#), an [S3 Bucket Policy](#), an [SNS Topic Policy](#), a [VPC Endpoint Policy](#), and an [SQS Queue Policy](#).

Select Type of Policy S3 Bucket Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a [description of elements](#) that you can use in statements.

Effect Allow Deny

Principal *

AWS Service Amazon S3 All Services (*)

Actions 1 Action(s) Selected All Actions (*)

Amazon Resource Name (ARN) arn:aws:s3:::awsplasticbucket

Add Conditions (Optional)

[Add Statement](#)

You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource	Conditions
• *	Allow	• s3:GetObject	arn:aws:s3:::awsplasticbucket	None

Step 3: Generate Policy

A *policy* is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

[Generate Policy](#) [Start Over](#)

Actions Select Actions All Actions (*)

Policy JSON Document

Click below to edit. To save the policy, copy the text below to a text editor. Changes made below will **not** be reflected in the policy generator tool.

```
{
  "Id": "Policy1708015753249",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1708015710454",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::awsplasticbucket",
      "Principal": "*"
    }
  ]
}
```

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as-is without warranty of any kind, whether express or implied.

[Close](#)

vii. Insert the generated JSON into policy and save.

Edit bucket policy [Info](#)

Bucket policy

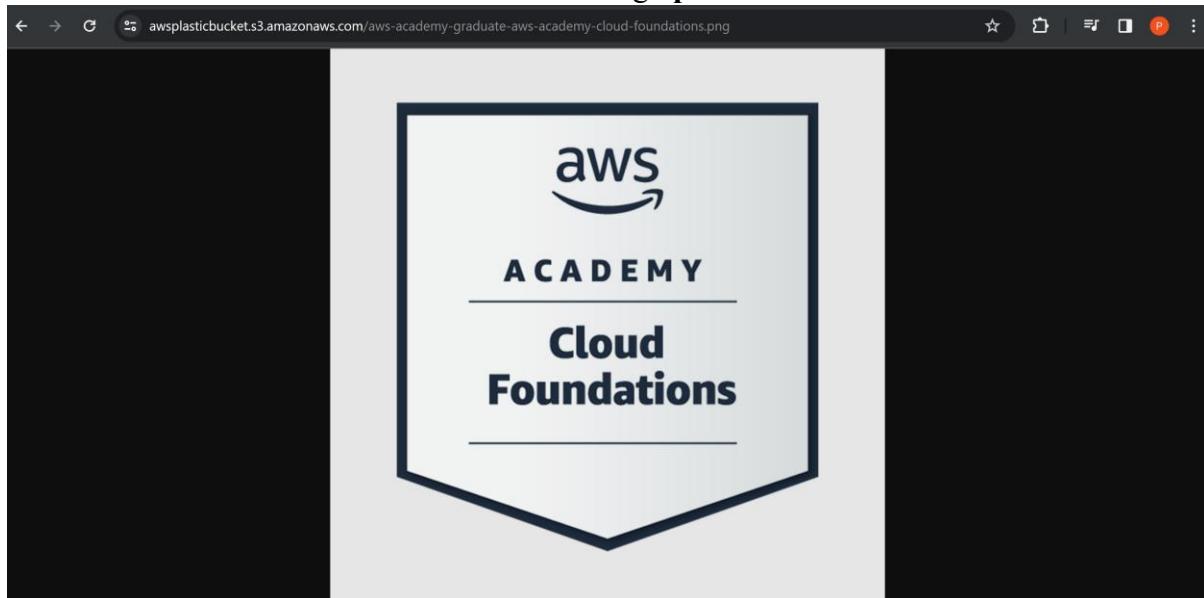
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

Bucket ARN
arn:aws:s3:::awsplasticbucket

Policy

```
1 ▼ [
2   "Id": "Policy1708015753249",
3   "Version": "2012-10-17",
4   "Statement": [
5     {
6       "Sid": "Stmt1708015710454",
7       "Action": [
8         "s3:GetObject"
9       ],
10      "Effect": "Allow",
11      "Resource": "arn:aws:s3:::awsplasticbucket",
12      "Principal": "*"
13    }
14  ]
15 ]
```

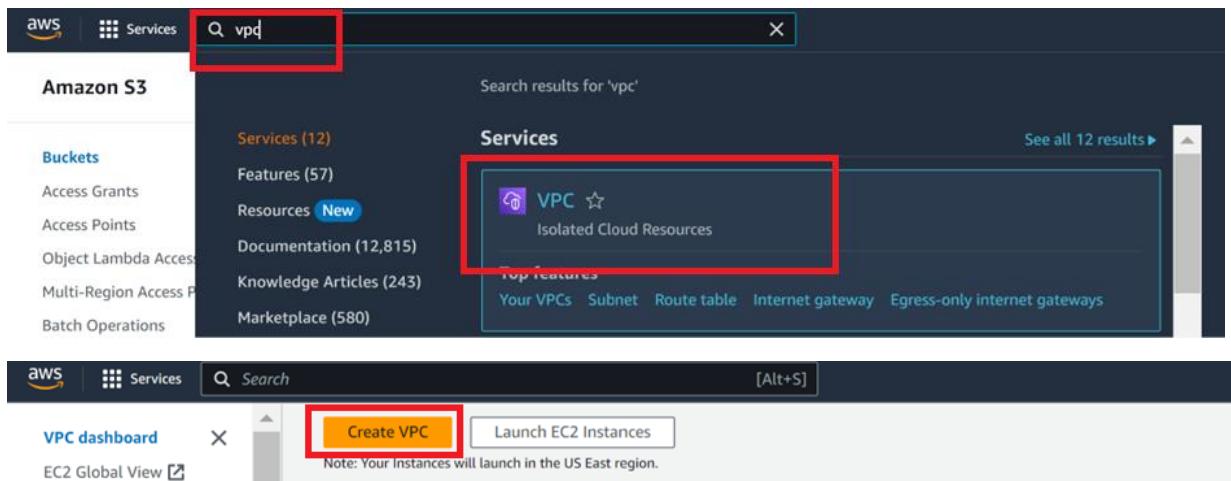
viii. Now we will access the Bucket through public URL.



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.

- i. Open AWS console and look for VPC and create VPC



- ii. Select the settings as per the steps.

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon S3 buckets, Amazon RDS databases, and Amazon Lambda functions.

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
project

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

Set up the VPC specifics within the VPC settings section located on the left-hand panel:

Select "VPC and more." Opt for "VPC and more."

Ensure "Auto-generate" remains selected under "Name tag auto-generation," but modify the entry from "project" to "lab."

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

Retain the setting of 1 for both the Number of public subnets and the Number of private subnets.

Number of Availability Zones (AZs) [Info](#)

Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

--	--	--

► [Customize AZs](#)

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 2

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

10.0.0.0/24	256 IPs
-------------	---------

Private subnet CIDR block in us-east-1a

10.0.128.0/24	256 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](#)

Broaden the section for customizing CIDR blocks of subnets.

Adjust the Public subnet CIDR block to 10.0.0.0/24 within us-east-1a.

Modify the Private subnet CIDR block to 10.0.1.0/24 within us-east-1a.

Configure NAT gateways for availability within a single AZ.

Opt not to use VPC endpoints. Ensure that both DNS hostnames and DNS resolution remain enabled.

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

Create VPC workflow

› Create subnet

30%

▼ Details

- ✓ Create VPC: vpc-0d756f07d22282118 [x]
- ✓ Enable DNS hostnames
- ✓ Enable DNS resolution
- ✓ Verifying VPC creation: vpc-0d756f07d22282118 [x]
- ✓ Create S3 endpoint: vpce-05425557a3b544374 [x]
- ✓ Create subnet: subnet-059d28c41e2a4a217 [x]
- … Create subnet
 - ① Create internet gateway
 - ② Attach internet gateway to the VPC
 - ③ Create route table
 - ④ Create route
 - ⑤ Associate route table
 - ⑥ Allocate elastic IP
 - ⑦ Create NAT gateway
 - ⑧ Wait for NAT Gateways to activate
 - ⑨ Create route table
 - ⑩ Create route
 - ⑪ Associate route table
 - ⑫ Verifying route table creation
 - ⑬ Associate S3 endpoint with private subnet route tables: vpce-05425557a3b544374 [x]

VPC > Your VPCs > vpc-0d756f07d22282118 / project-vpc			
Details		Info	
VPC ID vpc-0d756f07d22282118	State Available	DNS hostnames Enabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-0d51a27c377096dc	Main route table rtb-08f57dbd8198846ae	Main network ACL acl-0a66bad3e0d7b513c
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool -	IPv6 CIDR (Network border group) -

- iv. To add Subnet, click **Subnet** in left-hand side of the panel. It is situated just below *Your VPC*

The screenshot shows the AWS VPC dashboard. On the left, there's a sidebar with links: 'VPC dashboard', 'EC2 Global View [x]', 'Filter by VPC: Select a VPC', 'Virtual private cloud', 'Your VPCs' (which is highlighted in blue), 'Subnets', and 'Route tables'. The main content area has a breadcrumb path 'VPC > Your VPCs > vpc-0d756f07d22282118 / project-vpc'. Below the path, it says 'vpc-0d756f07d22282118 / project-vpc'. The main content is a table with two columns: 'Details' and 'Info'. The 'Details' column contains: 'VPC ID: vpc-0d756f07d22282118', 'Tenancy: Default'. The 'Info' column contains: 'State: Available', 'DHCP option set: dopt-0d51a27c3'. The overall interface is dark-themed.

- v. Select Create SubNet

State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses
Available	vpc-0106cbe3513a1507a	172.31.0.0/20	-	4091
Available	vpc-0106cbe3513a1507a	172.31.32.0/20	-	4091
Available	vpc-0106cbe3513a1507a	172.31.16.0/20	-	4087

- vi. Set subset name, availability zone, and add the IPv4-CIDR Subnet

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.
vpc-0d756f07d22282118 (project-vpc)

Associated VPC CIDRs
IPv4 CIDRs
10.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
my-subnet-01
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-1b

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16

IPv4 subnet CIDR block
10.0.2.0/24 256 IPs
< > ^ ^

► Tags - optional
[Remove](#)

[Add new subnet](#)

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

Subnets (9) [Info](#)

<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses
<input type="checkbox"/>	-	subnet-0e698f40951f56de1	Available	vpc-0106cbe3513a1507a	172.31.0.0/20	-	4091
<input type="checkbox"/>	-	subnet-0cc5f794af45f1269	Available	vpc-0106cbe3513a1507a	172.31.32.0/20	-	4091
<input type="checkbox"/>	-	subnet-0bbe9d9482ccca4b9	Available	vpc-0106cbe3513a1507a	172.31.16.0/20	-	4087
<input type="checkbox"/>	-	subnet-0513be5d486c897c6	Available	vpc-0106cbe3513a1507a	172.31.48.0/20	-	4091
<input type="checkbox"/>	-	subnet-0362a2e4a502fba72	Available	vpc-0106cbe3513a1507a	172.31.80.0/20	-	4090
<input type="checkbox"/>	-	subnet-091f0b1ac63f5962d	Available	vpc-0106cbe3513a1507a	172.31.64.0/20	-	4091
<input type="checkbox"/>	project-subnet-private1-us-east-1a	subnet-0f49bc7bc001726ea	Available	vpc-0d756f07d22282118 [proj...]	10.0.128.0/24	-	251
<input type="checkbox"/>	project-subnet-public1-us-east-1a	subnet-059d28c41e2a7a217	Available	vpc-0d756f07d22282118 [proj...]	10.0.0.0/24	-	250
<input type="checkbox"/>	my-aws-subnet-01	subnet-0cbaff6da5ad07b7a4	Available	vpc-0d756f07d22282118 [proj...]	10.0.2.0/24	-	251

- vii. To set up the Internet Gateway, select Internet gateway from left-bar and select Create internet gateway.

Name	Internet gateway ID	State	VPC ID	Owner
-	igw-03fa569db5943efc	Attached	vpc-0106cbe3513a1507a	794872146236
project-igw	igw-03f5cef5d3255e69f	Attached	vpc-0d756f07d22282118 [project-vec]	794872146236

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
-	rtb-03813de583f8a9ce4	-	-	Yes	vpc-0106cbe3513a1507a

- viii. Configure the Route Table by clicking on the Route Table and select the lab session.

Explicit subnet associations (1)		Edit subnet associations	
<input type="checkbox"/>	Find subnet association	Details	
Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
project-subnet-private1-us-east-1a	subnet-0f49bc7bc001726ea	10.0.128.0/24	-

- ix. Create Security Group with necessary rule for the VPC

Details			
Security group name	Security group ID	Description	VPC ID
my-web-server-group-01	sg-0e2334d839d3cf157	Allow SSH Access for our developers	vpc-0d756f07d22282118
Owner	Inbound rules count	Outbound rules count	
794872146236	0 Permission entries	1 Permission entry	

- x. Instantiate an EC2 instance utilizing the previously established security group and VPC. Embed a code within the user data box for execution upon launch. Return to the newly created instance once its status indicates "2 checks passed." Identify and retrieve the

public IP address associated with the instance.

The screenshot shows the AWS EC2 'Launch templates' section. A green success bar at the top says 'Successfully created testinstancefortesting(lt-054b6750524ae8766)'. Below it, a 'Next Steps' section lists options: 'Launch an instance', 'Launch instance from this template', 'Create an Auto Scaling group from your template', 'Create Auto Scaling group', 'Create Spot Fleet', and 'Create Spot Fleet'. At the bottom right is a 'View launch templates' button.

mytestinstance i-0bb102c4024244ff8 Running t2.micro 2/2 checks passed View alarms us-east-1b

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.

- i. First we start by searching IAM in AWS Console and we create a IAM User.

The screenshot shows the AWS search interface with 'iam' typed into the search bar. On the left, a sidebar lists categories like Services (11), Features (22), and Documentation. The main search results show 'Services' with 'IAM' highlighted as the top result. The IAM card includes a star icon, a description 'Manage access to AWS resources', and links for 'Groups', 'Users', 'Roles', 'Policies', and 'Access Analyzer'. Below it is another card for 'IAM Identity Center'.

- ii. Select User from the left side of the screen

The screenshot shows the AWS Identity and Access Management (IAM) service interface. In the left sidebar, under 'Access management', the 'Users' option is selected. The main content area is titled 'Users (0) Info' and contains the message 'An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.' Below this is a search bar and a table header with columns for 'User name', 'Path', 'Group', 'Last activity', and 'MFA'. A message at the bottom right says 'No resources to display'.

iii. Create a new user

This screenshot shows the 'Specify user details' step of the IAM User creation wizard. It includes fields for 'User name' (set to 'my-IAM-user'), 'Provide user access to the AWS Management Console' (unchecked), and a note about generating programmatic access keys. At the bottom are 'Cancel' and 'Next' buttons.

This screenshot shows the 'Set permissions' step. It has three options: 'Add user to group' (unchecked), 'Copy permissions' (unchecked), and 'Attach policies directly' (checked). A note says '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.' At the bottom are 'Cancel' and 'Next' buttons.

This screenshot shows the 'Permissions policies' step. It lists 20/1182 policies, including 'AccessAnalyzerServiceRolePolicy', 'AdministratorAccess', 'AdministratorAccess-Amplify', 'AdministratorAccess-AWSElasticBeanstalk', 'AlexaForBusinessDeviceSetup', and 'AlexaForBusinessFullAccess'. The table includes columns for 'Policy name', 'Type', and 'Attached entities'. At the bottom are 'Filter by Type' and 'Create policy' buttons.

Policy name	Type	Attached entities
AccessAnalyzerServiceRolePolicy	AWS managed	0
AdministratorAccess	AWS managed - job function	1
AdministratorAccess-Amplify	AWS managed	0
AdministratorAccess-AWSElasticBeanstalk	AWS managed	0
AlexaForBusinessDeviceSetup	AWS managed	0
AlexaForBusinessFullAccess	AWS managed	0

<input checked="" type="checkbox"/>	<input type="checkbox"/>	AlexaForBusinessFullAccess	AWS managed	0
<input checked="" type="checkbox"/>	<input type="checkbox"/>	AlexaForBusinessGatewayExecution	AWS managed	0
<input checked="" type="checkbox"/>	<input type="checkbox"/>	AlexaForBusinessLifesizeDelegatedAccessPolicy	AWS managed	0
<input checked="" type="checkbox"/>	<input type="checkbox"/>	AlexaForBusinessNetworkProfileServicePolicy	AWS managed	0
<input checked="" type="checkbox"/>	<input type="checkbox"/>	AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	0
<input checked="" type="checkbox"/>	<input type="checkbox"/>	AlexaForBusinessReadOnlyAccess	AWS managed	0
<input checked="" type="checkbox"/>	<input type="checkbox"/>	AmazonAPIGatewayAdministrator	AWS managed	0
<input checked="" type="checkbox"/>	<input type="checkbox"/>	AmazonAPIGatewayInvokeFullAccess	AWS managed	0
<input checked="" type="checkbox"/>	<input type="checkbox"/>	AmazonAPIGatewayPushToCloudWatchLogs	AWS managed	0
<input checked="" type="checkbox"/>	<input type="checkbox"/>	AmazonAppFlowFullAccess	AWS managed	0
<input checked="" type="checkbox"/>	<input type="checkbox"/>	AmazonAppFlowReadOnlyAccess	AWS managed	0
<input checked="" type="checkbox"/>	<input type="checkbox"/>	AmazonAppStreamFullAccess	AWS managed	0
<input checked="" type="checkbox"/>	<input type="checkbox"/>	AmazonAppStreamPCAAccess	AWS managed	0
<input checked="" type="checkbox"/>	<input type="checkbox"/>	AmazonAppStreamReadOnlyAccess	AWS managed	0
<input checked="" type="checkbox"/>	<input type="checkbox"/>	AmazonAppStreamServiceAccess	AWS managed	0

► Set permissions boundary - *optional*

[Cancel](#)

[Previous](#)

[Next](#)

Create user group

X

Create a user group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

User group name

Enter a meaningful name to identify this group.

Maximum 128 characters. Use alphanumeric and '+,-,@,_' characters.

Permissions policies (918)



[Create policy](#)

Filter by Type

Search

All ty... ▾

< 1 2 3 4 5 6 7 ... 46 > ⚙

<input type="checkbox"/>	Policy name	Type	Use...	Description
<input type="checkbox"/>	AdministratorAccess	AWS managed ...	Permis...	Provides full access to AWS service
<input type="checkbox"/>	AdministratorAcce...	AWS managed	None	Grants account administrative pern
<input type="checkbox"/>	AdministratorAcce...	AWS managed	None	Grants account administrative pern
<input type="checkbox"/>	AlexaForBusinessD...	AWS managed	None	Provide device setup access to Alex
<input type="checkbox"/>	AlexaForBusinessF...	AWS managed	None	Grants full access to AlexaForBusin
<input type="checkbox"/>	AlexaForBusinessG...	AWS managed	None	Provide gateway execution access t
<input type="checkbox"/>	AlexaForBusinessLi...	AWS managed	None	Provide access to Lifesize AVS devic
<input type="checkbox"/>	AlexaForBusinessP...	AWS managed	None	Provide access to Poly AVS devices
<input type="checkbox"/>	AlexaForBusinessR...	AWS managed	None	Provide read only access to AlexaFc

[Cancel](#)

[Create user group](#)

Create user group

Create a user group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

User group name
Enter a meaningful name to identify this group.

Maximum 128 characters. Use alphanumeric and '+,-,_,-' characters.

Permissions policies (3/918)

Filter by Type				
<input type="text" value="Search"/>	All ty... ▾	< 1 2 3 4 5 6 7 ... 46 >	<input type="button" value="Create policy"/>	
Policy name	Type	Use...	Description	
<input checked="" type="checkbox"/> <input type="button" value="AdministratorAccess"/>	AWS managed	Permis...	Provides full access to AWS services	
<input checked="" type="checkbox"/> <input type="button" value="AdministratorAcc..."/>	AWS managed	None	Grants account administrative perm	
<input checked="" type="checkbox"/> <input type="button" value="AdministratorAcc..."/>	AWS managed	None	Grants account administrative perm	
<input type="checkbox"/> <input type="button" value="AlexaForBusinessD..."/>	AWS managed	None	Provide device setup access to Alexa	
<input type="checkbox"/> <input type="button" value="AlexaForBusinessF..."/>	AWS managed	None	Grants full access to AlexaForBusin	
<input type="checkbox"/> <input type="button" value="AlexaForBusinessG..."/>	AWS managed	None	Provide gateway execution access t	
<input type="checkbox"/> <input type="button" value="AlexaForBusinessLi..."/>	AWS managed	None	Provide access to Lifesize AVS devic	
<input type="checkbox"/> <input type="button" value="AlexaForBusinessP..."/>	AWS managed	None	Provide access to Poly AVS devices	
<input type="checkbox"/> <input type="button" value="AlexaForBusinessR..."/>	AWS managed	None	Provide read only access to AlexaFc	

User was not created.
User: arn:aws:sts::058264497878:assumed-role/voclabs/user3017366=pujanshrestha240@gmail.com is not authorized to perform: iam:CreateUser on resource: arn:aws:iam::058264497878:user/my-IAM-user because no identity-based policy allows the iam:CreateUser action

We don't have access to create user and group with the provided account so, I am referring to the foundation course to assign group to the users (pre-created users and groups).

<input type="checkbox"/> user-1	/spl66/	0	-	-	<input checked="" type="radio"/> 8 minutes	-	Active - AKIA
<input type="checkbox"/> user-2	/spl66/	0	-	-	<input checked="" type="radio"/> 8 minutes	-	Active - AKIA
<input type="checkbox"/> user-3	/spl66/	0	-	-	<input checked="" type="radio"/> 8 minutes	-	Active - AKIA

Now select User groups from the left side-bar and select **Create Group**.

Identity and Access Management (IAM)

IAM > User groups

User groups (3) 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
<input type="checkbox"/> EC2-Admin	0	Defined	12 minutes ago
<input type="checkbox"/> EC2-Support	0	Defined	12 minutes ago
<input type="checkbox"/> S3-Support	0	Defined	12 minutes ago

Go to the user group which is under the users in the left panel, click the group

Name

The screenshot shows the AWS IAM User Groups page. A user group named "EC2-Support" is selected. The "Permissions" tab is active, displaying one managed policy: "AmazonEC2ReadOnlyAccess".

Policy name	Type	Attached entities
AmazonEC2ReadOnlyAccess	AWS managed	1

Here, we have selected EC2-Support which is a pre-created group. Upon selecting Permissions, we can see that there is one permission on the policy i.e., **AmazonEC2ReadOnlyAccess**.

Now click on the users tab and add users.

The screenshot shows the "Add users to EC2-Support" dialog. Under "Other users in this account", the user "user-1" is selected. The "Add users" button is highlighted.

The screenshot shows the EC2-Support group summary page. The "Users" tab is active, showing one user: "user-1". A green banner at the top indicates "1 user added to this group".

User name	Groups	Last activity	Creation time
user-1	0	None	44 minutes ago

Now we can create new user, create password or use generated password and login with the assigned roles within the group.

Specify user details

User details

User name: my-IAM-user
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](#).

Do you want to provide console access to a person?
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications. To do so, sign into the console by using the credentials of the management account in AWS Organizations, and then enable Identity Center. If you aren't the management account owner, contact the owner to perform this task.

Console password:

Autogenerated password
You can view the password after you create the user.

Custom password
Enter a custom password for the user.

Must be at least 8 characters long
Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # \$ % ^ & * | _ - (hyphen) = [] { }

Show password

Users must create a new password at next sign-in - Recommended
Users automatically get the IAMUserChangePassword [policy](#) to allow them to change their own password.

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**