

## 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.

Start by launching a new EC2 instance



- i. selecting an appropriate instance type and configuring the instance details.

The screenshot shows the 'Launch an instance' wizard. At the top, the breadcrumb navigation is 'EC2 > Instances > Launch an instance'. The main title is 'Launch an instance' with an 'Info' link. A sub-instruction reads: '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.' Below this, the 'Name and tags' section is shown, with a 'Name' input field containing 'Ec2 server' and a 'Add additional tags' link. The 'Application and OS Images (Amazon Machine Image)' section is expanded, showing a search bar with placeholder text 'Search our full catalog including 1000s of application and OS images'. It includes tabs for 'Recents' and 'Quick Start', and a grid of AMI icons for 'Amazon Linux', 'macOS', 'Ubuntu', 'Windows', 'Red Hat', and 'SUSE'. To the right, there's a 'Browse more AMIs' link with a note about including AMIs from AWS, Marketplace, and the Community.

- Select instance type as t2.micro

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

Instance type

t2.micro	Free tier eligible
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	

[Additional costs apply for AMIs with pre-installed software](#)

All generations [Compare instance types](#)

- Creating new Key pair

## Create key pair

**Key pair name**  
Key pairs allow you to connect to your instance securely.

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

**Key pair type**

<input checked="" type="radio"/> RSA RSA encrypted private and public key pair	<input type="radio"/> ED25519 ED25519 encrypted private and public key pair
---	--

**Private key file format**

<input checked="" type="radio"/> .pem For use with OpenSSH	<input type="radio"/> .ppk For use with PuTTY
---	--

**⚠️** When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more ↗](#)

[Cancel](#) [Create key pair](#)

**▼ 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](#)

## Create and configure a new Security Group

**▼ Network settings [Info](#)**

VPC - *required* [Info](#)

▼
(default)
 [Edit](#)

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, 103.10.29.99/32)  Remove

Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>
ssh	TCP	22
Source type <a href="#">Info</a>	Name <a href="#">Info</a>	Description - <i>optional</i> <a href="#">Info</a>
My IP	Add CIDR, prefix list or security	e.g. SSH for admin desktop
	103.10.29.99/32	

[Add security group rule](#)

## ▼ Summary

Number of instances | [Info](#)

1

### Software Image (AMI)

Amazon Linux 2023 AMI 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



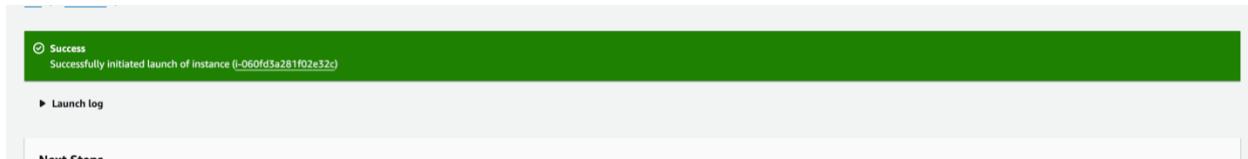
**Free tier:** In your first year includes  
750 hours of t2.micro (or t3.micro in  
the Regions in which t2.micro is  
unavailable) instance usage on free  
tier AMIs per month, 30 GiB of EBS  
storage, 2 million IOs, 1 GB of  
snapshots, and 100 GB of bandwidth  
to the internet.



[Cancel](#)

[Launch instance](#)

[Review commands](#)



## 1.1. Allocate an Elastic IP address to the instance

The screenshot shows the "Allocate Elastic IP address" configuration page. It includes sections for "Elastic IP address settings", "Public IPv4 address pool" (selected as "Amazon's pool of IPv4 addresses"), "Global static IP addresses", "Tags - optional", and buttons for "Allocate" and "Cancel".

**Elastic IP address settings** [Info](#)

**Network Border Group** [Info](#)

Search input: 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](#)

Elastic IP addresses (1/1)							
<input style="border: none; border-bottom: 1px solid #ccc; padding: 2px 10px; margin-right: 5px;" type="button" value="Actions"/> Allocate Elastic IP address							
<input type="text" value="Filter Elastic IP addresses"/>							< 1 > ⌂
<input type="button" value="Public IPv4 address: 44.196.3.52"/>	<input type="button" value="Clear filters"/>						
Name	Allocated IPv4 addr...	Type	Allocation ID	Reverse DNS record	Associated instance ID	Private IP adres	
<input checked="" type="checkbox"/> –	44.196.3.52	Public IP	eipalloc-062bbdfe209fd28a1	–	–	–	

## Opeining created elastic ip address

**Associate Elastic IP address**

Choose the instance or network interface to associate to this Elastic IP address (44.196.3.52)

Elastic IP address: 44.196.3.52

**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-060fd3a281f02e32c \(Ec2 server\) - running](#)
- [i-0d63dcae5732580d2 \(EC2 Server\) - running](#)
- [i-022827d3a2aef2738 \(EC2 Server\) - running](#)
- [i-06bcfc1a46016a8eb \(my server\) - running](#)
- [i-006f2305f86394850 \(my server\) - running](#)

Associated with a resource.

## Associate Elastic IP address

Choose the instance or network interface to associate to this Elastic IP address (44.196.3.52)

Elastic IP address: 44.196.3.52

### 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 reassigned to a different resource if it is already associated with a resource.

- Allow this Elastic IP address to be reassigned

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

**⌚ Elastic IP address associated successfully.**  
Elastic IP address 44.196.3.52 has been associated with instance i-060fd3a281f02e32c

## 44.196.3.52

[Actions](#) [Associate Elastic IP address](#)

### Summary

Allocated IPv4 address	Type	Allocation ID	Reverse DNS record
<a href="#">44.196.3.52</a>	<a href="#">Public IP</a>	<a href="#">eipalloc-062bbfe209fd28a1</a>	-
Association ID	Scope	Associated instance ID	Private IP address
<a href="#">eipassoc-0fe0e59ce123ba137</a>	<a href="#">VPC</a>	<a href="#">i-060fd3a281f02e32c</a>	<a href="#">172.31.27.248</a>
Network interface ID	Network interface owner account ID	Public DNS	NAT Gateway ID
<a href="#">eni-0611d2b7ad17b8629</a>	<a href="#">612362567483</a>	<a href="#">ec2-44-196-3-52.compute-1.amazonaws.com</a>	-
Address pool	Network Border Group		
<a href="#">Amazon</a>	<a href="#">us-east-1</a>		

Instances (1/5) <a href="#">Info</a>										
<input type="text"/> Find Instance by attribute or tag (case-sensitive)			Any state		Actions			Launch instances		
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
<input checked="" type="checkbox"/>	Ec2 server	i-060fd3a281f02e32c	<span>Running</span>  	t2.micro	<span>2/2 checks passed</span> 	<a href="#">View alarms</a> 	us-east-1d	ec2-54-87-200-208.co...	54.87.200.208	-
<input type="checkbox"/>	EC2 Server	i-0d63dcae5732580d2	<span>Running</span>  	t2.micro	<span>2/2 checks passed</span> 	<a href="#">View alarms</a> 	us-east-1c	ec2-34-238-39-29.com...	34.238.39.29	-
<input type="checkbox"/>	EC2 Server	i-022827d5a2ae2f738	<span>Running</span>  	t2.micro	<span>2/2 checks passed</span> 	<a href="#">View alarms</a> 	us-east-1c	ec2-5-87-219-128.com...	3.87.219.128	-
<input type="checkbox"/>	mv server	i-06bcfc1a46016a8eb	<span>Running</span>  	t2.micro	<span>2/2 checks passed</span> 	<a href="#">View alarms</a> 	us-east-1a	ec2-52-91-155-153.co...	52.91.155.153	-

Instance: i-060fd3a281f02e32c (Ec2 server)

[Details](#) [Status and alarms New](#) [Monitoring](#) [Security](#) [Networking](#) [Storage](#) [Tags](#)

▼ [Instance summary](#) [Info](#)

Instance ID  i-060fd3a281f02e32c (Ec2 server)	Public IPv4 address  54.87.200.208 <a href="#">[open address]</a> 	Private IPv4 addresses  172.31.27.248
IPv6 address -	Instance state <span>Running</span>	Public IPv4 DNS  ec2-54-87-200-208.compute-1.amazonaws.com <a href="#">[open address]</a> 
Hostname type IP name: ip-172-31-27-248.ec2.internal	Private IP DNS name (IPv4 only)  ip-172-31-27-248.ec2.internal	Elastic IP addresses -
Answer private resource DNS name IPv4 (A)	Instance type t2.micro	AWS Compute Optimizer finding  <a href="#">Opt-in to AWS Compute Optimizer for recommendations.</a>   <a href="#">Learn more</a> 
Auto-assigned IP address  54.87.200.208 [Public IP]	VPC ID  vpc-0d8fab51a5f972f19 	Subnet ID  subnet-07dc58050f08fba06 
IAM Role -	AMAZON	Auto Scaling Group name -
IMDSv2 Required		

▼ [Instance details](#) [Info](#)

Platform  Amazon Linux (Inferred)	AMI ID  ami-0e731c8a588258d0d	Monitoring disabled
Platform details  Linux/UNIX	AMI name  al2023-ami-2023.3.20240205.2-kernel-6.1-x86_64	Termination protection Disabled
Stop protection	Launch time	AMI location

## After allocation of elastic ip address in created ec2 instance

Instance summary for i-060fd3a281f02e32c (Ec2 server) <a href="#">Info</a>										
Updated less than a minute ago										
	Public IPv4 address		Private IPv4 addresses		Public IPv4 DNS		Elastic IP addresses		AWS Compute Optimizer finding	
Instance ID  i-060fd3a281f02e32c (Ec2 server)	 44.196.3.52 <a href="#">[open address]</a> 		 172.31.27.248		 ec2-44-196-3-52.compute-1.amazonaws.com <a href="#">[open address]</a> 		 44.196.3.52 [Public IP]		 <a href="#">Opt-in to AWS Compute Optimizer for recommendations.</a>   <a href="#">Learn more</a> 	
IPv6 address -	<span>Running</span>		Termination protection Disabled		Auto Scaling Group name -					
Hostname type IP name: ip-172-31-27-248.ec2.internal	Private IP DNS name (IPv4 only)  ip-172-31-27-248.ec2.internal		Instance type t2.micro		Instance ID  vpc-0d8fab51a5f972f19 		Subnet ID  subnet-07dc58050f08fba06 		AWS Compute Optimizer finding  <a href="#">Opt-in to AWS Compute Optimizer for recommendations.</a>   <a href="#">Learn more</a> 	
Answer private resource DNS name IPv4 (A)										
Auto-assigned IP address -										
IAM Role -										
IMDSv2 Required										

[Details](#) [Status and alarms New](#) [Monitoring](#) [Security](#) [Networking](#) [Storage](#) [Tags](#)

## 1.2. Connecting to the instance via SSH

Connecting to Ec2 instance

The screenshot shows the AWS EC2 Instances page with the instance `i-060fd3a281f02e32c` selected. The **SSH client** tab is active. The page provides instructions for connecting to the instance via SSH, including steps to open an SSH client, locate the private key file (`key-pair.pem`), run a command to ensure the key is not publicly viewable, and connect using the Public DNS (`ec2-54-87-200-208.compute-1.amazonaws.com`). It also includes an example command and a note about the default AMI username.

EC2 > Instances > i-060fd3a281f02e32c > Connect to instance

### Connect to instance Info

Connect to your instance i-060fd3a281f02e32c (Ec2 server) using any of these options

EC2 Instance Connect | Session Manager | **SSH client** | EC2 serial console

Instance ID  
i-060fd3a281f02e32c (Ec2 server)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is `key-pair.pem`
3. Run this command, if necessary, to ensure your key is not publicly viewable.  
chmod 400 "key-pair.pem"
4. Connect to your instance using its Public DNS:  
ec2-54-87-200-208.compute-1.amazonaws.com

Example:  
ssh -i "key-pair.pem" ec2-user@ec2-54-87-200-208.compute-1.amazonaws.com

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

- the ipv4 address of ec2 instance connected via ssh

```
Last login: Mon Feb 12 08:10:19 on console
utsha_mac@Utshas-MacBook-Pro Downloads % chmod 400 "key-pair.pem"
utsha_mac@Utshas-MacBook-Pro Downloads % ec2-54-87-200-208.compute-1.amazonaws.com
zsh: command not found: ec2-54-87-200-208.compute-1.amazonaws.com
utsha_mac@Utshas-MacBook-Pro Downloads % ssh -i "key-pair.pem" ec2-user@ec2-54-87-200-208.compute-1.amazonaws.com
The authenticity of host 'ec2-54-87-200-208.compute-1.amazonaws.com (54.87.200.208)' can't be established.
ED25519 key fingerprint is SHA256:c5k8iyTRsUwd+0J0bWYNw43fSEItnCfcMj0mwZ/0mc0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-54-87-200-208.compute-1.amazonaws.com' (ED25519) to the list of known hosts.

,
  #_
  ~\_ ####_
  ~\_ #####\
  ~~ \###|
  ~~  '#/ __ https://aws.amazon.com/linux/amazon-linux-2023
  ~~ V~' '-->
  ~~~ /
  ~~.._ _/
  _/_/
  _/m/'[ec2-user@ip-172-31-27-248 ~]$
```

## 1. S3 Storage Fundamental 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.

### 1.1. S3 bucket creation

Step-1: Create S3 bucket

Step-2: Provide general configuration. Select nearest aws region and assigning a bucket name.

**Create bucket** Info

Buckets are containers for data stored in S3. [Learn more](#)

**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

basic-s3bucket

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

### Step-3: Default configuration are kept as it is for rest.

The screenshot shows the 'Object Ownership' section with 'ACLs disabled (recommended)' selected. It also shows the 'Block Public Access settings for this bucket' section where 'Block all public access' is checked. A red box highlights the 'Block all public access' checkbox.

**Object Ownership**

**Bucket owner enforced**

**Block Public Access settings for this bucket**

**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.

Then, click create bucket and new bucket is created

The screenshot shows the 'General purpose buckets' list with one item: 'basic-s3bucket'. The table includes columns for Name, AWS Region, Access, and Creation date.

Name	AWS Region	Access	Creation date
basic-s3bucket	US East (N. Virginia) us-east-1	Bucket and objects not public	February 15, 2024, 19:18:51 (UTC+05:45)

## 1.2. Upload files

Step-1: Click Upload button to upload a files

The screenshot shows the AWS S3 console for the 'basic-s3bucket'. The 'Objects' tab is active. At the top, there are several buttons: Copy S3 URI, Copy URL, Download, Open, Delete, Actions (with a dropdown arrow), Create folder, and a large orange Upload button. Below these buttons is a search bar with placeholder text 'Find objects by prefix'. Underneath the search bar is a table header with columns: Name, Type, Last modified, Size, and Storage class. A message 'No objects' is displayed, followed by the sub-message 'You don't have any objects in this bucket.'. At the bottom of the table area is another orange 'Upload' button.

Step-2: Drag and drop the file that is to be uploaded and click upload. The remaining setting is set as default.

**Upload** [Info](#)

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, 263.0 B)

All files and folders in this table will be uploaded.

<input type="checkbox"/>	Name	Folder	Type
<input type="checkbox"/>	home.html	-	text/html

**Destination** [Info](#)

Destination  
s3://basic-s3bucket

▶ **Destination details**  
Bucket settings that impact new objects stored in the specified destination.

▶ **Permissions**  
Grant public access and access to other AWS accounts.

▶ **Properties**  
Specify storage class, encryption settings, tags, and more.

**Cancel** **Upload**

Then, files is uploaded sucessfully in assigned destination.

Upload succeeded  
View details below.

**Upload: status** [Close](#)

The information below will no longer be available after you navigate away from this page.

**Summary**

Destination	Succeeded	Failed
s3://basic-s3bucket	1 file, 263.0 B (100.00%)	0 files, 0 B (0%)

**Files and folders** (1 Total, 263.0 B)

<input type="checkbox"/>	Name	Folder	Type	Size	Status	Error
<input type="checkbox"/>	home.html	-	text/html	263.0 B	<span style="color: green;">Succeeded</span>	-

The details of uploaded files can be viewed

This screenshot shows the AWS S3 Object Details page for a file named 'home.html'. The top navigation bar includes 'Copy S3 URI', 'Download', 'Open', and 'Object actions'. Below the navigation, there are tabs for 'Properties', 'Permissions', and 'Versions', with 'Properties' currently selected. The 'Object overview' section displays various metadata fields:

Key	Value
Owner	awslabsco6975059t1703162515
AWS Region	US East (N. Virginia) us-east-1
Last modified	February 15, 2024, 19:32:05 (UTC+05:45)
Size	265.0 B
Type	html
Key	home.html
S3 URI	<a href="s3://basic-s3bucket/home.html">s3://basic-s3bucket/home.html</a>
Amazon Resource Name (ARN)	<a href="#">arn:aws:s3:::basic-s3bucket/home.html</a>
Entity tag (Etag)	<a href="#">df9699ca596137ba79dcb3452930c47d</a>
Object URL	<a href="https://basic-s3bucket.s3.amazonaws.com/home.html">https://basic-s3bucket.s3.amazonaws.com/home.html</a>

When the file is viewed from object url link, the permission accessed denied is shown, as the “Block all public access” setting was checked during file upload.

This screenshot shows a browser window displaying the XML error response for the object URL. The URL in the address bar is 'basic-s3bucket.s3.amazonaws.com/home.html'. The page content is as follows:

```
<Error>
<Code>AccessDenied</Code>
<Message>Access Denied</Message>
<RequestId>7DJG75JSW4B54B85</RequestId>
<HostId>5tG2v0fUHVvBlKwH6172gNFKGYNdEwGJueSXtEBMKaSbGnqV51aIAJhl+QzVj0ql+5F6mmSHmMQ=</HostId>
</Error>
```

But, the uploaded file can be accessed from the open button located at top right section of object detail page.

This screenshot shows a browser window with the title bar 'AWS'. The URL in the address bar is 'basic-s3bucket.s3.us-east-1.amazonaws.com/home.html?response-content-dispo...'. The page content is the same as the previous screenshot, showing the XML error response for an Access Denied error.

## Amazon Web Services

Get started with AWS

### 1.3. Setting up bucket policies for access control

Step-1: Select “permissions” tab and “edit” button of “Bucket policy” section to edit the policies of the bucket, which will take to new screen pf buclet policy.

The screenshot shows the AWS S3 Bucket Permissions Overview page. At the top, there are tabs: Objects, Properties, Permissions (which is selected), Metrics, Management, and Access Points. Below the tabs, a section titled "Permissions overview" shows "Access" status as "Bucket and objects not public". Under "Block public access (bucket settings)", it says "Block all public access" is turned "On". There is also a link to "Individual Block Public Access settings for this bucket". In the "Bucket policy" section, it states that public access is blocked because Block Public Access settings are turned on. A note indicates that to determine which settings are turned on, one should check the Block Public Access settings for this bucket. There are "Edit" and "Delete" buttons for the Bucket policy.

Step-2: Select “Policy generator” to generate the policy.

This navigated to new tab of policy generator. Here, policies are defines for access control.

Step-3: Select policy type as “S3 Bucket Policy”

#### 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

- SQS Queue Policy
- S3 Bucket Policy
- VPC Endpoint Policy
- IAM Policy
- SNS Topic Policy

#### Step 2: Add Statement(s)

Step-4: Fill the form as required. In effect “deny” and in action “PutPbject” is selected.

## 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** \*

Use a comma to separate multiple values.

**AWS Service** Amazon S3  All Services (\*)

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

**Amazon Resource Name (ARN)**

PutJobTagging  
 PutLifecycleConfiguration  
 PutMetricsConfiguration  
 PutMultiRegionAccessPointPolicy  
 PutObject  
 PutObjectAcl  
 PutObjectLegalHold

:\${BucketName}/\${KeyName}.  
alid. You must enter a valid ARN.

## Step 3: Generate Policy

ARN value of created s3 bucket is assigned in ARN section, this can be found in bucket properties section

basic-s3bucket [Info](#)

Objects Properties Permissions Metrics Management Access Points

**Bucket overview**

AWS Region US East (N. Virginia) us-east-1 Bucket ARN copied Bucket Name (ARN) arnaws:s3::basic-s3bucket Creation date February 15, 2024, 19:18:51 (UTC+05:45)

/\* is added after bucket ARN value.

## 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** \*

Use a comma to separate multiple values.

**AWS Service** Amazon S3  All Services (\*)

Use multiple statements to add permissions for more than one service.

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

**Amazon Resource Name (ARN)** arn:aws:s3:::basic-s3bu

ARN should follow the following format: arn:aws:s3:::\${BucketName}/\${KeyName}.  
Use a comma to separate multiple values.

**Add Conditions (Optional)**

**Add Statement**

Then, conditions for denying specific object to be uploaded. Here, we are denying any objects with Key s3:x-amz-server-side-encryption set to Null.

## 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** \*

Use a comma to separate multiple values.

**AWS Service** Amazon S3  All Services (\*)

Use multiple statements to add permissions for more than one service.

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

**Amazon Resource Name (ARN)** arn:aws:s3:::basic-s3bu

ARN should follow the following format: arn:aws:s3:::\${BucketName}/\${KeyName}.  
Use a comma to separate multiple values.

**Add Conditions (Optional)** Hide

Conditions are any restrictions or details about the statement.([More Details](#)).

Condition	Null
Key	s3:x-amz-server-side-encryption
Value	true

**Add Condition**

Condition	Keys
Null	• s3:x-amz-server-side-encryption: "true"

**Add Statement**

Click “Add Statement” and then json document of s3 bucket policy is generated with “Generate Policy”

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

Principal(s)	Effect	Action	Resource	Conditions
*	Deny	s3:PutObject	arn:aws:s3:::basic-s3bucket/*	• Null ◦ s3:x-amz-server-side-encryption: "true"

### 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](#)

**Policy JSON Document** x

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": "Policy1708008644406", "Version": "2012-10-17", "Statement": [ { "Sid": "Stmt1708008589437", "Action": [ "s3:PutObject" ], "Effect": "Deny", "Resource": "arn:aws:s3:::basic-s3bucket/*", "Condition": { "Null": { "s3:x-amz-server-side-encryption": "true" } }, "Principal": "*" } ] }
```

[Close](#)

The generated policy is copied and paste to bucket 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.

Bucket ARN

 arn:aws:s3:::basic-s3bucket

### Policy

```
1 ▾ {  
2     "Id": "Policy1708008644406",  
3     "Version": "2012-10-17",  
4     "Statement": [  
5         {  
6             "Sid": "Stmt1708008589437",  
7             "Action": [  
8                 "s3:PutObject"  
9             ],  
10            "Effect": "Deny",  
11            "Resource": "arn:aws:s3:::basic-s3bucket/*",  
12            "Condition": {  
13                "Null": {  
14                    "s3:x-amz-server-side-encryption": "true"  
15                }  
16            },  
17            "Principal": "*"  
18        }  
19    ]  
20 }
```

Then the changes is saved clicking “Save Changes” button.

 Successfully edited bucket policy. X

**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](#)

 Public access is blocked because Block Public Access settings are turned on for this bucket  
To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about [using Amazon S3 Block Public Access](#)

```
{  
  "Version": "2012-10-17",  
  "Id": "Policy1708008644406",  
  "Statement": [  
    {  
      "Sid": "Stmt1708008589437",  
      "Effect": "Deny",  
      "Principal": "*",  
      "Action": "s3:PutObject",  
      "Resource": "arn:aws:s3:::basic-s3bucket/*",  
      "Condition": {  
        "Null": {  
          "s3:x-amz-server-side-encryption": "true"  
        }  
      }  
    }  
  ]  
}
```

 Copy

## 2.4. Testing the policy

Uploading the same html file without specifying any encryption key

The screenshot shows the AWS S3 console interface for uploading files. At the top, there's a header with "Files and folders (1 Total, 263.0 B)" and buttons for "Remove", "Add files", and "Add folder". Below this, a note says "All files and folders in this table will be uploaded." A search bar with "Find by name" placeholder text and navigation arrows (< 1 >) is present. A table lists one file: "home.html" under the "Name" column and "-" under the "Folder" column. The "Name" column has a dropdown arrow. Below the table, a section titled "Destination" with an "Info" link is shown. It contains the destination path "s3://basic-s3bucket". Under "Destination details", it says "Bucket settings that impact new objects stored in the specified destination." Another section titled "Permissions" with an "Info" link follows, stating "Grant public access and access to other AWS accounts." Finally, a section titled "Properties" with an "Info" link is shown.

Server side encryption can be updated from “Properties” section

The screenshot shows the AWS S3 console interface for managing server-side encryption. A section titled "Server-side encryption" with an "Info" link is displayed. It states "Server-side encryption protects data at rest." Below this, a heading "Server-side encryption" is followed by two options: a selected radio button "Do not specify an encryption key" and an unselected radio button "Specify an encryption key". The "Do not specify an encryption key" option includes a note: "The bucket settings for default encryption are used to encrypt objects when storing them in Amazon S3." The "Specify an encryption key" option includes a note: "The specified encryption key is used to encrypt objects before storing them in Amazon S3." At the bottom, a warning message in a yellow box states: "⚠ If your bucket policy requires objects to be encrypted with a specific encryption key, you must specify the same encryption key when you upload objects. Otherwise, uploads will fail."

The access is denied as the encryption key is not specified while uploading the file.

The screenshot shows the AWS S3 'Upload: status' page. At the top, there is a red header bar with the message 'upload failed' and a link 'View details below.' Below the header, the title 'Upload: status' is displayed. A note says 'The information below will no longer be available after you navigate away from this page.' On the right, there is a 'Close' button. The main area is divided into sections: 'Summary' (Destination: s3://basic-s3bucket, Status: Failed, Details: 1 file, 263.0 B (100.00%)), 'Files and folders' (selected tab), and 'Configuration'. The 'Files and folders' section shows a table with one item: 'home.html' (Type: text/html, Size: 263.0 B, Status: Failed, Error: Access Denied). There is also a search bar labeled 'Find by name'.

Now, for uploading the file, below setup is configured

The screenshot shows the 'Server-side encryption' configuration page. It includes sections for 'Server-side encryption' (Info: Server-side encryption protects data at rest.), 'Server-side encryption' settings (radio buttons for 'Do not specify an encryption key' (selected) and 'Specify an encryption key'), 'Encryption settings' (radio buttons for 'Use bucket settings for default encryption' and 'Override bucket settings for default encryption' (selected)), and 'Encryption type' (radio buttons for 'Server-side encryption with Amazon S3 managed keys (SSE-S3)' (selected), 'Server-side encryption with AWS Key Management Service keys (SSE-KMS)', and 'Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)'). A note at the bottom states: 'Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the [Amazon S3 pricing page](#). [ ]'.

Now, the file is uploaded successfully after adding encryption key.

⌚ upload succeeded  
View details below.

Upload: status

The information below will no longer be available after you navigate away from this page.

**Summary**

Destination	Succeeded	Failed
s3://basic-s3bucket	⌚ 1 file, 263.0 B (100.0%)	⌚ 0 files, 0 B (0%)

[Files and folders](#) [Configuration](#)

**Files and folders** (1 Total, 263.0 B)

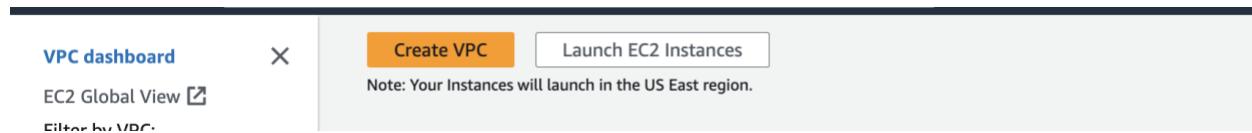
Name	Folder	Type	Size	Status	Error
home.html	-	text/html	263.0 B	⌚ Succeeded	-

## 2. VPC Configuration

- **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.

### 2.1. Create VPC

Navigate to VPC dashboard and click “Create VPC” button to create a new VPC



Configure the VPC form and assign the requested values

The screenshot shows the 'Create VPC' configuration form. It includes sections for 'VPC settings', 'Tags', and buttons for 'Cancel' and 'Create VPC'.

**VPC settings**

- Resources to create**:  VPC only  VPC and more
- Name tag - optional**: basic-vpc
- IPv4 CIDR block**:  CIDR block size must be between /16 and /28.
- IPv6 CIDR block**:  No IPv6 CIDR block  IPAM-allocated IPv6 CIDR block  Amazon-provided IPv6 CIDR block  IPv6 CIDR owned by me
- Tenancy**: Default

**Tags**

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

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

You can add 49 more tags

Then, a new VPC is created

vpc-06e62a52af76c05d5 / basic-vpc			
Details		Info	
VPC ID <a href="#">vpc-06e62a52af76c05d5</a>	State <span style="color: green;">Available</span>	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP option set <a href="#">dopt-00f56b0378df23930</a>	Main route table <a href="#">rtb-095eb7150db0d1327</a>	Main network ACL <a href="#">acl-0979983b5675ac330</a>
Default VPC No	IPv4 CIDR 10.0.0.0/25	IPv6 pool -	IPv6 CIDR (Network border group) -
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups <span style="color: red;">Failed to load rule groups</span>	Owner ID <a href="#">612362567483</a>	

## 2.2. Add Subnets

Step-1: Navigate to subnet section of VPC dashboard and configure subnet.

Step:-2: Select created VPC ID

### VPC

VPC ID  
Create subnets in this VPC.

vpc-06e62a52af76c05d5 (basic-vpc) ▾

**Associated VPC CIDRs**

IPv4 CIDRs  
10.0.0.0/25

Step-3: Assign subnet name and select nearest possible availability zone and then create subnet

## Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

### Subnet 1 of 1

#### Subnet name

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

The name can be up to 256 characters long.

#### Availability Zone 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

64 IPs



#### ▼ Tags - optional

##### Key

##### Value - optional

RemoveAdd new tag

You can add 49 more tags.

RemoveAdd new subnetCancelCreate subnet

Then, the subnet is created successfully.

Subnets (1) <small>Info</small>								
<input type="text" value="Q. Find resources by attribute or tag"/> Actions  Create subnet								
<input type="checkbox"/> Subnet ID : subnet-0d6a108fc3e4d690d								
<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses	
	vpc-subnet-01	subnet-0d6a108fc3e4d690d		vpc-06e62a52af76c05d5   basic...	10.0.0.0/26	-	59	

## 2.3. Setup Internet Gateway

Step-1: Navigate to “Internet gateways” and select “Create internet gateway”.



Step-2: Assign gateway name and then create

### 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"/> <span>X</span>	<input type="text" value="internet-gateway"/> <span>X</span> <span>Remove</span>

**Add new tag**  
You can add 49 more tags.

Cancel Create internet gateway

VPC > [Internet gateways](#) > igw-02865be69c54e7fe8

### igw-02865be69c54e7fe8 / internet-gateway

Actions ▾

Details	Info
Internet gateway ID <a href="#">igw-02865be69c54e7fe8</a>	State <input checked="" type="radio"/> Detached
	VPC ID -
	Owner <a href="#">612362567483</a>

#### Tags

Manage tags < 1 > @

Key	Value
Name	internet-gateway

Step-3: Attach the gateway to vpc by selecting created internet gateway. Click on actions and then select “Attach VPC”. This navigates to “Attach to VPC” page.

Internet gateways (1/2) <a href="#">Info</a>					
<input type="checkbox"/>	Name	Internet gateway ID	State	VPC ID	Owner
<input type="checkbox"/>	-	igw-0a4669731cca36081	Attached	vpc-0d8fab51a5f972f19	612362567483
<input checked="" type="checkbox"/>	internet-gateway	igw-02865be69c54e7fe8	Detached	-	612362567483

[Actions ▾](#)
[Create internet gateway](#)
  
[View details](#) | [Attach to VPC](#) | [Detach from VPC](#) | [Manage tags](#) | [Delete internet gateway](#)

Step-4: Select the created VPC and then click “Attach internet gateway”

[VPC](#) > [Internet gateways](#) > [Attach to VPC \(igw-02865be69c54e7fe8\)](#)

## Attach to VPC (igw-02865be69c54e7fe8) [Info](#)

**VPC**

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

**Available VPCs**

Attach the internet gateway to this VPC.

X

**AWS Command Line Interface command**

Cancel
[Attach internet gateway](#)

igw-02865be69c54e7fe8 / internet-gateway				
<a href="#">Details</a> <a href="#">Info</a>		<a href="#">Actions ▾</a>		
Internet gateway ID <a href="#">igw-02865be69c54e7fe8</a>	State <span style="color: green;">Attached</span>	VPC ID <a href="#">vpc-06e62a52af76c05d5   basic-vpc</a>	Owner <a href="#">612362567483</a>	

Now, the newly created VPC state status is attached

Internet gateways (2) <a href="#">Info</a>					
<input type="checkbox"/>	Name	Internet gateway ID	State	VPC ID	Owner
<input type="checkbox"/>	-	igw-0a4669731cca36081	Attached	vpc-0d8fab51a5f972f19	612362567483
<input checked="" type="checkbox"/>	internet-gateway	igw-02865be69c54e7fe8	Attached	vpc-06e62a52af76c05d5   basic-vpc	612362567483

## 2.4. Configure route table

Navigate to “Route Tables” and click “Create route table” to create a new route table. This navigates to “Create route table” page.

Step-1: Assign route table name

Step-2: Select VPC

**Create route table** Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

**Route table settings**

**Name - optional**  
Create a tag with a key of 'Name' and a value that you specify.

route-table-01

**VPC**  
The VPC to use for this route table.

vpc-06e62a52af76c05d5 (basic-vpc)

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

**Key** Name **Value - optional** route-table-01 **Remove**

Add new tag

You can add 49 more tags.

Cancel **Create route table**

Route table rtb-00bd8094b07273fd8 | route-table-01 was created successfully.

VPC > Route tables > rtb-00bd8094b07273fd8

rtb-00bd8094b07273fd8 / route-table-01 Actions ▾

**Details** Info

Route table ID rtb-00bd8094b07273fd8	Main No	Explicit subnet associations -	Edge associations -
VPC vpc-06e62a52af76c05d5   basic-vpc	Owner ID 612362567483		

**Routes** Subnet associations Edge associations Route propagation Tags

Routes (1)		Edit routes	
<small>Filter routes</small>		<small>Both ▾</small>	
Destination 10.0.0.0/25	Target local	Status Active	Propagated No

Now, the route table is created.

Route tables (3) <a href="#">Info</a>							Actions		<a href="#">Create route table</a>
	Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC	Owner ID		
<input type="checkbox"/>	-	<a href="#">rtb-06ce5a6546a6cf3c8</a>	-	-	Yes	<a href="#">vpc-0d8fab51a5f972f19</a>	612362567483		
<input type="checkbox"/>	-	<a href="#">rtb-095eb7150db0d1327</a>	-	-	Yes	<a href="#">vpc-06e62a52af76c05d5   basic...</a>	612362567483		
<input checked="" type="checkbox"/>	route-table-01	<a href="#">rtb-00bd8094b07273fd8</a>	-	-	No	<a href="#">vpc-06e62a52af76c05d5   basic...</a>	612362567483		

## 2.5. Attaching internet gateway to the route table

Step-1: Select the route table and click edit routes

rtb-00bd8094b07273fd8 / route-table-01

Details [Routes](#) Subnet associations Edge associations Route propagation Tags

Routes (1)

Destination	Target	Status	Propagated
10.0.0.0/25	local	Active	No

Step-2: Configure the edit route form

Select Internet Gateway and then newly created internet gateway

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/25	local	Active	No
0.0.0.0/0	Internet Gateway	-	No

Add route [Remove](#)

Cancel [Preview](#) [Save changes](#)

Updated routes for rtb-00bd8094b07273fd8 / route-table-01 successfully

VPC > Route tables > rtb-00bd8094b07273fd8 / route-table-01

**Details Info**

Route table ID rtb-00bd8094b07273fd8	Main No	Explicit subnet associations -	Edge associations -
VPC vpc-06e62a52af76c05d5   basic-vpc	Owner ID 612362567483		

**Routes (2)**

Destination	Target	Status	Propagated
0.0.0.0/0	igw-02865be69c54e7fe8	Active	No
10.0.0.0/25	local	Active	No

## 2.6. Subnet associations

Step-1: Navigate to “Subnet associations” tab

Step-2: Select the created subnet and save the associations

VPC > Route tables > rtb-00bd8094b07273fd8 > Edit subnet associations

**Edit subnet associations**

Change which subnets are associated with this route table.

**Available subnets (1/1)**

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
vpc-subnet-01	subnet-0d6a108fc3e4d690d	10.0.0.0/26	-	Main (rtb-095eb7150db0d1327)

**Selected subnets**

subnet-0d6a108fc3e4d690d / vpc-subnet-01 X
--

Cancel **Save associations**

## 2.7. Setting up a simple EC2 instance

Create a new EC2 instance and in network setting select the creted VPC and subnet and set “Auto-assign public IP” as enable. Create new ssh group

## 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

64-bit (x86)

#### Boot mode

uefi-preferred

#### AMI ID

ami-0e731c8a588258d0d

Verified provider

## ▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-06e62a52af76c05d5 (basic-vpc)  
10.0.0.0/25



Subnet [Info](#)

subnet-0d6a108fc3e4d690d [vpc-subnet-01](#)  
VPC: vpc-06e62a52af76c05d5 Owner: 612362567483 Availability Zone: us-east-1a  
IP addresses available: 59 CIDR: 10.0.0.0/26



[Create new subnet](#)

Auto-assign public IP [Info](#)

Enable

Firewall (security groups) [Info](#)

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

[Create security group](#)

[Select existing security group](#)

Security group name - required

new-ssh-group

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](#)

security group

### Inbound Security Group Rules

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

[Remove](#)

Type [Info](#)

ssh

Protocol [Info](#)

TCP

Port range [Info](#)

22

Source type [Info](#)

Anywhere

Source [Info](#)

Add CIDR, prefix list or security

Description - optional [Info](#)

e.g. SSH for admin desktop

0.0.0.0/0

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.

[Add security group rule](#)

► Advanced network configuration

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

1x  GiB  [▼](#) Root volume (Not encrypted)

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

[Add new volume](#)

**Click refresh to view backup information** [⟳](#)  
The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems [Edit](#)

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

**Success**  
Successfully initiated launch of instance i-06b9823b29c8cf89

[Launch log](#)

**Instance: i-06b9823b29c8cf89 (vpc-ec2-instance)**

Details	Status and alarms <a href="#">New</a>	Monitoring	Security	Networking	Storage	Tags
<b>Instance summary</b> <a href="#">Info</a>						
Instance ID <a href="#">i-06b9823b29c8cf89 (vpc-ec2-instance)</a>	Public IPv4 address <a href="#">52.203.162.230 [open address]</a>	Private IPv4 addresses <a href="#">10.0.0.44</a>				
IPv6 address -	Instance state <a href="#">Running</a>	Public IPv4 DNS -				
Hostname type IP name: ip-10-0-44.ec2.internal	Private IP DNS name (IPv4 only) <a href="#">ip-10-0-44.ec2.internal</a>	Elastic IP addresses -				
Answer private resource DNS name -	Instance type <a href="#">t2.micro</a>	AWS Compute Optimizer finding <a href="#">Opt-in to AWS Compute Optimizer for recommendations.   Learn more</a>				
Auto-assigned IP address <a href="#">52.203.162.230 [Public IP]</a>	VPC ID <a href="#">vpc-06e62a52af76c05d5 (basic-vpc)</a>	Auto Scaling Group name -				
IAM Role -	Subnet ID <a href="#">subnet-0d6a108fc3e4d690d (vpc-subnet-01)</a>					
IMDSv2 Required						
<b>Instance details</b> <a href="#">Info</a>						
Platform <a href="#">Amazon Linux (Inferred)</a>	AMI ID <a href="#">ami-0e731c8a588258d0d</a>	Monitoring disabled				
Platform details <a href="#">Linux/UNIX</a>	AMI name <a href="#">al2023-ami-2023.3.20240205.2-kernel-6.1-x86_64</a>	Termination protection Disabled				

```
utsha_mac@Utshas-MacBook-Pro Downloads % chmod 400 "key-pair.pem"
utsha_mac@Utshas-MacBook-Pro Downloads % ssh -i "key-pair.pem" ec2-user@52.203.162.230
,      #
~\_  ####_      Amazon Linux 2023
~~ \####\_
~~ \###|
~~   `#/ ___  https://aws.amazon.com/linux/amazon-linux-2023
~~     V~' '->
~~~   /
~~_._. /'
~/ /'
~/m/'
```

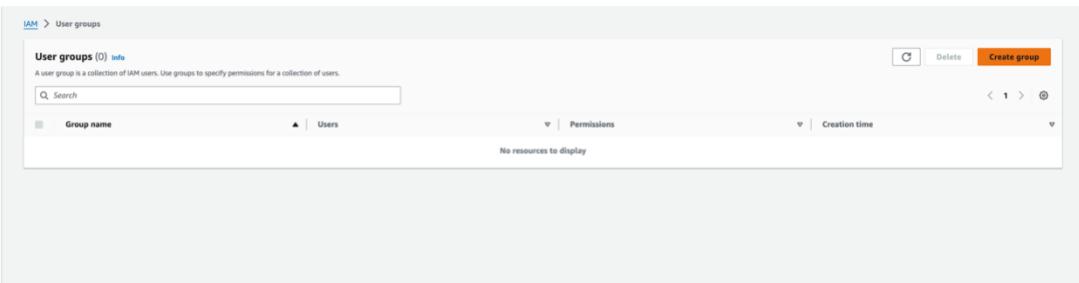
### 3. IAM Users and Roles Lab

- **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.

#### 3.1. Create new IAM user group

Step-1: Search fro IAM in and navigate to IAM dashboard

Step-2: From left navigation bar select “User group”



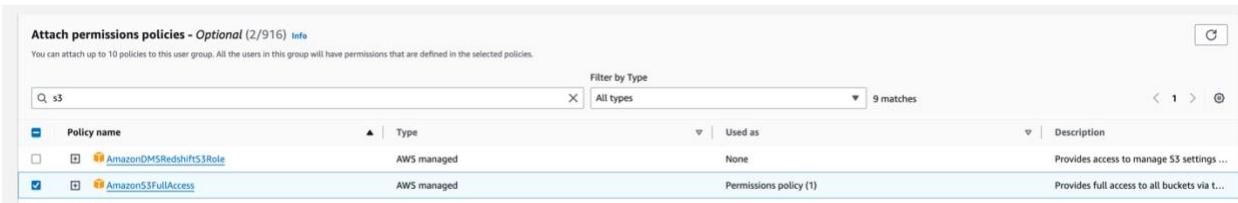
The screenshot shows the AWS IAM User Groups page. On the left, there's a navigation sidebar with options like Dashboard, User groups, Roles, Policies, and Account settings. The main area has a heading "User groups (0) Info" and a sub-section "A user group is a collection of IAM users. Use groups to specify permissions for a collection of users." Below this is a search bar and a table with columns for Group name, Users, Permissions, and Creation time. A note at the bottom says "No resources to display". At the top right, there are "Create group", "Delete", and navigation buttons.

Step-3: Select “Create group” and provide required configuration



The screenshot shows the "Create user group" configuration page. It has a header "Create user group" and a section "Name the group" with a text input field containing "developers". Below it is a "User group name" field with the same value, accompanied by a note: "Enter a meaningful name to identify this group." There's also a note: "Maximum 128 characters. Use alphanumeric and '+-,@\_,-' characters." At the bottom, there are "Next Step" and "Cancel" buttons.

Step-4: Apply policies to manage permission. Here, “AmazonS3FullAccess” and “AmazonEc2FullAccess” policies is attached.



The screenshot shows the "Attach permissions policies" page. It has a header "Attach permissions policies - Optional (2/916) Info" and a note: "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." Below is a search bar, a "Filter by Type" dropdown set to "All types", and a table with columns for Policy name, Type, Used as, and Description. Two policies are listed: "AmazonDMSRedshiftS3Role" (AWS managed, None, "Provides access to manage S3 settings ...") and "AmazonS3FullAccess" (AWS managed, "Permissions policy (1)", "Provides full access to all buckets via t...").

**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.

Policy name	Type	Used as	Description
<input type="checkbox"/> <a href="#">AmazonEC2ContainerRegistryFullAccess</a>	AWS managed	None	Provides administrative access to Amazon EC2 Container Registry.
<input type="checkbox"/> <a href="#">AmazonEC2ContainerRegistryPowerUser</a>	AWS managed	None	Provides full access to Amazon EC2 Container Registry.
<input type="checkbox"/> <a href="#">AmazonEC2ContainerRegistryReadOnly</a>	AWS managed	Permissions policy (1)	Provides read-only access to Amazon EC2 Container Registry.
<input type="checkbox"/> <a href="#">AmazonEC2ContainerServiceAutoscaleRole</a>	AWS managed	None	Policy to enable Task AutoScaling for Amazon ECS.
<input type="checkbox"/> <a href="#">AmazonEC2ContainerServiceEventsRole</a>	AWS managed	None	Policy to enable CloudWatch Events for Amazon ECS.
<input type="checkbox"/> <a href="#">AmazonEC2ContainerServiceforEC2Role</a>	AWS managed	None	Default policy for the Amazon EC2 Role for AWS Lambda.
<input type="checkbox"/> <a href="#">AmazonEC2ContainerServiceRole</a>	AWS managed	None	Default policy for Amazon ECS service role.
<input checked="" type="checkbox"/> <a href="#">AmazonEC2FullAccess</a>	AWS managed	None	Provides full access to Amazon EC2 via the AWS SDK, CLI, and API.
<input type="checkbox"/> <a href="#">AmazonEC2ReadOnlyAccess</a>	AWS managed	None	Provides read-only access to Amazon EC2.

**User group was not created.**  
 User: arn:aws:sts::612362567483:assumed-role/vocabs/user3009561+utshashretha07@gmail.com is not authorized to perform: iam:CreateGroup on resource: arn:aws:iam::612362567483:group/developers because no identity-based policy allows the iam:CreateGroup action

### Create user group

**Name the group**

User group name  
 Enter a meaningful name to identify this group.  
  
 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
<input type="text" value="Search"/>

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.

Policy name	Type	Used as	Description
<input type="checkbox"/> <a href="#">AmazonDMSRedshiftS3Role</a>	AWS managed	None	Provides access to manage S3 settings for Amazon DMS.
<input checked="" type="checkbox"/> <a href="#">AmazonS3FullAccess</a>	AWS managed	Permissions policy (1)	Provides full access to all buckets via the AWS SDK, CLI, and API.
<input type="checkbox"/> <a href="#">AmazonS3ObjectLambdaExecutionRolePolicy</a>	AWS managed	None	Provides AWS Lambda functions permission to access objects in S3.
<input type="checkbox"/> <a href="#">AmazonS3OutpostsFullAccess</a>	AWS managed	None	Provides full access to Amazon S3 on Outposts.
<input type="checkbox"/> <a href="#">AmazonS3OutpostsReadOnlyAccess</a>	AWS managed	None	Provides read only access to Amazon S3 on Outposts.
<input type="checkbox"/> <a href="#">AmazonS3ReadOnlyAccess</a>	AWS managed	Permissions policy (1)	Provides read only access to all buckets via the AWS SDK, CLI, and API.
<input type="checkbox"/> <a href="#">AWSBackupServiceRolePolicyForS3Backup</a>	AWS managed	None	Policy containing permissions necessary for AWS Backup to back up objects in S3.
<input type="checkbox"/> <a href="#">AWSBackupServiceRolePolicyForS3Restore</a>	AWS managed	None	Policy containing permissions necessary for AWS Backup to restore objects from S3.
<input type="checkbox"/> <a href="#">QuickSightAccessForS3StorageManagementAnalyticsReadonlyAccess</a>	AWS managed	None	Policy used by QuickSight team to access S3 storage management and analytics.

Need to try with cloud foundation