

1. EC2 Basics Lab

Objective: To understand the process of setting up and managing an Amazon EC2 instance.

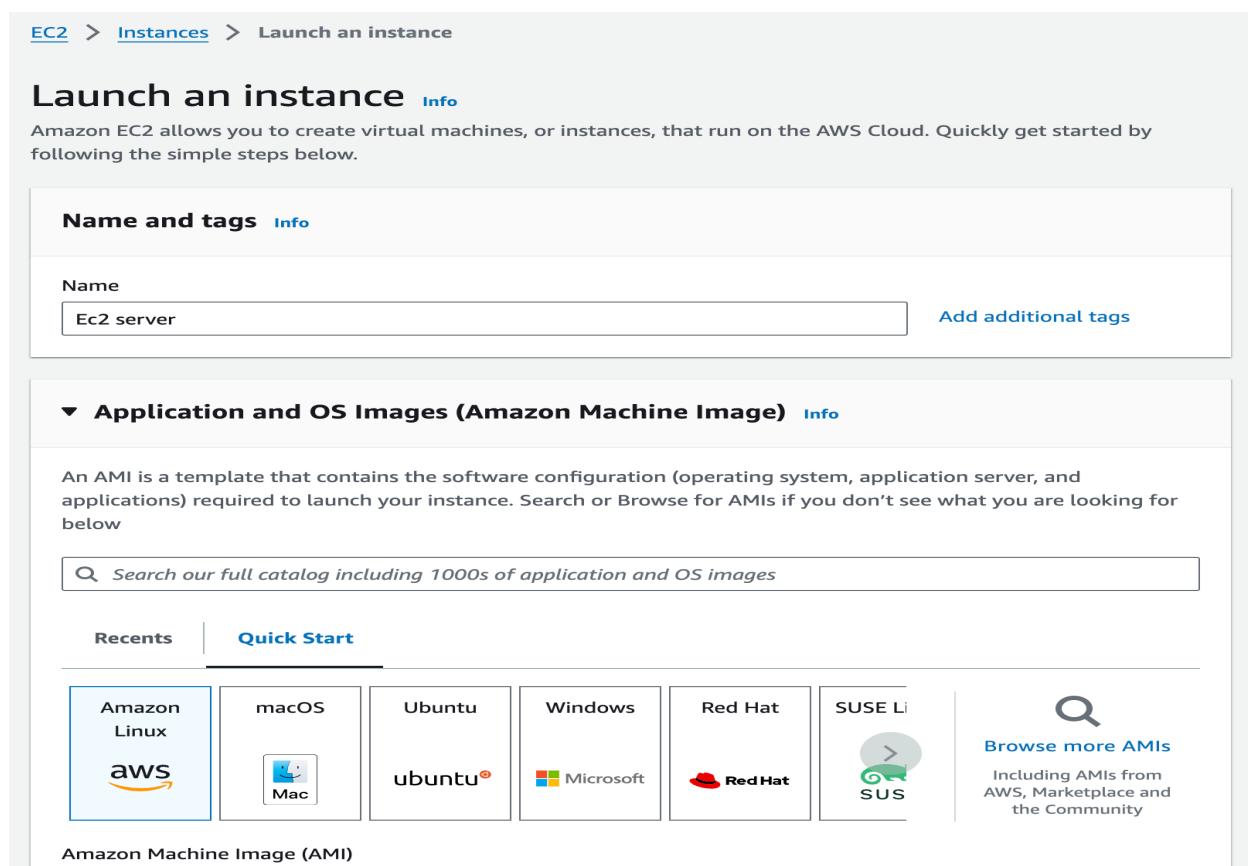
Approach: Students will start by launching a new EC2 instance, selecting an appropriate instance type and configuring the instance details. They will then create and configure a new Security Group, and allocate an Elastic IP address to the instance. The lab will also include connecting to the instance 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.



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

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

Recent AMIs Quick Start

Amazon Linux	macOS	Ubuntu	Windows	Red Hat	SUSE Linux Enterprise Server
--------------	-------	--------	---------	---------	------------------------------

Amazon Machine Image (AMI)

Browse more AMIs 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	

[All generations](#)

[Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

- 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) ▼

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)

Type Info	Protocol Info	Port range Info
ssh	TCP	22
Source type Info	Name Info	Description - <i>optional</i> Info
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

Allocate Elastic IP address [Info](#)

Elastic IP address settings [Info](#)

Network Border Group [Info](#)

[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](#)

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

Instances (1/5) Info										
<input type="text" value="Find Instance by attribute or tag (case-sensitive)"/> Any state										
	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	Running View details Logs	t2.micro	2/2 checks passed View alarms	+	us-east-1d	ec2-54-87-200-208.co...	54.87.200.208	-
<input type="checkbox"/>	EC2 Server	i-063dcae5732580d2	Running View details Logs	t2.micro	2/2 checks passed View alarms	+	us-east-1c	ec2-34-238-39-29.com...	34.238.39.29	-
<input type="checkbox"/>	EC2 Server	i-022827d5a2ae2f738	Running View details Logs	t2.micro	2/2 checks passed View alarms	+	us-east-1c	ec2-3-87-219-128.com...	3.87.219.128	-
<input type="checkbox"/>	mv server	i-06bcfc1a46016a8eb	Running View details Logs	t2.micro	2/2 checks passed View alarms	+	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 [open address]	Private IPv4 addresses 172.31.27.248	
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-54-87-200-208.compute-1.amazonaws.com [open address]	
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 Opt-in to AWS Compute Optimizer for recommendations. Learn more	
Auto-assigned IP address 54.87.200.208 [Public IP]	VPC ID vpc-0d8fab51a5f972f19	Subnet ID subnet-07dc58050f08fba06	Auto Scaling Group name -
IAM Role -	AMI ID ami-0e731c8a588258d0d	Launch time	AMI location
IMDSv2 Required	AMI name al2023-ami-2023.3.20240205.2-kernel-6.1-x86_64	Termination protection Disabled	
Stop protection			

▼ [Instance details](#) [Info](#)

Platform Amazon Linux (Inferred)	Monitoring disabled
Platform details Linux/UNIX	Termination protection Disabled
Stop protection	AMI location

After allocation of elastic ip address in created ec2 instance

Instance summary for i-060fd3a281f02e32c (Ec2 server) Info										
Updated less than a minute ago										
	Name	Instance ID	Public IPv4 address	Private IPv4 addresses	Instance state	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
<input checked="" type="checkbox"/>	Ec2 server	i-060fd3a281f02e32c (Ec2 server)	44.196.3.52 [open address]	172.31.27.248	Running View details Logs	+	us-east-1d	ec2-44-196-3-52.compute-1.amazonaws.com	[open address]	-
<input type="checkbox"/>	EC2 Server	i-063dcae5732580d2	Running View details Logs	54.87.200.208	2/2 checks passed View alarms	+	us-east-1c	ec2-34-238-39-29.com...	34.238.39.29	-
<input type="checkbox"/>	EC2 Server	i-022827d5a2ae2f738	Running View details Logs	54.87.200.208	2/2 checks passed View alarms	+	us-east-1c	ec2-3-87-219-128.com...	3.87.219.128	-
<input type="checkbox"/>	mv server	i-06bcfc1a46016a8eb	Running View details Logs	54.87.200.208	2/2 checks passed View alarms	+	us-east-1a	ec2-52-91-155-153.co...	52.91.155.153	-

Instance summary for i-060fd3a281f02e32c (Ec2 server) [Info](#)

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

1.2. Connecting to the instance via SSH

Connecting to Ec2 instance

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.

,
#_
~\_ ####_      Amazon Linux 2023
~\_ #####\
~~ \###|
~~  \#/ ___ https://aws.amazon.com/linux/amazon-linux-2023
~~  \~' '-->
~~\_ / \
~~.._/_/
~/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

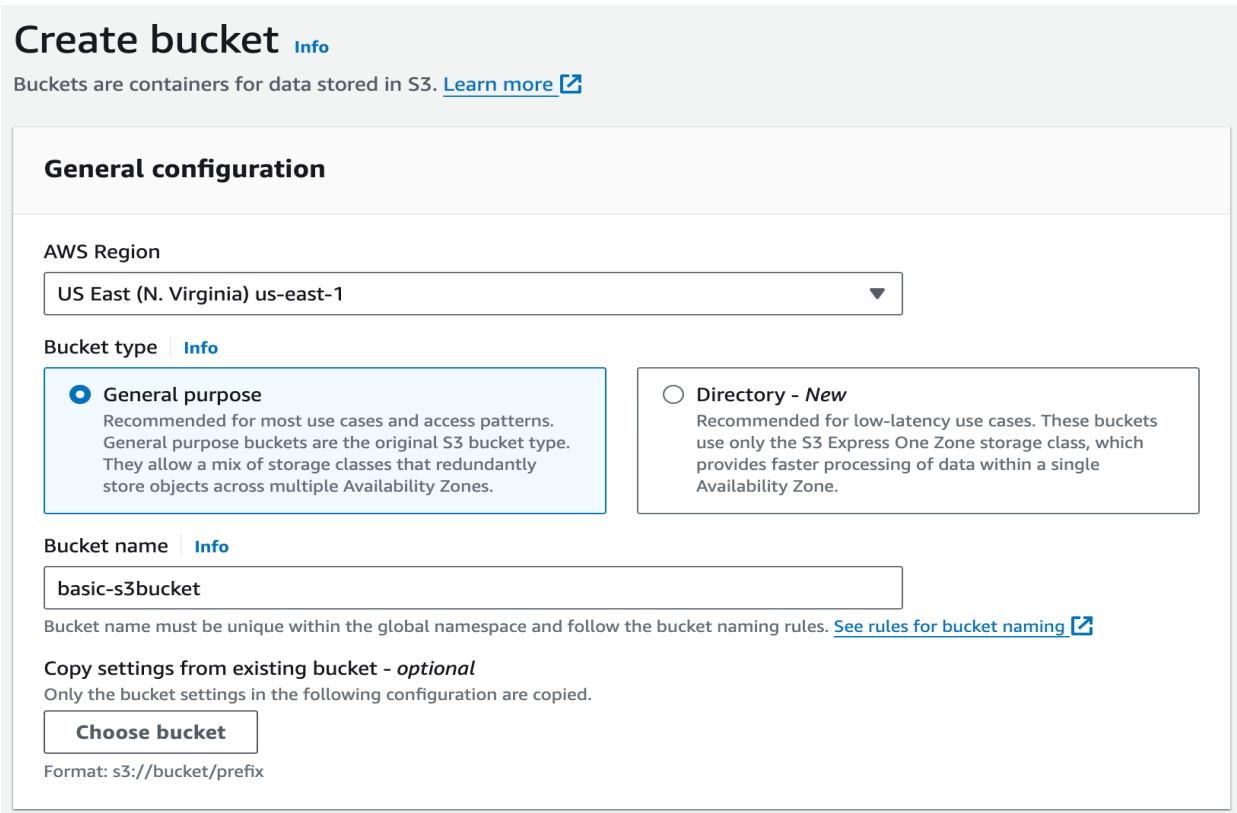
Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

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

ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

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

Object Ownership
Bucket owner enforced

Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

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

- Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- Block public access to buckets and objects granted through any access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

Then, click create bucket and new bucket is created

The screenshot shows the 'General purpose buckets (2)' page. A red box highlights the 'Create bucket' button.

General purpose buckets (2) Info
Buckets are containers for data stored in S3. [Learn more](#)

C Copy ARN Empty Delete

Q Find buckets by name < 1 > ⚙️

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's a toolbar with various actions: Copy S3 URI, Copy URL, Download, Open, Delete, Actions (with a dropdown arrow), Create folder, and a large orange Upload button. Below the toolbar, a message says 'Objects (0)' and provides instructions for using Amazon S3 inventory. A search bar labeled 'Find objects by prefix' is present. The main area has 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, there's 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)		Remove	Add files	Add folder
All files and folders in this table will be uploaded.				
<input type="text"/> Find by name		< 1 >		
<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
<code>s3://basic-s3bucket</code>	1 file, 263.0 B (100.00%)	0 files, 0 B (0%)

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

Files and folders (1 Total, 263.0 B)

<input type="text"/> Find by name						
Name	Folder	Type	Size	Status	Error	
home.html	-	text/html	263.0 B	Succeeded	-	

The details of uploaded files can be viewed

This screenshot shows the AWS S3 Object Details page for a file named 'home.html'. The 'Properties' tab is selected. Key details shown include:

- Owner:** awsabsc0w6975059t1703162515
- AWS Region:** US East (N. Virginia) us-east-1
- Last modified:** February 15, 2024, 19:32:05 (UTC+05:45)
- Size:** 263.0 B
- Type:** html
- Key:** home.html
- S3 URI:** s3://basic-s3bucket/home.html
- Amazon Resource Name (ARN):** arn:aws:s3:::basic-s3bucket/home.html
- Entity tag (Etag):** df9699ca596137ba79dcb3452930c47d
- Object URL:** https://basic-s3bucket.s3.amazonaws.com/home.html

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 'AccessDenied' exception. The error message includes the Request ID, Host ID, and a long string of random characters.

```
<Error>
<Code>AccessDenied</Code>
<Message>Access Denied</Message>
<RequestId>7DJD75JSW4B54B85</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 file 'home.html' successfully loaded. The title bar indicates the file has been opened.

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: Bucket and objects not public". Under "Block public access (bucket settings)", it says "Block all public access: On" and provides a link to "Individual Block Public Access settings for this bucket". In the "Bucket policy" section, it states "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." It includes "Edit" and "Delete" buttons. A note at the bottom indicates that public access is blocked because Block Public Access settings are turned on for this bucket, with a link to "Amazon S3 Block Public Access".

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

[Edit](#) [Delete](#)

2.4. Testing the policy

Uploading the same html file without specifying any encryption key

Files and folders (1 Total, 263.0 B)

All files and folders in this table will be uploaded.

<input type="checkbox"/>	Name	Folder
<input type="checkbox"/>	home.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**

Server side encryption can be updated from “Properties” section

Server-side encryption [Info](#)

Server-side encryption protects data at rest.

Server-side encryption

Do not specify an encryption key
The bucket settings for default encryption are used to encrypt objects when storing them in Amazon S3.

Specify an encryption key
The specified encryption key is used to encrypt objects before storing them in Amazon S3.

⚠ 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 an orange header bar with the message 'upload failed' and a link 'View details below.' Below this, the title 'Upload: status' is displayed, along with a 'Close' button. A note says 'The information below will no longer be available after you navigate away from this page.' The main section is titled 'Summary' and contains three rows of data:

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

Below the summary, there are two tabs: 'Files and folders' (selected) and 'Configuration'. Under 'Files and folders', it says '(1 Total, 263.0 B)' and shows a table with one row:

Name	Folder	Type	Size	Status	Error
home.html	-	text/html	263.0 B	Failed	Access Denied

Now, for uploading the file, below setup is configured

The screenshot shows the 'Encryption' configuration page. It includes sections for 'Server-side encryption', 'Encryption settings', and 'Encryption type'.

Server-side encryption (Info):
Server-side encryption protects data at rest.

Server-side encryption:
 Do not specify an encryption key: The bucket settings for default encryption are used to encrypt objects when storing them in Amazon S3.
 Specify an encryption key: The specified encryption key is used to encrypt objects before storing them in Amazon S3.

Encryption settings (Info):
 Use bucket settings for default encryption
 Override bucket settings for default encryption

Encryption type (Info):
 Server-side encryption with Amazon S3 managed keys (SSE-S3)
 Server-side encryption with AWS Key Management Service keys (SSE-KMS)
 Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
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 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](#) [Configuration](#)

Files and folders (1 Total, 263.0 B)

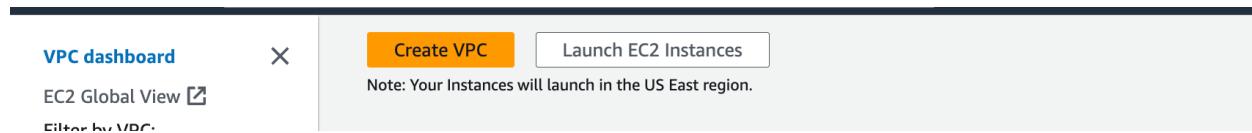
Name	Folder	Type	Size	Status	Error
home.html	-	text/html	263.0 B	⌚ Succeeded	-

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. At the top, a note says 'A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.' The form is divided into sections:

- VPC settings**:
 - Resources to create**: A note says 'Create only the VPC resource or the VPC and other networking resources.' Two radio buttons are shown: VPC only (selected) and VPC and more.
 - Name tag - optional**: A note says 'Creates a tag with a key of 'Name' and a value that you specify.' An input field contains 'basic-vpc'.
 - IPv4 CIDR block**: A note says 'CIDR block size must be between /16 and /28.' An input field contains '10.0.0.0/25'.
 - IPv6 CIDR block**: A note says 'No IPv6 CIDR block selected.' Three radio buttons are shown: No IPv6 CIDR block (selected), IPAM-allocated IPv6 CIDR block, Amazon-provided IPv6 CIDR block, and IPv6 CIDR owned by me.
 - Tenancy**: A note says 'Default selected.' A dropdown menu shows 'Default'.
- Tags**: A note says '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.' A table shows a single tag:

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

A note below says 'You can add 49 more tags.'
- At the bottom right, there are 'Cancel' and 'Create VPC' buttons.

Then, a new VPC is created

vpc-06e62a52af76c05d5 / basic-vpc			
Details		Info	
VPC ID vpc-06e62a52af76c05d5	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-00f56b0378df23930	Main route table rtb-095eb7150db0d1327	Main network ACL acl-0979983b5675ac330
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 Failed to load rule groups	Owner ID 612362567483	

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.



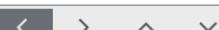
IPv4 VPC CIDR block Info

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 Clear filters								
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		

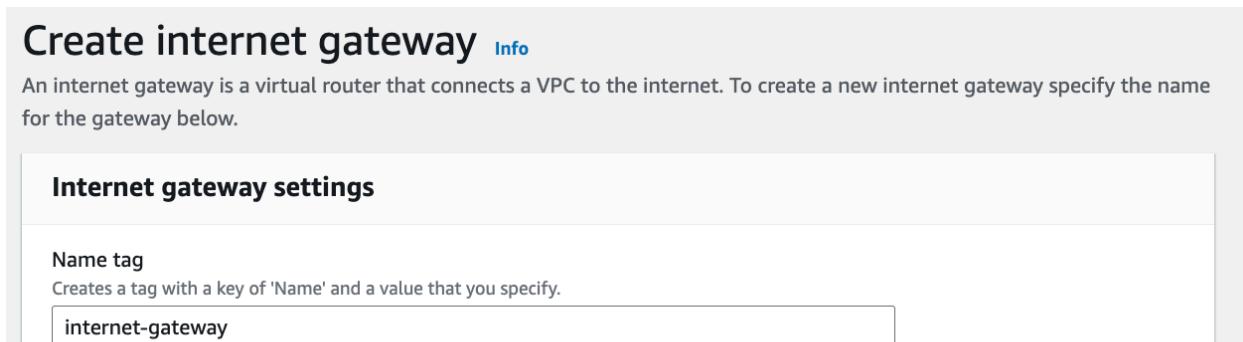
2.3. Setup Internet Gateway

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



The screenshot shows the AWS VPC console. In the top navigation bar, there is a link to 'Internet gateways (1) Info'. Below the navigation bar, there is a search bar with placeholder text 'Search'. On the right side of the header, there are several buttons: a refresh icon, an 'Actions' dropdown menu, and an orange 'Create internet gateway' button. Below the header, there is a small navigation area with icons for back, forward, and refresh.

Step-2: Assign gateway name and then create



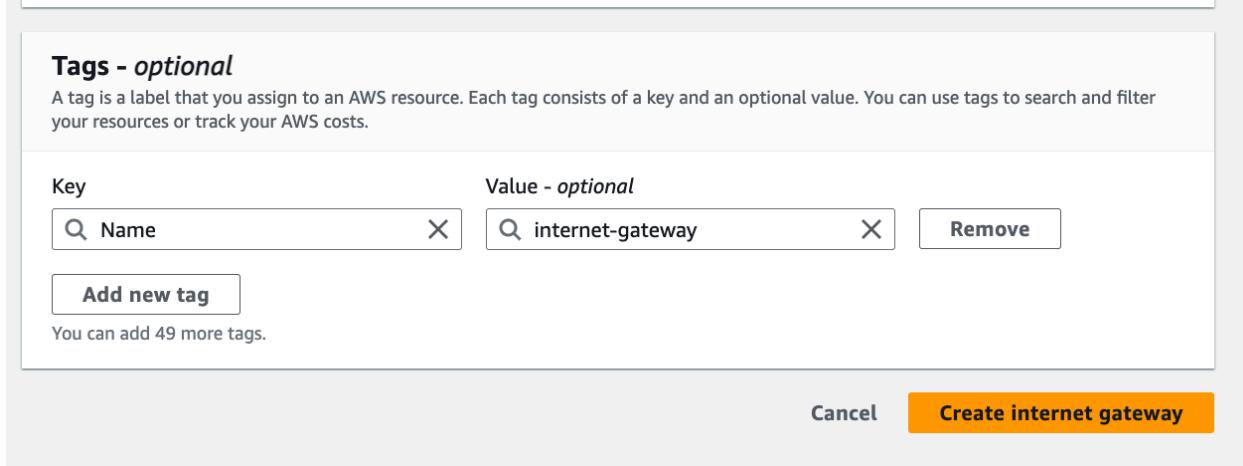
Create internet gateway Info

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.

internet-gateway



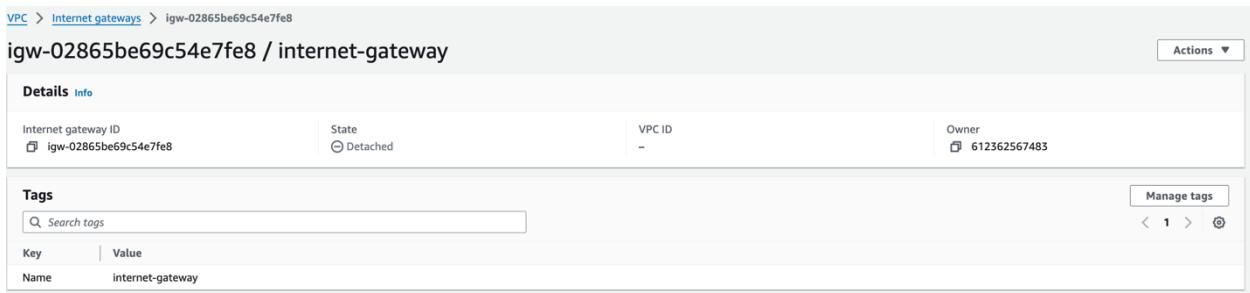
Tags - optional
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
<input type="text" value="Name"/> X	<input type="text" value="internet-gateway"/> X

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 igw-02865be69c54e7fe8	State <input checked="" type="radio"/> Detached	VPC ID -	Owner 612362567483
--	--	-------------	---------------------------------------

Tags

Manage tags

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) Info					
<input type="button" value="Actions ▾"/> Create internet gateway					
<input type="button" value="View details"/> < 1 > @					
Name	Internet gateway ID	State	VPC ID	Owner	
-	igw-0a4669731cca36081	Attached	vpc-0d8fab51a5f972f19	612362567483	
<input checked="" type="checkbox"/> internet-gateway	igw-02865be69c54e7fe8	Detached	-	612362567483	

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					
<input type="button" value="Actions ▾"/>					
Internet gateway ID igw-02865be69c54e7fe8	State Attached	VPC ID vpc-06e62a52af76c05d5 basic-vpc	Owner 612362567483		

Now, the newly created VPC state status is attached

Internet gateways (2) Info					
<input type="button" value="Actions ▾"/> Create internet gateway					
<input type="button" value="View details"/> < 1 > @					
Name	Internet gateway ID	State	VPC ID	Owner	
-	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.

VPC
The VPC to use for this route table.

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="route-table-01"/> X 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 <input type="text" value="rtb-00bd8094b07273fd8"/>	Main <input type="checkbox"/>	Owner ID <input type="text" value="612362567483"/>	Explicit subnet associations -	Edge associations -
--	----------------------------------	---	-----------------------------------	------------------------

Routes Subnet associations Edge associations Route propagation Tags

Routes (1)		Edit routes	
<input type="text" value="Filter routes"/>		Both < 1 > Both	
Destination	Target	Status	Propagated
10.0.0.0/25	local	<input checked="" type="checkbox"/> Active	No

Now, the route table is created.

Route tables (3) Info							Actions		Create route table
<input type="checkbox"/> Name		Route table ID	Explicit subnet associ...	Edge associations	Main	VPC			Owner ID
<input type="checkbox"/>	-	rtb-06ce5a6546a6cf3cb	-	-	Yes	vpc-0d8fab51a5f972f19	<	1	612362567483
<input type="checkbox"/>	-	rtb-095eb7150db0d1327	-	-	Yes	vpc-06e62a52af76c05d5 basic...	<	1	612362567483
<input checked="" type="checkbox"/>	route-table-01	rtb-00bd8094b07273fd8	-	-	No	vpc-06e62a52af76c05d5 basic...	<	1	612362567483

2.5. Attaching internet gateway to the route table

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

route-table-01 rtb-00bd8094b07273fd8 - - No vpc-06e62a52af76c05d5 | basic... 612362567483

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
Q. 0.0.0.0/0	Internet Gateway	-	No

Add route Remove Cancel Preview Save changes

The screenshot shows the AWS VPC Route Tables interface. At the top, a green header bar indicates "Updated routes for rtb-00bd8094b07273fd8 / route-table-01 successfully". Below this, the breadcrumb navigation shows "VPC > Route tables > rtb-00bd8094b07273fd8 / route-table-01". On the right, there is an "Actions" dropdown menu.

The main content area displays the "rtb-00bd8094b07273fd8 / route-table-01" details. It includes sections for "Details" and "Info". Under "Details", the "Route table ID" is rtb-00bd8094b07273fd8, "Main" is set to "No", "Owner ID" is vpc-06e62a52af76c05d5 | basic-vpc, and "Explicit subnet associations" and "Edge associations" are both listed as "-".

The "Routes" tab is selected, showing two routes:

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

The screenshot shows the "Edit subnet associations" dialog box. The title is "Edit subnet associations" and it says "Change which subnets are associated with this route table." The "Available subnets (1/1)" section lists one subnet: "vpc-subnet-01" with Subnet ID "subnet-0d6a108fc3e4d690d" and IPv4 CIDR "10.0.0.0/26". The "Route table ID" is "Main (rtb-095eb7150db0d1327)". In the "Selected subnets" section, "subnet-0d6a108fc3e4d690d / vpc-subnet-01" is selected. At the bottom, there are "Cancel" and "Save associations" buttons.

2.7. Setting up a simple EC2 instance

Create a new EC2 instance and in network setting select the created 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

[Create new VPC](#)
[Edit](#)

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](#)
[Edit](#)

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	Protocol Info	Port range Info
ssh	TCP	22
Source type Info	Source Info	Description - optional Info
Anywhere	Add CIDR, prefix list or security <input type="text" value="0.0.0.0/0"/> X	e.g. SSH for admin desktop

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

[Add security group rule](#)

► Advanced network configuration

Configure storage [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-06b9823b29c8c8f89

[Launch log](#)

Instance: i-06b9823b29c8c8f89 (vpc-ec2-instance)

Details	Status and alarms New	Monitoring	Security	Networking	Storage	Tags
Instance summary Info						
Instance ID i-06b9823b29c8c8f89 (vpc-ec2-instance)	Public IPv4 address 52.203.162.230 [open address]	Private IPv4 addresses 10.0.0.44				
IPv6 address -	Instance state Running	Public IPv4 DNS -				
Hostname type IP name: ip-10-0-44.ec2.internal	Private IP DNS name (IPv4 only) ip-10-0-44.ec2.internal	Elastic IP addresses -				
Answer private resource DNS name -	Instance type t2.micro	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more				
Auto-assigned IP address 52.203.162.230 [Public IP]	VPC ID vpc-06e62a52af76c05d5 (basic-vpc)	Auto Scaling Group name -				
IAM Role -	Subnet ID subnet-0d6a108fc3e4d690d (vpc-subnet-01)					
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				

```
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/'
```

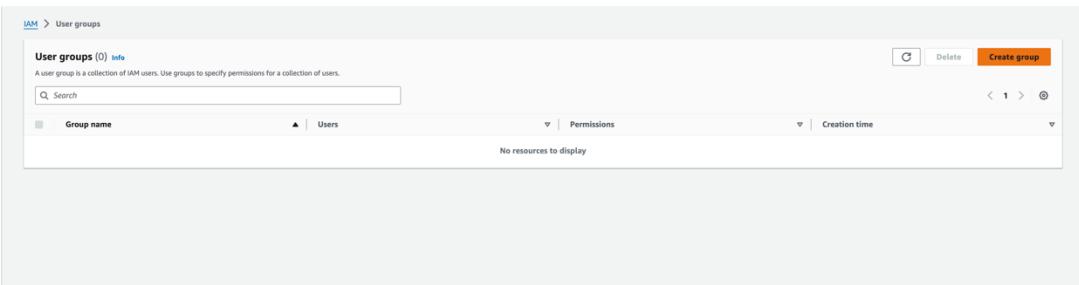
3. IAM Users and Roles Lab

- **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 from IAM in and navigate to IAM dashboard

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



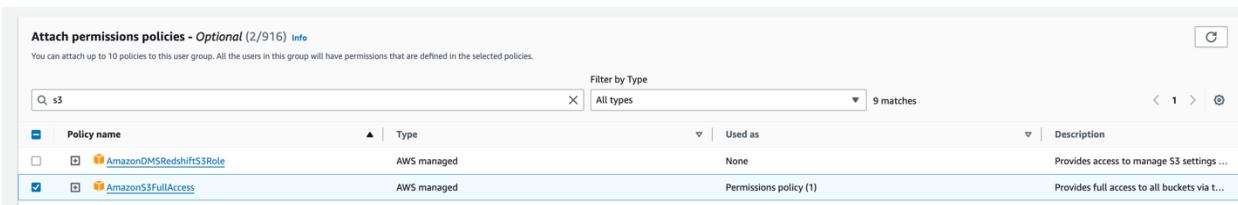
The screenshot shows the IAM User Groups page. On the left, there's a navigation sidebar with options like Dashboard, User groups, Roles, Policies, and Account settings. The main area has a heading "User groups (0) Info" and a sub-section "A user group is a collection of IAM users. Use groups to specify 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 message 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" form. It has a header "Create user group" and a section "Name the group". Below it is a "User group name" field containing "developers". There's a note: "Enter a meaningful name to identify this group." and a character limit note: "Maximum 128 characters. Use alphanumeric and '+,-,@-' characters." The entire form is contained within a light gray box.

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..."). The "AmazonS3FullAccess" policy is selected, indicated by a checked checkbox.

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"/> AmazonEC2ContainerRegistryFullAccess	AWS managed	None	Provides administrative access to Amazon EC2 Container Registry
<input type="checkbox"/> AmazonEC2ContainerRegistryPowerUser	AWS managed	None	Provides full access to Amazon EC2 Container Registry
<input type="checkbox"/> AmazonEC2ContainerRegistryReadOnly	AWS managed	Permissions policy (1)	Provides read-only access to Amazon EC2 Container Registry
<input type="checkbox"/> AmazonEC2ContainerServiceAutoscaleRole	AWS managed	None	Policy to enable Task AutoScaling for Amazon ECS
<input type="checkbox"/> AmazonEC2ContainerServiceEventsRole	AWS managed	None	Policy to enable CloudWatch Events for Amazon ECS
<input type="checkbox"/> AmazonEC2ContainerServiceforEC2Role	AWS managed	None	Default policy for the Amazon EC2 Role for Amazon ECS
<input type="checkbox"/> AmazonEC2ContainerServiceRole	AWS managed	None	Default policy for Amazon ECS service role
<input checked="" type="checkbox"/> AmazonEC2FullAccess	AWS managed	None	Provides full access to Amazon EC2 via the AWS Lambda function
<input type="checkbox"/> AmazonEC2ReadOnlyAccess	AWS managed	None	Provides read-only access to Amazon EC2

User group was not created.
 User: arn:awssts::612362567483:assumed-role/vocabs/user3009561+utshashretha07@gmail.com is not authorized to perform: iam:CreateGroup on resource: arn:aws:siam::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=""/>

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"/> AmazonDMSRedshiftS3Role	AWS managed	None	Provides access to manage S3 settings via AWS Lambda functions
<input checked="" type="checkbox"/> AmazonS3FullAccess	AWS managed	Permissions policy (1)	Provides full access to all buckets via AWS Lambda functions
<input type="checkbox"/> AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	None	Provides AWS Lambda functions permission to access objects in S3
<input type="checkbox"/> AmazonS3OutpostsFullAccess	AWS managed	None	Provides full access to Amazon S3 on Outposts
<input type="checkbox"/> AmazonS3OutpostsReadOnlyAccess	AWS managed	None	Provides read only access to Amazon S3 on Outposts
<input type="checkbox"/> AmazonS3ReadOnlyAccess	AWS managed	Permissions policy (1)	Provides read only access to all buckets via AWS Lambda functions
<input type="checkbox"/> AWSBackupServiceRolePolicyForS3Backup	AWS managed	None	Policy containing permissions necessary for AWS Backup to access S3
<input type="checkbox"/> AWSBackupServiceRolePolicyForS3Restore	AWS managed	None	Policy containing permissions necessary for AWS Backup to restore objects from S3
<input type="checkbox"/> QuickSightAccessForS3StorageManagementAnalyticsReadOnlyAccess	AWS managed	None	Policy used by QuickSight team to access S3

[Cancel](#) [Create group](#)

As we have not access to create group in provided lab “AWS learner Lab” above error message is displayed.

3.2. Create new user

This part is implemented in “AWS Cloud Foundations” Lab and the steps involved for this is listed below.

Step-1: Navigate to IAM dashboard

The screenshot shows the AWS IAM 'Users' page. On the left, there's a sidebar with 'Identity and Access Management (IAM)' and various navigation options like 'Dashboard', 'Access management', 'User groups', 'Roles', 'Policies', 'Identity providers', 'Account settings', 'Access reports', 'Access Analyzer', 'External access', 'Unused access', 'Analyzer settings', 'Credential report', and 'Organization activity'. The main area displays a table titled 'Users (4) Info' with the following data:

User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in	Access key ID	Active key
awsstudent	/	Access denied	Access denied	-	Access denied	-	Access denied	Access denied
user-1	/spl66/	0	-	-	59 minutes	-	Active - AKIAW3MEB2...	59 min
user-2	/spl66/	0	-	-	59 minutes	-	Active - AKIAW3MEB2...	59 min
user-3	/spl66/	0	-	-	59 minutes	-	Active - AKIAW3MEB2...	59 min

Step-2: Click create user and then this will navigate to create user page. Required configuration is provided.

The screenshot shows the 'Specify user details' page. It has a header 'Specify user details' and a section 'User details' with a 'User name' field containing 'utsha-user'. Below it is a note about character restrictions. There's a checkbox for 'Provide user access to the AWS Management Console - optional' which is checked. A callout box provides information about using Identity Center for console access. The 'Console password' section includes a radio button for 'Custom password' which is selected, and a password input field with '*****'. There are also notes about password complexity and a checkbox for 'Users must create a new password at next sign-in - Recommended'. A note at the bottom explains how to generate access keys. At the bottom right are 'Cancel' and 'Next' buttons.

Step-3: After that, select attach policies directly and give permission to the newly created user.

IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

Set permissions

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

Permissions options

- Add user to group Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
- Copy permissions Copy all group memberships, attached managed policies, and inline policies from an existing user.
- Attach policies directly Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1177)

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

Filter by Type		Attached entities
<input type="text" value="s3"/>	All types	12 matches
<input checked="" type="checkbox"/> Policy name AmazonS3FullAccess	Type	0
<input type="checkbox"/> AmazonDMSRedshiftS3Role	AWS managed	0
<input type="checkbox"/> AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	0
<input type="checkbox"/> AmazonS3OutpostsFullAccess	AWS managed	0
<input type="checkbox"/> AmazonS3OutpostsReadOnlyAccess	AWS managed	0
<input type="checkbox"/> AmazonS3ReadOnlyAccess	AWS managed	1
<input type="checkbox"/> AWSBackupServiceRolePolicyForS3Backup	AWS managed	0
<input type="checkbox"/> AWSBackupServiceRolePolicyForS3Restore	AWS managed	0
<input type="checkbox"/> AWSS3OnOutpostsServiceRolePolicy	AWS managed	0
<input type="checkbox"/> IVSRecordToS3	AWS managed	0
<input type="checkbox"/> QuickSightAccessForS3StorageManagementAnalytics...	AWS managed	0

Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name utsha-user	Console password type Custom password	Require password reset Yes
-------------------------	--	-------------------------------

Permissions summary

Name	Type	Used as
AmazonS3FullAccess	AWS managed	Permissions policy
IAMUserChangePassword	AWS managed	Permissions policy

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

[Cancel](#) [Previous](#) **Create user**

In this way new user can be created.