

# Basic Labs

## 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.

## 2. S3 Storage Fundamentals Lab

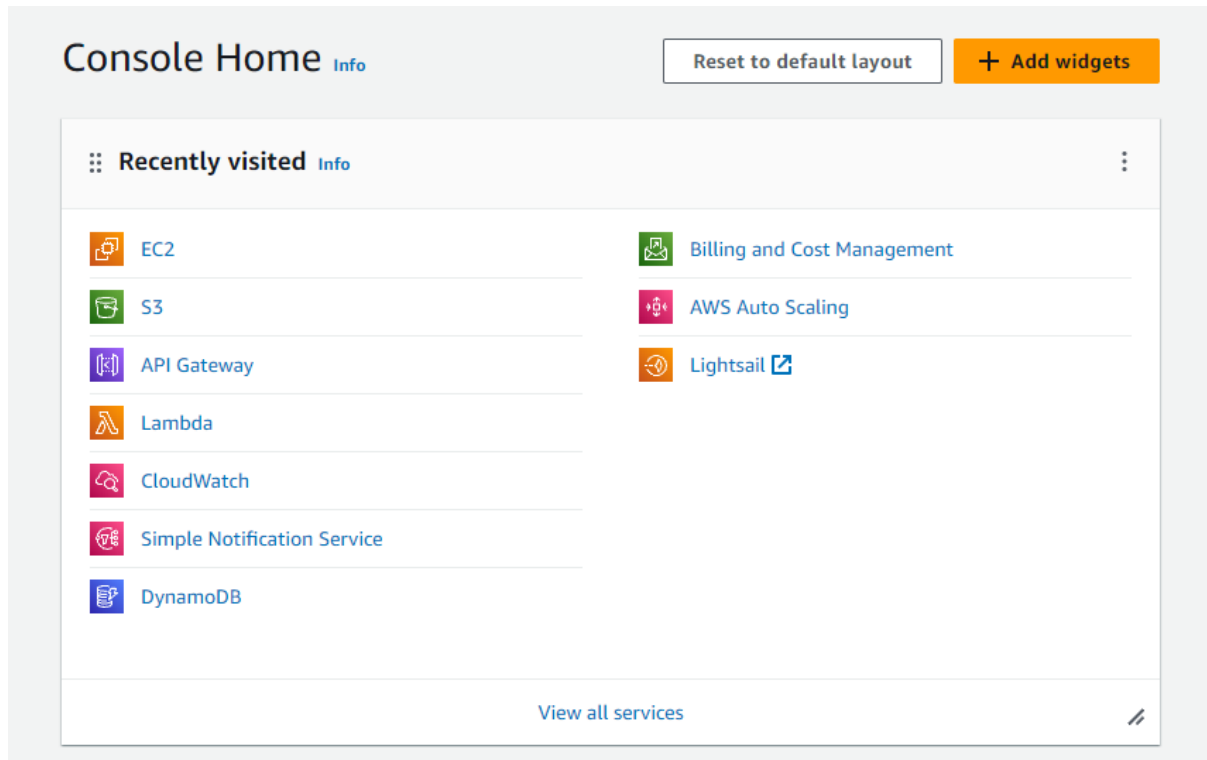
- **Objective:** To gain hands-on experience with Amazon S3 by performing basic storage operations.
- **Approach:** This lab involves creating an S3 bucket, uploading files to it, and setting up bucket policies for access control. Students will explore the S3 management console, learn about object storage,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

## 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.

# EC2 Basics Lab

Go to EC2 from AWS CONSOLE



## 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-0440d3b780d96b29d (64-bit (x86), uefi-preferred) / ami-0f93c02efd1974b8b (64-bit (Arm), uefi)  
Virtualization: hvm    ENA enabled: true    Root device type: ebs

Free tier eligible ▼

### Description

Amazon Linux 2023 AMI 2023.3.20240219.0 x86\_64 HVM kernel-6.1

Architecture

64-bit (x86) ▼

Boot mode

uefi-preferred

AMI ID

ami-0440d3b780d96b29d

Verified provider

## ▼ 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 launch Ec2 Instance

EC2 > Instances > Launch an instance










Launching instance  
Launch initiation

79%

► Details

Please wait while we launch your instance.  
Do not close your browser while this is loading.

Click on Instances you can find the new created instances

<input type="checkbox"/>	Name  ▲	Instance ID	Instance state ▼	Instance type ▼	Status check	Alarm
<input type="checkbox"/>	new-workshop	<a href="#">i-01cc84c45ef22699a</a>	 Running  	t2.micro	 Initializing <a href="#">View a</a>	<a href="#">View a</a>
<input type="checkbox"/>	new-workshop	<a href="#">i-0b2e94bbc45df6363</a>	 Running  	t2.micro	 Initializing <a href="#">View a</a>	<a href="#">View a</a>

Now allocate an Elastic IP address to this instance

## Allocate Elastic IP address [Info](#)

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

Network border group [Info](#)

Q us-east-1 X

Public IPv4 address pool

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

Global static IP addresses

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

Create accelerator

### 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 address allocated successfully.  
Elastic IP address 54.164.87.169
Associate this Elastic IP address X

Elastic IP addresses (1)
Actions ▾
Allocate Elastic IP address

Q Find resources by attribute or tag

Public IPv4 address : 54.164.87.169 X

Clear filters

< 1 > ⚙️

	Name	Allocated IPv4 addr...	Type	Allocation ID	Reve
<input type="checkbox"/>	-	<a href="#">54.164.87.169</a>	Public IP	eipalloc-037626ceaf3ce0058	-

So that Elastic IP address has been allocated

Open the created IP Address.

54.164.87.169

Actions ▼

Associate Elastic IP address

### Summary

Allocated IPv4 address

54.164.87.169

Type

Public IP

Allocation ID

eipalloc-037626ceaf3ce0058

Reverse DNS record

–

Association ID

–

Scope

VPC

Associated instance ID

–

Private IP address

–

Network interface ID

–

Network interface owner account ID

–

Public DNS

–

NAT Gateway ID

–

Address pool

Amazon

Network border group

us-east-1

### Tags(0)

Manage tags

< 1 > ⚙

Key

Value

No tags associated with this resource

Click the Manage tags button to add your first tag

Manage tags

Click on Associate Elastic IP Address

## Associate Elastic IP address


Choose the instance or network interface to associate to this Elastic IP address (54.164.87.169)

**Elastic IP address: 54.164.87.169**

### 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

 Choose an instance



### Private IP address

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

 Choose a private IP address

### Reassociation

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

- ☐ Allow this Elastic IP address to be reassociated

Cancel

Associate

## Associate Elastic IP address

Choose the instance or network interface to associate to this Elastic IP address (54.164.87.169)

**Elastic IP address: 54.164.87.169**

### 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-0d2a424fab6235f0d (Test1) - running

i-06c8f85ae671a47cb (Test1) - running

i-01cc84c45ef22699a (new-workshop) - running

i-0b2e94bbc45df6363 (new-workshop) - running

☐ Allow this Elastic IP address to be reassociated

Cancel

Associate

Now choose the Instance that we created previously .



[EC2](#) > [Elastic IP addresses](#) > [54.164.87.169](#) > Associate Elastic IP address

## Associate Elastic IP address


Choose the instance or network interface to associate to this Elastic IP address (54.164.87.169)

**Elastic IP address: 54.164.87.169**

### Resource type

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

- ☒ Instance  
☐ Network interface

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

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

### Instance

### Private IP address

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

### Reassociation

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

- ☐ Allow this Elastic IP address to be reassociated

Cancel

Associate

Now click on associate button after assigning private IP address

✓ Elastic IP address associated successfully.  
Elastic IP address 54.164.87.169 has been associated with instance i-01cc84c45ef22699a

[EC2](#) > [Elastic IP addresses](#) > 54.164.87.169

54.164.87.169

Actions ▼

Associate Elastic IP address

### Summary

Allocated IPv4 address 📄 54.164.87.169	Type 📄 Public IP	Allocation ID 📄 eipalloc-037626ceaf3ce0058	Reverse DNS record –
Association ID 📄 eipassoc-0cbce1d56f46b4659	Scope 📄 VPC	Associated instance ID <a href="#">i-01cc84c45ef22699a</a>	Private IP address 📄 172.31.17.17
Network interface ID <a href="#">eni-0e64a39724481862f</a>	Network interface owner account ID 📄 695125708392	Public DNS 📄 ec2-54-164-87-169.compute-1.amazonaws.com	NAT Gateway ID –
Address pool 📄 Amazon	Network border group 📄 us-east-1		

Now Elastic IP is finally showing in our EC2 Instance

### Instance summary for i-01cc84c45ef22699a (new-workshop) [Info](#)



Connect

Instance state ▼

Actions ▼

Updated less than a minute ago

Instance ID 📄 i-01cc84c45ef22699a (new-workshop)	Public IPv4 address 📄 54.164.87.169 <a href="#">open address</a>	Private IPv4 addresses 📄 172.31.17.17
IPv6 address –	Instance state ✓ Running	Public IPv4 DNS 📄 ec2-54-164-87-169.compute-1.amazonaws.com <a href="#">open address</a>
Hostname type IP name: ip-172-31-17-17.ec2.internal	Private IP DNS name (IPv4 only) 📄 ip-172-31-17-17.ec2.internal	Elastic IP addresses 📄 54.164.87.169 [Public IP]
Answer private resource DNS name IPv4 (A)	Instance type t2.micro	AWS Compute Optimizer finding 🔔 Opt-in to AWS Compute Optimizer for recommendations. <a href="#">Learn more</a>
Auto-assigned IP address –	VPC ID 📄 vpc-0699b7ab8798d3d2e	Auto Scaling Group name –
IAM Role –	Subnet ID 📄 subnet-0cee20dff6edfee1	
IMDSv2 Required		

Now we have to connect the instance via SSH

[EC2](#) > [Instances](#) > [i-01cc84c45ef22699a](#) > [Connect to instance](#)

## Connect to instance [Info](#)

Connect to your instance i-01cc84c45ef22699a (new-workshop) using any of these options


EC2 Instance Connect



Session Manager

**SSH client**


EC2 serial console


Instance ID

 i-01cc84c45ef22699a (new-workshop)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is Test.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.  
 `chmod 400 "Test.pem"`
4. Connect to your instance using its Public DNS:  
 `ec2-54-164-87-169.compute-1.amazonaws.com`

Example:

 `ssh -i "Test.pem" ec2-user@ec2-54-164-87-169.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.

Cancel

```
ec2-user@ip-172-31-17-17:~  
Microsoft Windows [Version 10.0.22000.2777]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\User\Downloads>chmod 400 "Test.pem"  
'chmod' is not recognized as an internal or external command,  
operable program or batch file.  
  
C:\Users\User\Downloads>ssh -i "Test.pem" ec2-user@54.164.87.169  
The authenticity of host '54.164.87.169 (54.164.87.169)' can't be established.  
ECDSA key fingerprint is SHA256:zTzvLcy/tpvaaPV2GWh0JVkpYxvhiMxgKkti3ETeG8Y.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '54.164.87.169' (ECDSA) to the list of known hosts.  
  
      #_  
    ~\  #####_      Amazon Linux 2023  
  ~~~ \  #####\  
  ~~~  \###|  
  ~~~   \#/_____  
  ~~~    V~' '->      https://aws.amazon.com/linux/amazon-linux-2023  
  ~~~  
  ~~~  .  _/_____  
  ~~~   /  _/_____  
  ~~~  /m/ ' _/_____  
[ec2-user@ip-172-31-17-17 ~]$
```

Connection Success of EC2 Instance via SSH Key.

## S3 Storage Fundamentals Lab

First Create a S3 Bucket

General purpose buckets (1) [Info](#)

Copy ARN

Empty

Delete

Create bucket

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

Find buckets by name

< 1 >

	Name ▲	AWS Region ▼	Access ▼	Creation date ▼
<input type="radio"/>	<a href="#">workshop-buckets3</a>	US East (N. Virginia) us-east-1	Bucket and objects not public	February 18, 2024, 20:10:37 (UTC+05:45)

Click on Create Bucket

[Amazon S3](#) > [Buckets](#) > Create bucket

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](#)

basiclabs-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

## 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.

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

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

### Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

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](#).

Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

☐ Disable
   
☒ Enable

► **Advanced settings**

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

Cancel Create bucket

Set bucket name and leave the rest as it is and click on Create Bucket

General purpose buckets   Directory buckets				
<div> <b>General purpose buckets (2)</b> <a href="#">Info</a> <span>↻</span> <span>Copy ARN</span> <span>Empty</span> <span>Delete</span> <span>Create bucket</span> </div> <p>Buckets are containers for data stored in S3. <a href="#">Learn more</a></p> <div> <input type="text" value="Find buckets by name"/> <span>&lt; 1 &gt;</span> <span>⚙</span> </div>				
	Name ▲	AWS Region ▼	Access ▼	Creation date ▼
<input type="radio"/>	basiclabs-s3bucket	US East (N. Virginia) us-east-1	Bucket and objects not public	February 23, 2024, 13:37:14 (UTC+05:45)
<input type="radio"/>	workshop-buckets3	US East (N. Virginia) us-east-1	Bucket and objects not public	February 18, 2024, 20:10:37 (UTC+05:45)

So the New bucket has been created with the name basiclabs-s3bucket

Now the next task will be to Upload files

To upload files click on the new bucket that we just created.

General purpose buckets

Directory buckets

General purpose buckets (2) [Info](#)

Copy ARN

Empty

Delete

Create bucket

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

< 1 >

	Name ▲	AWS Region ▼	Access ▼	Creation date ▼
<input type="radio"/>	<a href="#">basiclabs-s3bucket</a>	US East (N. Virginia) us-east-1	Bucket and objects not public	February 23, 2024, 13:37:14 (UTC+05:45)
<input type="radio"/>	<a href="#">workshop-buckets3</a>	US East (N. Virginia) us-east-1	Bucket and objects not public	February 18, 2024, 20:10:37 (UTC+05:45)

[Amazon S3](#) > [Buckets](#) > [basiclabs-s3bucket](#)

basiclabs-s3bucket [Info](#)

Objects

Properties

Permissions

Metrics

Management

Access Points

Objects (0) [Info](#)

Copy S3 URI

Copy URL

Download

Open

Delete

Actions ▼

Create folder

Upload

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

< 1 >

	Name ▲	Type ▼	Last modified ▼	Size ▼	Storage class ▼
No objects You don't have any objects in this bucket.					

Upload

Then click on upload button



[Amazon S3](#) > [Buckets](#) > [basiclabs-s3bucket](#) > Upload

## 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 (0)

Remove

Add files

Add folder

All files and folders in this table will be uploaded.

< 1 >

<input type="checkbox"/>	Name	Folder	Type	Size
--------------------------	------	--------	------	------

**No files or folders**

You have not chosen any files or folders to upload.

Then drag and drop file to be uploaded

## 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, 864.0 B)

[Remove](#)[Add files](#)[Add folder](#)

All files and folders in this table will be uploaded.

Find by name < 1 >

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	Test.html	-	text/html	864.0 B

### Destination [Info](#)

Destination

[s3://basiclabs-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](#)

Now upload the file .

### Files and folders (1 Total, 864.0 B)


Find by name < 1 >


Name	Folder	Type	Size	Status	Error
<a href="#">Test.html</a>	-	text/html	864.0 B	✓ Succeeded	-


Detail of the uploaded file can be viewed by clicking on It.

Amazon S3 > Buckets > basiclabs-s3bucket > Test.html

## Test.html Info

 Copy S3 URI

 Download

Open 

Object actions ▼

Properties

Permissions

Versions

### Object overview

Owner

awslabsc0w6974879t1703160632

AWS Region

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

Last modified

February 23, 2024, 13:52:06  
(UTC+05:45)


Size

864.0 B


Type

html


Key

 Test.html


S3 URI

 s3://basiclabs-s3bucket/Test.html


Amazon Resource Name (ARN)

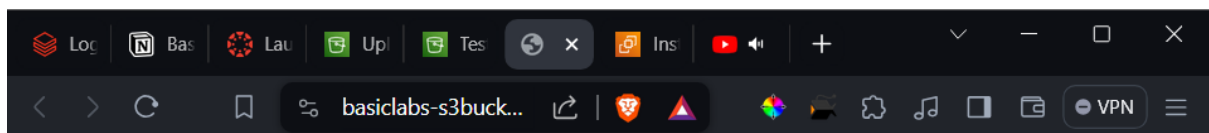
 arn:aws:s3:::basiclabs-s3bucket/Tes  
t.html

Entity tag (Etag)

 b362130ef50dd00bd226d0a37e4c  
340f

Object URL

 https://basiclabs-s3bucket.s3.amaz  
onaws.com/Test.html



## Welcome to My AWS Website



Amazon Web Services (AWS) is a cloud computing platform that provides a wide range of services, including compute, storage, databases, machine learning, and more. It's widely used by businesses and developers to build scalable and reliable applications.

Uploaded file can be accessed by clicking on the open button on the object overview page.

# Setting up bucket policies for Access Control


Click on Permissions of the bucket we created.


The screenshot shows the Amazon S3 console interface for the bucket 'basiclabs-s3bucket'. The breadcrumb navigation at the top reads 'Amazon S3 > Buckets > basiclabs-s3bucket'. Below the bucket name, there is an 'Info' link and a set of tabs: 'Objects', 'Properties', 'Permissions' (which is selected), 'Metrics', 'Management', and 'Access Points'. The 'Permissions overview' section shows the 'Access' status as 'Bucket and objects not public'. Below this, the 'Block public access (bucket settings)' section has an 'Edit' button. The text explains that public access is blocked by default and provides a link to 'Learn more'. The 'Block all public access' setting is shown as 'On' with a green checkmark. A link to 'Individual Block Public Access settings for this bucket' is provided. The 'Bucket policy' section has 'Edit' and 'Delete' buttons. It states that the bucket policy is written in JSON and provides a link to 'Learn more'. At the bottom, a blue information box states: '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' with a link and an external icon.


Click on Edit Bucket and then policy Generator which will redirect you to the new page.

## Edit bucket policy [Info](#)


### Bucket policy

[Policy examples](#) 

[Policy generator](#) 

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

Bucket ARN

 `arn:aws:s3:::basiclabs-s3bucket`

### Policy

1

#### Edit statement

#### Select a statement

Select an existing statement in the policy or add a new statement.

[+ Add new statement](#)

[+ Add new statement](#)



## AWS Policy Generator

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

### Step 1: Select Policy Type

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

Select Type of Policy

S3 Bucket Policy

SQS Queue Policy

S3 Bucket Policy

VPC Endpoint Policy

IAM Policy

SNS Topic Policy

### Step 2: Add Statement(s)

A statement is the formal description of a 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 

-- Select Actions --

☐ All Actions ('\*')

Amazon Resource Name (ARN)

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

[Add Conditions \(Optional\)](#)

### 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.

**Add one or more statements above to generate a policy.**

# AWS Policy Generator

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

## Step 1: Select Policy Type

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

Select Type of Policy 

S3 Bucket Policy

## Step 2: Add Statement(s)

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

Effect

☒ Allow

☐ Deny

Principal

Use a comma to separate multiple values.

AWS Service

Amazon S3

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

☐ All Services ('\*')

Actions

-- Select Actions --

☐ All Actions ('\*')

Amazon Resource Name (ARN)

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

Add Conditions (Optional)

Add Statement

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

Principal(s)	Effect	Action	Resource	Conditions
<div><div>•</div><div>*</div></div>	Deny	<div><div>•</div><div>s3:PutObject</div></div>	arn:aws:s3:::basiclabs-s3bucket/*	<div><div>•</div><div>Null<ul style="list-style-type: none"><li>s3:x-amz-server-side-encryption:<div>"true"</div></li></ul></div></div>

Select Type of Policy S3 Bucket Policy

## Step 2: Add Statement(s)

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

Effect ☒ Allow ☐ Deny

Principal

Use a comma to separate multiple values.

### Policy JSON Document

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

```
{
  "Id": "Policy1708676898825",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1708676897441",
      "Action": [
        "s3:PutObject"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:s3:::basiclabs-s3bucket/*",
      "Condition": {
        "Null": {
          "s3:x-amz-server-side-encryption": "true"
        }
      },
      "Principal": "*"
    }
  ]
}
```

Close

Generate Policy

Start Over

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.

©2010, Amazon Web Services LLC or its affiliates. All rights reserved.

An **amazon.com** company




## Edit bucket policy [Info](#)

### Bucket policy

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

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

Bucket ARN

 arn:aws:s3:::basiclabs-s3bucket

### Policy

```
1 {
2   "Id": "Policy1708676950435",
3   "Version": "2012-10-17",
4   "Statement": [
5     {
6       "Sid": "Stmt1708676897441",
7       "Action": [
8         "s3:PutObject"
9       ],
10      "Effect": "Deny",
11      "Resource": "arn:aws:s3:::basiclabs-s3bucket/*",
12      "Condition": {
13        "Null": {
14          "s3:x-amz-server-side-encryption": "true"
15        }
16      },
17      "Principal": "*"
18    }
19  ]
20 }
```

[+ Add new statement](#)

### Edit statement

#### Select a statement


Select an existing statement in the policy or add a new statement.


[+ Add new statement](#)


JSON Ln 20, Col 1

## Edit bucket policy [Info](#)


### Bucket policy

[Policy examples](#) 

[Policy generator](#) 

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

Bucket ARN

 `arn:aws:s3:::basiclabs-s3bucket`

### Policy

1

#### Edit statement

##### Select a statement

Select an existing statement in the policy or add a new statement.

[+ Add new statement](#)

[+ Add new statement](#)