

# IS 698 – Cloud Computing & Resource Management

## Lab 3a - Amazon S3 - Managing Buckets, Files, Access Control, and Hosting a Static Website

### Part 1: Creating an S3 bucket

The screenshot shows the Amazon S3 console landing page. At the top, there's a navigation bar with the AWS logo, a search bar, and user account information. The main content area has a dark header with the text "Storage Amazon S3 Store and retrieve any amount of data from anywhere". Below this, there's a "How it works" section featuring a video player with the AWS logo and the URL "aws.amazon.com/S3". To the right of the video, there are three sidebars: "Create a bucket" with a "Create bucket" button, "Pricing" with a link to the "AWS Simple Monthly Calculator", and "Resources" with links to "User guide", "API reference", "FAQs", "Discussion forums", and "S3 on the AWS news blog". At the bottom, there's a "Common tasks" section.

The screenshot shows the "Create bucket" page in the Amazon S3 console. The page has a breadcrumb trail: "Amazon S3 > Buckets > Create bucket". The main heading is "Create bucket" with an "Info" link. Below the heading, there's a sub-heading "Buckets are containers for data stored in S3." The page is divided into three main sections: "General configuration", "Object Ownership", and "Block Public Access settings for this bucket". In the "General configuration" section, the "AWS Region" is set to "US East (N. Virginia) us-east-1". The "Bucket type" is set to "General purpose" (recommended for most use cases). The "Bucket name" is "firstawsbucket698". In the "Object Ownership" section, "ACLs disabled (recommended)" is selected. In the "Block Public Access settings for this bucket" section, "Block all public access" is checked. The page also includes a "Format: s3://bucket/prefix" field and a "Choose bucket" button.

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](#)

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Downloaded from <http://ajph.org/>

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

---

Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. [Learn more](#)

\_\_\_\_\_

\_\_\_\_\_

Buckets are containers for data stored in S3.

Find buckets by name

Name	AV
------	----

# Part 2: Uploading a File into the S3 Bucket Via Console

aws

Search

[Option+S]

United States (N. Virginia)

HitakshiTannaAWSAccount

Amazon S3

Buckets

firstawsbucket698

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 SDKs 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 (4 total, 2.7 MB)

All files and folders in this table will be uploaded.

Find by name

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	1.png	-	image/png	1.0 MB
<input type="checkbox"/>	2.png	-	image/png	621.6 KB
<input type="checkbox"/>	3.png	-	image/png	649.9 KB
<input type="checkbox"/>	4.png	-	image/png	428.7 KB

Destination

info

Destination

[s3://firstawsbucket698](#)

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

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

aws

Search

[Option+S]

United States (N. Virginia)

HitakshiTannaAWSAccount

Upload succeeded

For more information, see the [Files and folders](#) table.

Close

Upload: status

After you navigate away from this page, the following information is no longer available.

Summary

Destination

[s3://firstawsbucket698](#)

Succeeded

4 files, 2.7 MB (100.00%)

Failed

0 files, 0 B (0%)

Files and folders

Configuration

Files and folders (4 total, 2.7 MB)

Find by name

Name	Folder	Type	Size	Status	Error
<a href="#">1.png</a>	-	image/png	1.0 MB	Succeeded	-
<a href="#">2.png</a>	-	image/png	621.6 KB	Succeeded	-
<a href="#">3.png</a>	-	image/png	649.9 KB	Succeeded	-
<a href="#">4.png</a>	-	image/png	428.7 KB	Succeeded	-

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

## Via AWS CLI

```
hitakshi - zsh - 95x25
(base) hitakshi@Hitakshis-MacBook-Pro ~ % aws s3 cp ~/Desktop/iris.arff s3://firstawsbucket698/
upload: Desktop/iris.arff to s3://firstawsbucket698/iris.arff
(base) hitakshi@Hitakshis-MacBook-Pro ~ %
```

## Verifying successful file upload

The screenshot shows the AWS Management Console for the bucket 'firstawsbucket698'. The 'Objects' tab is selected, displaying a list of five objects. The object 'iris.arff' is highlighted, indicating it has been successfully uploaded.

Name	Type	Last modified	Size	Storage class
1.png	png	February 18, 2025, 19:54:19 (UTC-05:00)	1.0 MB	Standard
2.png	png	February 18, 2025, 19:54:19 (UTC-05:00)	621.6 KB	Standard
3.png	png	February 18, 2025, 19:54:19 (UTC-05:00)	649.9 KB	Standard
4.png	png	February 18, 2025, 19:54:19 (UTC-05:00)	428.7 KB	Standard
iris.arff	arff	February 18, 2025, 19:58:34 (UTC-05:00)	7.3 KB	Standard

## Part 3: Enabling Versioning on the Bucket

aws

Search

[Option+S]

United States (N. Virginia)

HitakshiTannaAWSAccount

Amazon S3 > Buckets > firstawsbucket698 > Edit Bucket Versioning

### Edit Bucket Versioning [Info](#)

#### Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

#### Bucket Versioning

☐ Suspend  
This suspends the creation of object versions for all operations but preserves any existing object versions.

☒ Enable

After enabling Bucket Versioning, you might need to update your lifecycle rules to manage previous versions of objects.

#### Multi-factor authentication (MFA) delete

An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

Disabled

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

## Re-uploading the same file

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws

Search

[Option+S]

United States (N. Virginia)

HitakshiTannaAWSAccount

Amazon S3 > Buckets > firstawsbucket698 > 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 SDKs 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, 7.3 KB)

All files and folders in this table will be uploaded.

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	iris.arff	-	-	7.3 KB

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

#### Destination [Info](#)

**Destination**  
[s3://firstawsbucket698](#)

► **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](#)



aws

Search

[Option+S]

United States (N. Virginia)

HitakshiTannaAWSAccount

Amazon S3

Buckets

firstawsbucket698

Successfully edited bucket policy.

Individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access

Off

Individual Block Public Access settings for this bucket

Bucket policy

EditDelete

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::firstawsbucket698/*"
    }
  ]
}
```

Copy

Object Ownership [Info](#)

Edit

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.

# Create an IAM policy and attached it to users

Step 1

Specify permissions

Step 2

Review and create

## Specify permissions

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

Policy editor

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "s3:*",
7       "Resource": "arn:aws:s3:::firstawsbucket698/*"
8     }
9   ]
10 }
11 }
```

Visual

JSON

Actions

Edit statement

Select a statement

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

+ Add new statement

+ Add new statement

JSON Ln 11, Col 1

6025 of 6144 characters remaining

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Search

[Option+5]

IAM

Policies

698lab3a

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management

Access reports

Access Analyzer

External access

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies

Resource control policies

IAM Identity Center

AWS Organizations

698lab3a

Edit

Delete

Policy details

Type

Customer managed

Creation time

February 18, 2025, 22:00 (UTC-05:00)

Edited time

February 18, 2025, 22:00 (UTC-05:00)

ARN

arn:aws:iam::140023386861:policy/698lab3a

Permissions

Entities attached

Tags

Policy versions

Last Accessed

Attached as a permissions policy (2)

To grant permissions to an entity, attach a permissions policy to it.

Search

Filter by Entity type

All types

Entity name

Entity type

ConsoleUser

IAM Users

ProgrammaticUser

IAM Users

Attached as a permissions boundary (0)

Use this policy as a permissions boundary to control the maximum permissions that an entity can have. This is an advanced feature used to delegate permissions management to others.

Search

Filter by Entity type

All types

Entity name

Entity type

Policy not set as a permissions boundary for any entity.

Set this policy as a permissions boundary

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



## Part 5: Hosting a Static Website on S3

### Enabled Static Website hosting

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

**Static website hosting**

☐ Disable

☒ Enable

**Hosting type**

☒ Host a static website

Use the bucket endpoint as the web address. [Learn more](#)

☐ Redirect requests for an object

Redirect requests to another bucket or domain. [Learn more](#)

For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see [Using Amazon S3 Block Public Access](#)

**Index document**

Specify the home or default page of the website.

index.html

**Error document - optional**

This is returned when an error occurs.

error.html

**Redirection rules - optional**

Redirection rules, written in JSON, automatically redirect webpage requests for specific content. [Learn more](#)

1
---

### Index.html

```
index.html X
Users > hitakshi > Desktop > index.html > ...
1 <html>
2 <head><title>My S3 Website</title></head>
3 <body>
4   <h1>Welcome to My Static Website on S3</h1>
5 </body>
6 </html>
7
```

# Uploaded to S3 bucket

Upload succeeded

For more information, see the Files and folders table.

Close

Upload: status

Close

After you navigate away from this page, the following information is no longer available.

Summary

Destination

s3://firstawsbucket698

Succeeded

1 file, 120.0 B (100.00%)

Failed

0 files, 0 B (0%)

Files and folders

Configuration

Files and folders (1 total, 120.0 B)

Find by name

Name	Folder	Type	Size	Status	Error
<a href="#">index.html</a>	-	text/html	120.0 B	Succeeded	-

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

# Allowed Public Access and Enabled a Bucket policy

Amazon S3

Buckets

firstawsbucket698

Object Ownership

info

Edit

Block public access (bucket settings)

Edit

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 all your S3 buckets and 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 your buckets or objects within you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access

Off

Individual Block Public Access settings for this bucket

Bucket policy

Edit

Delete

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](#)

Copy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::firstawsbucket698/*"
    }
  ]
}
```

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

## Accessed the Website



## Summary:

This lab involved managing Amazon S3 by creating a bucket, uploading files, configuring access control, enabling versioning, and hosting a static website. The process began with creating an S3 bucket in the AWS Management Console, ensuring a globally unique name, and selecting a preferred region. Public access was initially blocked for security.

Files were uploaded to the S3 bucket using both the AWS Console and AWS CLI. Versioning was then enabled in the bucket settings, and a new version of the file was uploaded to verify version control. Access control was configured by creating a bucket policy to allow public read access and an IAM policy to manage permissions for specific users. One issue was encountered while creating the bucket policy, which was resolved by unchecking the Block all public access checkbox in the bucket permissions.

Finally, static website hosting was enabled by uploading an index.html file and modifying the bucket's permissions to allow public access. The website was successfully accessed using the provided Bucket Website Endpoint.