

FR. CONCEICAO RODRIGUES COLLEGE OF ENGINEERING

Department of Computer Engineering

Course, Subject & Experiment Details

Practical No:	
Title:	To study and Implement Storage as a Service using Own Cloud/ AWS S3, Glaciers/ Azure Storage.
Name of the Student:	Warren Fernandes
Roll No:	8940
Date of Performance:	28/03/2022
Date of Submission:	28/03/2022

Evaluation:

Sr. No.	Rubric	Grade
1	On time submission/completion (2)	
2	Preparedness (2)	
3	Skill (4)	
4	Output (2)	

Signature of the Teacher

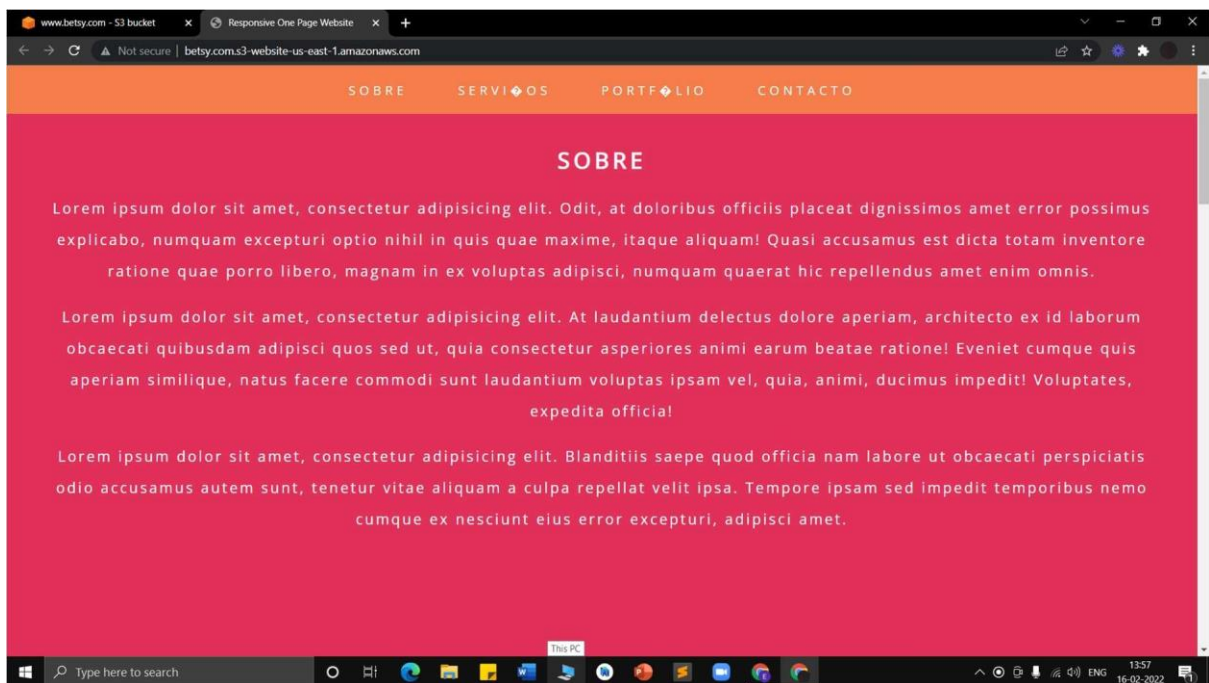
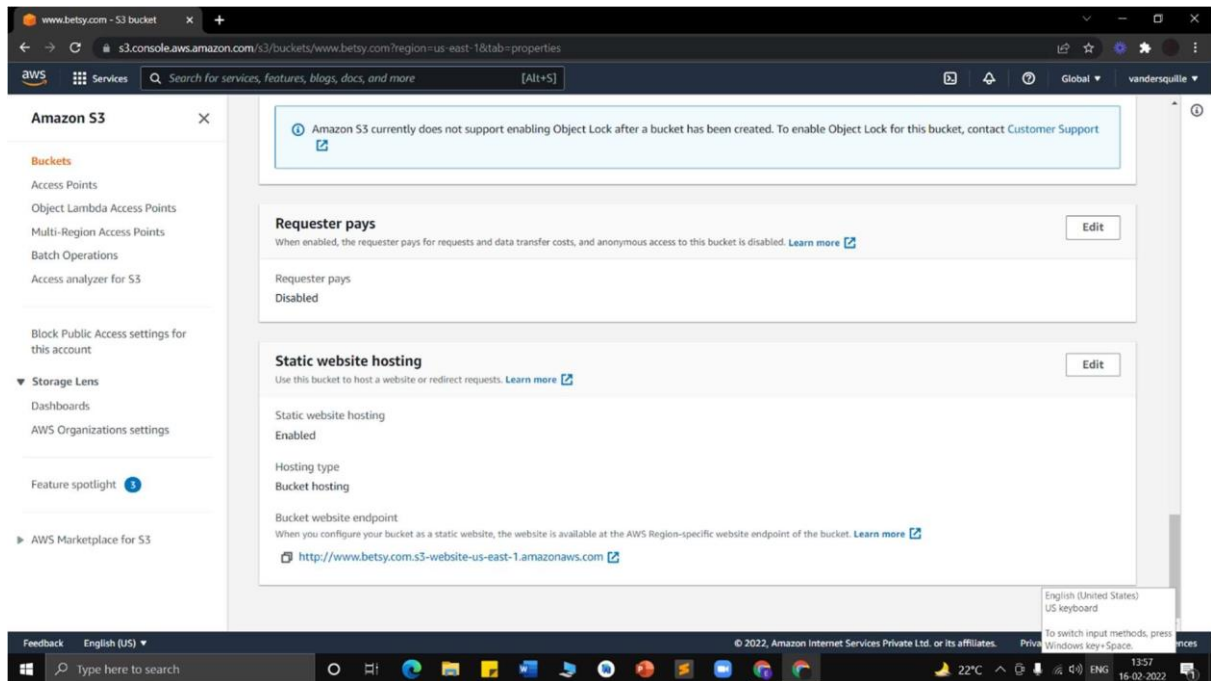
AWS S3

The screenshot shows the Amazon S3 Management Console in the 'us-east-1' region. The left sidebar contains navigation links for Buckets, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, Access analyzer for S3, Storage Lens, and AWS Marketplace for S3. The main content area displays an 'Account snapshot' and a 'Buckets (2)' section. The buckets table lists two buckets: 'www.betsy.com' and 'www.yfoh.com', both in the 'us-east-1' region with 'Public' access.

Name	AWS Region	Access	Creation date
www.betsy.com	US East (N. Virginia) us-east-1	Public	February 15, 2022, 09:41:46 (UTC+05:30)
www.yfoh.com	US East (N. Virginia) us-east-1	Public	February 10, 2022, 14:47:43 (UTC+05:30)

The screenshot shows the 'Objects' page for the 'www.betsy.com' bucket. The left sidebar is the same as the previous screenshot. The main content area shows the bucket's 'Publicly accessible' status and tabs for Objects, Properties, Permissions, Metrics, Management, and Access Points. The 'Objects (5)' section lists five objects: 'contact.css', 'contact.html', 'home.css', 'home.html', and 'home.js'. Each object's details, including type, last modified date, size, and storage class, are displayed.

Name	Type	Last modified	Size	Storage class
contact.css	css	February 15, 2022, 10:15:18 (UTC+05:30)	1013.0 B	Standard
contact.html	html	February 15, 2022, 10:15:19 (UTC+05:30)	6.2 KB	Standard
home.css	css	February 15, 2022, 10:09:14 (UTC+05:30)	5.0 KB	Standard
home.html	html	February 15, 2022, 10:09:15 (UTC+05:30)	6.5 KB	Standard
home.js	js	February 15, 2022, 10:09:16 (UTC+05:30)	1.1 KB	Standard



www.betsy.com - S3 bucket

s3.console.aws.amazon.com/s3/bucket/www.betsy.com/property/website/edit?region=us-east-1

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

Access analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

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.

home.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](#)

Feedback English (US)

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Type here to search

www.betsy.com - S3 bucket

s3.console.aws.amazon.com/s3/buckets/www.betsy.com/?region=us-east-1&tab=permissions

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

Access analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

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](#)

Edit Delete

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](#)

Copy


```
{
  "Version": "2012-10-17",
  "Id": "Policy1644901249894",
  "Statement": [
    {
      "Sid": "Stmt1644901248542",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3::www.betsy.com/*"
    }
  ]
}
```

https://s3.console.aws.amazon.com/s3/#

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Type here to search

www.betsy.com - S3 bucket x AWS Policy Generator x +
awspolicygen.s3.amazonaws.com/policygen.html



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 ☐ 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::www.betsy.com

ARN should follow the following format: arn:aws:s3:::(BucketName)/?(Keyname).
Use a comma to separate multiple values.

Add Conditions (Optional)

Add Statement

Type here to search

ADA... 13:59 16-02-2022

www.betsy.com - S3 bucket x AWS Policy Generator x +
awspolicygen.s3.amazonaws.com/policygen.html

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:aws:s3::www.betsy.com

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 statement:

Principal

Effect ☒ Allow ☐ Deny

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

Amazon Resource Name (ARN) arn:aws:s3::www.betsy.com

ARN should follow the following format: arn:aws:s3:::(BucketName)/?(Keyname).
Use a comma to separate multiple values.

Add Conditions (Optional)

Add Statement

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": "Policy1645000178281",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1645000178391",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3::www.betsy.com/*",
      "Principal": "*"
    }
  ]
}
```

Close

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 you are 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

Type here to search

ADA... 13:59 16-02-2022

www.betsy.com - S3 bucket x AWS Policy Generator x +

s3.console.aws.amazon.com/s3/buckets/www.betsy.com?region=us-east-1&tab=permissions

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

Access analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight 3

AWS Marketplace for S3

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](#)

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

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": "Policy1645000178281",
  "Statement": [
    {
      "Sid": "Stmt1645000170391",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::www.betsy.com/*"
    }
  ]
}
```

[Copy](#)

Feedback English (US)

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Type here to search

ADA...

1400

16-02-2022

www.betsy.com - S3 bucket x AWS Policy Generator x +

s3.console.aws.amazon.com/s3/buckets/www.betsy.com?region=us-east-1&tab=permissions

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

Access analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight 3

AWS Marketplace for S3

Block public access (bucket settings)

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](#)

[Edit](#)

Block all public access

Off

Individual Block Public Access settings for this bucket

- ☒ 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.

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](#)

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

Public access is blocked because Block Public Access settings are turned on for this bucket

Feedback English (US)

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Type here to search

ADA...

1400

16-02-2022

Experiment 5: Amazon Web Services Post Lab Questions

Q1. What's the Difference between Domain Name and Web Hosting?

A domain name is your website's address on the web. It identifies the website and lets people find it via their Chromes or Firefox.

Web hosting (or web host, or web server, or just hosting) is the place where your website files (and all your website data) are kept, and from where the website can be accessed by your website visitors. Most commonly, a web server is a specialized type of computer. Basically, when a visitor puts your website's domain name into their web browser window, that domain name is then taken and decoded to figure out what specific web host (web server) it points to. Once this is done, the website gets displayed to the visitor. This will surely come as no surprise, but the web is quite a complicated creation, and domains and hosting are just a small part of a bigger puzzle. Luckily for everyone, you really don't need to be an expert on those things to be able to launch a website for your business and show it to the world.

Q2. What is Amazon s3 and the benefits of using it?

Amazon Simple Storage Service (Amazon S3), is the most fundamental and global Infrastructure as a Service (IaaS) solution provided by Amazon Web Services (AWS). Using Amazon S3 facilitates highly-scalable, secured and low-latency data storage from the cloud. With its simple web service interface, it is easy to store and retrieve data on Amazon S3 from anywhere on the web. All you need to do is choose a region (which is a separate geographic area, choose the closest one to you), create a S3 bucket and start storing data.

Amazon S3 is a pioneer in cloud data storage and has uncountable benefits ☐

Reliable Security:

- All-time Availability:
- Very Low cost:
- Ease of Migration:
- The Simplicity of Management:

• Reliable Security:

When created, Amazon S3 buckets are usable only by the identity that created them (IAM policy grants are the exception). You can set access permissions for each file, each bucket, or via IAM (Identity access management), which provides a complete control over how, where and by whom the data can be frequently accessed. With these set of rules and permissions, you can make sure that there is no unauthorized access to your data.

• All-time Availability:

Amazon S3 gives every user, its service access to the same highly scalable, reliable, fast, inexpensive data storage infrastructure that Amazon uses to run its own global network of websites. S3 Standard is designed for 99.99% availability and Standard – IA is designed for 99.9% availability. Both are backed by the Amazon S3 Service Level Agreement, which is strictly followed by Amazon.

- Very Low cost:

With Amazon S3, you only pay for the data you use, which in itself is a very low price equivalent to \$0.022 / GB and ~\$0.0125 / GB for infrequent access. You can also define policies to migrate the data automatically to the infrequent access which further reduces the cost as Amazon Glacier is even cheaper(~\$0.004 / GB).

- Ease of Migration:

With Amazon S3 you get multiple options (rsync, S3 command line interface and Glacier command line interface) for Cloud Data Migration which are cost effective and it is very simple to transfer a large amount of data to Amazon S3 or out of Amazon S3. Amazon S3 Storage also provides you with the option to import or export data to any physical device or on any network.

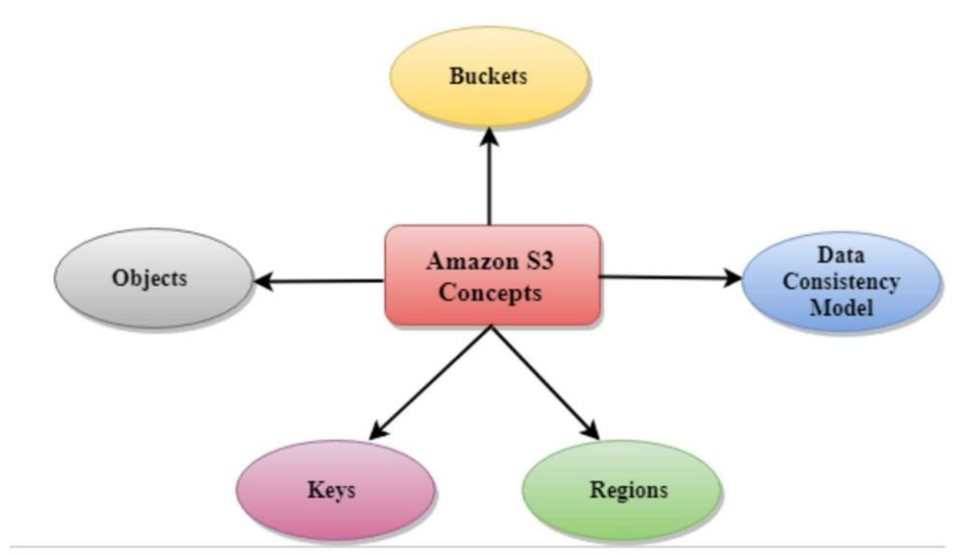
- The Simplicity of Management:

Amazon S3 has a very user-friendly web interface which takes out the usual hard work of maintaining security, optimizing storage classes and managing the data transfer in the most suitable way. You can define its own lifecycle policy, define replication rules and configure the Amazon S3 inventory. It also allows you to configure request metrics and storage classes analysis with many filters to have a better look at your storage.

Q3. What are bucket policies in the Amazon s3?

A bucket policy is type of Resource based Policy; similar to an IAM Identity based Policy except it is applied to an AWS managed resource. In addition to Bucket Policies, there are other types of resource-based IAM Policies such as KMS Key Policy; SQS Policy, and VPC Endpoints.

Q4. Explain the core concepts of Amazon s3.



□ Buckets

A bucket is a container used for storing the objects.

Every object is incorporated in a bucket.

For example, if the object named photos/tree.jpg is stored in the treeimage bucket, then it can be addressed by using the URL <http://treeimage.s3.amazonaws.com/photos/tree.jpg>.

A bucket has no limit to the amount of objects that it can store. No bucket can exist inside of other buckets.

S3 performance remains the same regardless of how many buckets have been created.

The AWS user that creates a bucket owns it, and no other AWS user cannot own it.

Therefore, we can say that the ownership of a bucket is not transferrable.

The AWS account that creates a bucket can delete a bucket, but no other AWS user can delete the bucket.

□ Objects

Objects are the entities which are stored in an S3 bucket.

An object consists of object data and metadata where metadata is a set of name-value pair that describes the data.

An object consists of some default metadata such as date last modified, and standard HTTP metadata, such as Content type. Custom metadata can also be specified at the time of storing an object.

It is uniquely identified within a bucket by key and version ID.

□ Key

A key is a unique identifier for an object.

Every object in a bucket is associated with one key.

An object can be uniquely identified by using a combination of bucket name, the key, and optionally version ID.

For example, in the URL <http://jtp.s3.amazonaws.com/2019-01-31/Amazons3.wsdl> where "jtp" is the bucket name, and key is "2019-01-31/Amazons3.wsdl"

Regions

You can choose a geographical region in which you want to store the buckets that you have created.

A region is chosen in such a way that it optimizes the latency, minimize costs or address regulatory requirements.

Objects will not leave the region unless you explicitly transfer the objects to another region.

☐ Data Consistency Model

Amazon S3 replicates the data to multiple servers to achieve high availability.

Two types of model:

- ☐ Read-after-write consistency for PUTS of new objects.

For a PUT request, S3 stores the data across multiple servers to achieve high availability.

A process stores an object to S3 and will be immediately available to read the object.

A process stores a new object to S3, it will immediately list the keys within the bucket.

It does not take time for propagation, the changes are reflected immediately.

- ☐ Eventual consistency for overwrite PUTS and DELETES

For PUTS and DELETES to objects, the changes are reflected eventually, and they are not available immediately.

If the process replaces an existing object with the new object, you try to read it immediately. Until the change is fully propagated, the S3 might return prior data. If the process deletes an existing object, immediately try to read it. Until the change is fully propagated, the S3 might return the deleted data.

If the process deletes an existing object, immediately list all the keys within the bucket. Until the change is fully propagated, the S3 might return the list of the deleted key.