

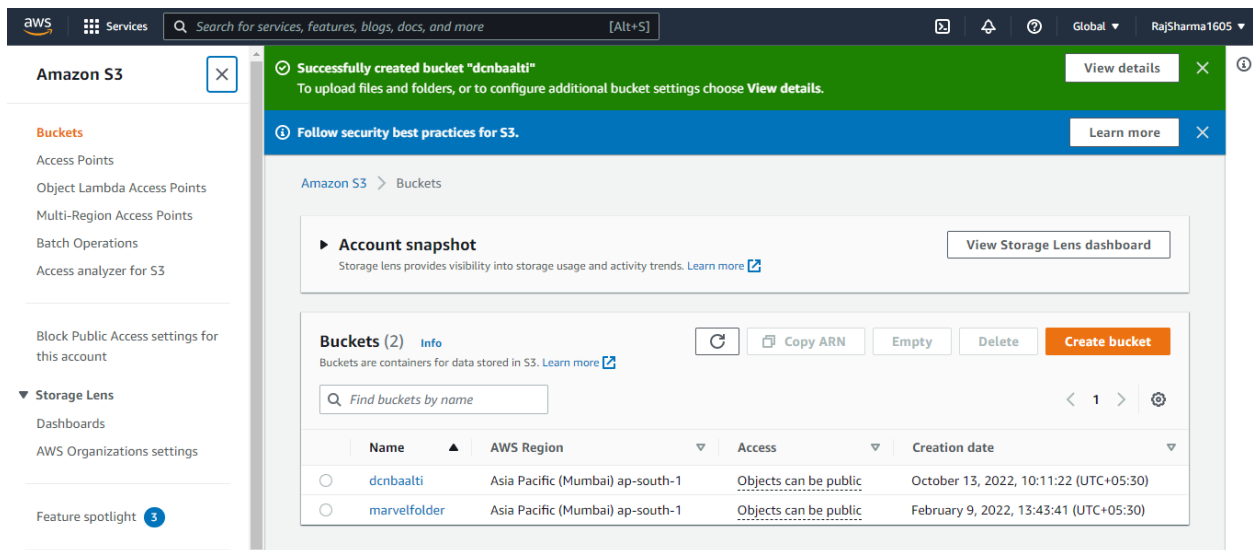
DCN Experiment – 4

Submitted by – Raj Sharma (RA2011028010055)

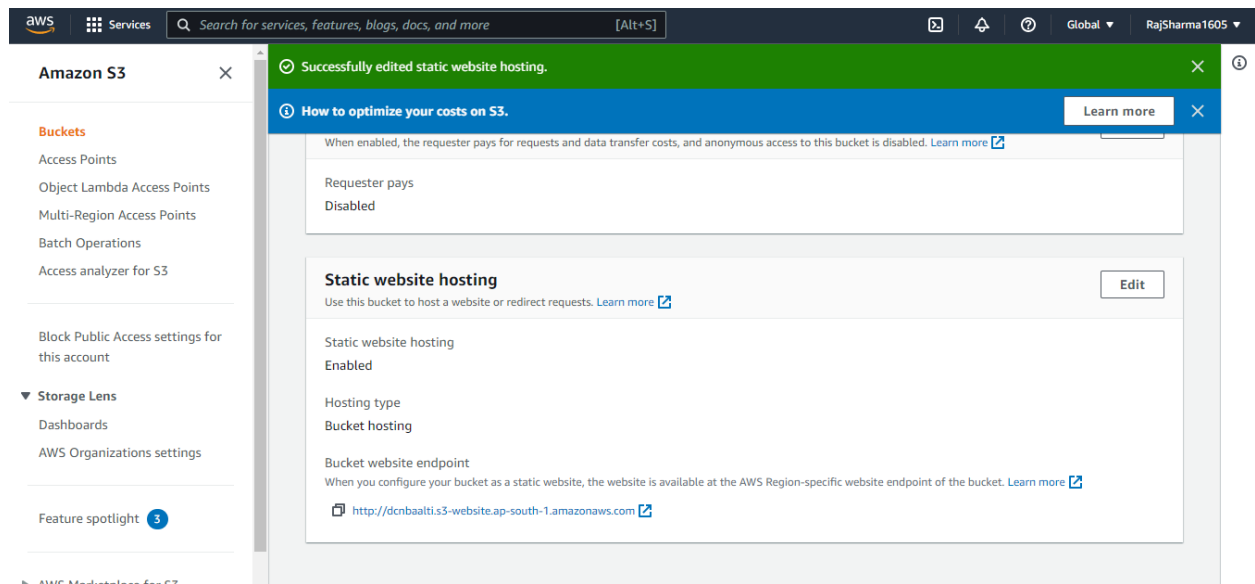
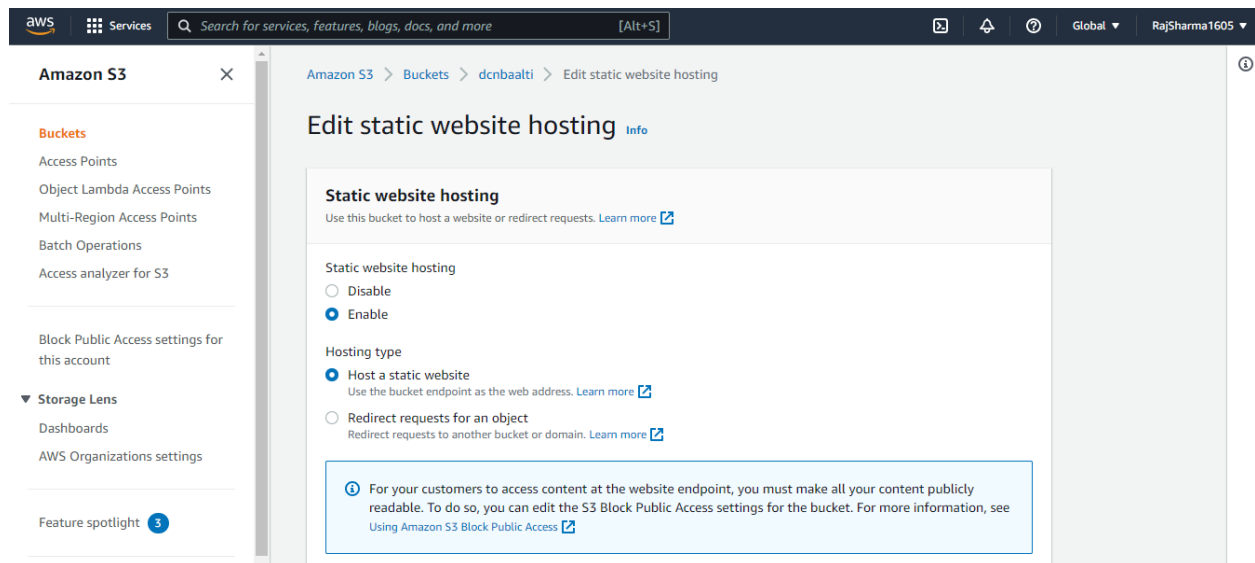
AIM: To create a static website on Amazon S3 using AWS system manager.

PROCEDURE:

- 1) Sign in to the AWS Management Console and click on Amazon S3 Console at <https://console.aws.amazon.com/s3/>.
- 2) Click on create a bucket.
- 3) Enter the name of the bucket and the region you want to create it in
- 4) Accept the default settings and then click on create a bucket



- 5) In the buckets list, click on the bucket you just created and choose properties, then under static website hosting click the enable option.



6) Then click on the upload option after selecting your bucket and upload your project files(index.html,style.css,main.js). Also, make sure that the project files you will upload have proper names as they are case-sensitive.

aws Services Search for services, features, blogs, docs, and more [Alt+S] Global RajSharma1605

Upload succeeded
View details below.

Summary

Destination s3://dcnbaalti	Succeeded 1 file, 11.0 KB (100.00%)	Failed 0 files, 0 B (0%)
-------------------------------	--	-----------------------------

Files and folders Configuration

Files and folders (1 Total, 11.0 KB)

Find by name

Name	Folder	Type	Size	Status	Error
awsindex.html.docx	-	application/vnd.openxmlformats-officedocument.wordprocessingml.document	11.0 KB	Succeeded	-

7) After configuring the website you can use the endpoint to test the website out.

8) choose the name of the bucket you just configured and then choose permissions under that block public access will be visible, click on the edit option and save the changes.

aws Services Search for services, features, blogs, docs, and more [Alt+S] Global RajSharma1605

Successfully edited Block Public Access settings for this bucket.

Follow security best practices for S3. Learn more

Amazon S3 > Buckets > dcnbaalti

dcnbaalti

Info

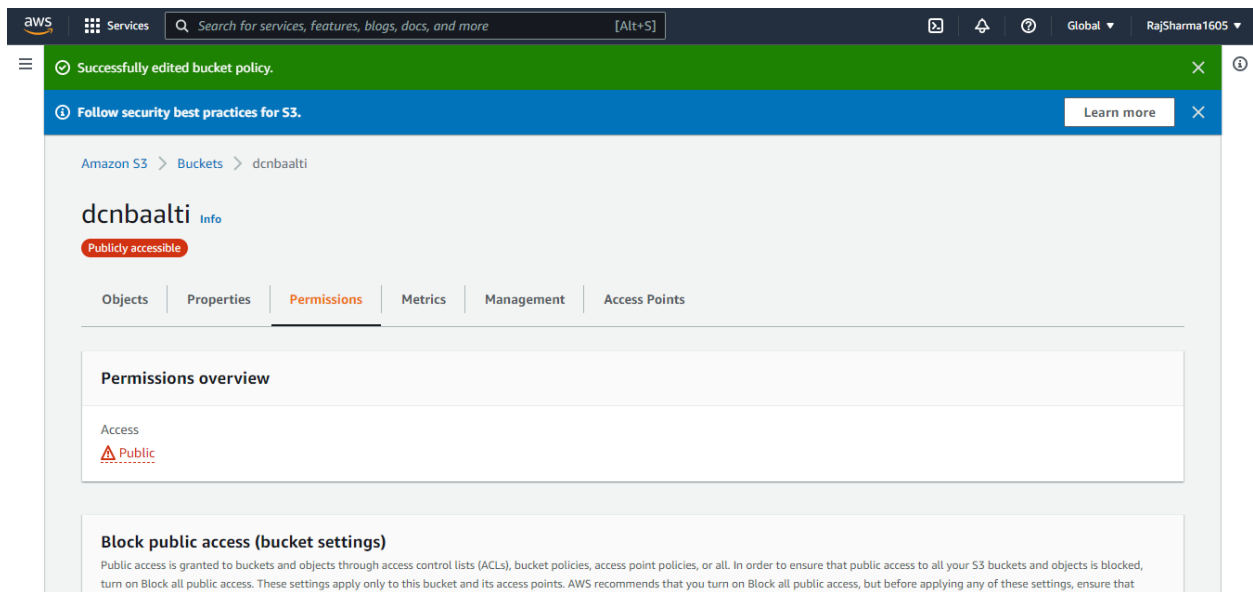
Objects Properties Permissions Metrics Management Access Points

Permissions overview

Access
Objects can be public

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



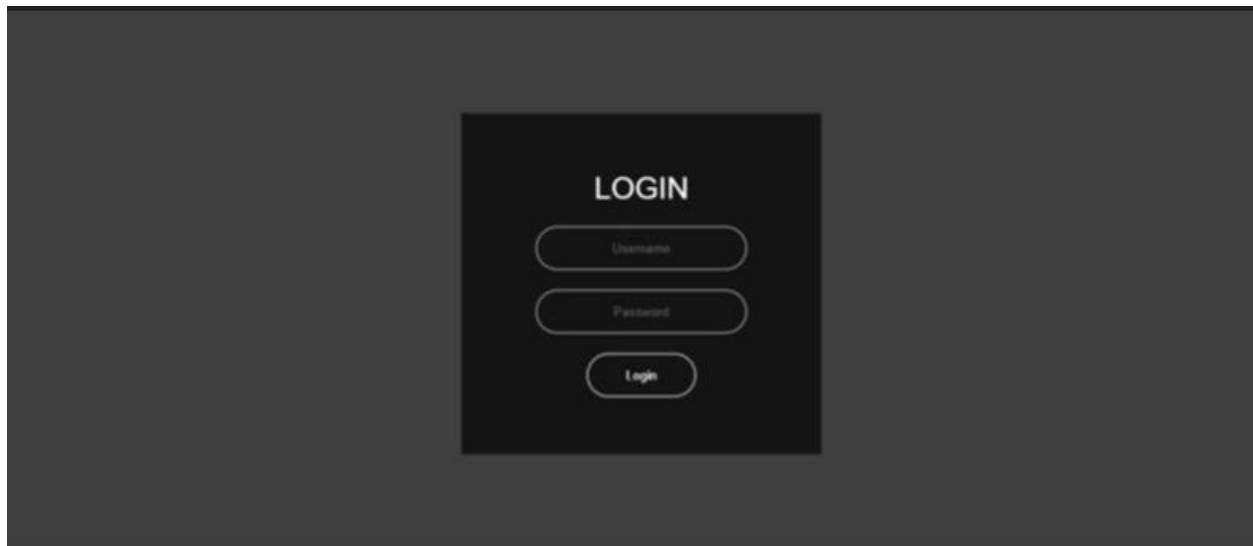
9) under the bucket permissions there will be a bucket policy, click on that and paste this code into the bucket policy editor:

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

10) Click on save changes .

11) Under the buckets, choose the name of your bucket which you just created, and in the properties, choose a static website hosting - then choose your bucket endpoint .

12) Now you can access your website as it has successfully been hosted.



13) Make sure to clean up after this experiment by deleting the AWS Resources that have been just allocated . After you have deleted these resources, your website will no longer be available .

RESULT: A static website has been successfully created on Amazon S3 using AWS System Manager.