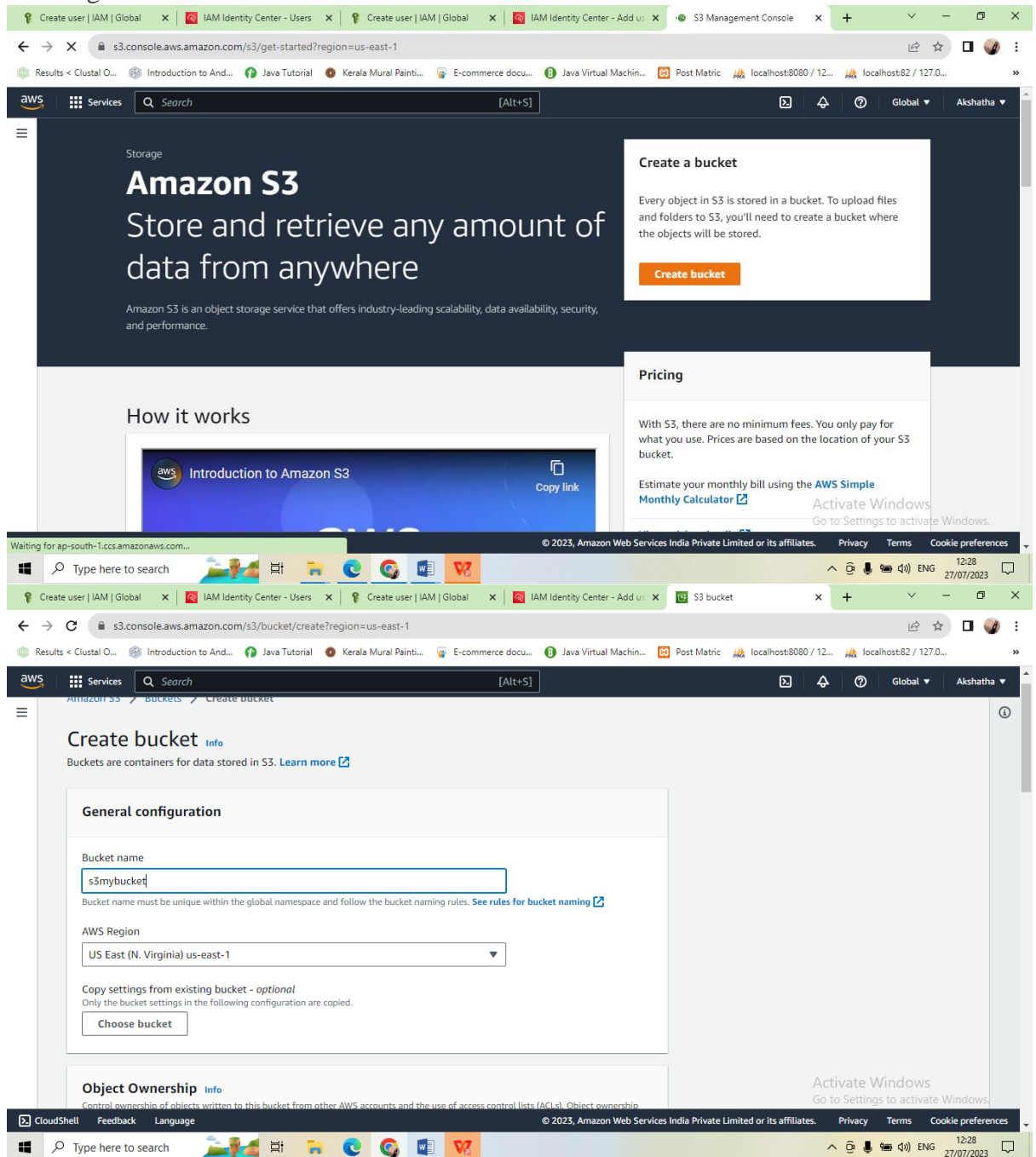# Phase5-18 Policies and Permissions

- Implement policies and permissions on an S3 bucket
- Creating a bucket

- Click on the *Permission* section.

- Go to *Bucket Policy*.

- It will open the console where you can add policy.

Screen 1: S3 Management Console - Bucket created

Tabs: Create user | IAM | Global — IAM Identity Center - Users — Create user | IAM | Global — IAM Identity Center - Add us — S3 Management Console

URL: s3.console.aws.amazon.com/s3/buckets?region=us-east-1

aws — Services — Search [Alt+S] — Global ▾ — Akshatha ▾

⊘ Successfully created bucket "awsslbucket"
To upload files and folders, or to configure additional bucket settings choose View details.

View details ✕

Amazon S3 > Buckets

▸ Account snapshot
Storage lens provides visibility into storage usage and activity trends. Learn more ⧉

View Storage Lens dashboard

Buckets (1) Info
Buckets are containers for data stored in S3. Learn more ⧉

Copy content — Empty — Delete — Create bucket

Find buckets by name

< 1 >

	Name ▲	AWS Region ▽	Access ▽	Creation date ▽
○	awsslbucket	US East (N. Virginia) us-east-1	Bucket and objects not public	July 27, 2023, 12:33:48 (UTC+05:30)

CloudShell — Feedback — Language — © 2023, Amazon Web Services India Private Limited or its affiliates. — Privacy — Terms — Cookie preferences

---

Screen 2: awsslbucket - S3 bucket - Permissions

URL: s3.console.aws.amazon.com/s3/buckets/awsslbucket?region=us-east-1&tab=permissions

aws — Services — Search [Alt+S] — Global ▾ — Akshatha ▾

Amazon S3 > Buckets > awsslbucket

awsslbucket Info

Objects — Properties — **Permissions** — Metrics — Management — Access Points

Permissions overview

Access
Bucket and objects not 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 storage use cases. Learn more ⧉

Edit

CloudShell — Feedback — Language — © 2023, Amazon Web Services India Private Limited or its affiliates. — Privacy — Terms — Cookie preferences

Screenshot 1

Create user | IAM | Global   IAM Identity Center - Users   Create user | IAM | Global   IAM Identity Center - Add us   awsslbucket - S3 bucket

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

Results < Clustal O...   Introduction to And...   Java Tutorial   Kerala Mural Painti...   E-commerce docu...   Java Virtual Machin...   Post Matric   localhost:8080 / 12...   localhost:82 / 127.0...

aws   Services   Search   [Alt+S]   Global ▼   Akshatha ▼

⊘ On

▶ 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 ↗

ⓘ **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** ↗

No policy to display.   Copy

CloudShell   Feedback   Language   © 2023, Amazon Web Services India Private Limited or its affiliates.   Privacy   Terms   Cookie preferences

Type here to search   ENG   12:34   27/07/2023

Screenshot 2

Create user | IAM | Glo   IAM Identity Center -   Create user | IAM | Glo   IAM Identity Center -   awsslbucket - S3 buck   AWS Policy Generator

awspolicygen.s3.amazonaws.com/policygen.html

Results < Clustal O...   Introduction to And...   Java Tutorial   Kerala Mural Painti...   E-commerce docu...   Java Virtual Machin...   Post Matric   localhost:8080 / 12...   localhost:82 / 127.0...

amazon web services

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   [▼]

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   [▼]   ☐ All Services ('*')
Use multiple statements to add permissions for more than one service.

Actions   [ ]

Type here to search   ENG   12:35   27/07/2023

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

Add Conditions (Optional)

[**Add Statement**]

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.

- Paste the JSON in the policy console of bucket and click on *Save*.

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

Policy examples   Policy generator

Bucket ARN

arn:aws:s3:::awsslbucket

Policy

```
1  {
2      "Id": "Policy1690441945701",
3      "Version": "2012-10-17",
4      "Statement": [
5          {
6              "Sid": "Stmt1690441930637",
7              "Action": [
8                  "s3:CreateBucket"
9              ],
10             "Effect": "Allow",
11             "Resource": "arn:aws:s3:::awsslbucket",
12             "Principal": {
13                 "AWS": [
14                     "Allow creation"
```

Edit statement

Select a statement

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

+ Add new statement

```
1  {
2      "Id": "Policy1690441945701",
3      "Version": "2012-10-17",
4      "Statement": [
5          {
6              "Sid": "Stmt1690441930637",
7              "Action": [
8                  "s3:CreateBucket"
9              ],
10             "Effect": "Allow",
11             "Resource": "arn:aws:s3:::awsslbucket",
12             "Principal": {
13                 "AWS": [
14                     "Allow creation"
15                 ]
16             }
17         }
18     ]
19  }
```

Edit statement

Select a statement

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

+ Add new statement