



Placement Empowerment Program
Cloud Computing and DevOps Centre

**create an IAM role with permissions.
Assign the role to your VM and
verify its effect by attempting
permitted/denied actions.**

Name: Abdur Rahman M.R

Department : CSE



Introduction

Amazon Simple Storage Service (S3) is a scalable object storage service offered by AWS that allows you to store and retrieve data. It's widely used for storing backups, files, images, and other data. S3 buckets act as containers for storing data, and you can configure various settings for access control, encryption, logging, and versioning.

In this guide, you'll learn how to:

1. **Create an S3 bucket.**
2. **Upload files to the bucket.**
3. **Configure the bucket's public or private access.**
4. **Test accessibility.**

Overview

1. **S3 Buckets:** Storage containers for objects.
2. **Public Access Configuration:** You can control whether your objects are publicly accessible or not.
3. **Bucket Policies:** Define access permissions for specific users or roles.
4. **Public Access Block Settings:** Prevent the accidental exposure of sensitive data by restricting public access.

Step-by-Step Overview

1. Create an S3 Bucket

Create Role

Attach Permissions:

Name the Role:

Using AWS CLI:

```
aws s3api create-bucket --bucket asmybk --region  
us-east-1 --create-bucket-configuration  
LocationConstraint=us-east-1
```

2. Upload Files to the S3 Bucket

Using AWS CLI:

```
aws s3 cp /path/to/your/file.txt s3://asmybk/
```

Bucket policy

The bucket policy, written in JSON, provides access to the object

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

Configure Bucket Access

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
"Sid": "PublicReadGetObject",  
"Effect": "Allow",  
"Principal": "*",  
"Action": "s3:GetObject",  
"Resource": "arn:aws:s3:::asmybk/*"  
}  
]  
}
```

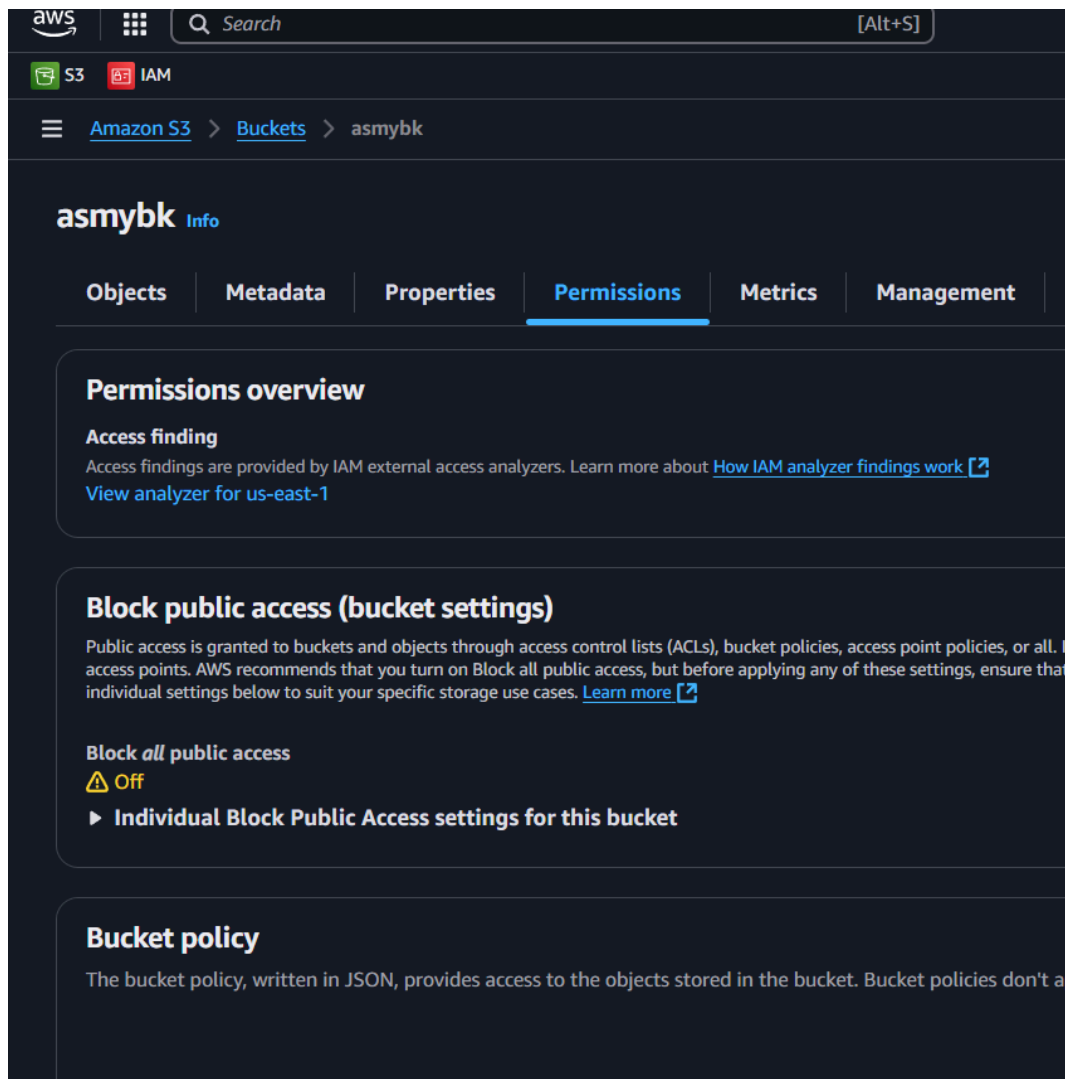
Using AWS CLI:

```
aws s3api put-bucket-policy --bucket asmybk --policy  
"{\"Version\":\"2012-10-17\",\"Statement\":  
[{\"Sid\":\"PublicReadGetObject\",\"Effect\":\"Allow\",  
\"Principal\":\"*\",\"Action\":\"s3:GetObject\",\"Res  
ource\":\"arn:aws:s3:::asmybk/*\"}]}"
```

Restrict Public Access

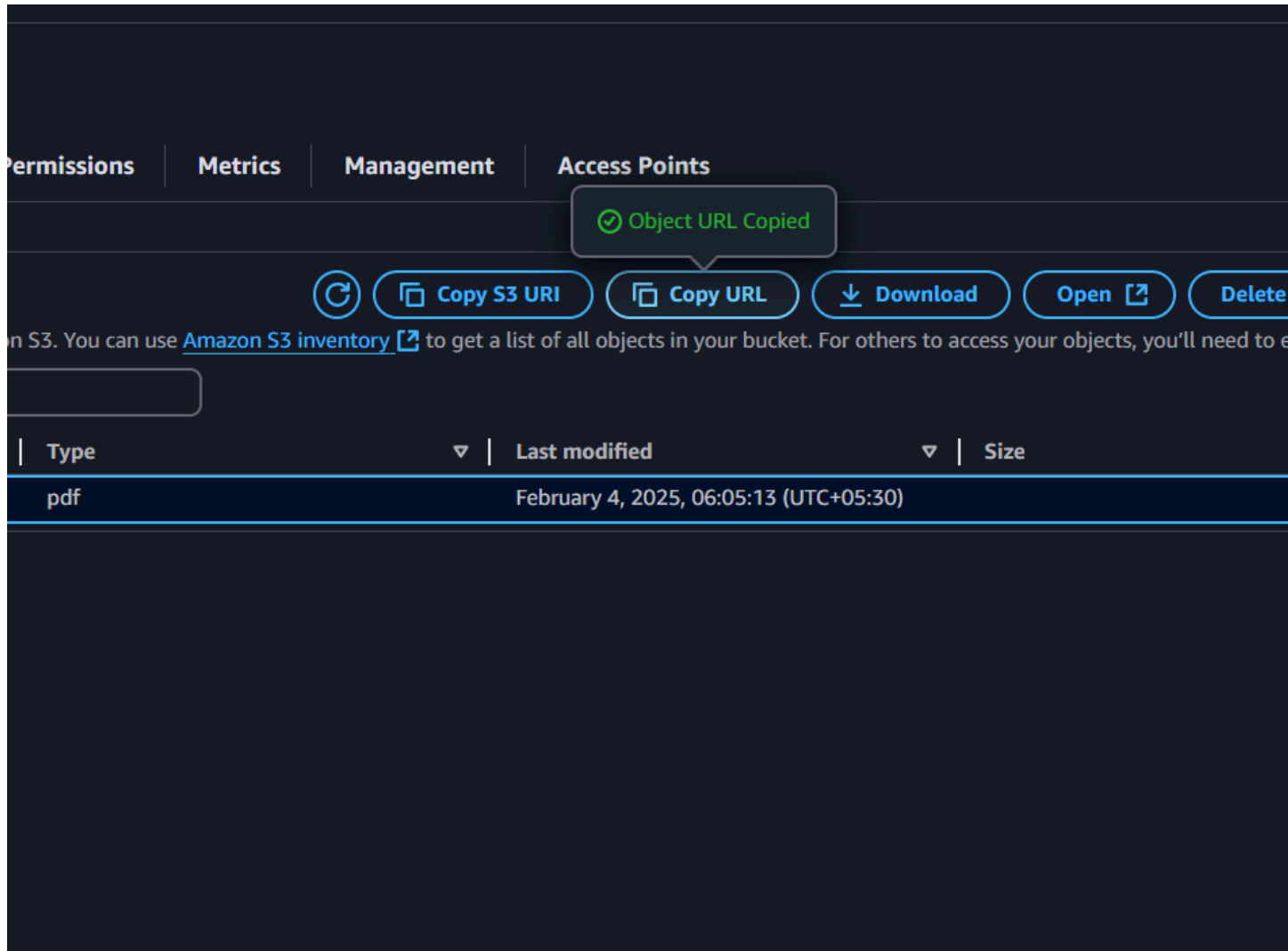
Go to your bucket's **Permissions** tab.

Under **Block Public Access**, enable **Block all public access**.
Save the changes.



Using AWS CLI:



```
aws s3api put-bucket-public-access-block --bucket  
asmybk --public-access-block-configuration "  
{\"BlockPublicAcls\":true,\"IgnorePublicAcls\":true,\"Blo  
ckPublicPolicy\":true,\"RestrictPublicBuckets\":true}"
```



TEST IT BY COPYING THE URL AND PAST IT TO YOUR WEB

→ ↺ asmybk.s3.us-east-1.amazonaws.com/POC-10.pdf

☰ POC- 1 / 5 | 100% + | 📄 ↻





Placement Empowerment Program
Cloud Computing and DevOps Course

Create an IAM role with permissions.
Assign the role to your VM and
verify its effect by attempting
permitted/forbidden actions.

Notes: Akshar Reddyan M.B. | Department: CSE

1



Introduction

In this POC, we will create an IAM role with permissions to access S3 buckets and EC2 instances. We will then assign this role to an EC2 instance and verify its effect by attempting permitted/forbidden actions.

Objective

- Create an IAM role with permissions to access S3 buckets and EC2 instances.
- Assign the IAM role to an EC2 instance and verify its effect by attempting permitted/forbidden actions.
- Verify the permissions by attempting permitted/forbidden actions.



Prerequisites


- Access to an AWS account.
- Access to an EC2 instance.

Steps to Follow

- Create the IAM Role for S3 Access
- Assign IAM Role to EC2 Instance

Verify Permissions





Placement Empowerment Cloud Computing and