CloudFolks

Amazon S3
Simple Storage Service

Public Access

1 Introduction

1. Public access means anyone on the internet can view or interact with the contents of your S3 bucket.
2. This can be useful for hosting static websites or sharing files, but it also poses a security risk if not managed carefully.
3. Two Ways to Grant Public Access
   1. ACLs (Access Control Lists)
      1. These are permissions associated with individual objects within your bucket.
      2. Example — An ACL might say Allow public read access to this specific image file.
      3. Important Note
         1. ACLs are an older way of managing permissions and are less flexible than bucket policies.
         2. AWS recommends using bucket policies whenever possible.
   2. Bucket Policies
      1. These are JSON documents attached to your S3 bucket.
      2. They define who can do what with your bucket and its contents.
      3. Example

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

2 Block Public Access

1. 1
2. 1
3. 25
3. Here we have 4 options
   1. Block public access to buckets and objects granted through new access control lists (ACLs)
      1. Prevents Creation of new public ACLs on buckets and objects
      2. Does not Affect existing public ACLs
   2. Block Public Access to Buckets and Objects Granted Through Any ACLs
      1. Prevents Public access to buckets and objects even if allowed by existing or new ACLs
      2. Ensure no object is publicly accessible due to any ACL configuration.
      3. Stronger protection compared to blocking only new ACLs.
   3. Block public access to buckets and objects granted through new public bucket or access point policies
      1. Prevents Creation of new bucket policies that allow public access to the bucket or its objects.
      2. Prevents Creation of new access point policies that allow public access to objects through specific access points.
      3. Does not Affect existing public bucket or access point policies
   4. Block Public and Cross-Account Access to Buckets and Objects Through Any Public Bucket or Access Point Policies
      1. Public access — Completely blocks public access to buckets and objects even if a public bucket or access point policy exists.
      2. Cross-account access — Also blocks access from other AWS accounts if the access is granted through a public bucket or access point policy.
      3. Impose the strictest level of access control on S3 buckets and objects.
      4. Ensure that only authorized users and services within your own AWS account can access the resources.

3 Make an S3 Bucket or Object Public using Bucket Policy

1. Bucket policies are JSON-based access policies that provide a centralized way to manage permissions for buckets and the objects within them.
2. You can use these policies to grant public access to your S3 resources.
3. Bucket Policies — Example

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

1. Version — This specifies the version of the policy language.
2. Statement — This contains an array of individual statements.
3. Sid — This is an optional identifier for the statement
4. Effect — This specifies whether the statement allows or denies the action.
5. Principal — This specifies the entity to which the permission is granted. The asterisk ("*") means the permission is granted to everyone (i.e., it's public).
6. Action — This lists the specific action that is allowed or denied.