COURSEWARE

S3 Bucket Policies

Contents

Overview

S3 bucket polices allow us to control who and what can access objects in our S3 buckets.

Bucket Privacy

By default, S3 buckets are private, this means that only the root user has access to the bucket. For the majority of use cases this is sufficient, as the buckets will normally be used to save data from other applications.

Giving an S3 public access means that anybody with the URL for the bucket can access its contents, for hosting a static website this is ideal, however when you need to keep data private you need to keep your bucket private!

You can also control access to your Bucket, using these means you can set who has access, and what access they have.

`aws_s3_intro_1.png`

Security

A bucket policy is where we can define explicit access or denial of access to our data at a bucket level. These polices are written using JSON, meaning that we have very configurable policies with granular access.

An Access Control List (ACL) is how we can give explicit access or denial of access to our data for users from outside of our own AWS Accounts.

The permissions we can add are quite broad for example `Write Objects`.

Amazon recommends that you use Bucket Policies to apply permission to a bucket as ACL's are a legacy access control mechanism. If you are concerned with controlling who can access a bucket then make use of bucket policies to explicitly describe **who** has access, and **what** they can do.

Tutorial

For this task we will be modifying the bucket policy of an existing bucket.

Pre-Requisites

- An S3 Bucket with a file already uploaded.

Changing access

Using the Management Console select an existing bucket, ensure you have a file uploaded to the bucket.

Click the **Permissions** tab across the top.

For this task we will be momentarily allowing public access to the bucket, to do this, click the **Block public access** button.

Click the **Edit** button further down the page.

Ensure that the **Block *all* public access** checkbox is unticked.

Click the blue **Save** button.

You will need to type **confirm** into the box in order to apply this change, remember AWS recommends that you never make the contents of a bucket public.

Checking the object

Navigate back to the **Overview** tab.

Select the check box next to one of you objects.

In the pop-out window on the right hand side, click the **Object URL** Link.

Access Denied!, but you just enabled public access? The public access was provided to the **bucket**, not the objects in the bucket. To rectify this need to set the bucket policy.

Rectifying the issue

Navigate back to the **Overview** tab of the bucket.

Click the **Permissions** tab.

Now click the **Bucket Policy** button.

Copy the code below into the Bucket policy editor, ensure that you change the name of the bucket to reflect the current bucket you are working with.

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

Click the blue **Save** button.

Again navigate to the **Object URL** Link you tried earlier, you should see now that the file is rendered by your browser.

Clean-up

The last step is to undo everything we have done, you can delete the bucket policy, Block all Public Access or simply delete the bucket. Ensure that the contents of your bucket are once again private before moving on.

Exercises

There are no exercises for this module.