Introduction to Amazon Simple Storage Service (S3)

SPL-65 - Version 2.2.2

Overview

This lab introduces you to Amazon Simple Storage Service (Amazon S3) using the AWS Management Console.

Amazon Simple Storage Service (Amazon S3) is storage for the Internet. You can use Amazon S3 to store and retrieve any amount of data at any time, from anywhere on the web.

Topics Covered

By the end of this lab, you will be able to:

- Create a bucket in Amazon S3
- Add an object to your bucket
- Manage access permissions on an object
- Create a Bucket Policy
- Use bucket versioning

Task 1: Create a Bucket

In this task you will create an Amazon S3 bucket. Every object in Amazon S3 is stored in a bucket.

- In the **AWS Management Console**, on the **Services** menu, click **S3**.
- Click **Create bucket** then configure:
  - **Bucket name:**
  - Replace **NUMBER** with a random number
  - Leave **Region** at its default value

Selecting a particular region allows you to optimize latency, minimize costs, or address regulatory requirements. Objects stored in a region never leave that region unless you explicitly transfer them to another region.

The **Copy settings from an existing bucket** option can be used to make it easier to create buckets that use the same settings as another bucket. For this lab, you are not going to use this option.

- Click **Next**

You will be presented with the **(2) Configure options** dialog box.

- Read the short descriptions for the categories listed.

By default these properties are disabled. For this lab, you will enable versioning.

- For **Versioning**, Select **Keep all versions of an object in the same bucket**.
- Click **Next**

You will be presented with the **(3) Set permissions** dialog box.

- Examine the **Manage users** section. (Point to the information icons to view explanations.)

By default, the owner of a bucket has full permissions for the bucket and objects within the bucket.

- Examine the **Manage public permissions** section.

By default, there is no public read access to newly created buckets.

- Examine the **Manage system permissions** section.

Access logs contain details about requests to your S3 buckets. An access log record can contain a request type, the resource specified in the request, and the time and date the request was processed.

- Click **Next**
- Review the settings and then click **Create bucket**

If you receive an error stating **The requested bucket name is not available**, then click the first **Edit** link, change the bucket name and try again until it works.
You have now successfully created a bucket.

Task 2: Upload an Object to the Bucket

Now that you have created a bucket, you are ready to store objects.
An **object** can be any kind of file: a text file, a photo, a video, a zip file, etc.
When you add an object to Amazon S3, you have the option of including **metadata** with the object and setting **permissions** to control access to the object.
In this task you will upload objects to your S3 bucket.

- Right-click this link and download the picture to your computer: Sheep.jpg
- In the **S3 Management Console**, click your bucket that starts with the name *mybucket*.
- Click **Upload**

This launches an upload wizard that will assist you in uploading files. Using this wizard you can upload files, either by selecting them from a file chooser or by dragging them to the S3 window.

- At the **(1) Select files** dialog box, click **Add files** then configure:
- Browse to and select the **Sheep.jpg** file that you downloaded
- Click **Upload**

You can watch the progress of the upload from within the Transfer panel at the bottom of the screen. Since this is a very small file, you might not see the transfer. Once your file has been uploaded, it will be displayed in the bucket.

Task 3: Make Your Object Public

In this task you will configure permissions on your object so that it is publicly accessible.

First, you will attempt to access the object to confirm that it is private by default.

- Click the **Sheep.jpg** file.
- Copy the S3 **Link** displayed at the bottom of the window.

The link should look similar to this: *https://s3-us-west-2.amazonaws.com/mybucket45647467/Sheep.jpg*

- Open a new web browser tab, paste the link into the address field, and hit enter.

You should receive an **Access Denied** error. This is because objects in Amazon S3 are private by default.

```
- <Error>
    <Code>AccessDenied</Code>
    <Message>Access Denied</Message>
    <RequestId>FE0D5225A793BDFC</RequestId>
  - <HostId>
      08+RKXYE0qYI5C2ShCtZgoyqQwsXYoZTtLzITvu7rQm2daqKgZRsDd6V3ID69WSsrMd+xcB+moY=
    </HostId>
  </Error>
```

You will now configure the object to be publicly accessible.

- Keep this browser tab open, but return to the web browser tab with the S3 Management Console.

- In the **S3 Management Console**, click the **Permissions** tab, then configure:
- Under the **Public access** section, select **Everyone**.
- Select **Read object**
- Click **Save**
- Return to the browser tab that displayed **Access Denied** and refresh the page.

Your picture should be now be displayed because it is publicly accessible.

- Close the web browser tab that is displaying your picture and return to the web browser tab with the Amazon S3 Management Console.

In this example, you granted read access only to a specific object. If you wish to grant access to an entire bucket, you would use a **Bucket Policy**.

Task 4: Create a Bucket Policy

A **Bucket Policy** is a set of permissions associated with an Amazon S3 bucket. It can be used to control access to a whole bucket or to specific directories within a bucket.
You will now upload a new file and verify that it is not publicly accessible.

- Right-click this link and download the picture to your computer: Eiffel.jpg
- In the S3 Management Console tab, click the name of your bucket at the top of the window.

- Click **Upload** and use the same upload process to upload the Eiffel.jpg file. This is the same upload process you used in task 2.

- Click on the **Eiffel.jpg** name.
- Copy the S3 **Link** displayed at the bottom of the window.
- Open a new web browser tab, paste the link into the address field, and then press **Enter**.

Once again, **Access Denied** will be displayed. You will now configure a Bucket Policy to grant access to *all* objects in the bucket without having to specify permissions on each object individually.

- Keep this browser tab open, but return to the web browser tab with the S3 Management Console.

- Click the name of your bucket at the top of the window.

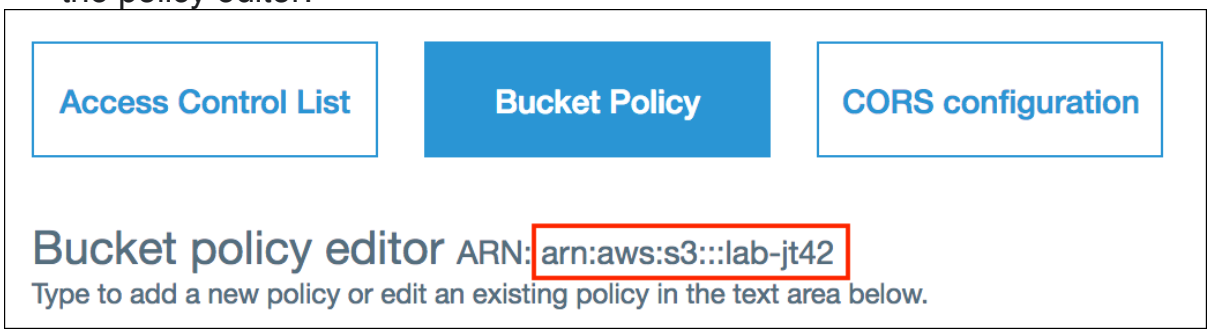
You should see a list of the objects in your bucket. If not, navigate back to your bucket so that you see the list of objects you have uploaded.

- Click the **Permissions** tab.
- In the **Permissions** tab, click **Bucket Policy**

A blank **Bucket policy editor** is displayed. Bucket policies can be created manually, or they can be created with the assistance of the **AWS Policy generator**.

Before creating the policy, you will need to copy the ARN (Amazon Resource Name) of your bucket.

- Copy the **ARN** of your bucket to the clipboard. It is displayed at the top of the policy editor:



It should look similar to: *arn:aws:s3:::lab-xxxx*

- Click the **Policy generator** link at the bottom of the page.

A new web browser tab will open with the AWS Policy Generator.

- In the **AWS Policy Generator** window, configure the following:
- **Select Type of Policy:** *S3 Bucket Policy*
- **Principal:**

This means that *anyone* will be able to perform the actions in the policy.

- **Actions:** *GetObject*

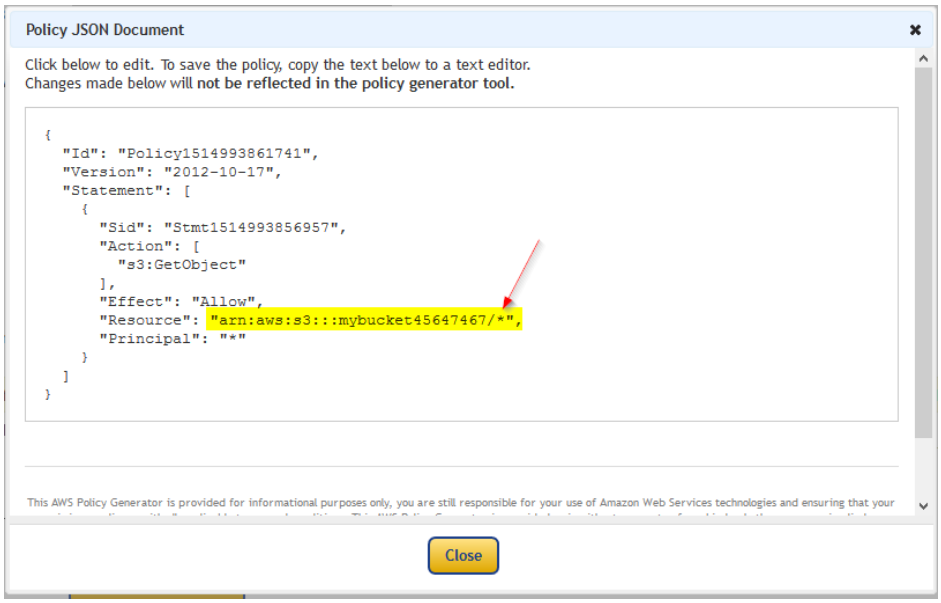
The get *GetObject* action grants permission for objects to be retrieved from Amazon S3.

- **Amazon Resource Name (ARN):** Paste the ARN that you previously copied.
- At the end of the ARN, append

The ARN should look similar to: *arn:aws:s3:::lab-xxx/**
An Amazon Resource Name (ARN) is a standard way to refer to resources within AWS. In this case, the ARN is referring to your S3 bucket. Adding /* to the end of the bucket name allows the policy to apply to all objects *within* the bucket.

- Click **Add Statement**.
- Click **Generate Policy**.

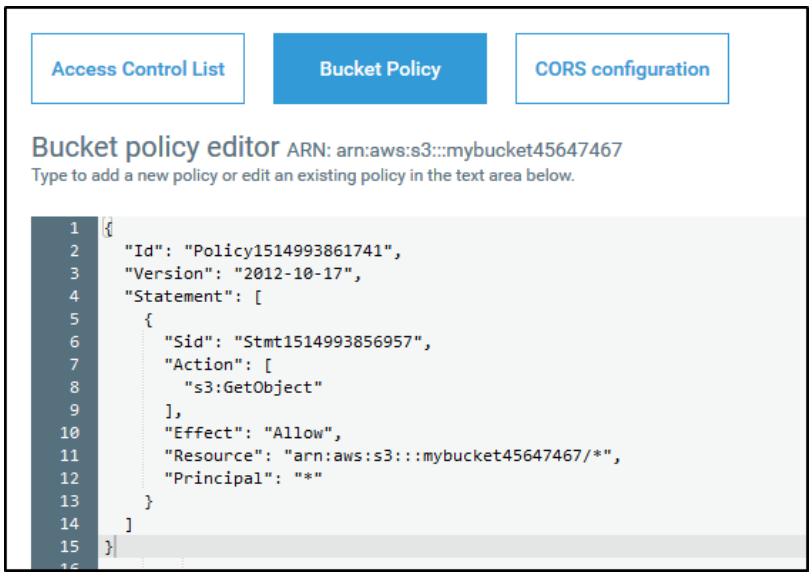
Your bucket policy is now displayed. It should look similar to:



Confirm that appears after your bucket name as highlighted in the above picture.

- Copy the policy to your clipboard.

- Close the web browser tab and return to the web browser tab with the **Bucket policy editor**.
- Paste the bucket policy into the **Bucket policy editor**.



- Click **Save**

You have just applied a bucket policy to your bucket. All objects in your bucket should now be publicly accessible.

- Return to the browser tab that displayed **Access Denied** and refresh the page.

You should now see a picture of the Eiffel Tower. This is because the Bucket Policy applies to the bucket *as a whole*, without having to grant individual permissions to each object individually.

- Keep this browser tab open, but return to the web browser tab with the S3 Management Console.

Task 5: Explore Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning you can easily recover from both unintended user actions and application failures. In this task, you will upload a different version of the Eiffel Tower picture.

- Right-click this link and save the picture to your computer using the same name: Eiffel.jpg

While this file has the same name as the previous file, it is a different picture.

- In the S3 Management Console, click the **Overview** tab.
- Click **Upload** and use the same upload process to upload the new Eiffel.jpg picture.

This is the same upload process you used in task 2.

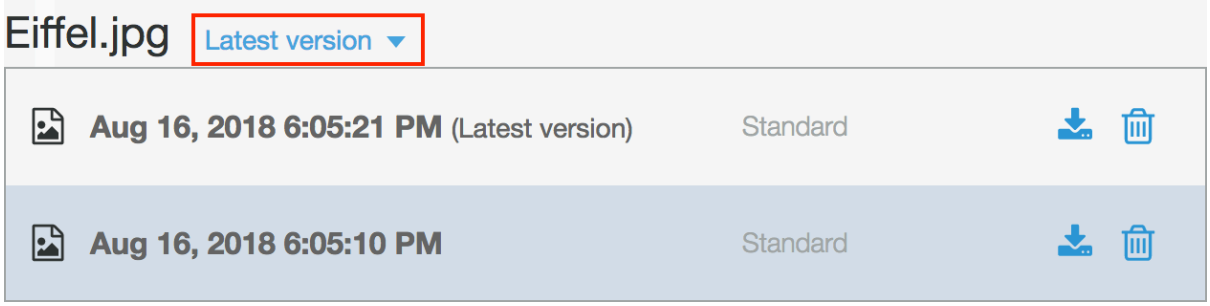
- Go to the browser tab that has the picture of the Eiffel tower.

- Take note of the contents of the picture, then refresh the page.

You should now see a different picture. Amazon S3 always returns the *latest version*of an object if a version is not otherwise specified.
You can also obtain a list of available versions in the S3 Management Console.

- Close the web browser tab displaying the Eiffel Tower.

- In the Amazon S3 Management Console, click the name of the **Eiffel.jpg** object.
- Click **Latest version** beside the object name and select the bottom version (which is *not* the latest version):



- Click **Open**

You should now see the first version of the picture using the S3 Management Console.

However, if you try to access the older Eiffel Tower picture using the S3 URL link, you will receive an access denied message. This is expected in the lab because you only have permission to access the latest version of the object. In order to access the previous version of the object, you need to update your bucket policy to have the **"s3:GetObjectVersion"** permission. Here is an example bucket policy that allows you to access the older version using the link.

```
{
  "Id": "Policy1515004677493",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1515004675884",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::mybucket456456456/*",
      "Principal": "*"
    }
  ]
}
```