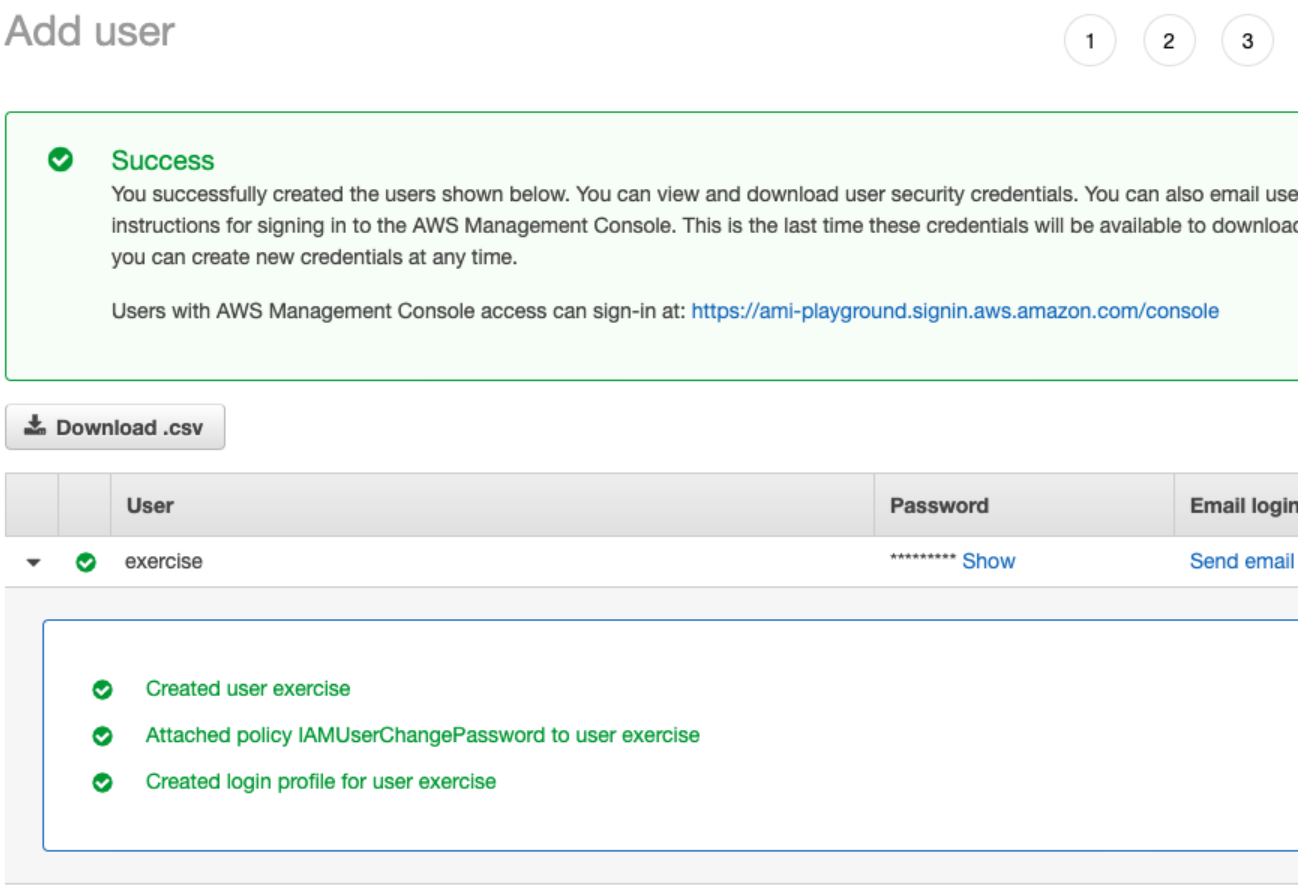
While logged in as the **manager** user account via an incognito/private browser window, create the **exercise**IAM user as follow:

1. Navigate to the IAM console
2. From the left sidebar menu, click on Users
3. Click on **Add user** button and name it **exercise-user**
4. Select the option **AWS Management Console access** and uncheck the **Require password reset** option
5. Skip the **Set permissions** and create the user by clicking through the **Next** button
6. Note the password for the **exercise** user and click the **Close** button




### Granting Permissions For The Exercise User

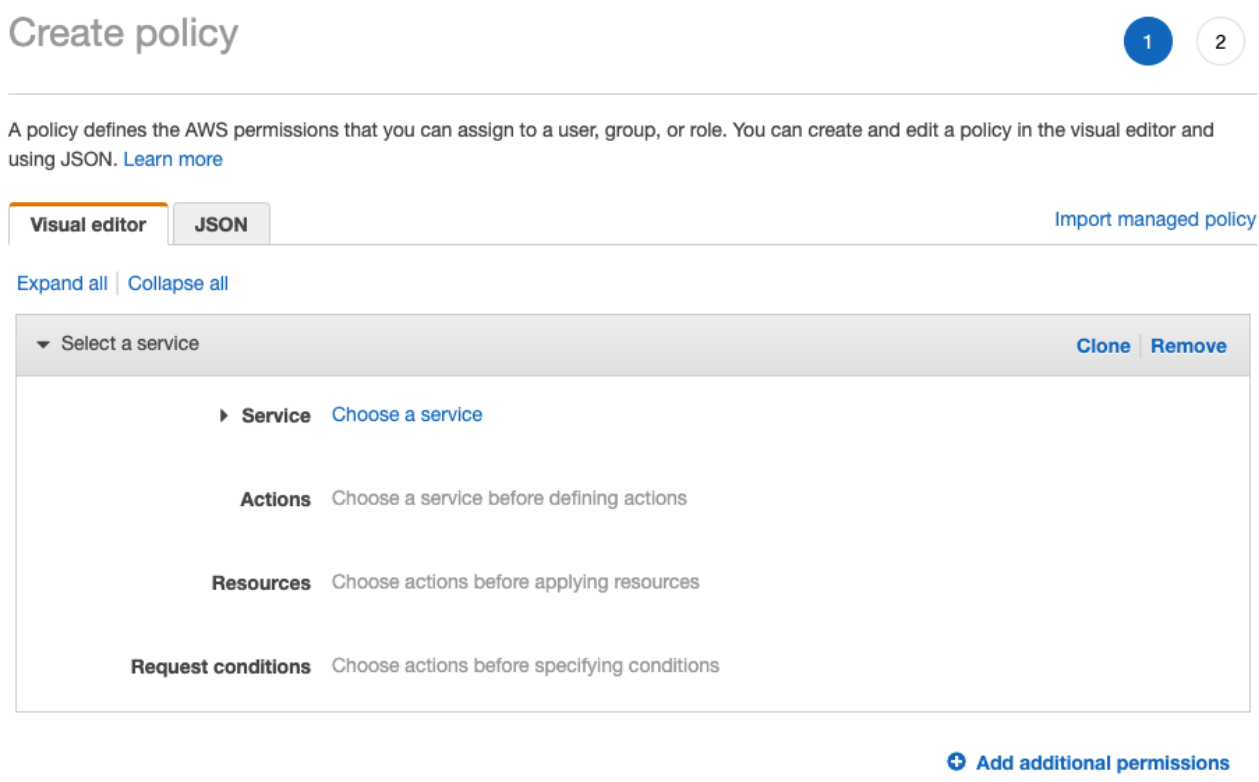
In order for the **exercise** user to be able to download/upload content on the S3 bucket we need the following permissions:

**ListAllMyBuckets** - allow listing all the buckets in the console **ListBucket** - allow listing a specific bucket content **GetObject** - allow retrieving a file

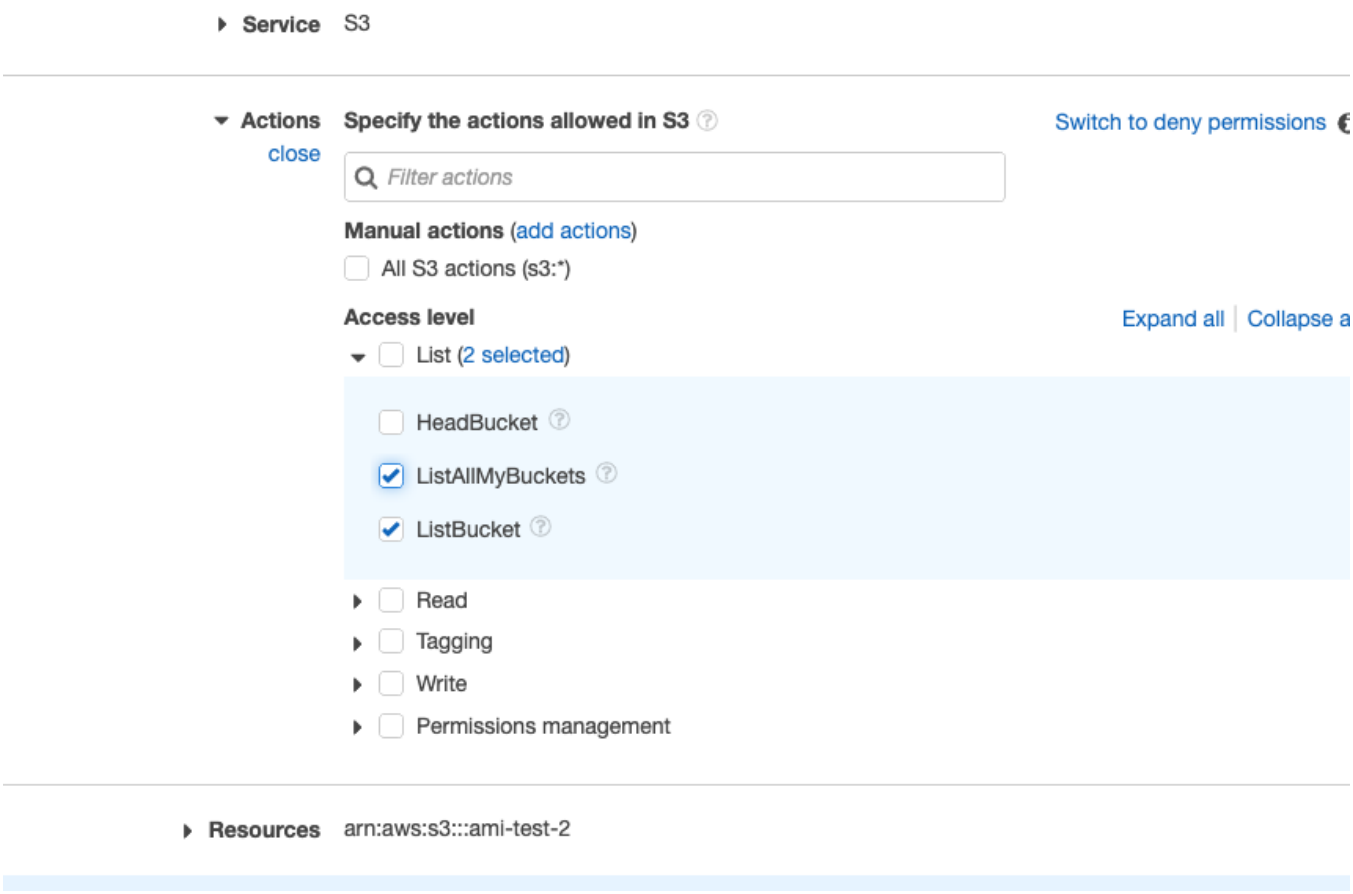
**Note:** for upload permission we would need the **PutObject** permission (this is not a requirement for this exercise)

## Creating an IAM Inline Policy

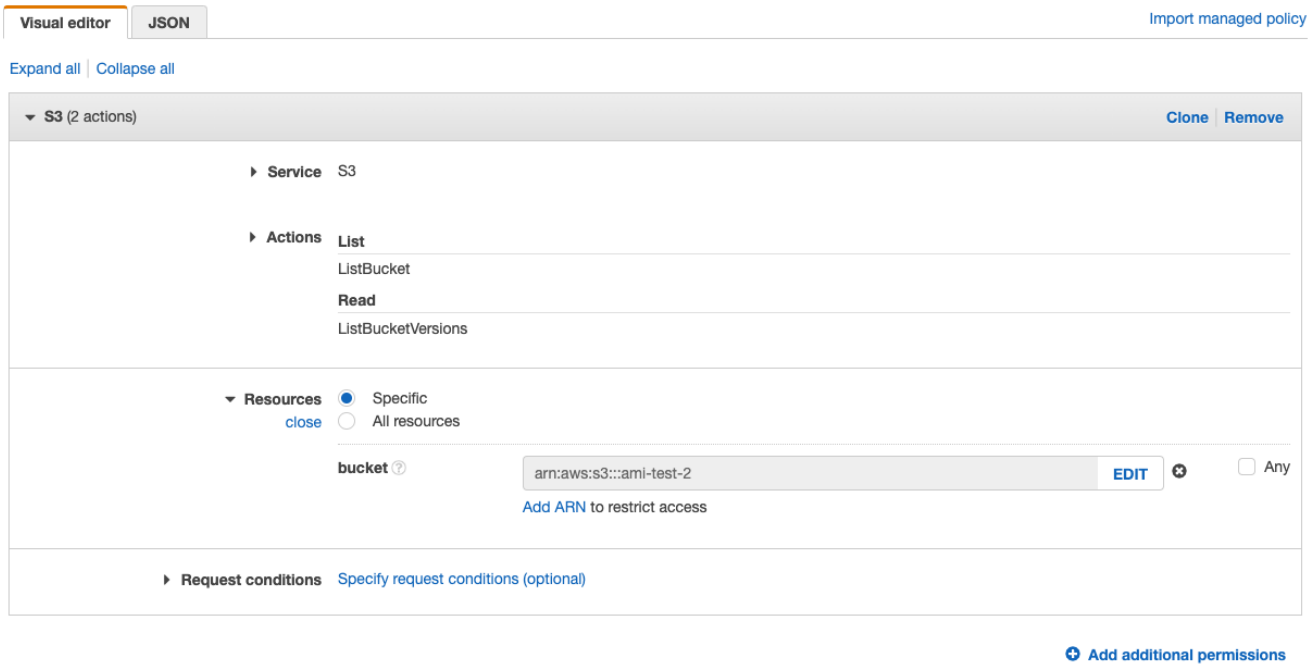
1. Click the **exercise** user to get into the user details
2. Click the **+ Add inline policy** link to create a new policy

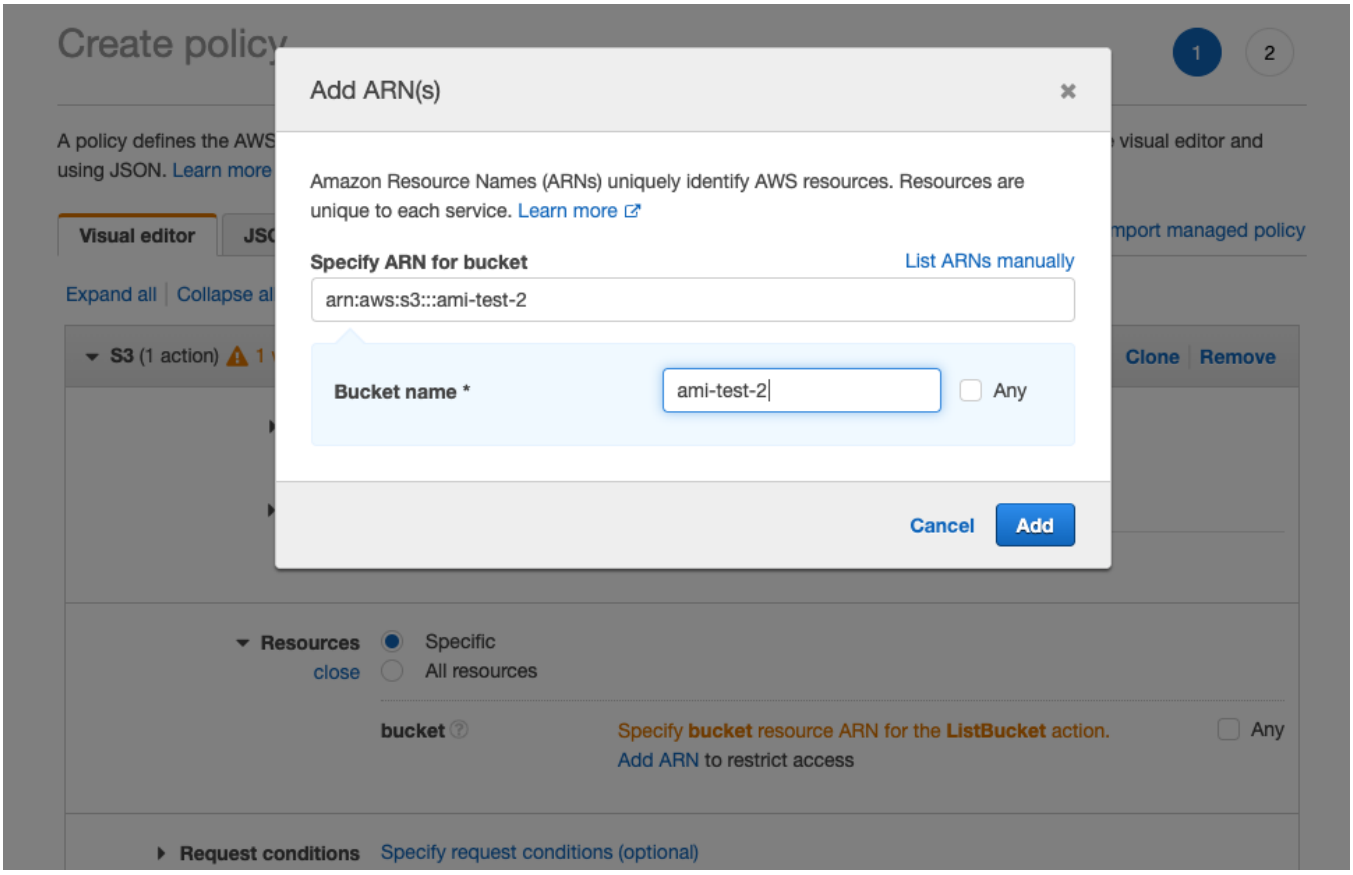



3. In the **Service** field Select **S3**
4. Type **ListBucket** in the **Actions** field and select **ListBucket** as well as **ListAllMyBuckets**



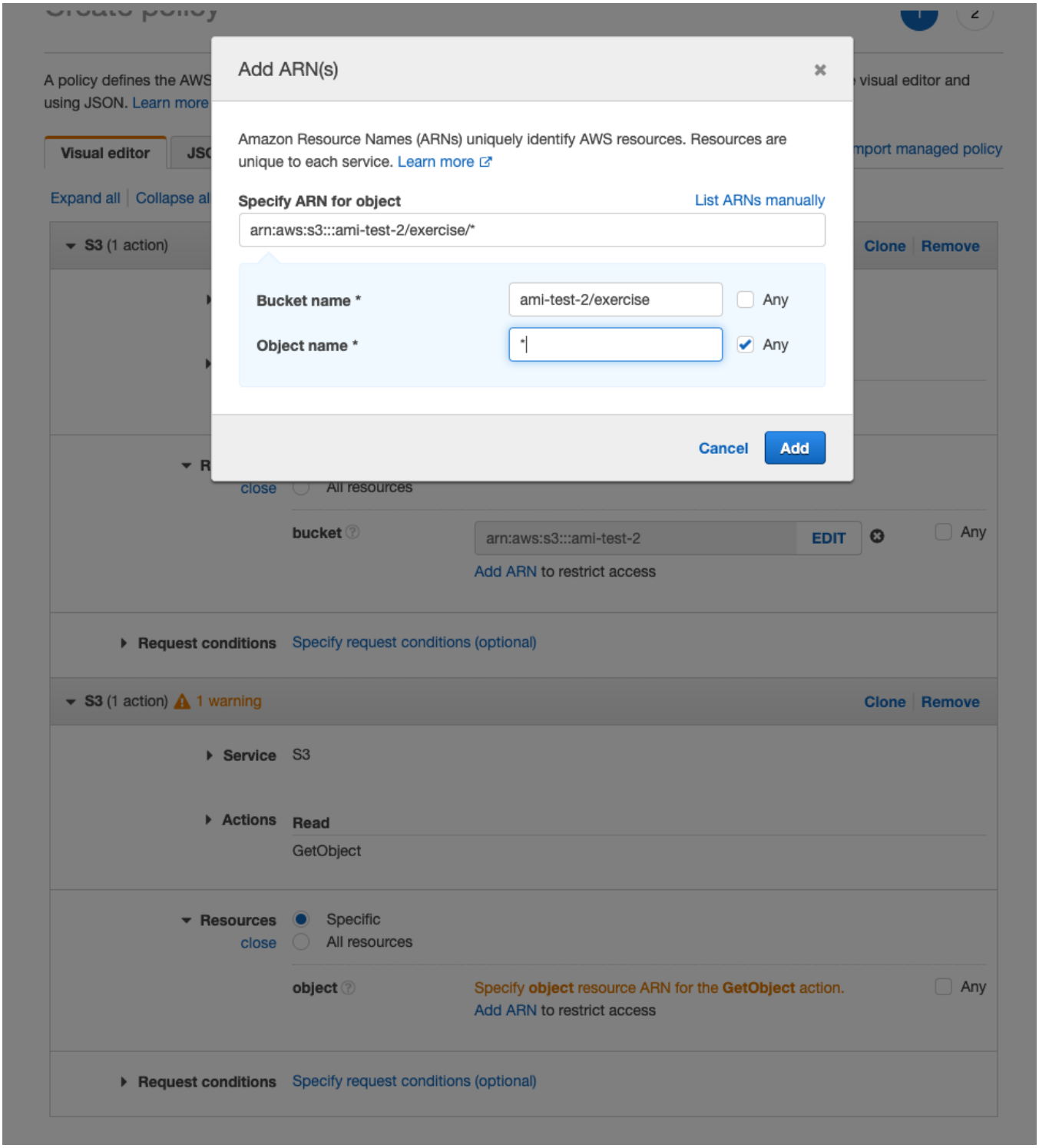

5. Under the **Resources**dropdown, select **Specific** and set the bucket name to the bucket name you have created previously



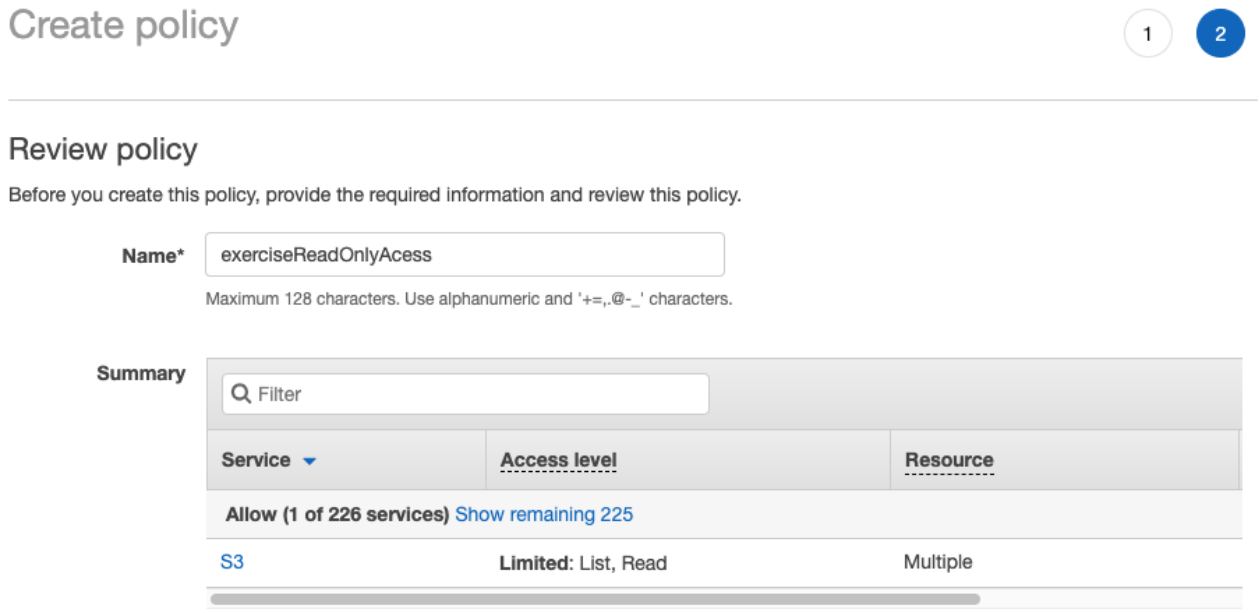



### Read-Only (GetObject) Permissions

1. Click the **Add additional permissions** link
2. Select **S3** at the **Service** field and type **GetObject** in the **Actions** field
3. Select the **GetObject** option
4. Now let's limit the user access to the **exercise** folder, expand the **Resources** section and click on **Add ARN** link
5. Fill in the bucket name and in the object field type the folder name **exercise**
6. Since objects are just files and not folder the bucket name will hold the folder name to access, so click on the **Any** checkbox to grant read on any object in the **exercise** folder

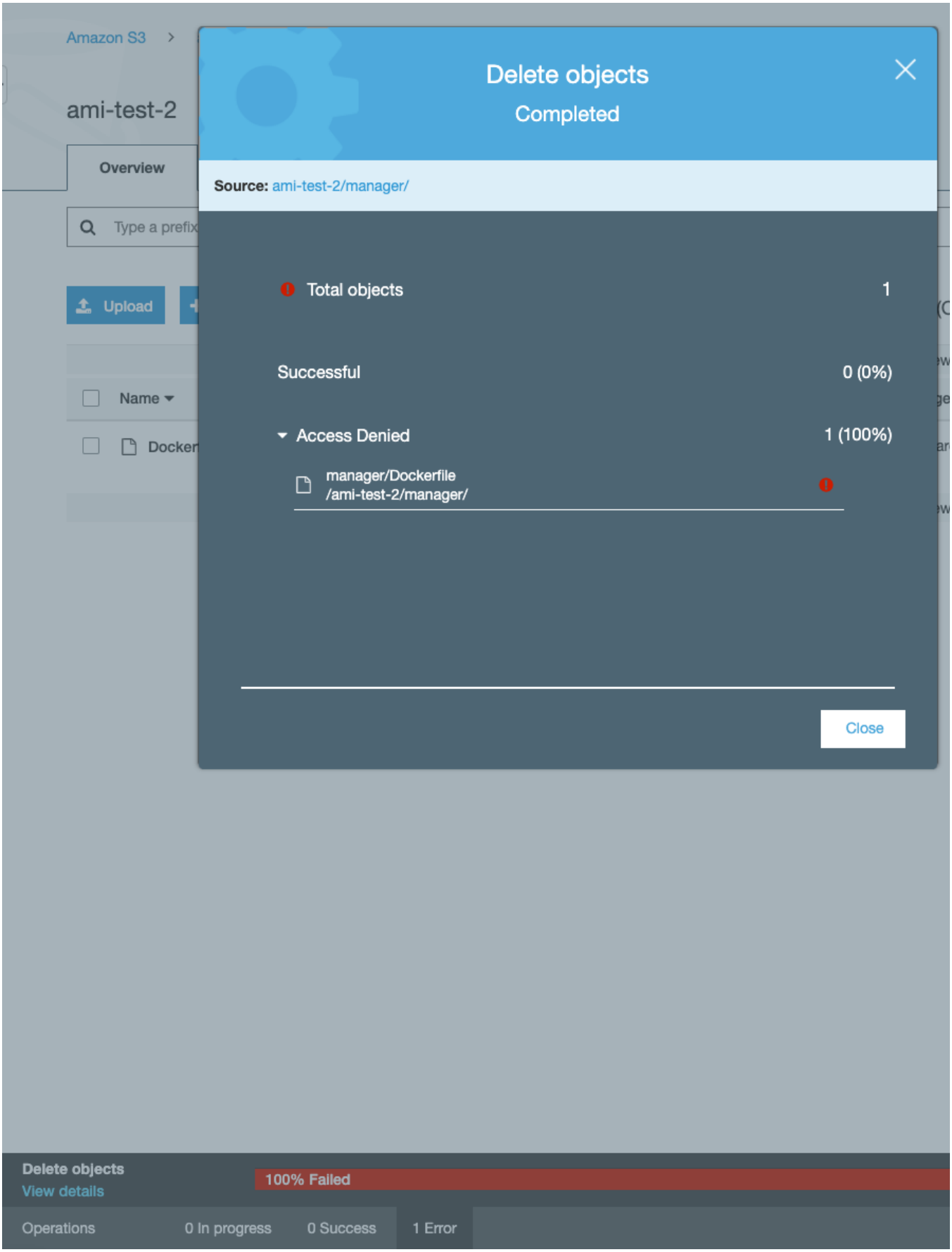



7. Name the policy **exerciseReadOnlyAccess** and create it




## Part-2: Validation

1. Using the **exercise** user in a new incognito/private browser window log in to the AWS console
2. Navigate to the S3 bucket and click on the bucket you have created
3. You should be able to see both folders **manager** and **exercise** - you should only be able to download any file from the **exercise** folder and none from the **manager** folder
4. Click on the **exercise** folder and select a file, try to delete it from the **Actions** button and verify you get a **permission denied** error


Amazon S3
ami-test-2
Overview
Type a prefix
Upload
Name
Docker
Delete objects
Completed
Source: ami-test-2/manager/
Total objects 1
Successful 0 (0%)
Access Denied 1 (100%)
manager/Dockerfile
/ami-test-2/manager/
Close
Delete objects
View details
100% Failed
Operations
0 In progress
0 Success
1 Error