

While logged in as the **manager** user account via an incognito/private browser window, create the **exerciseIAM** 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

Add user

1

2

3



Success

You successfully created the users shown below. You can view and download user security credentials. You can also email use instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://ami-playground.signin.aws.amazon.com/console>



Download .csv

	User	Password	Email login
▼	✓ exercise	***** Show	Send email

- ✓ Created user exercise
- ✓ Attached policy IAMUserChangePassword to user exercise
- ✓ Created login profile for user exercise

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

Create policy

1

2

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor

JSON

[Import managed policy](#)[Expand all](#) | [Collapse all](#)

▼ Select a service

[Clone](#) | [Remove](#)► **Service** [Choose a service](#)**Actions** Choose a service before defining actions**Resources** Choose actions before applying resources**Request conditions** Choose actions before specifying conditions[+ Add additional permissions](#)

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

► **Service** S3

▼ **Actions** Specify the actions allowed in S3 ?

close

[Switch to deny permissions](#) €

Manual actions ([add actions](#))

☐ All S3 actions (s3:*)

Access level

[Expand all](#) | [Collapse a](#)

▼ ☐ List (2 selected)

☐ HeadBucket ?

☒ ListAllMyBuckets ?

☒ ListBucket ?

► ☐ Read

► ☐ Tagging

► ☐ Write

► ☐ Permissions management

► **Resources** arn:aws:s3:::ami-test-2

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

Visual editor

JSON

[Import managed policy](#)

[Expand all](#) | [Collapse all](#)

▼ S3 (2 actions)

Clone Remove

► Service S3

► Actions List

ListBucket

Read

ListBucketVersions

▼ Resources

close

☒ Specific

☐ All resources

bucket ?

arn:aws:s3:::ami-test-2

EDIT

✖

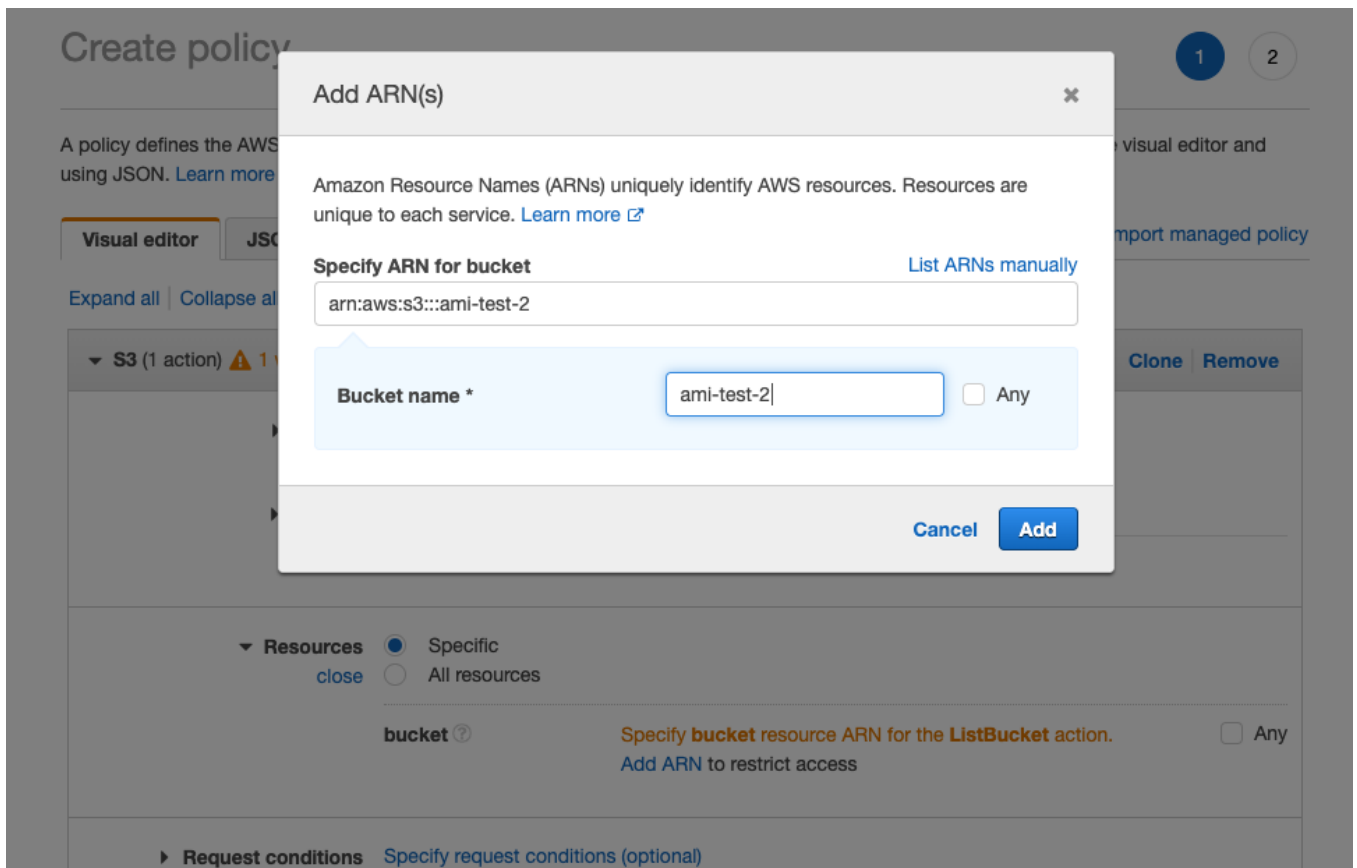
☐ Any

[Add ARN to restrict access](#)

► Request conditions

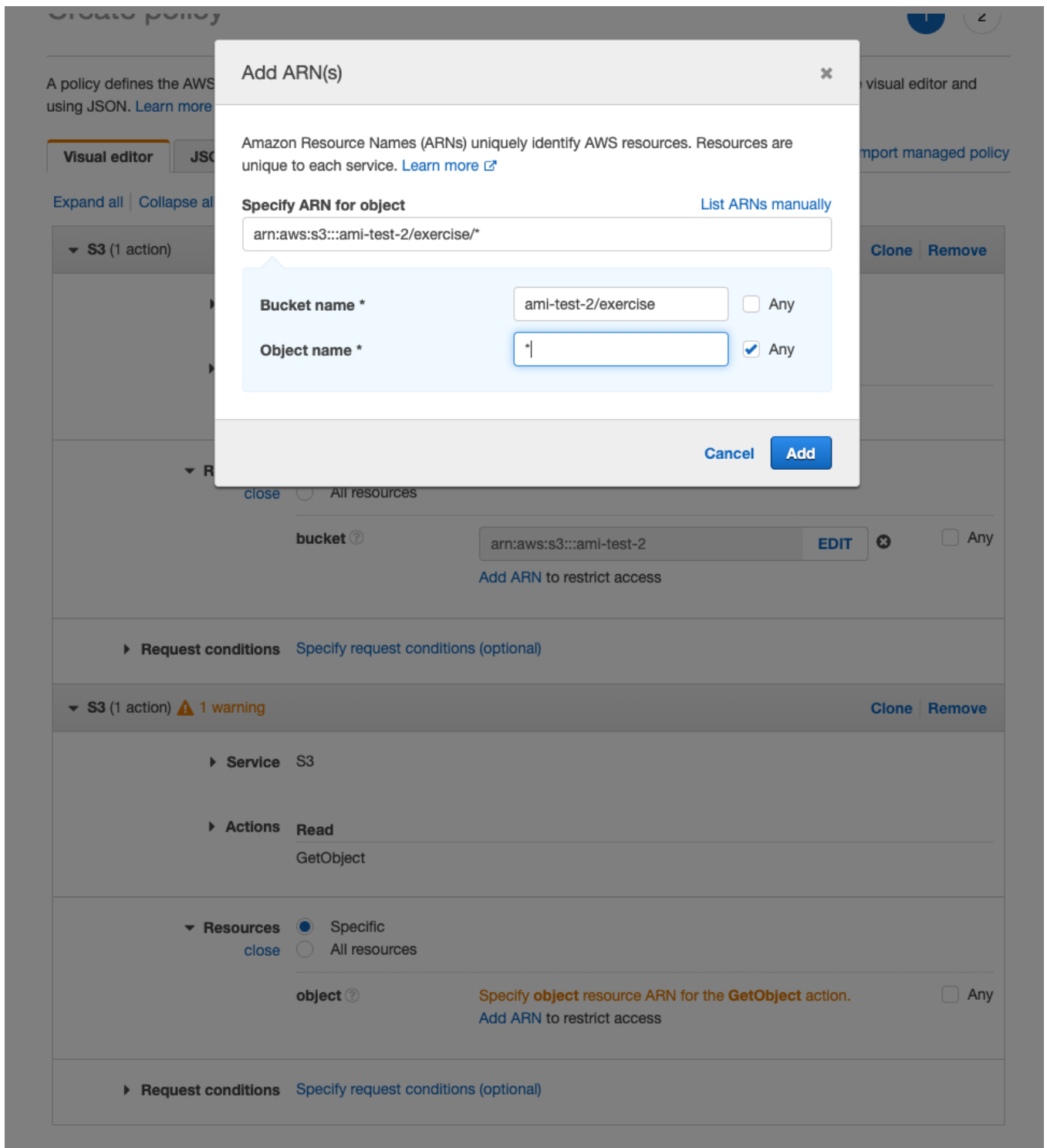
[Specify request conditions \(optional\)](#)

[Add additional permissions](#)



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

Create policy

1

2

Review policy

Before you create this policy, provide the required information and review this policy.

Name*
Maximum 128 characters. Use alphanumeric and '+=, @-_' characters.

Summary

Q Filter		
Service ▼	Access level	Resource
Allow (1 of 226 services) Show remaining 225		
S3	Limited: List, Read	Multiple

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

Q

Type a prefix

Upload

Name ▾

Docker

Delete objects

Completed

Source: [ami-test-2/manager/](#)

1

Total objects

0 (0%)

Successful

1 (100%)

Access Denied

manager/Dockerfile

/ami-test-2/manager/

Close

Delete objects

View details

100% Failed

Operations

0 In progress

0 Success

1 Error