

Activity 1: Recap on creating an IAM user and using permission boundaries	1
Activity 2: Creating an IAM Role for EC2 to only be able to list objects in a specific S3 bucket	5

Activity 1: Recap on creating an IAM user and using permission boundaries

For Step 4 of this activity, feel free to also experiment by attaching other AWS Managed policies to other services as well(As long as it isn't AdministratorAccess or PowerUserAccess)

1. Go to the IAM service in AWS
2. On the left, click on the "Users" tab and select "Create User"
3. Create a user with AWS Management console access and use a custom password. Also uncheck the tickbox which says "Users must create a new password at next sign-in - Recommended". So your page should look something like this below(without the blue box):

[IAM](#) > [Users](#) > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

Specify user details


User details

User name

jaz-demo-user

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☒ Provide user access to the AWS Management Console - *optional*
If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

 **Are you providing console access to a person?**

User type

☐ Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to t

☒ I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AW

Console password


☐ Autogenerated password
You can view the password after you create the user.

☒ Custom password
Enter a custom password for the user.

- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # \$

☐ Show password

☐ Users must create a new password at next sign-in - Recommended
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

 If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspa

4. In the set permissions page, select “Attach policies directly” and attach the following AWS Managed policies to this user:
 - a. [AmazonS3FullAccess](#)
 - b. [AmazonDynamoDBFullAccess](#)
5. And then select “Create User”

Review and create


Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name	Console password type	Require password reset
jaz-demo-user	Autogenerated	No

Permissions summary

< 1 >

Name 	Type	Used as
AmazonDynamoDBFullAccess	AWS managed	Permissions policy
AmazonS3FullAccess	AWS managed	Permissions policy

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel

Previous

Create user

- Open a new in-cognito or private browser. Here, we will log into the AWS account with the new user created. Type <https://255945442255.signin.aws.amazon.com/console> and key in the IAM user name and password that you just created.



Sign in as IAM user

Account ID (12 digits) or account alias

255945442255

IAM user name

jaz-demo-user

Password

.....

☐ Remember this account

Sign in

[Sign in using root user email](#)

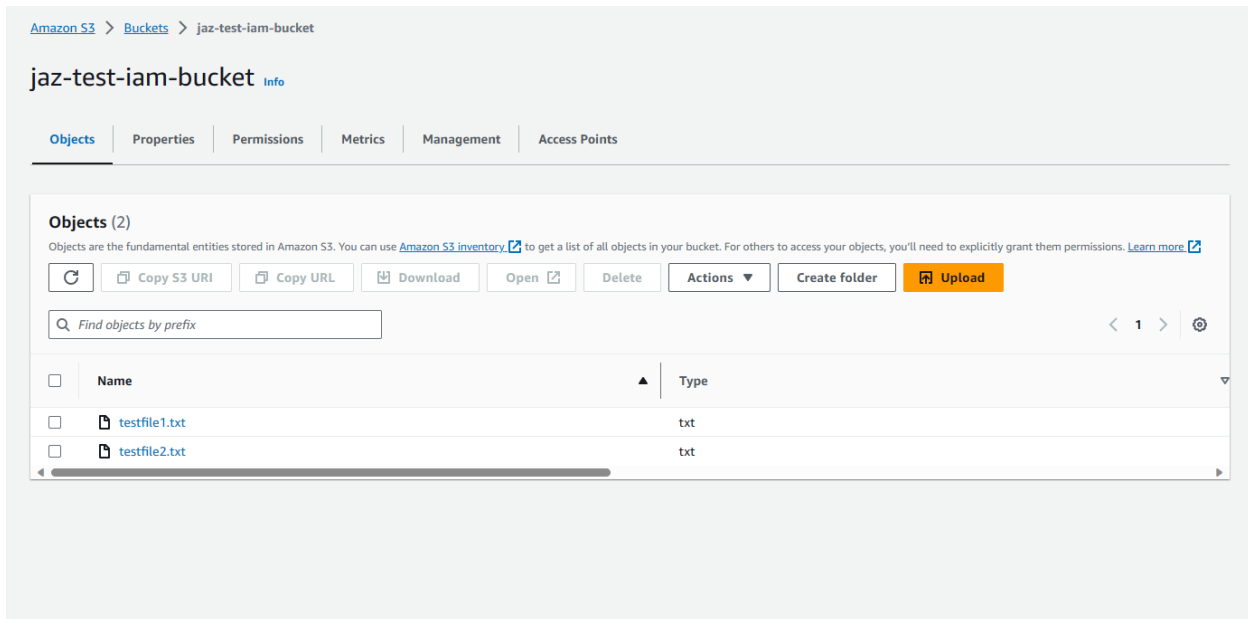
[Forgot password?](#)

- Once logged in, verify that the user has the relevant access to the services you have granted access to. In this case, S3 and DynamoDB based on the above example.
- Now we can attach a permission boundary to the above created user.

9. Go back to your original window / main aws user, and then attach the following permission boundary to the IAM user:
 - a. [AmazonS3FullAccess](#)
10. Recap: After attaching the above permission boundary, what would be the resulting permissions of the IAM user? Verify this by going back to your incognito window and logging in into your IAM user.
11. After this activity, remember to delete the IAM user that you created in this activity.

Activity 2: Creating an IAM Role for EC2 to only be able to list objects in a specific S3 bucket

1. Create a new S3 bucket with default configurations and upload some random files into it



2. Create EC2 with the following configurations:
 - a. Amazon Linux 2023 AMI
 - b. In any of the 2 public subnets in c4_sandbox_vpc
 - c. Attach “allow-ssh” security group
 - d. Select Advanced Details -> Metadata Version -> Set to V1 and V2(token optional)

Metadata version [Info](#)

V1 and V2 (token optional)

- e.
3. In this case, since we want to restrict our EC2 only to a specific bucket, we cant use AWS Managed policies anymore. We have to create our own custom policy to achieve this.
 4. Go to IAM service -> Click on policies on the left and select “Create Policy”
 5. For the services, Select S3 and check “ListAllMyBuckets” and “ListBucket”. When you select “ListBucket”, it would automatically prompt you to select “All” or “Specific.” In this case, we would select “Specific” and then select “Add Arns”. Then we would input the name of the S3 bucket we created in step 1. So should look something like this:

▼ S3

Allow

2 Actions

📄

🗑️

Specify what actions can be performed on specific resources in [S3](#).

▼ Actions allowed

Specify actions from the service to be allowed.

🔍 Filter Actions

Effect

☒ Allow
 ☐ Deny

Manual actions | [Add actions](#)

☐ All S3 actions (s3:*)

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

▼ List (Selected 2/12)

☐ All list actions

☐ ListAccessPoints [Info](#)

☒ ListBucket [Info](#)

☐ ListJobs [Info](#)

☐ ListStorageLensConfigurations [Info](#)

☐ ListAccessPointsForObjectLambda [Info](#)

☐ ListBucketMultipartUploads [Info](#)

☐ ListMultipartUploadParts [Info](#)

☐ ListStorageLensGroups [Info](#)

☒ ListAllMyBuckets [Info](#)

☐ ListBucketVersions [Info](#)

☐ ListMultiRegionAccessPoints [Info](#)

☐ ListTagsForResource [Info](#)

► Read (54)

► Write (45)

► Permissions management (15)

► Tagging (12)

▼ Resources

Specify resource ARNs for these actions.

☐ All
 ☒ Specific

bucket [Info](#)

arn:aws:s3:::jaz-test-iam-bucket

✎

🗑️

☐ Any

[Add ARNs](#) to restrict access.

- Click on next and give your IAM policy a meaningful name and then click on create policy. Example of my policy below:

[IAM](#) > [Policies](#) > jaz-test-ec2-s3-policy

jaz-test-ec2-s3-policy [Info](#)

[Delete](#)

Policy details

Type	Creation time	Edited time	ARN
Customer managed	November 17, 2023, 23:57 (UTC+08:00)	November 17, 2023, 23:57 (UTC+08:00)	arn:aws:iam::255945442255:policy/jaz-test-ec2-s3-policy

[Permissions](#) | [Entities attached](#) | [Tags](#) | [Policy versions \(1\)](#) | [Access Advisor](#)

Permissions defined in this policy [Info](#) [Edit](#) [Summary](#) [JSON](#)

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Allow (1 of 385 services) [Show remaining 384 services](#)

Service	Access level	Resource	Request condition
S3	Limited: List	Multiple	None

- Click on Roles on the left and select “Create Role”
- For service or use case, Select “EC2” and then click next
- Look for the policy you created in the search tab provided, and then select your policy

[IAM](#) > [Roles](#) > Create role

Step 1
[Select trusted entity](#)

Step 2
Add permissions

Step 3
Name, review, and create

Add permissions [Info](#)

Permissions policies (1/1153) [Info](#) [Refresh](#)

Choose one or more policies to attach to your new role.

[X](#) [Filter by Type](#) [All types](#) 2 matches [<](#) [1](#) [>](#) [Settings](#)

☒ [jaz-test-ec2-s3-policy](#)

☐ [jazeel-temp-user-2.6-policies](#)

[Set permissions boundary - optional](#)

[Cancel](#) [Previous](#) [Next](#)

- Click on next, then give your role a meaningful and unique name as well. You should have something like this:

[EC2](#) > [Instances](#) > [i-0a42f29a5140eb4d8](#) > Modify IAM role

Modify IAM role [Info](#)

Attach an IAM role to your instance.

Instance ID

 [i-0a42f29a5140eb4d8](#) (jaz-access-s3)

IAM role

Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

jaz-test-ec2-s3-role ▼



[Create new IAM role](#) 

Cancel

Update IAM role

14. Now we just need to verify the permissions are right.
15. Connect to your EC2 instance to run the following commands:
 - a. `aws s3 ls`
 - b. `aws s3 ls s3://name-of-the-bucket-you-created-in-step-1`
 - c. `aws s3 ls s3://other-s3-buckets-in-the-account`

```
[ec2-user@ip-10-0-101-183 ~]$ aws s3 ls s3://jaz-test-iam-bucket
2023-11-17 15:07:41          0 testfile1.txt
2023-11-17 15:07:41          0 testfile2.txt
[ec2-user@ip-10-0-101-183 ~]$ aws s3 ls s3://hangyong
An error occurred (AccessDenied) when calling the ListObjectsV2 operation: Access Denied
[ec2-user@ip-10-0-101-183 ~]$
```