

Amazon S3 - How to Add IAM policy permissions

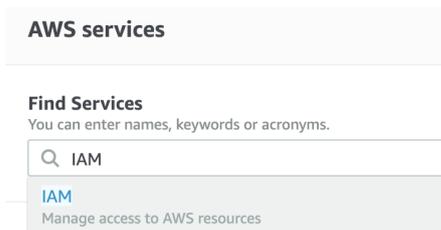
Last Modified on 03/16/2020 3:18 pm EDT

To provision an instance with the Amazon S3 connector successfully, you need to add the required IAM policy permissions to Amazon S3.

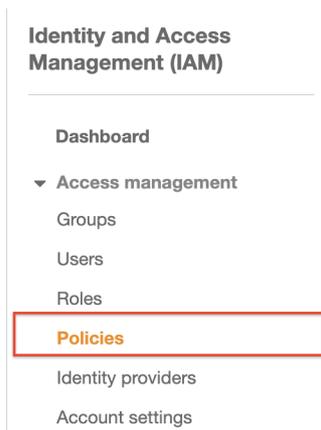
Note: It returns a 403 if the 's3:ListBucket' permissions are not enabled.

Here's how you can add the required permissions.

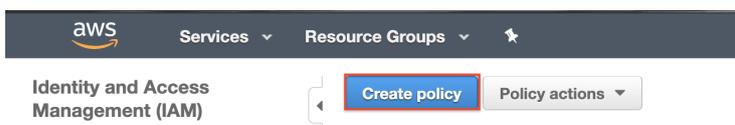
1. Via a web browser, go to <https://aws.amazon.com/console/>
2. Sign in to Amazon Web Services using your credentials.
3. Once logged in, enter IAM in the search bar.



4. Click 'Policies' on the Navigation panel to your left.



5. Click on 'Create Policy'.



6. Add 's3:ListBucket' as the action and your bucket as the resource.

Visual editor JSON

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": "s3:ListBucket",
8       "Resource": "arn:aws:s3:::test-bucket"
9     }
10  ]
11 }

```

- Click 'Review Policy'.
- On the console that appears, review your policy. Click 'Create Policy'.

Review policy

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

Description
Maximum 1000 characters. Use alphanumeric and '+,=,@,_' characters.

Summary

Service	Access level	Resource	Request condition
Allow (1 of 201 services) Show remaining 200			
S3	Limited: List	BucketName string like test-bucket	None

* Required

[Cancel](#) [Previous](#) [Create policy](#)

- On the navigation panel, click 'Users'.

Identity and Access Management (IAM)

▼ AWS Account (830413348874)

- Dashboard
- Groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings
- Credential report

- Select a User and click on 'Add Permissions'.

Summary

Delete user

User ARN [redacted]

Path /

Creation time [redacted]

Permissions Groups Tags Security credentials Access Advisor

Permissions policies

Get started with permissions

This user doesn't have any permissions yet. Get started by adding the user to a group, copying permissions from another user, or attaching a policy directly. [Learn more](#)

Add permissions

Add inline policy

11. Attach the newly created policy to the user.

Add permissions to jimmyce

1 2

Grant permissions

Use IAM policies to grant permissions. You can assign an existing policy or create a new one.

Add user to group

Copy permissions from existing user

Attach existing policies directly

Create policy

Refresh

Filter policies [dropdown] [input: Require] Showing 1 result

Policy name	Type	Used as
Required-Permission	Customer managed	None

Once you have added the policy to the user, you can provision an instance with the Amazon S3 connector successfully.