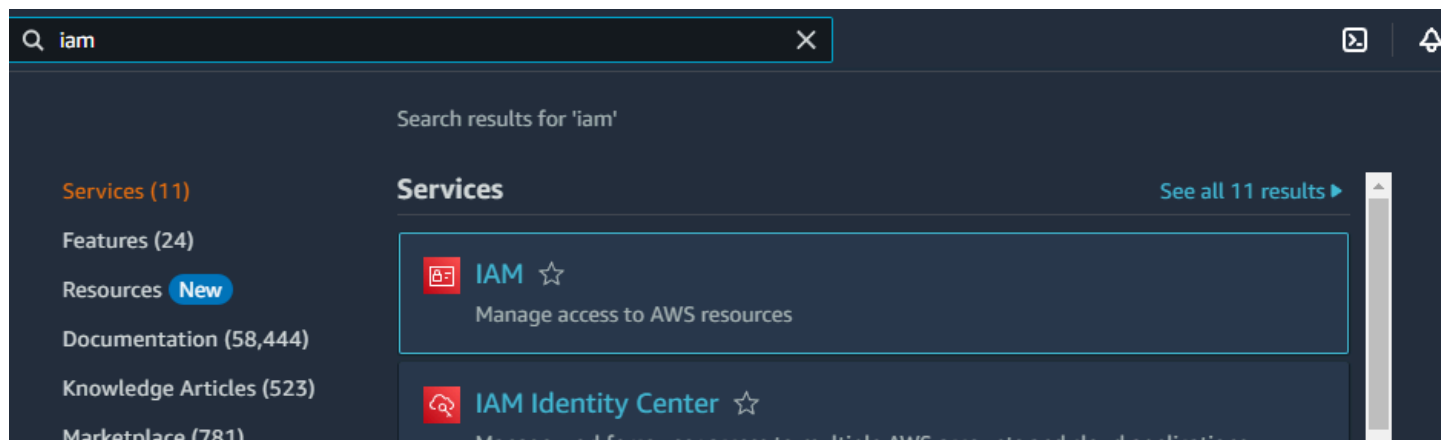


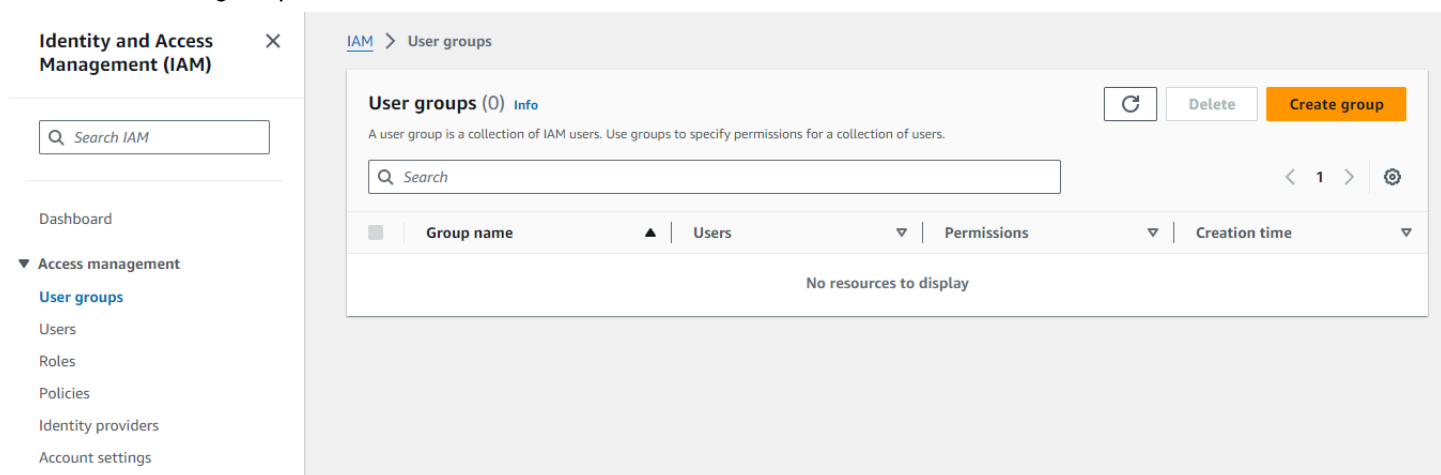
Create IAM User

- Create user group
- Create policy and attach to group
- Create user and add to group
- Create access keys

Select the IAM service

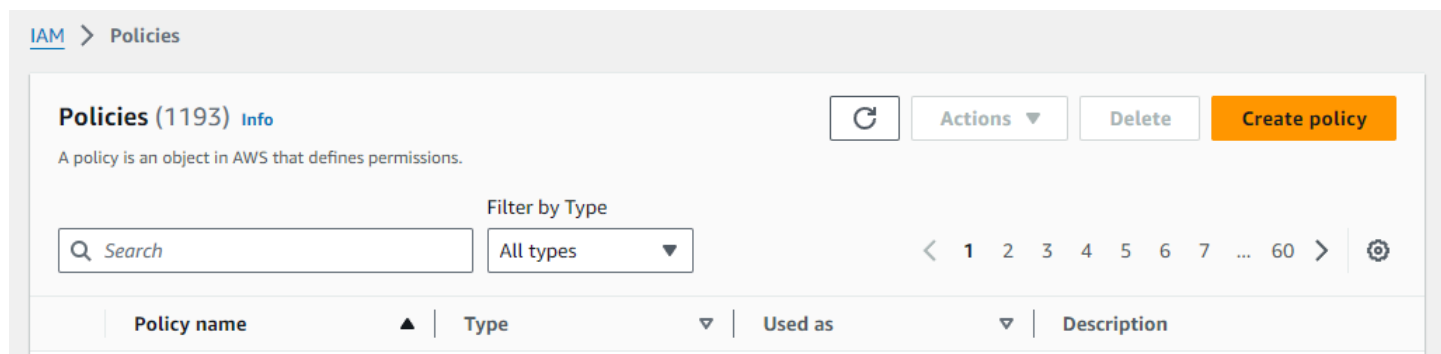


Select "User groups".



Select "Create group" and enter a descriptive name for the group.

Select "Policies" in the left-hand menu.



Select "Create policy" to create a new policy that will be attached to the group.

Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

VisualJSONActions

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "s3:*",
8         "s3-object-lambda:*"
9       ],
10      "Resource": [
11        "arn:aws:s3:::bucketname",
12        "arn:aws:s3:::bucketname/*"
13      ]
14    }
15  ]
16 }
```

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

+ Add new statement

Select "JSON".
Edit the policy to match the above.

Alternatively:
From the "Actions" dropdown menu, you can import the bucket policy created previously.

Import policy

X

Policies (1193)

Q s3

X

12 matches

< 1 2 >

	Policy name	Used as	Description
<input type="radio"/>	AmazonDMSRedshiftS3Role	None	Provides access to manage S3 settings for Redshift endpoints for DMS.
<input type="radio"/>	AmazonS3FullAccess	None	Provides full access to all buckets via the AWS Management Console.

Select "Next".

Review and create [Info](#)

Review the permissions, specify details, and tags.

Policy details

Policy name

Enter a meaningful name to identify this policy.

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

Description - *optional*

Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+=, @-_' characters.

Enter a descriptive name for the policy and (optionally) a description.
Save the policy.

Return to the group created previously.

[Users](#) | [Permissions](#) | [Access Advisor](#)

Permissions policies (0) [Info](#)
You can attach up to 10 managed policies.

Filter by Type
All types

Refresh

Simulate

Remove

Add permissions ▲
Attach policies
Create inline policy

< 1 > ⚙

<input type="checkbox"/>	Policy name ↗	Type	Attached entities
No resources to display			

Under the “Permissions” tab of the group, select “Add permissions”, then “Attach policies”.
Attach the newly created policy.

Select “Users” from the IAM menu.

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

Users (0) [Info](#)
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

< 1 > ⚙

Refresh

Delete

Create user

<input type="checkbox"/>	User name	Path	Group	Last activity	MFA	Password age	...
No resources to display							

Select “Create user”.

Specify user details

User details

User name

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.

i If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Cancel

Next

Enter the user's name and select "Next".

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions.

[Learn more](#)

Permissions options



Add user to group

Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.



Copy permissions

Copy all group memberships, attached managed policies, and inline policies from an existing user.



Attach policies directly

Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

User groups (1)



Create group

Search

< 1 >



Group name



Users



Attached polici...



Created



Select the group to add the user to, and select "Next" again.

Review the user and select "Create user".

Select the user from the group or from “Users” in the IAM menu.

Summary

ARN arn:aws:iam::058264300185:user/animalhouseuser	Console access Disabled	Access key 1 Create access key
Created May 03, 2024, 14:58 (UTC+01:00)	Last console sign-in -	

Select “Create access key” to generate the access keys.
Download the csv file.
The file contains your ‘access key ID’ and ‘secret access key’ which will be added to your config vars on Heroku.
Do not share the keys with anyone.

Access key ID,Secret access key