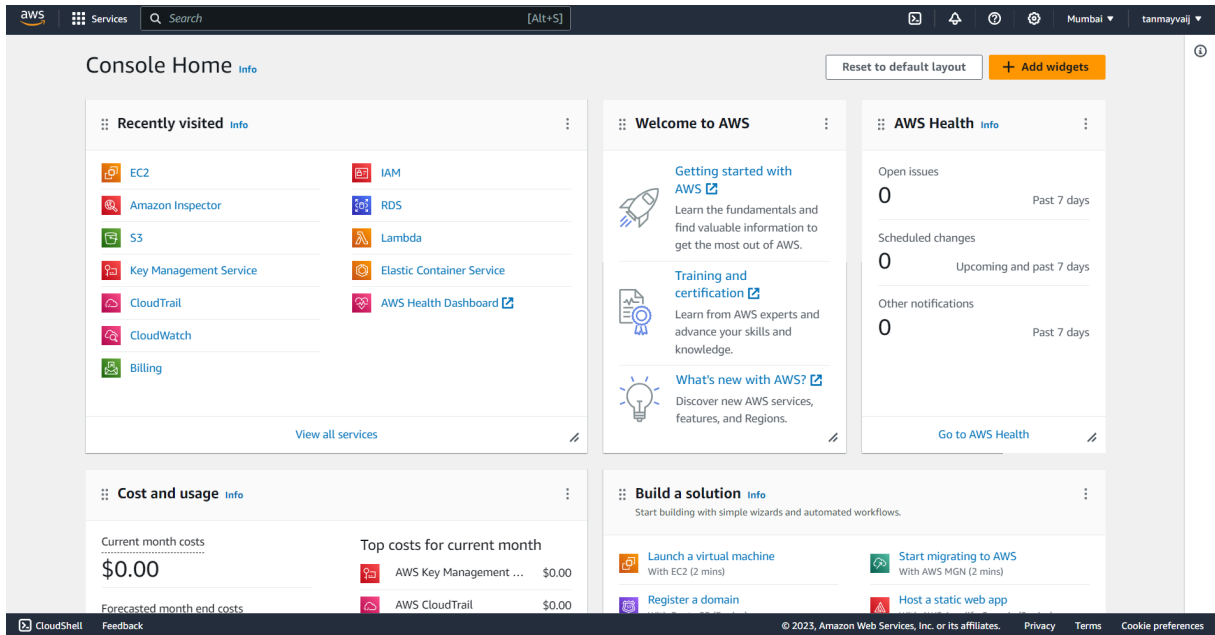
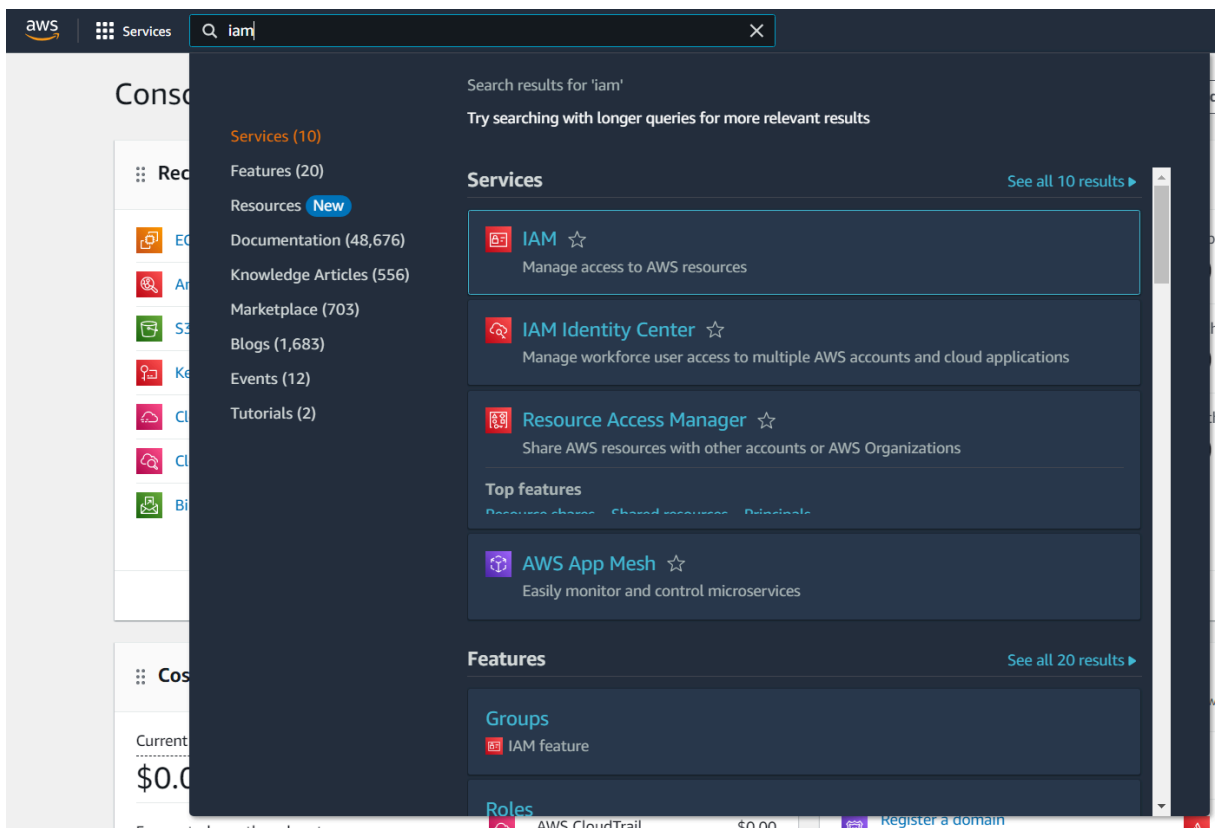


Demonstration of IAM Users, Group, AWS Managed Policy Granular Access

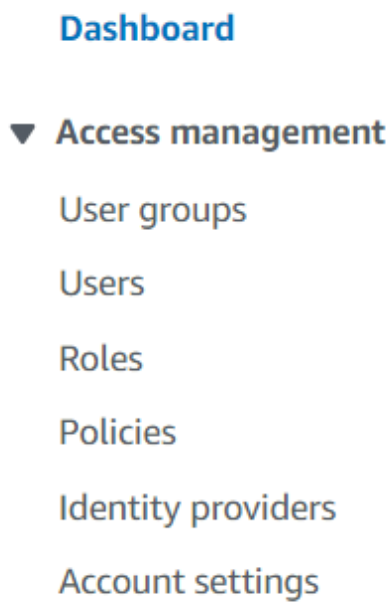
1. Sign into AWS Console.



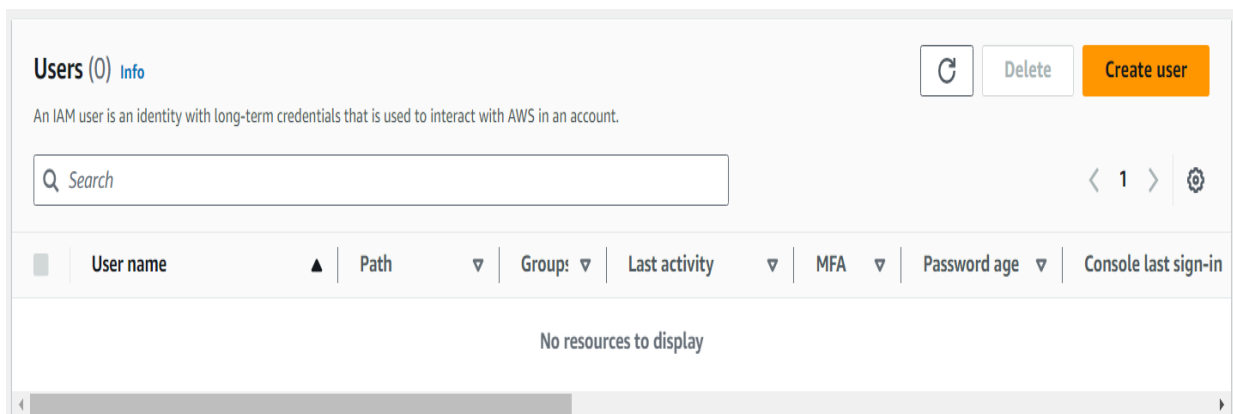
2. Search and open IAM dashboard.



3. Click on the “Users” in the side menu.



4. Click on “Create user”.




5. Enter the username, check the “Provide user access to the AWS Management Console”, and set a custom password.

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.

 **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 their AWS accounts and cloud applications.

☒ 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 AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

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 ! @ # \$ % ^ & * () _ + - (hyphen) = [] { } | ' "

☐ 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.


6. Select the “Add user to group” and then click on “Create group”.

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.

 **Get started with groups**
Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

Create group

7. Give a group name, search and select the AmazonEC2FullAccess. Then select the group in which you want to add the user.

User groups (1/1)

Q Search

< 1 >

☒

Group name

Users

Attached policies

Created

☒

[dev](#)

0

[AmazonEC2FullAccess](#)

2023-11-23 (Now)

8. Then in the users section, the created user appears.

Users (1) [Info](#)

Q Search

< 1 >

☐

User name

Path

Group:

Last activity

MFA

Password age

Console last sign-in

☐

[user1](#)

/

[1](#)

-

Now

-

9. Repeat the same process and create another two user with permission for AmazonS3FullAccess and AdministratorAccess respectively.

Users (3) [Info](#)

Q Search

< 1 >

☐

User name

Path

Group:

Last activity

MFA

Password age

Console last sign-in

☐

[user1](#)

/

[1](#)

-

4 minutes

-

☐

[user2](#)

/

[1](#)

-

1 minute

-

☐

[user3](#)

/

0

-


-

-

10. Copy the Sign-in URL for IAM users and paste it into browser url and sign in into user1 account.

AWS Account


Account ID

 760444148665


Account Alias


Create

Sign-in URL for IAM users in this account

 <https://760444148665.signin.aws.amazon.com/console>



11. Try to create a bucket and AWS will not allow to do so, as there is no permission provided for S3.

 After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.








Failed to create bucket

- To create a bucket, the `s3:CreateBucket` permission is required.
- To apply the **Bucket owner preferred** or **Object writer** setting for **Object Ownership**, the `s3:PutBucketOwnershipControls` permission is required.

View your permissions in the [IAM console](#) . Learn more about [Identity and Access Management in Amazon S3](#) .

► API response

12. Then sign in to user2, and try to create an instance, AWS shows the error message.

	Name 	Instance ID	Instance state 	Instance type 	Status check	Alarm status	Availability Zone 	Public IPv4 DN...
<p>You are not authorized to perform this operation. User: arn:aws:iam::760444148665:user/user2 is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action</p>								

13. Now sign in to user3, and try to create both, AWS will allow as user3 is having AdministratorAccess.

Instances [Info](#)

Refresh

Connect

Instance state ▾

Actions ▾

Launch instances ▾

Find Instance by attribute or tag (case-sensitive)

< 1 > ⚙

Name ✎ ▾

Instance ID

Instance state ▾

Instance type ▾

Status check

Alarm status

Availability Zone ▾

Public IPv4 DNS

No instances

You do not have any instances in this region

Launch instances

☑ Successfully created bucket "myuniquebucket12345678"

View details

×

To upload files and folders, or to configure additional bucket settings, choose [View details](#).

Amazon S3 > Buckets

▶ Account snapshot

View Storage Lens dashboard

Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

Buckets (1) [Info](#)

Refresh

Copy ARN

Empty

Delete

Create bucket

Find buckets by name

< 1 > ⚙

Name ▲

AWS Region ▾

Access ▾

Creation date ▾

○

myuniquebucket12345678

Asia Pacific (Mumbai) ap-south-1

Bucket and objects not public

November 23, 2023, 17:06:50 (UTC+05:30)