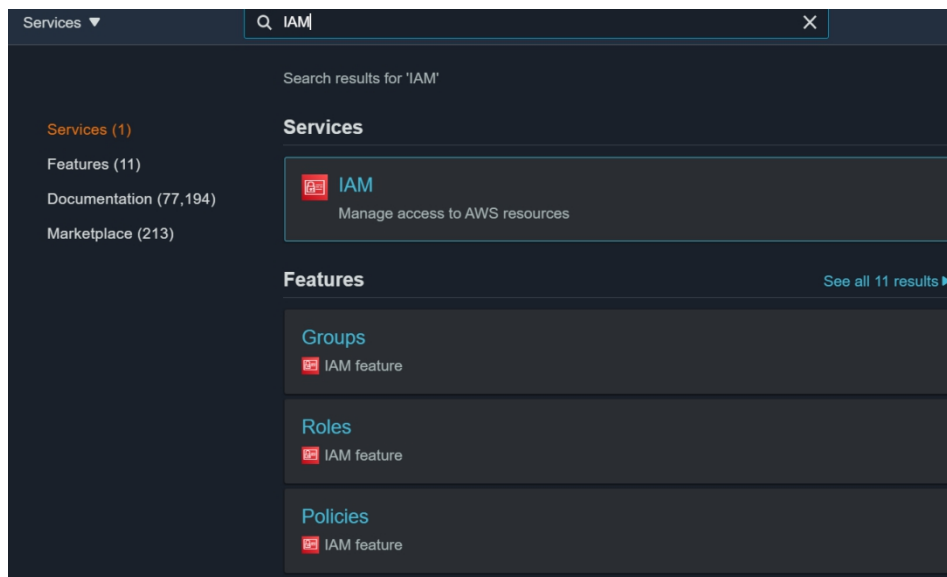


AWS_IAM_1

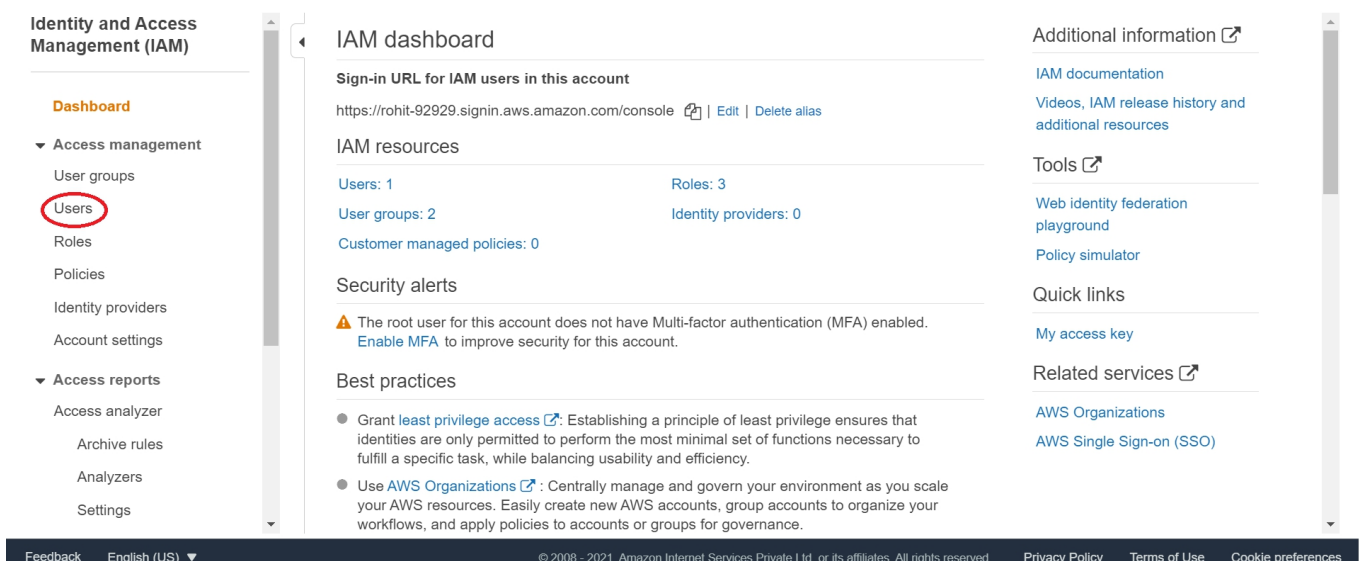
Creating user and assigning them to groups with IAM policies.

by: Anand Sharma

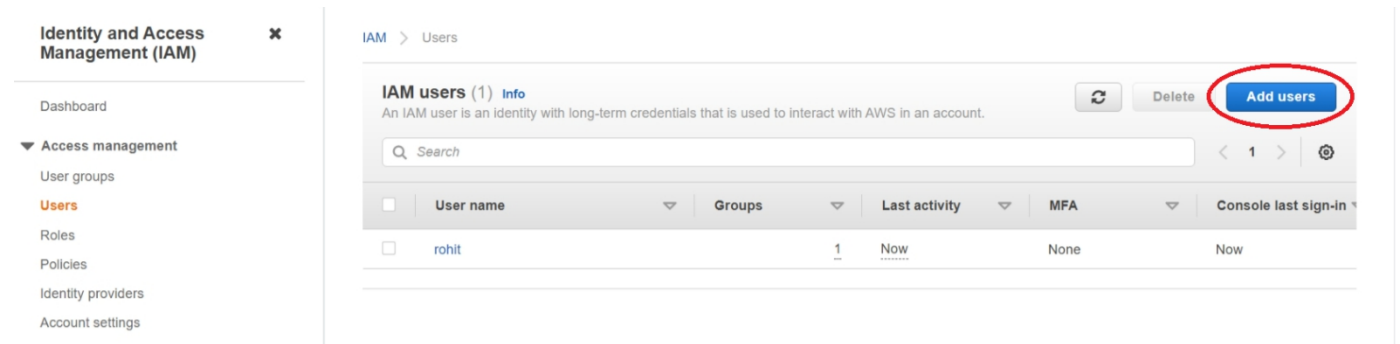
To create a new **User** for **AWS** navigate to your root user account and then hit **IAM** inside the search bar on the **AWS MANGEMENT CONSOLE** as shown in the figure below:



Now inside the **IAM** console navigate to **users** sections



Now inside the user section hit the **add user** button



Now fill the details as per your requirement

Add user

12345

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

user_one

+ Add another user

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type*

☐ Programmatic access

Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☒ AWS Management Console access

Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password*

☐ Autogenerated password

☒ Custom password

.....

☐ Show password

Require password reset

☐ User must create a new password at next sign-in

Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

* Required

Cancel

Next: Permissions


Now we add the user to a group which has administrator access **IAM policy** attached to the group

Add user

1 2 3 4 5

Set permissions

 Add user to group

 Copy permissions from existing user

 Attach existing policies directly

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](#)

Add user to group

Create group

Refresh

Search		Showing 2 results
Group	Attached policies	
<input checked="" type="checkbox"/> admins	AdministratorAccess	
<input type="checkbox"/> developers	None	

Set permissions boundary

Set a permissions boundary to control the maximum permissions this user can have. This is an advanced feature used to delegate permission management to others. [Learn more](#)

- ☒ Create user without a permissions boundary
- ☐ Use a permissions boundary to control the maximum user permissions

Cancel Previous Next: Tags

Now we are adding a tag for the user we are creating

Add user

1 2 3 4 5

Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. [Learn more](#)

Key	Value (optional)	Remove
user	Test_user	×
Add new key		

You can add 49 more tags.

Cancel Previous Next: Review

Review your setting and then hit **create user**

Add user

1 2 3 **4** 5

Review

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

User details

User name	user_one
AWS access type	AWS Management Console access - with a password
Console password type	Custom
Require password reset	No
Permissions boundary	Permissions boundary is not set

Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	admins

Tags

The new user will receive the following tag

Key	Value
user	Test_user

[Cancel](#)

[Previous](#)

[Create user](#)

Now hit the **Download.csv** button, this CSV file contains the details of the user created and can be viewed later so for safety purpose download this file in your local machine

Add user

1 2 3 4 **5**



Success

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

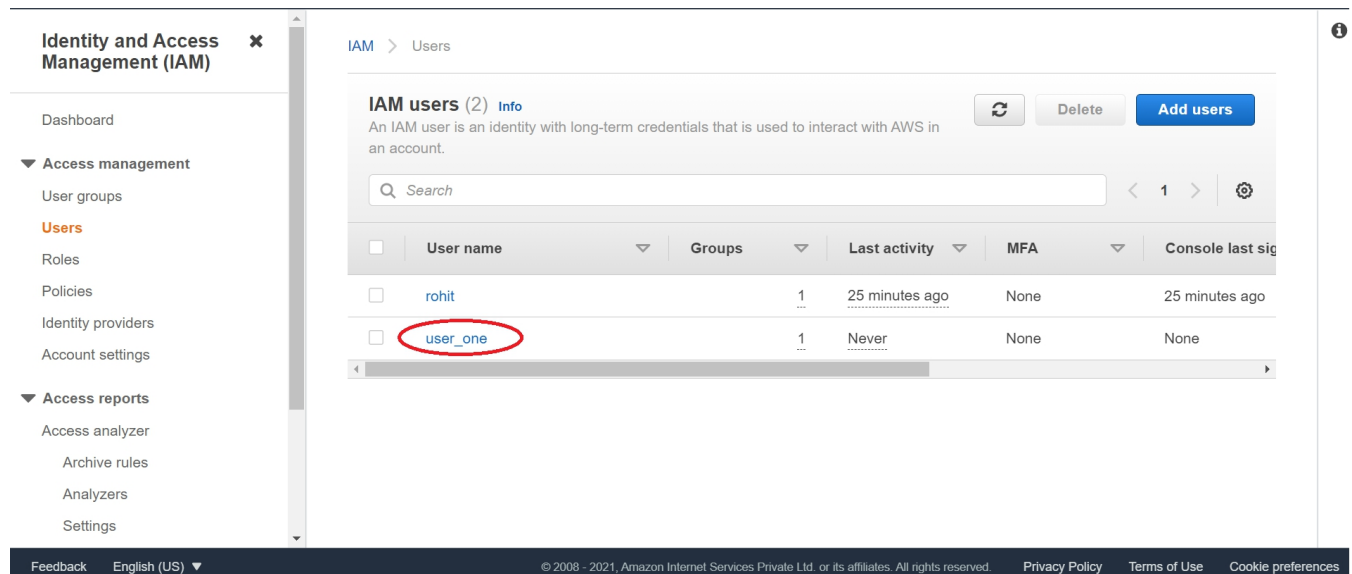
Users with AWS Management Console access can sign-in at: <https://rohit-92929.signin.aws.amazon.com/console>

[Download .csv](#)

User	Email login instructions
user_one	Send email

[Close](#)

Now navigate to the **users** tab in the **IAM console** you can find the new created user which is attached to the group and with **IAM policies** attached to it



Identity and Access Management (IAM)

Dashboard

▼ Access management

- User groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings

▼ Access reports

- Access analyzer
- Archive rules
- Analizers
- Settings

IAM > Users

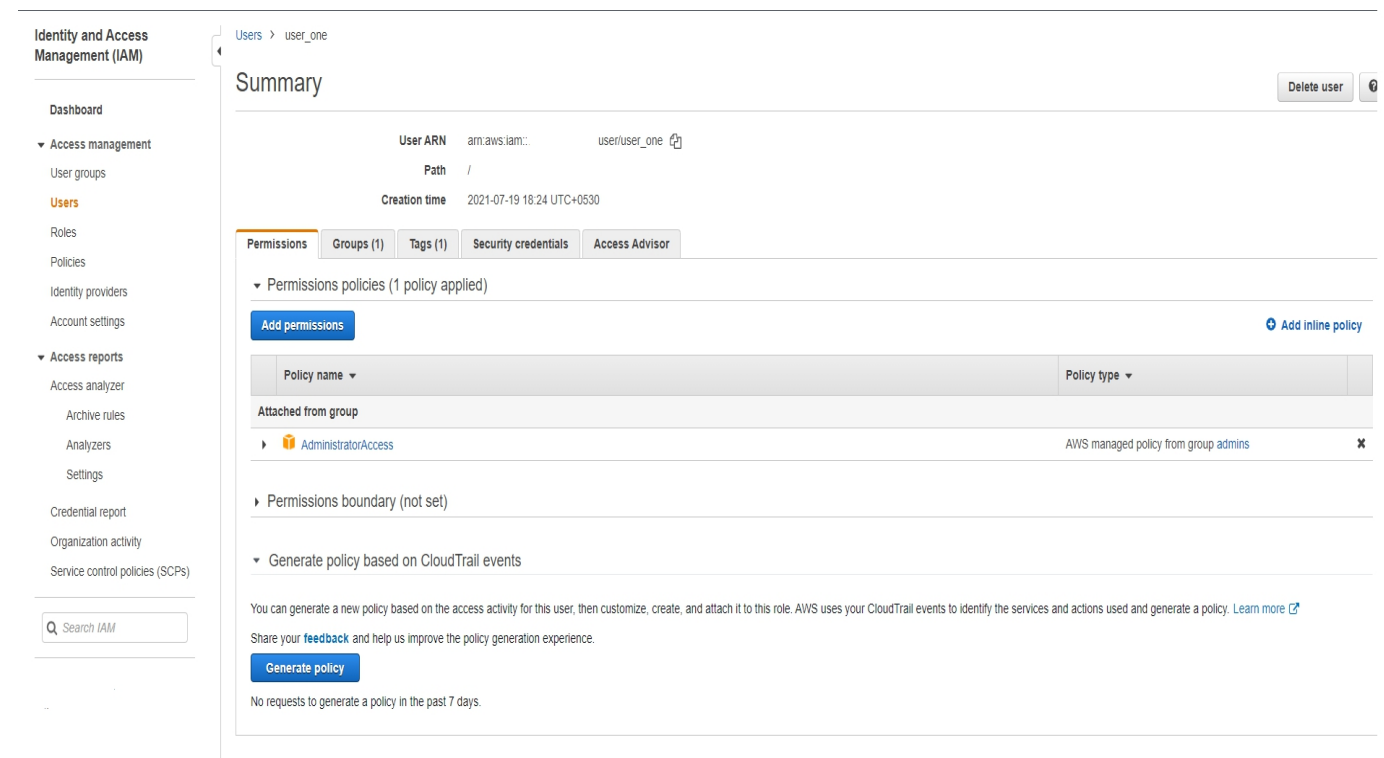
IAM users (2) [Info](#)

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

<input type="checkbox"/>	User name	Groups	Last activity	MFA	Console last sign-in
<input type="checkbox"/>	rohit	1	25 minutes ago	None	25 minutes ago
<input type="checkbox"/>	user_one	1	Never	None	None

Feedback English (US) © 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use Cookie preferences

The details of the user that was created can be seen by clicking the user that we just created and we can find the details of that user



Identity and Access Management (IAM)

Dashboard

▼ Access management

- User groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings

▼ Access reports

- Access analyzer
- Archive rules
- Analizers
- Settings

Credential report

Organization activity

Service control policies (SCPs)

Users > user_one

Summary [Delete user](#) [Info](#)

User ARN: `arn:aws:iam::user:user_one`

Path: `/`

Creation time: 2021-07-19 18:24 UTC+0530

Permissions Groups (1) Tags (1) Security credentials Access Advisor

▼ Permissions policies (1 policy applied)

[Add permissions](#) [Add inline policy](#)

Policy name	Policy type
Attached from group	
AdministratorAccess	AWS managed policy from group admins

Permissions boundary (not set)

▼ Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. [Learn more](#)

Share your **feedback** and help us improve the policy generation experience.

[Generate policy](#)

No requests to generate a policy in the past 7 days.