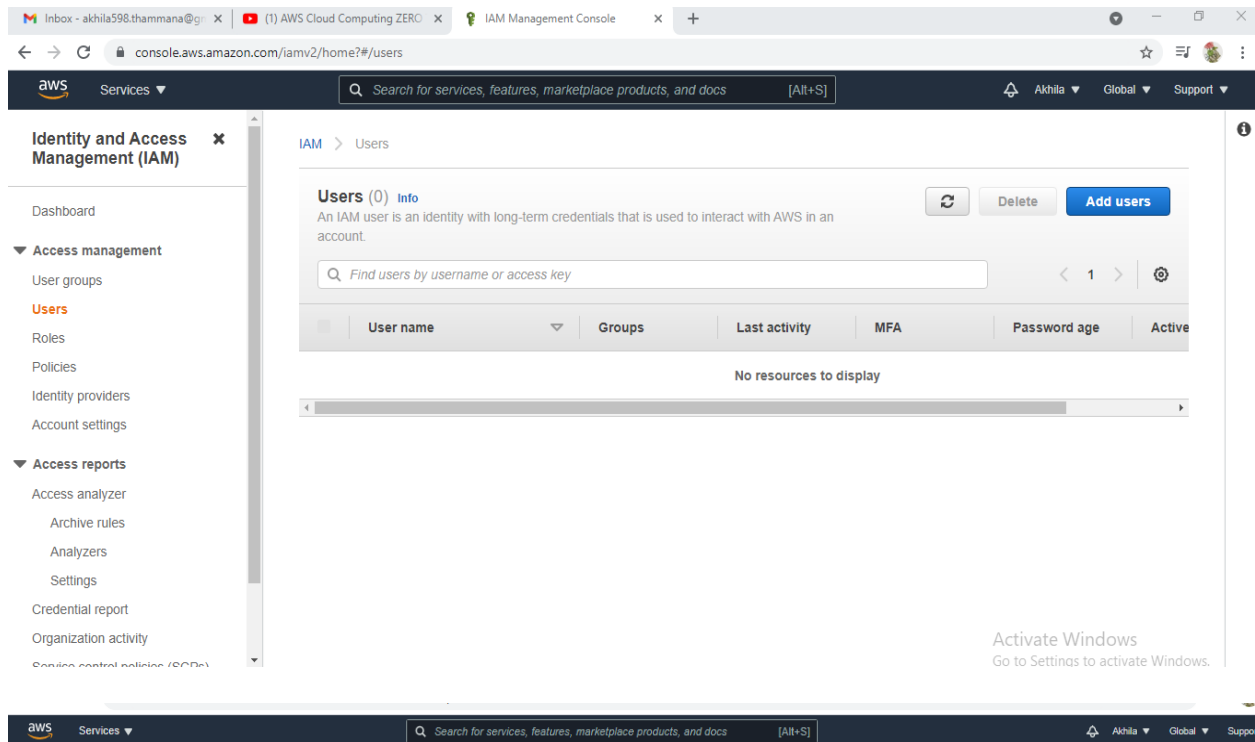


Assignment-1

Working with IAM

Creating User1



Add user

1 2 3 4 5

Set user details

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

User name*

[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](#)

Activate Windows
Go to Settings to activate Windows.

User1 permissions (AmazonEc2Fullaccess)

aws

Services

Search for services, features, marketplace products, and docs

[All+5]

Akhila

Global

Support

1

2

3

4

5

Set permissions

Add user to group

Copy permissions from existing user

Attach existing policies directly

Create policy

Filter policies

ec2

Showing 25 results

	Policy name	Type	Used as
<input type="checkbox"/>	AmazonEC2ContainerRegistryFullAccess	AWS managed	None
<input type="checkbox"/>	AmazonEC2ContainerRegistryPowerUser	AWS managed	None
<input type="checkbox"/>	AmazonEC2ContainerRegistryReadOnly	AWS managed	None
<input type="checkbox"/>	AmazonEC2ContainerServiceAutoscaleRole	AWS managed	None
<input type="checkbox"/>	AmazonEC2ContainerServiceEventsRole	AWS managed	None
<input type="checkbox"/>	AmazonEC2ContainerServiceforEC2Role	AWS managed	None
<input type="checkbox"/>	AmazonEC2ContainerServiceRole	AWS managed	None
<input checked="" type="checkbox"/>	AmazonEC2FullAccess	AWS managed	None
<input type="checkbox"/>	AmazonEC2ReadOnlyAccess	AWS managed	None
<input type="checkbox"/>	AmazonEC2RoleforAWSCodeDeploy	AWS managed	None
<input type="checkbox"/>	AmazonEC2RoleforAWSCodeDeployLimited	AWS managed	None

Cancel

Previous

Next: Tags

Activate Windows

Go to Settings to activate Windows.

aws

Services

Search for services, features, marketplace products, and docs

[All+5]

Akhila

Global

Support

1

2

3

4

5

Add user

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
<input type="text" value="Add new key"/>	<input type="text"/>	

You can add 50 more tags.

Cancel

Previous

Next: Review

Activate Windows

Go to Settings to activate Windows.

aws

Services

Search for services, features, marketplace products, and docs

[Alt+S]

Akhila

Global

Support

Add user

12345

Review

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

User details

User name

User1

AWS access type

Programmatic access and AWS Management Console access

Console password type

Custom

Require password reset

Yes

Permissions boundary

Permissions boundary is not set

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	AmazonEC2FullAccess
Managed policy	IAMUserChangePassword

Tags

No tags were added.

Cancel

Previous

Create user

Activate Windows
Go to Settings to activate Windows.

Creating user2

User2 permissions (S3FullAccess)

aws

Services

console.aws.amazon.com/iam/home#/users\$new?step=permissions&accessKey&login&userNames=User2&passwordReset&passwordType=manual&permissionT...

Search for services, features, marketplace products, and docs

[Alt+S]

Akhila

Global

Support

Add user

12345

Set permissions

Add user to group

Copy permissions from existing user

Attach existing policies directly

Create policy

Filter policies

s3

Showing 6 results

	Policy name	Type	Used as
<input type="checkbox"/>	AmazonDMSRedshiftS3Role	AWS managed	None
<input checked="" type="checkbox"/>	AmazonS3FullAccess	AWS managed	None
<input type="checkbox"/>	AmazonS3OutpostsFullAccess	AWS managed	None
<input type="checkbox"/>	AmazonS3OutpostsReadOnlyAccess	AWS managed	None
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	AWS managed	None
<input type="checkbox"/>	QuickSightAccessForS3StorageManagementAnalyticsReadOnly	AWS managed	None

Set permissions boundary

Cancel

Previous

Next: Tags

Activate Windows
Go to Settings to activate Windows.

Creating user3

User3 permissions (Amazon API gateway administrator)

Identity and Access Management (IAM)

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analysts

Settings

Credential report

Organization activity

Service control policies (SCPs)

Search IAM

AWS account ID: 80885367189

New feature to generate a policy based on CloudTrail events.

AWS uses your CloudTrail events to identify the services and actions used and generate a least privileged policy that you can attach to this user.

Users > User3

Summary

Delete user

User ARN

am:aws:iam:700885367189:user3

Path

/

Creation time

2021-08-01 15:50 UTC+0530

Permissions

Groups (1)

Tags

Security credentials

Access Advisor

Permissions policies (3 policies applied)

Add permissions

Add inline policy

Policy name	Policy type	
Attached directly		
IAMUserChangePassword	AWS managed policy	x
AmazonAPIGatewayAdministrator	AWS managed policy	x
Show 2 more		
Permissions boundary (not set)		
Generate policy based on CloudTrail events		

Creating Group and adding users

Group permissions (Cloud watch Full access)

Identity and Access Management (IAM)

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analysts

Settings

Credential report

Organization activity

Service control policies (SCPs)

Search IAM

AWS account ID: 80885367189

User group name

Assignment-one

Maximum 128 characters. Use alphanumeric and hyphen characters.

Add users to the group - Optional (Selected 3/3)

Add inline policy

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user can belong to up to 10 groups.

Search

1

User name	Groups	Last activity	Creation time
User1	0	None	11 minutes ago
User2	0	None	4 minutes ago
User3	0	None	2 minutes ago

Attach permissions policies - Optional (Selected 1/89)

Add inline policy

Then attach up to 10 policies to this user group. All the users in the group will have permissions that are defined in the selected policies.

Filter policies by property or policy name and press enter

21 matches

1

2

Policy Name	Type	Description
CloudWatchEventsBuiltinTargetExecutionAccess	AWS managed	Allows built-in targets in Ar
CloudWatchAgentAdminPolicy	AWS managed	Full permissions required t
CloudWatchAgentServerPolicy	AWS managed	Permissions required to us
CloudWatchEventsReadOnlyAccess	AWS managed	Provides read-only access
AmazonAPIGatewayPushToCloudWatchLogs	AWS managed	Allows API Gateway to pus
CloudWatchFullAccess	AWS managed	Provides full access to Cl
CloudWatchActionMetricsAccess	AWS managed	Provides read-only access
AWSAppSyncPushToCloudWatchLogs	AWS managed	Allows AppSync to push lo

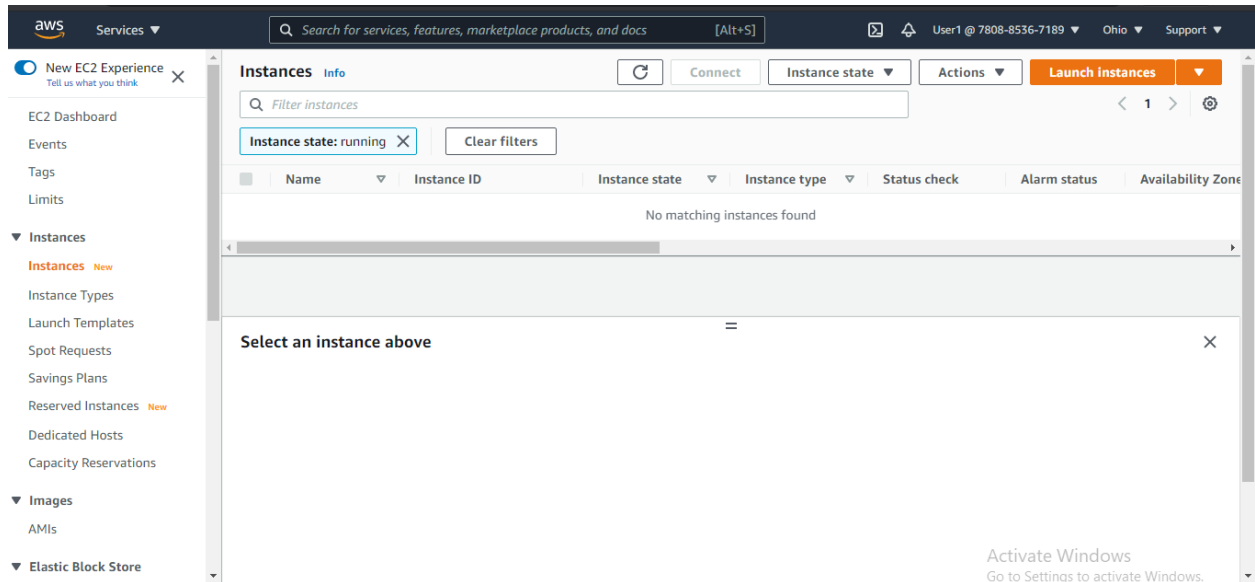
Added users to group

The screenshot shows the AWS IAM console interface. The left sidebar contains the navigation menu for Identity and Access Management (IAM), including options like Dashboard, Access management, User groups, Roles, Policies, Identity providers, Account settings, Access reports, and various reports. The main content area is titled 'User groups (1)' and includes a search bar and a table of user groups. The table has columns for Group name, Users, Permissions, and Creation time. One group, 'Assignment-one', is listed with 3 users, a status of 'Defined', and a creation time of 'Now'. There are buttons for 'Create group', 'Delete', and 'Refresh' at the top right of the table.

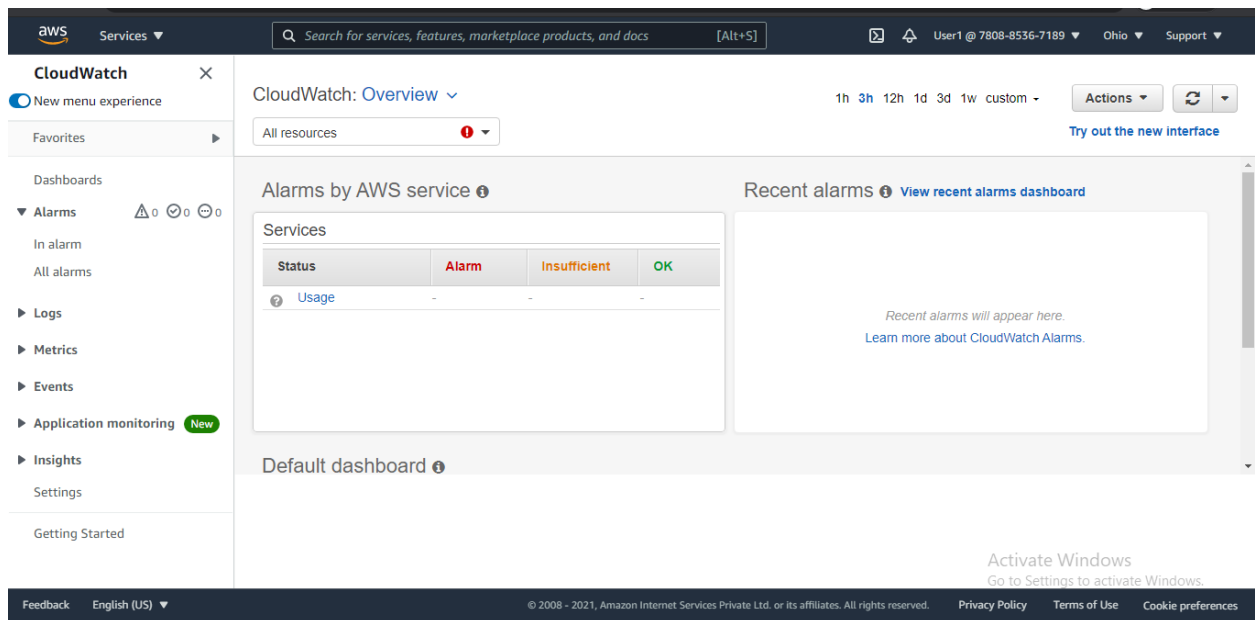
Login to user1 and changing password

The screenshot shows the AWS login page for user1. The page displays the AWS account ID (780885367189) and the IAM user name (User1). It includes fields for Old password, New password, and Retype new password, followed by a 'Confirm password change' button. A link to 'Sign in using root user email' is also visible. The page is in English, as indicated by the language dropdown at the bottom.

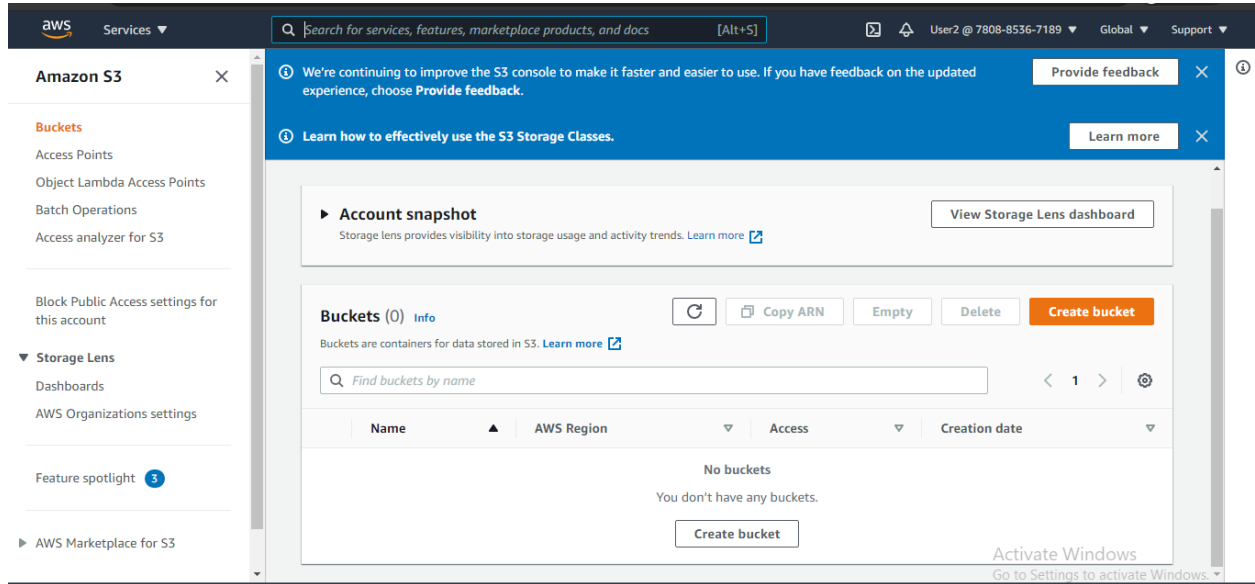
Checking User1 permission



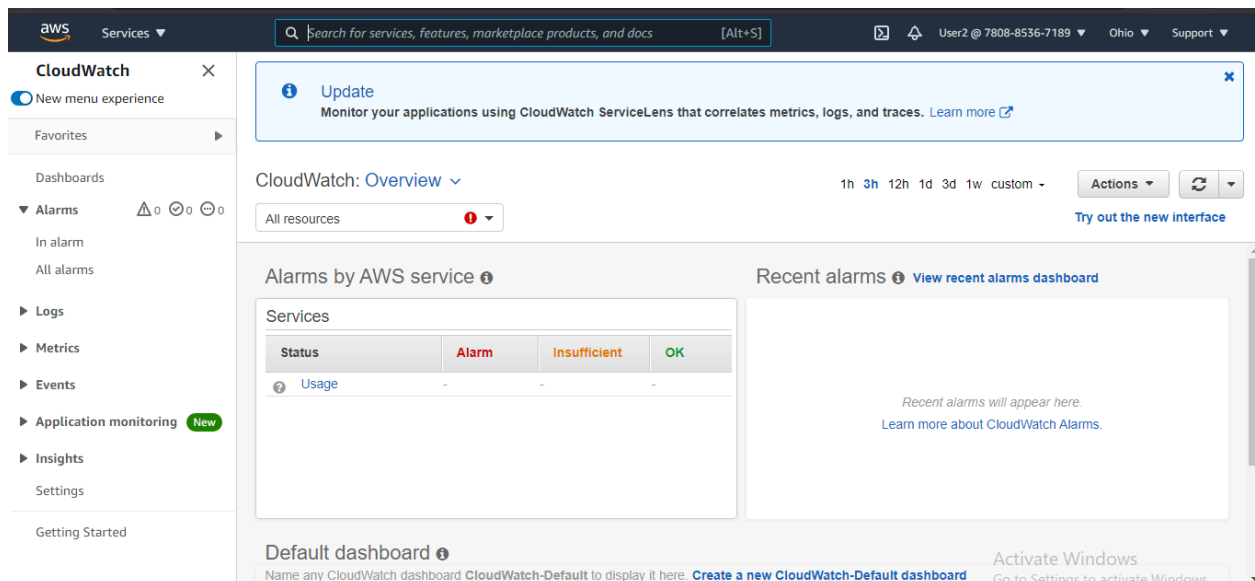
Checking group permissions to user1



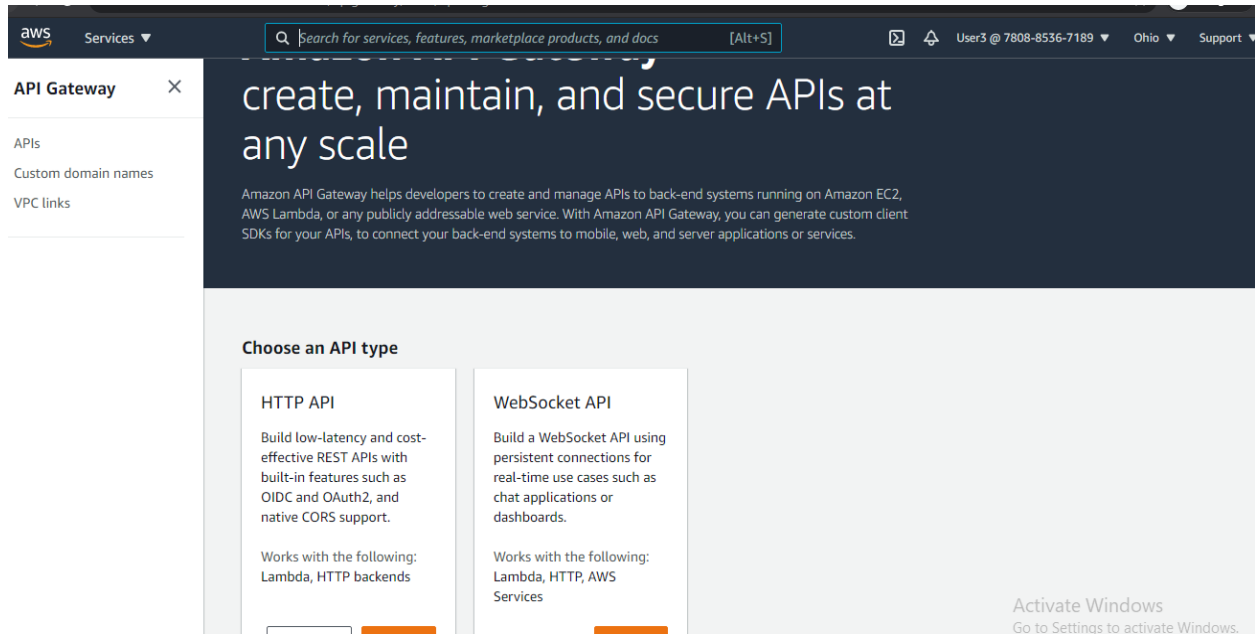
Checking User2 permission



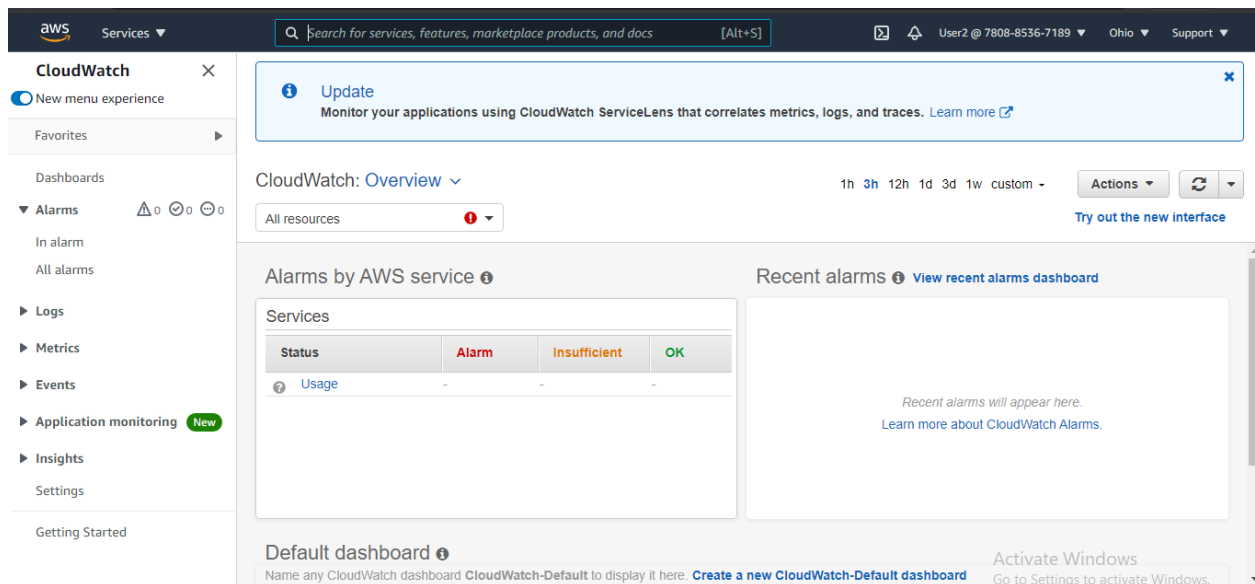
Checking group permission to user2



Checking User3 permission



Checking group permission to user3



Checked which policy gives access to IAM

Created User4 and its permissions (IAM FULLACCESS)

Summary

User ARN: `arn:aws:iam::78085367189:user/User4`
Path: `/`
Creation time: 2021-08-01 16:23 UTC+0530

Permissions | Groups | Tags | Security credentials | Access Advisor

Permissions policies (2 policies applied)

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

Policy name	Policy type	
Attached directly		
IAMFullAccess	AWS managed policy	X
IAMUserChangePassword	AWS managed policy	X
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](#)

Checking user4 Permissions

Add user

1 2 3 4 5

Set user details

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

User name*

[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.

[Cancel](#) [Next: Permissions](#)