IAM

IAM stands for identify & access management; this refers to policies, processes & technologies used to manage identity & access of resources & services within an organization. This is designed to ensure that only authorized users/groups can access the sensitive data/ application / platform. This helps us to prevent unauthorized access & misuse of any data or services.This manages users & their level of access to AWS console & the resources. This is very important according to the administration point of view in which the user is given different access.

These permissions are further divided into 4 types:

1) Centralized
2) Access.
3) Permission
4) Identity.

1) **Centralized**
   It gives you centralized control over your AWS account.

2) Access
   It also gives shared access to your account.

3) **Permission**
   This gives you granular permission,this means that users can have different levels of access. Different users will have different levels of access within the same organization.

4) Identity federation
   This enables the user to login using their credentials stored in active directory, facebook, linkedin, google.

   Multi-factor authentication : User is granted access only after successful completion of multiple independent authentication mechanisms. For eg. When users provide username & password this works as one set of authentication mechanisms & the second level of authentication is via google authenticator where a token is generated as password.

   Temporary access : It also provides temporary access for user or device and service for example if you develop a mobile or web based application you can configure the user to have temporary access to resources within your account for example to enable access to retrieve data located in S3 bucket or in DynamoDB.

Password rotation policy: This allows you to set up your own password.

Integrated : It is integrated with different AWS services.

Compliance : Supports PCI DSS compliance.

These were some features of IAM.

The key terminology that are used in **IAM** are -

User: The users are referred to as end users who have logged in into the AWS console & they are also interacting in the AWS by running API commands.

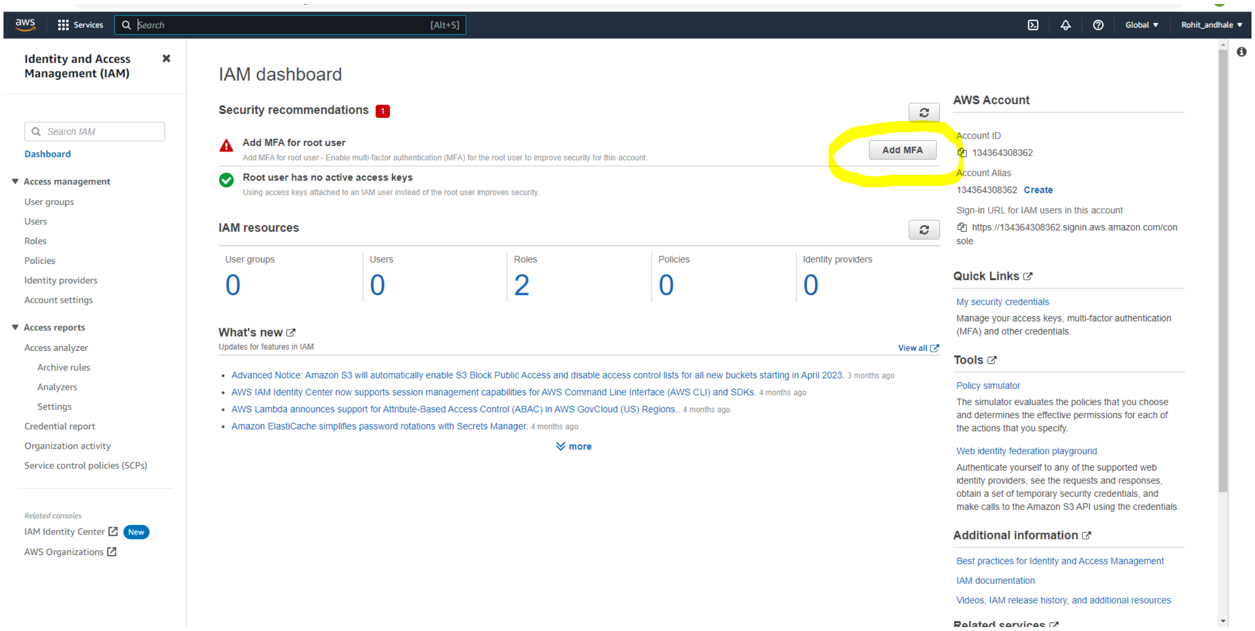
Groups: The group are collection of users that are grouped together with common set of permissions suppose you work in a marketing team & you need to access (Read & write) certain files that are stored in **S3** buckets, we need to specify specific set of permissions for all the users that are working in marketing department. Once you create a group you need to add a specific user into that group which will have a similar set of permissions.

Roles: We can create a set of roles, we can assign them to user applications or services to give access to AWS resources. So role is used to define a set of permissions for ex. S3 bucket access, dynamo DB access to database admin.

Policy: Policies are made up of documents called policy documents, these documents are in a format that is called JSON & they give permission to which user, group, role will access which resources.

IAM : Policy simulators check for the authentic users, these are authorized to run the resources. Test policies that are attached already to existing user groups, it is the best way to check any suspected IAM user group.

Click on : **Add MFA**



IAM dashboard

Security recommendations 1

Add MFA for root user
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

Root user has no active access keys
Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

User groups	Users	Roles	Policies	Identity providers
0	0	2	0	0

What's new
Updates for features in IAM

- Advanced Notice: Amazon S3 will automatically enable S3 Block Public Access and disable access control lists for all new buckets starting in April 2023. 3 months ago
- AWS IAM Identity Center now supports session management capabilities for AWS Command Line Interface (AWS CLI) and SDKs. 4 months ago
- AWS Lambda announces support for Attribute-Based Access Control (ABAC) in AWS GovCloud (US) Regions.. 4 months ago
- Amazon ElastiCache simplifies password rotations with Secrets Manager. 4 months ago

AWS Account

Account ID
134364308362

Account Alias
134364308362

Sign-in URL for IAM users in this account
https://134364308362.signin.aws.amazon.com/console

Quick Links

My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.

Tools

Policy simulator
The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.

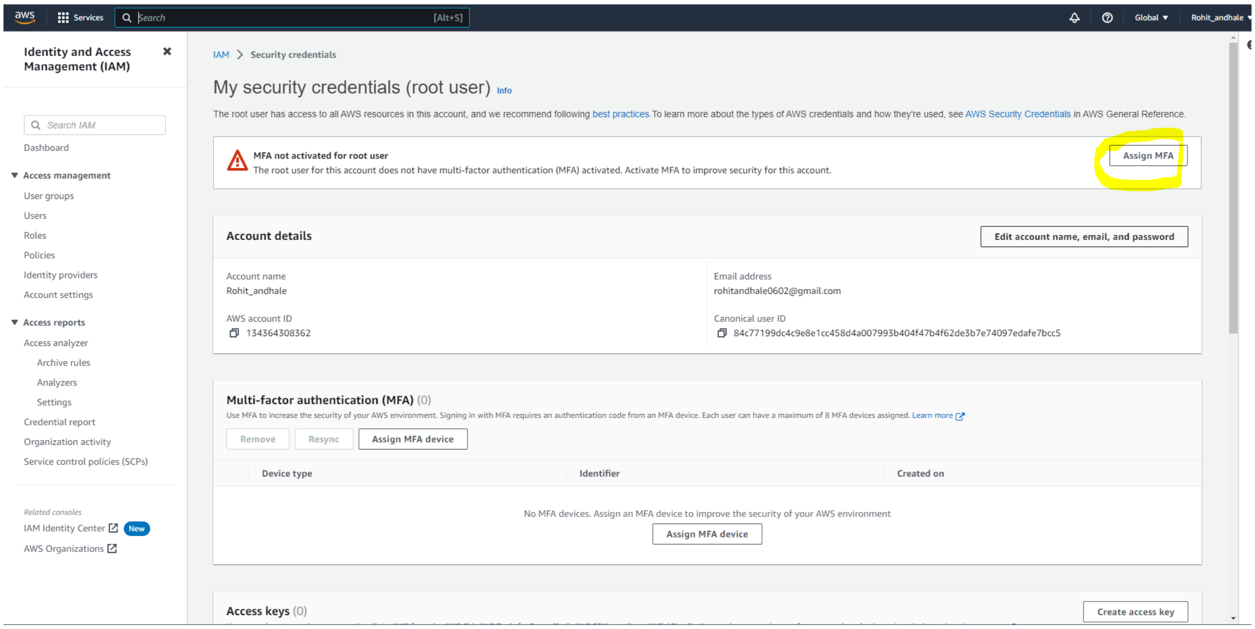
Web identity federation playground
Authenticate yourself to any of the supported web identity providers, see the requests and responses, obtain a set of temporary security credentials, and make calls to the Amazon S3 API using the credentials.

Additional information

Best practices for Identity and Access Management
IAM documentation
Videos, IAM release history, and additional resources

Related services

Click on : **Assign MFA**



My security credentials (root user)

The root user has access to all AWS resources in this account, and we recommend following best practices. To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference.

MFA not activated for root user
The root user for this account does not have multi-factor authentication (MFA) activated. Activate MFA to improve security for this account.

Account details

Account name
Rohit_andhale

Email address
rohitandhale0602@gmail.com

AWS account ID
134364308362

Canonical user ID
84c77199dc4c9e8e1cc458d4a007993b404f47b4f62de3b7e74097edafe7bcc5

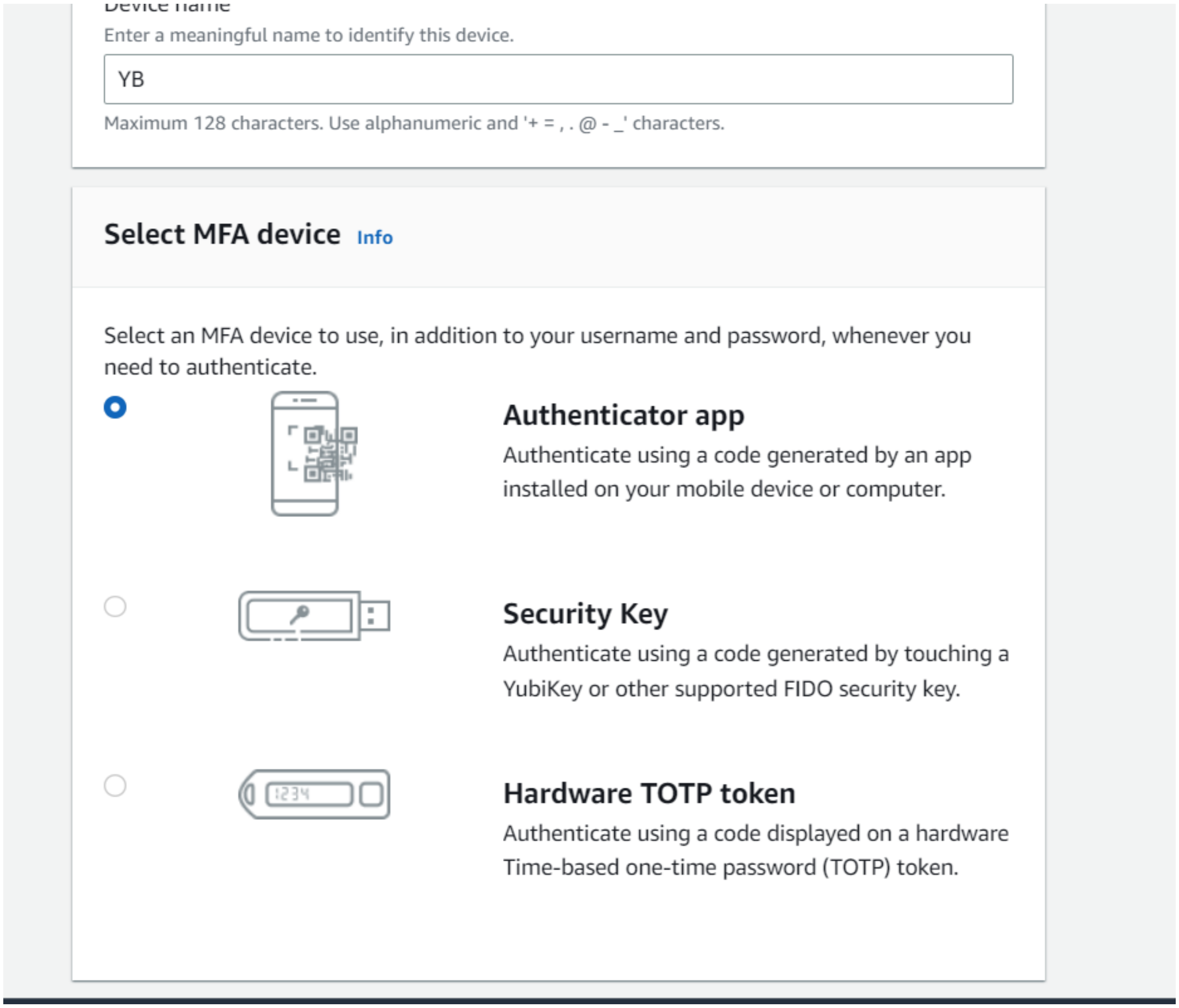
Multi-factor authentication (MFA) (0)
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more

Device type	Identifier	Created on

No MFA devices. Assign an MFA device to improve the security of your AWS environment

Access keys (0)

1) Add device name :
2) Scroll down.
3) Click on **next**



Device name

Enter a meaningful name to identify this device.

YB

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

Select MFA device Info

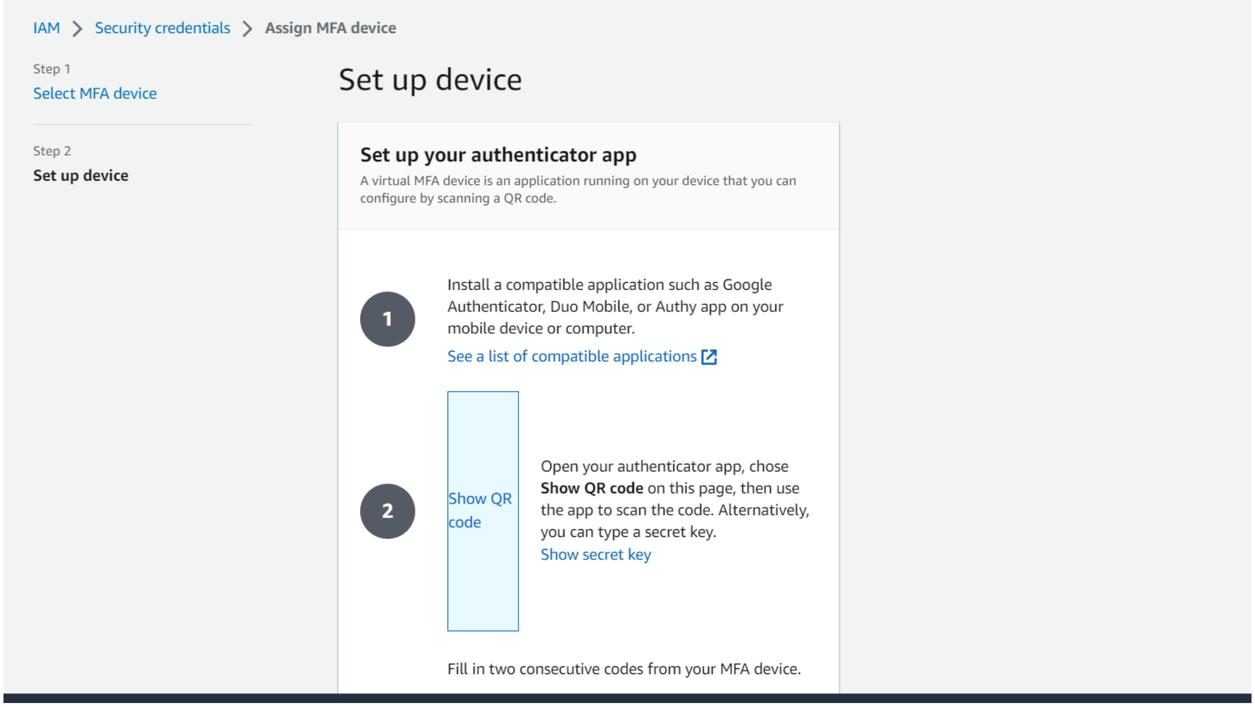
Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.

● **Authenticator app**
Authenticate using a code generated by an app installed on your mobile device or computer.

○ **Security Key**
Authenticate using a code generated by touching a YubiKey or other supported FIDO security key.

○ **Hardware TOTP token**
Authenticate using a code displayed on a hardware Time-based one-time password (TOTP) token.

1st option click on : **see a list of compatible application**



IAM > Security credentials > Assign MFA device

Step 1
Select MFA device

Step 2
Set up device

Set up device

Set up your authenticator app

A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

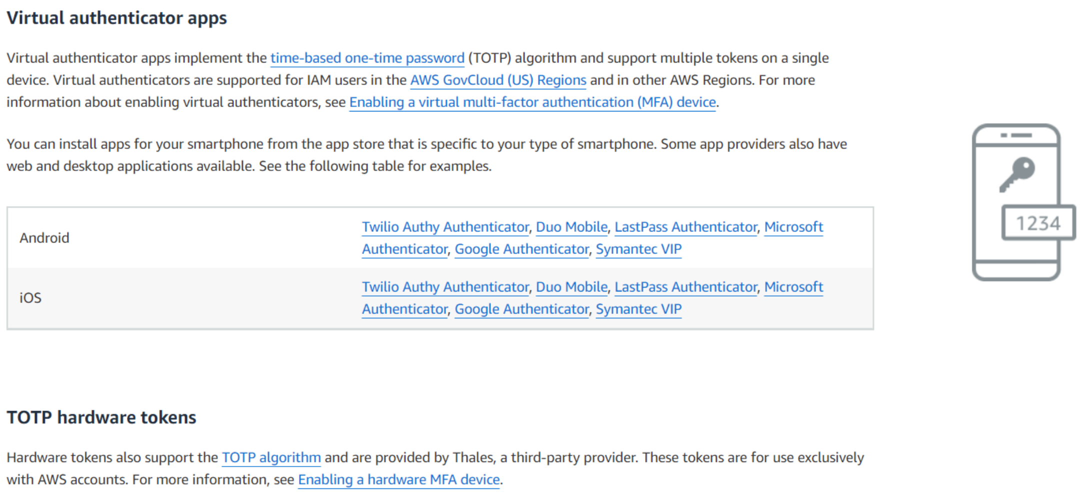
1 Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.
See a list of compatible applications

2 Show QR code

Open your authenticator app, chose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key.
Show secret key

Fill in two consecutive codes from your MFA device.

1) Install Google Authenticator on your mobile.
2) Click on : **Android / iOS Google Authenticator**



Virtual authenticator apps

Virtual authenticator apps implement the time-based one-time password (TOTP) algorithm and support multiple tokens on a single device. Virtual authenticators are supported for IAM users in the AWS GovCloud (US) Regions and in other AWS Regions. For more information about enabling virtual authenticators, see Enabling a virtual multi-factor authentication (MFA) device.

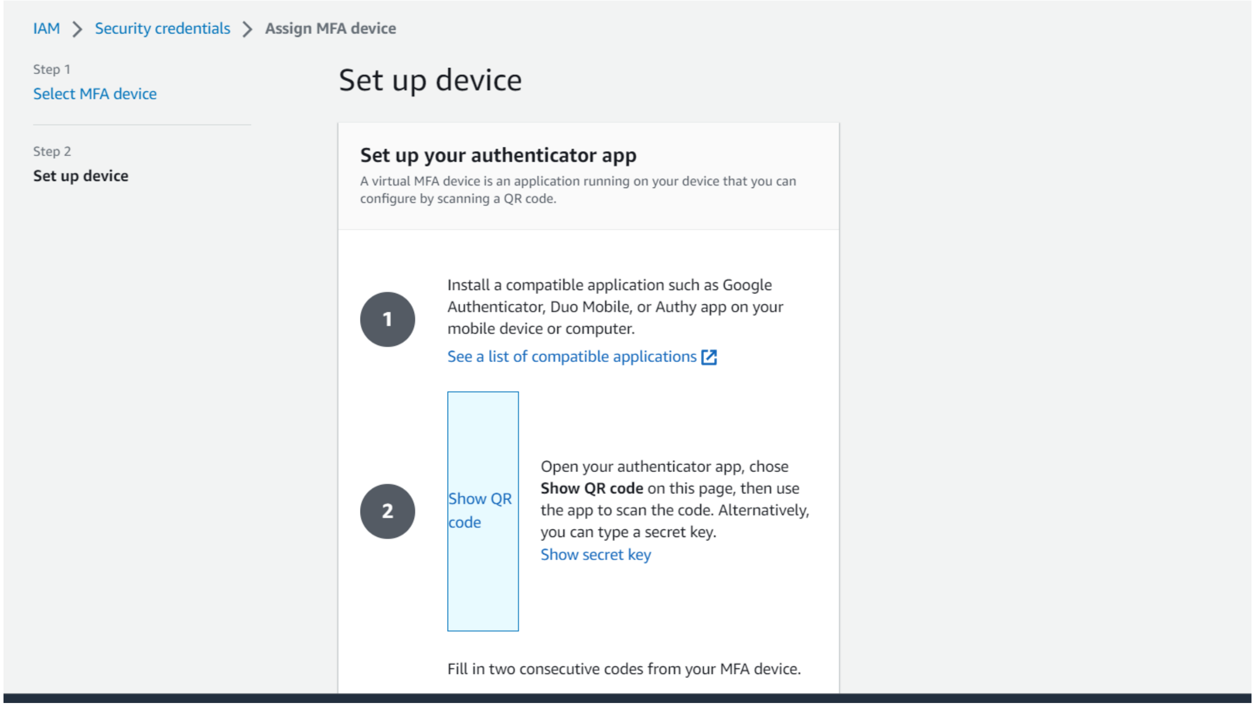
You can install apps for your smartphone from the app store that is specific to your type of smartphone. Some app providers also have web and desktop applications available. See the following table for examples.

Android	Twilio Authy Authenticator, Duo Mobile, LastPass Authenticator, Microsoft Authenticator, Google Authenticator, Symantec VIP
iOS	Twilio Authy Authenticator, Duo Mobile, LastPass Authenticator, Microsoft Authenticator, Google Authenticator, Symantec VIP

TOTP hardware tokens

Hardware tokens also support the TOTP algorithm and are provided by Thales, a third-party provider. These tokens are for use exclusively with AWS accounts. For more information, see Enabling a hardware MFA device.

1) Click on 2nd option for QR Code
2) Scan QR code and fill both codes.
3) After click on **ADD MFA**


IAM > Security credentials > Assign MFA device
Step 1
Select MFA device
Step 2
Set up device
1
2
Show QR code
Show secret key
See a list of compatible applications

Set up device

Set up your authenticator app

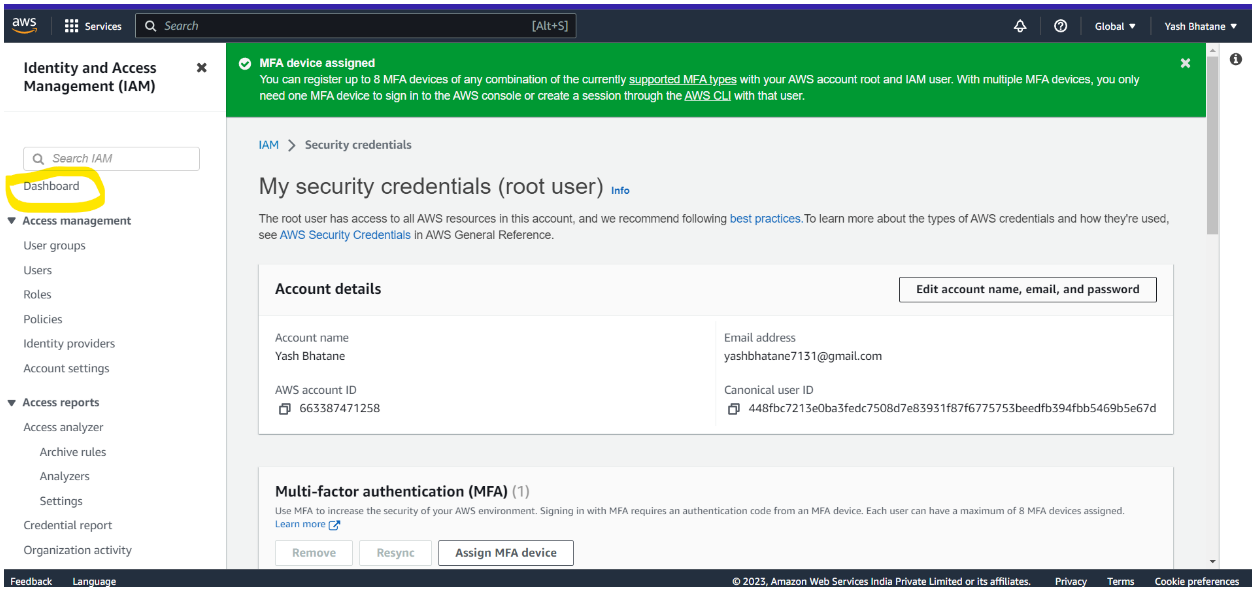
A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

1. Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer. See a list of compatible applications

2. Open your authenticator app, chose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key. Show secret key

Fill in two consecutive codes from your MFA device.

1) This page will appear
2) Click on dashboard



MFA device assigned
You can register up to 8 MFA devices of any combination of the currently supported MFA types with your AWS account root and IAM user. With multiple MFA devices, you only need one MFA device to sign in to the AWS console or create a session through the AWS CLI with that user.

My security credentials (root user)

The root user has access to all AWS resources in this account, and we recommend following best practices.To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference.

Account details

Account name
Yash Bhatane

Email address
yashbhatane7131@gmail.com

AWS account ID
663387471258

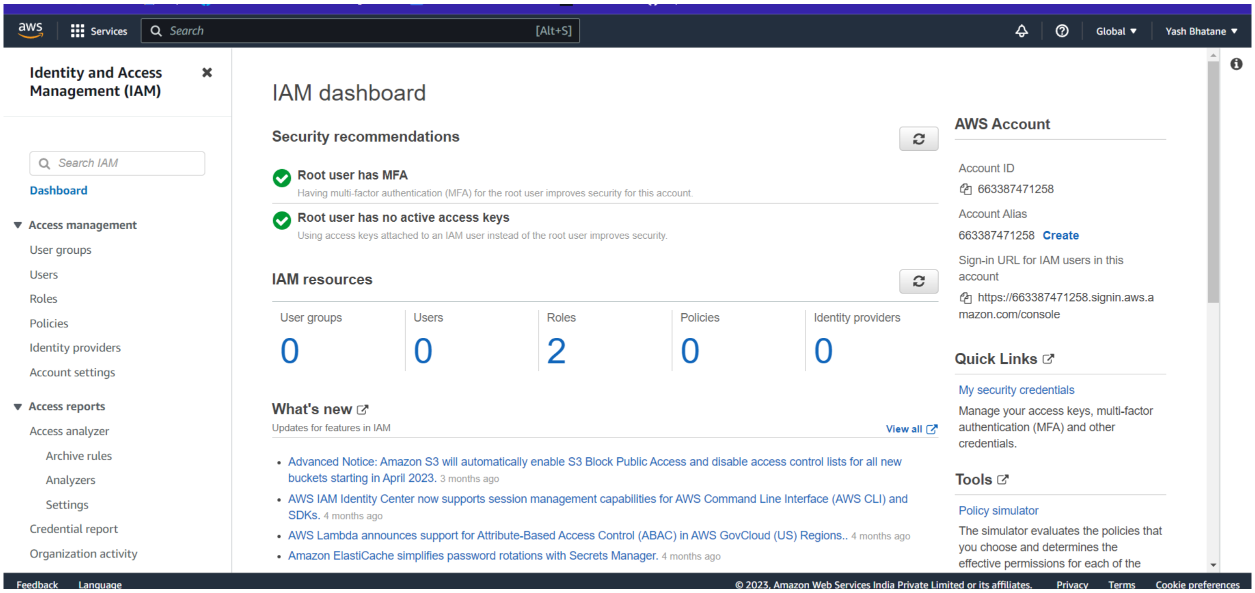
Canonical user ID
448fbc7213e0ba3fedc7508d7e83931f87f6775753beedfb394fbb5469b5e67d

Multi-factor authentication (MFA) (1)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more

© 2023, Amazon Web Services India Private Limited or its affiliates.

Next Page :



aws Services Search [Alt+S] Global ▼ Yash Bhatane ▼

Identity and Access Management (IAM) ✖

Search IAM

Dashboard

▼ Access management
- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

▼ Access reports
- Access analyzer
  - Archive rules
  - Analyzers
  - Settings
- Credential report
- Organization activity

IAM dashboard

Security recommendations

✓ **Root user has MFA**
Having multi-factor authentication (MFA) for the root user improves security for this account.

✓ **Root user has no active access keys**
Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

User groups	Users	Roles	Policies	Identity providers
0	0	2	0	0

What's new
Updates for features in IAM
View all

- Advanced Notice: Amazon S3 will automatically enable S3 Block Public Access and disable access control lists for all new buckets starting in April 2023. 3 months ago
- AWS IAM Identity Center now supports session management capabilities for AWS Command Line Interface (AWS CLI) and SDKs. 4 months ago
- AWS Lambda announces support for Attribute-Based Access Control (ABAC) in AWS GovCloud (US) Regions.. 4 months ago
- Amazon ElastiCache simplifies password rotations with Secrets Manager. 4 months ago

AWS Account

Account ID
663387471258

Account Alias
663387471258 **Create**

Sign-in URL for IAM users in this account
https://663387471258.signin.aws.amazon.com/console

Quick Links

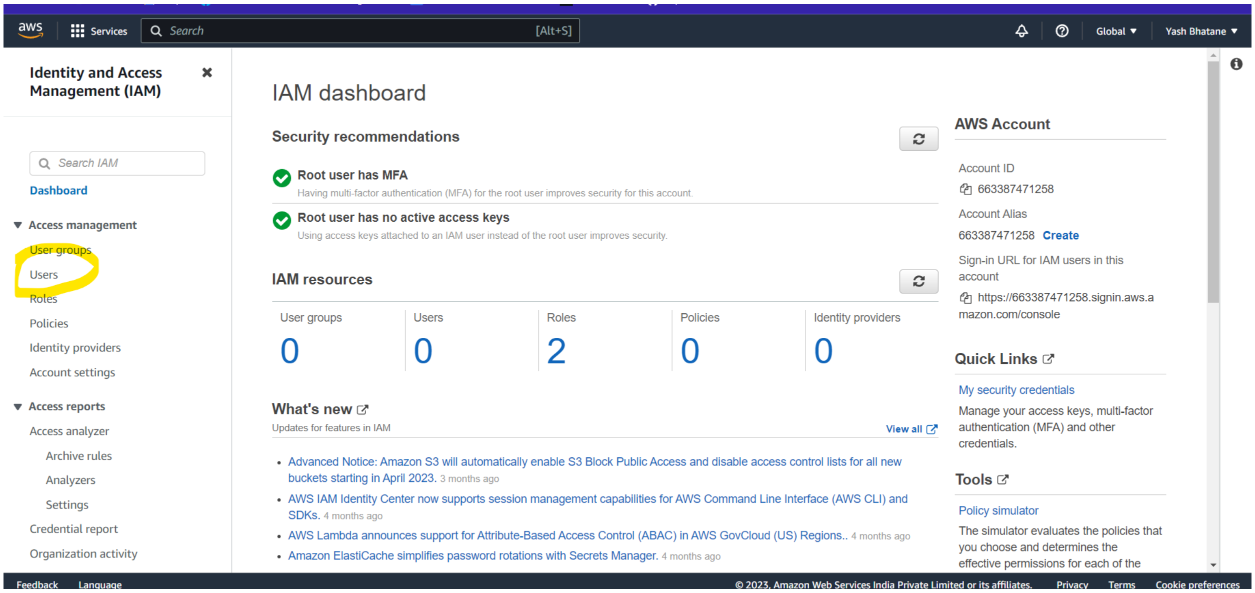
My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.

Tools

Policy simulator
The simulator evaluates the policies that you choose and determines the effective permissions for each of the

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Click on : **Users**



aws Services Search [Alt+S] Global ▼ Yash Bhatane ▼

Identity and Access Management (IAM) ✖

Search IAM

Dashboard

▼ Access management
- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

▼ Access reports
- Access analyzer
  - Archive rules
  - Analyzers
  - Settings
- Credential report
- Organization activity

IAM dashboard

Security recommendations

✓ **Root user has MFA**
Having multi-factor authentication (MFA) for the root user improves security for this account.

✓ **Root user has no active access keys**
Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

User groups	Users	Roles	Policies	Identity providers
0	0	2	0	0

What's new
Updates for features in IAM
View all

- Advanced Notice: Amazon S3 will automatically enable S3 Block Public Access and disable access control lists for all new buckets starting in April 2023. 3 months ago
- AWS IAM Identity Center now supports session management capabilities for AWS Command Line Interface (AWS CLI) and SDKs. 4 months ago
- AWS Lambda announces support for Attribute-Based Access Control (ABAC) in AWS GovCloud (US) Regions.. 4 months ago
- Amazon ElastiCache simplifies password rotations with Secrets Manager. 4 months ago

AWS Account

Account ID
663387471258

Account Alias
663387471258 **Create**

Sign-in URL for IAM users in this account
https://663387471258.signin.aws.amazon.com/console

Quick Links

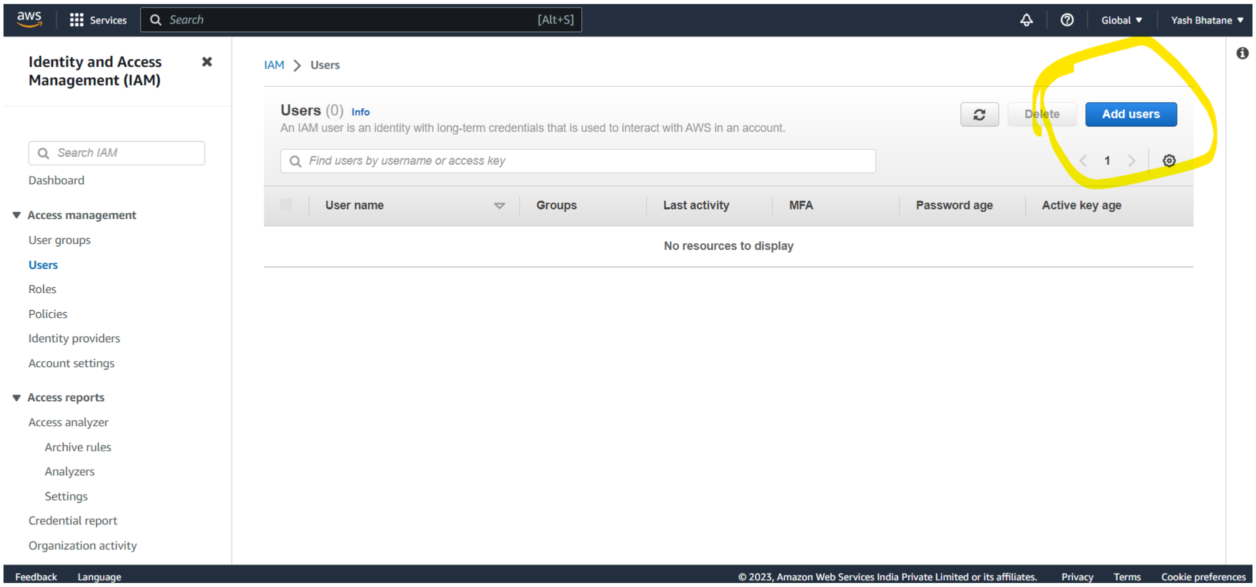
My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.

Tools

Policy simulator
The simulator evaluates the policies that you choose and determines the effective permissions for each of the

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Click on : **Add Users**



Users (0) Info

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

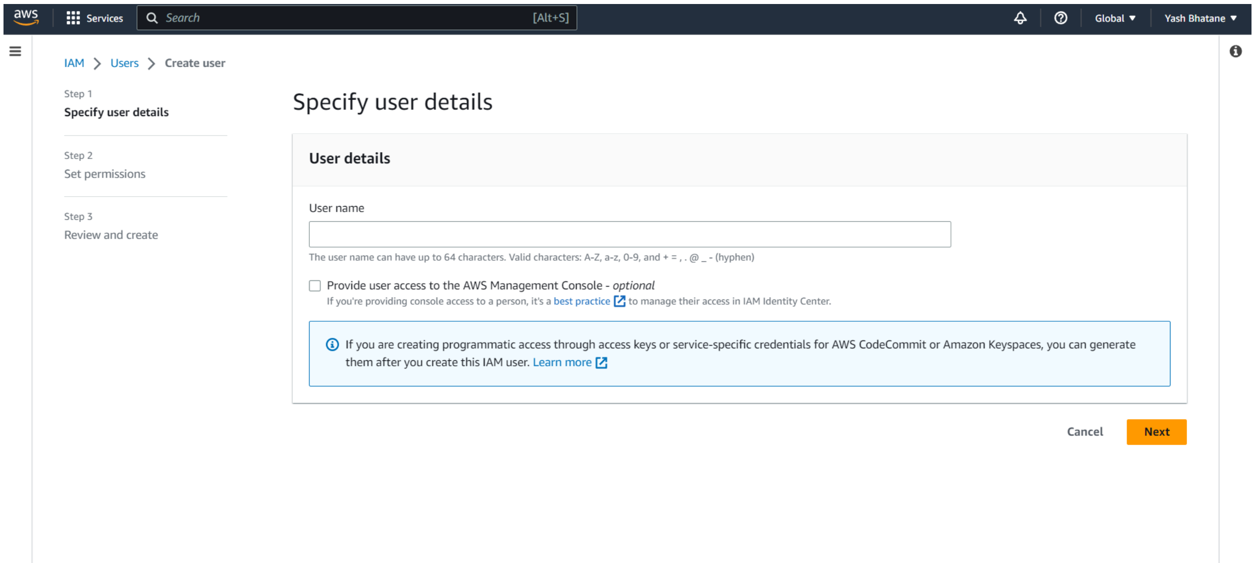
User name	Groups	Last activity	MFA	Password age	Active key age

No resources to display

© 2023, Amazon Web Services India Private Limited or its affiliates.

1) Enter user name :

2) Click on **next**



Specify user details

User details

User name

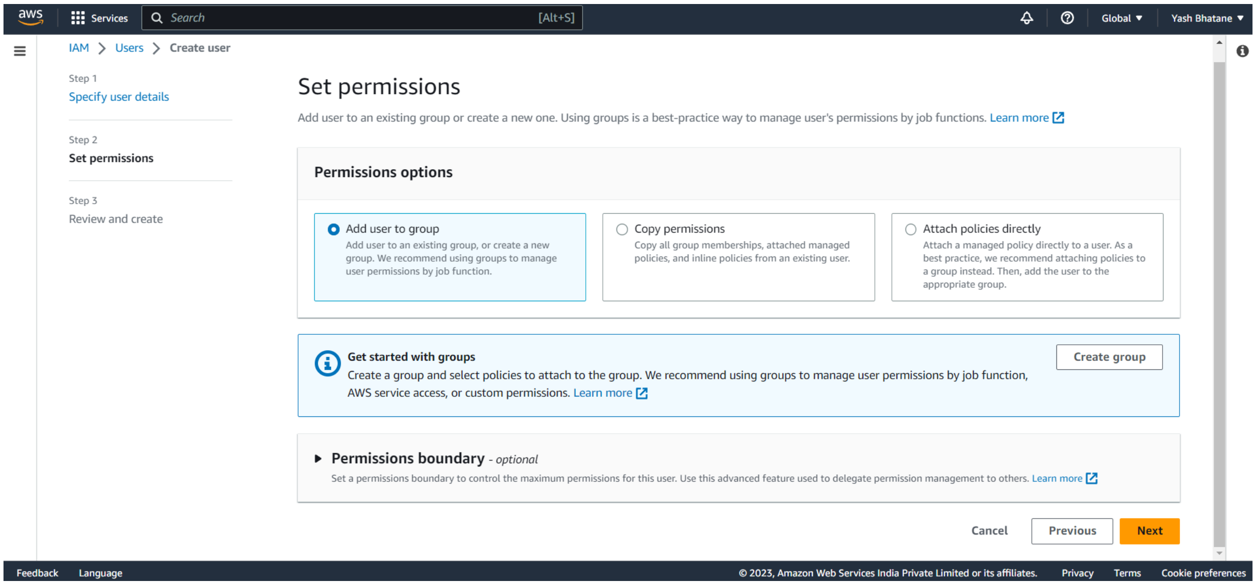
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

□ 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.

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

Click on **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.

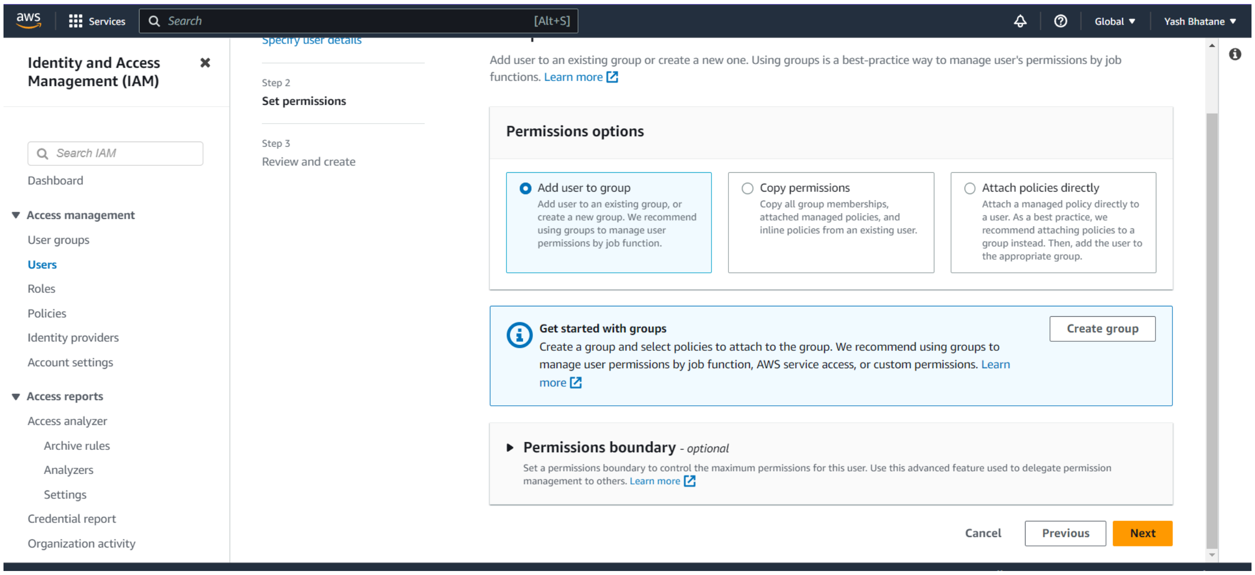
○ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

○ 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.

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

▸ Permissions boundary - *optional*
Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. Learn more

Click **Next**



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.

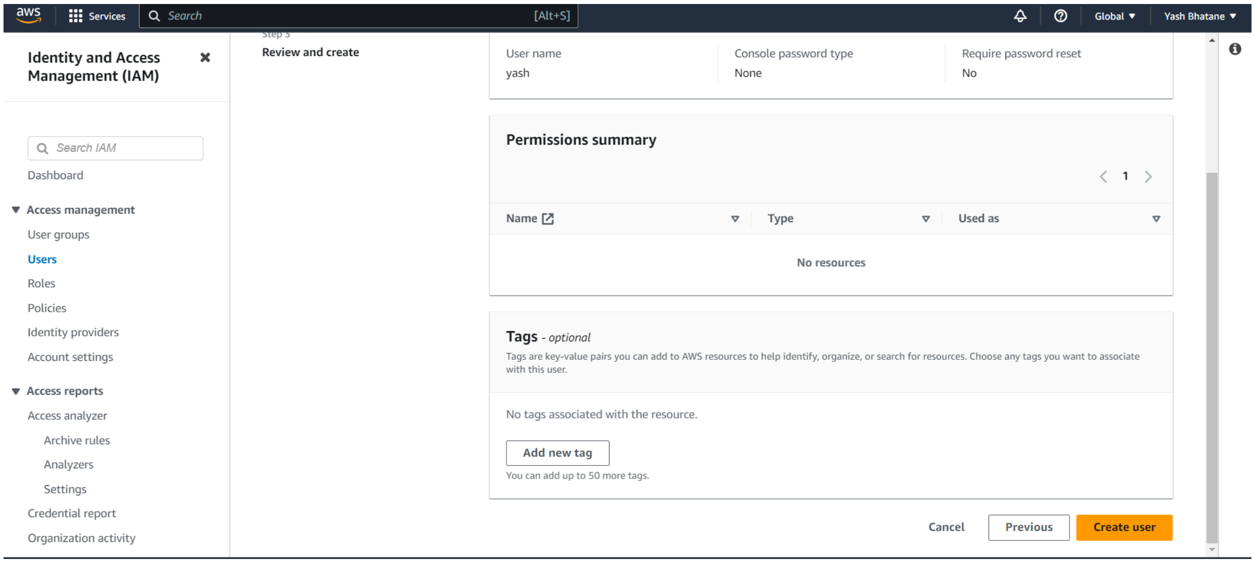
○ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

○ 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.

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

▸ Permissions boundary - *optional*
Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. Learn more

1) Scroll down
2) Click on **Create User**



aws Services Search [Alt+S] Global ▼ Yash Bhatane ▼

Identity and Access Management (IAM) ✖

Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

Organization activity

Step 3

Review and create

User name	Console password type	Require password reset
yash	None	No

Permissions summary

‹ 1 ›

Name	Type	Used as
No resources		

Tags - *optional*

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

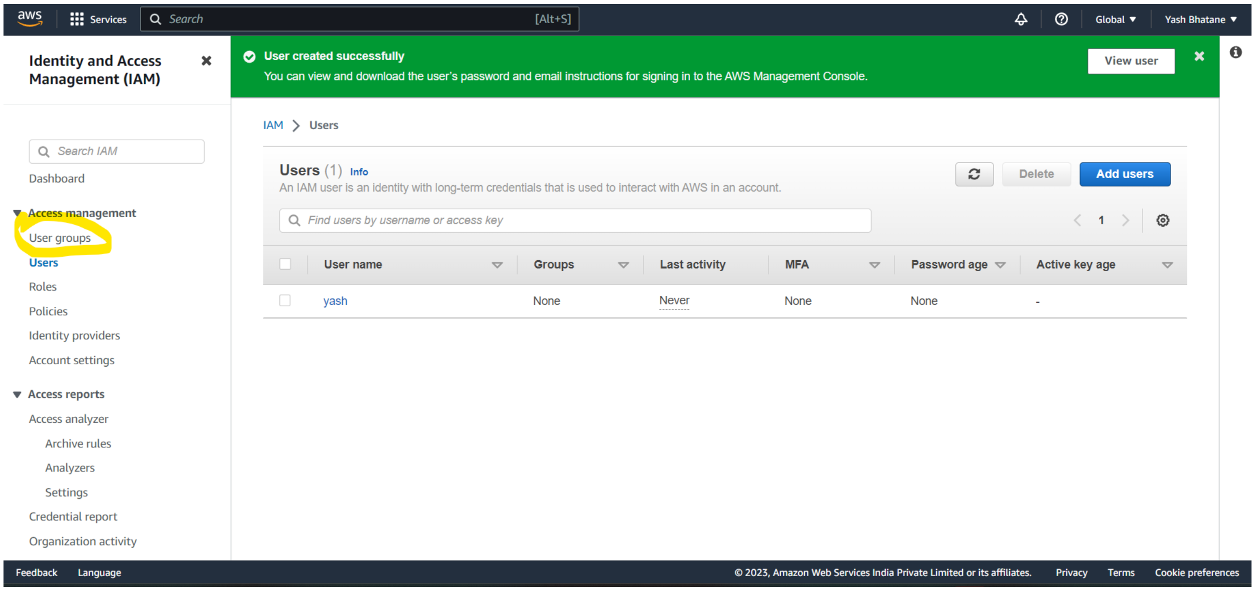
No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel Previous Create user

Click on : **User Groups**



aws Services Search [Alt+S] Global ▼ Yash Bhatane ▼

Identity and Access Management (IAM) ✖

Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

Organization activity

User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

View user ✖

IAM > Users

Users (1) Info

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

Delete Add users

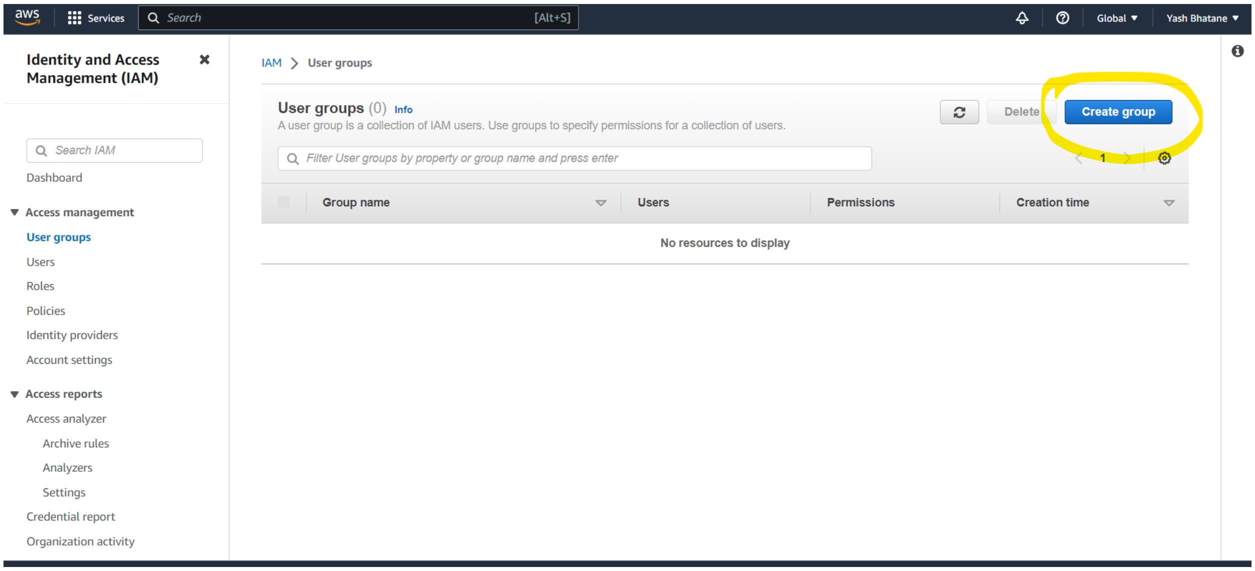
Find users by username or access key

‹ 1 ›

□	User name	Groups	Last activity	MFA	Password age	Active key age
□	yash	None	Never	None	None	-

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Click On : Create Group



User groups (0) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

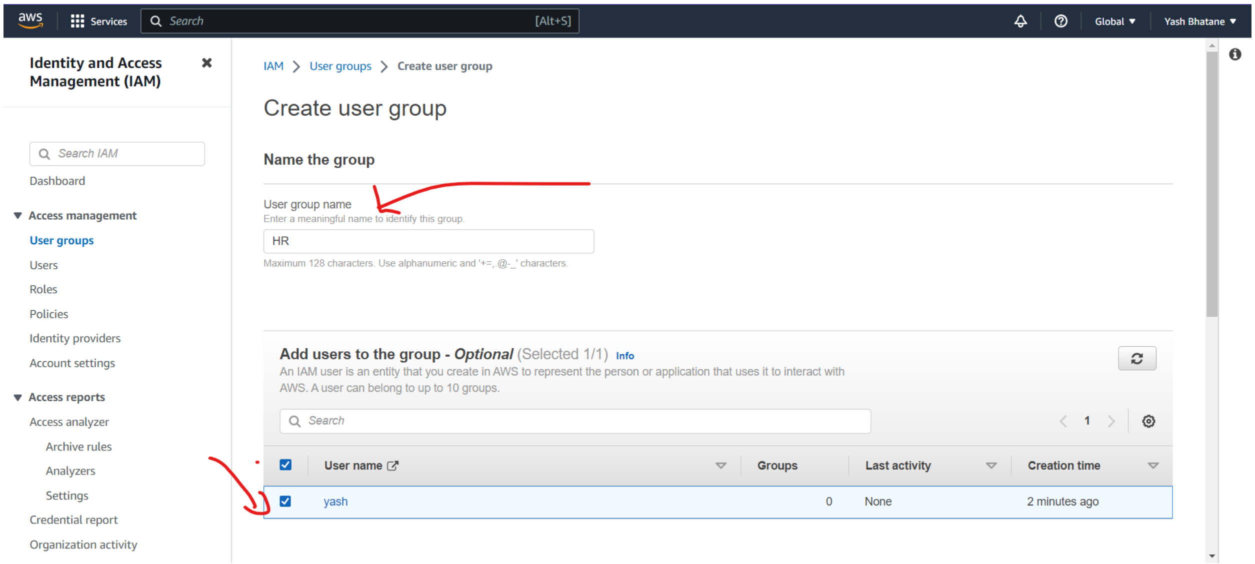
Filter User groups by property or group name and press enter

□	Group name	Users	Permissions	Creation time

No resources to display

1) Enter group name :

2) Select your user :



Create user group

Name the group

User group name

Enter a meaningful name to identify this group.

HR

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

Add users to the group - *Optional* (Selected 1/1) Info

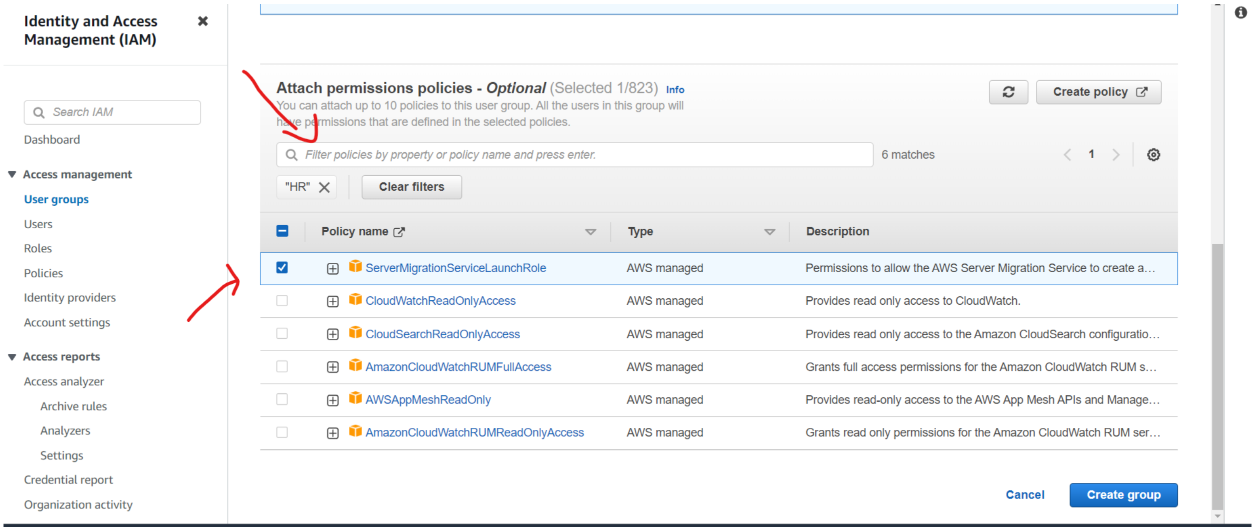
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user can belong to up to 10 groups.

Search

☑	User name	Groups	Last activity	Creation time
☑	yash	0	None	2 minutes ago

1) Search **HR** Permissions here

2) Select 1st option



Attach permissions policies - *Optional* (Selected 1/823) Info

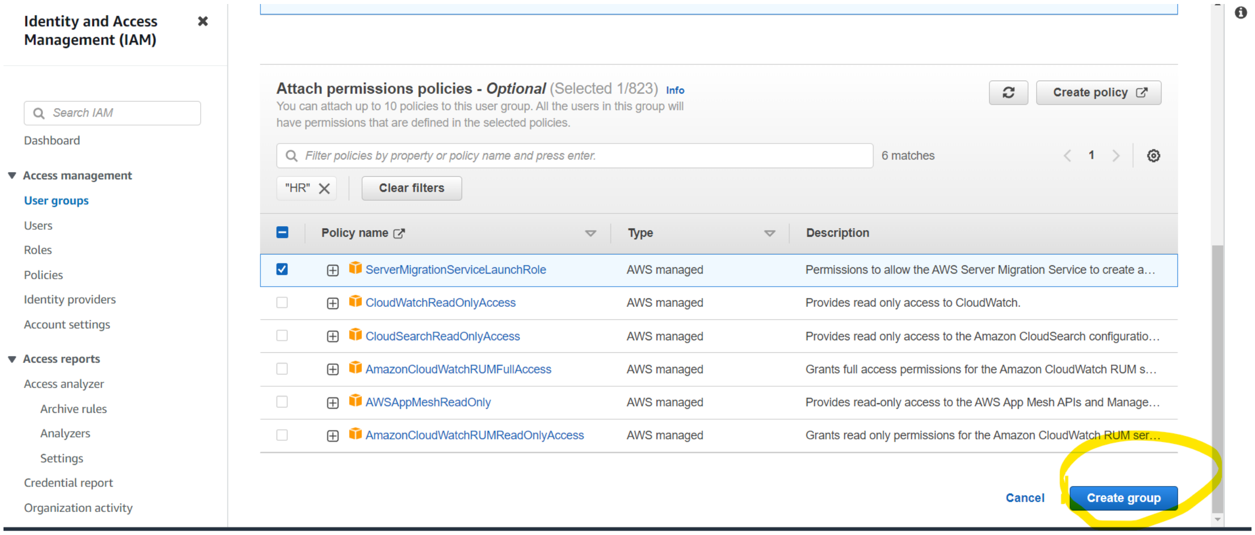
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter policies by property or policy name and press enter. 6 matches 1

"HR" ✕

☐	Policy name	Type	Description
☑	ServerMigrationServiceLaunchRole	AWS managed	Permissions to allow the AWS Server Migration Service to create a…
☐	CloudWatchReadOnlyAccess	AWS managed	Provides read only access to CloudWatch.
☐	CloudSearchReadOnlyAccess	AWS managed	Provides read only access to the Amazon CloudSearch configuratio…
☐	AmazonCloudWatchRUMFullAccess	AWS managed	Grants full access permissions for the Amazon CloudWatch RUM s…
☐	AWSAppMeshReadOnly	AWS managed	Provides read-only access to the AWS App Mesh APIs and Manage…
☐	AmazonCloudWatchRUMReadOnlyAccess	AWS managed	Grants read only permissions for the Amazon CloudWatch RUM ser…

Click on : **Create group**


Attach permissions policies - *Optional* (Selected 1/823) Info

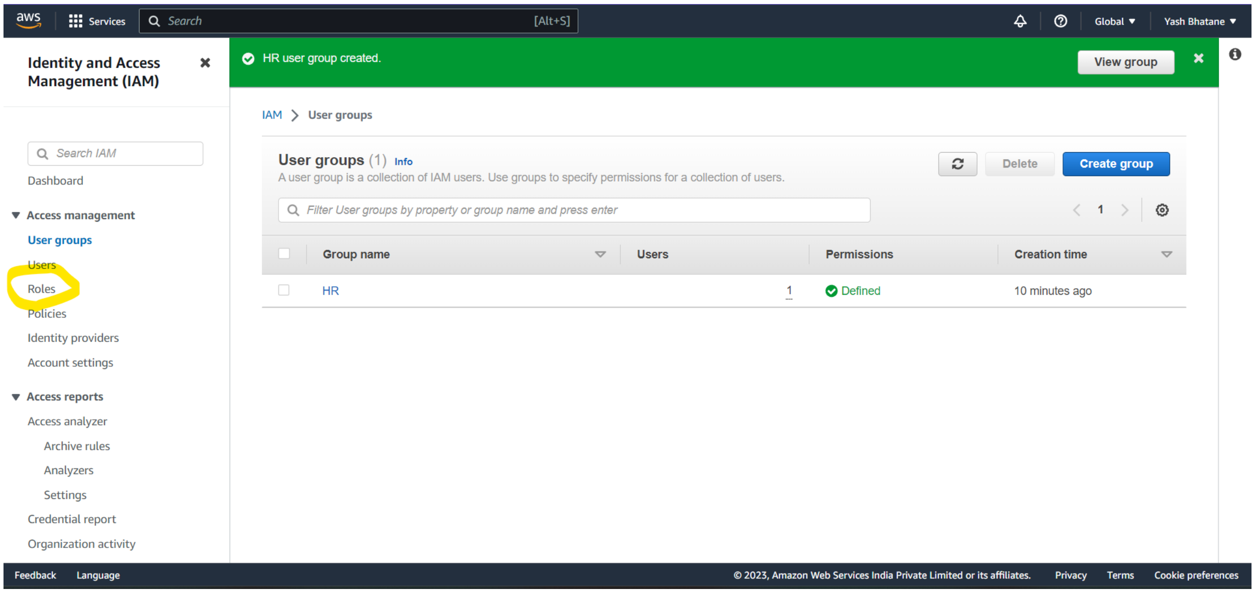
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter policies by property or policy name and press enter. 6 matches 1

"HR" ✕

☐	Policy name	Type	Description
☑	ServerMigrationServiceLaunchRole	AWS managed	Permissions to allow the AWS Server Migration Service to create a…
☐	CloudWatchReadOnlyAccess	AWS managed	Provides read only access to CloudWatch.
☐	CloudSearchReadOnlyAccess	AWS managed	Provides read only access to the Amazon CloudSearch configuratio…
☐	AmazonCloudWatchRUMFullAccess	AWS managed	Grants full access permissions for the Amazon CloudWatch RUM s…
☐	AWSAppMeshReadOnly	AWS managed	Provides read-only access to the AWS App Mesh APIs and Manage…
☐	AmazonCloudWatchRUMReadOnlyAccess	AWS managed	Grants read only permissions for the Amazon CloudWatch RUM ser…

Click on : **Roles**



HR user group created.

Identity and Access Management (IAM)

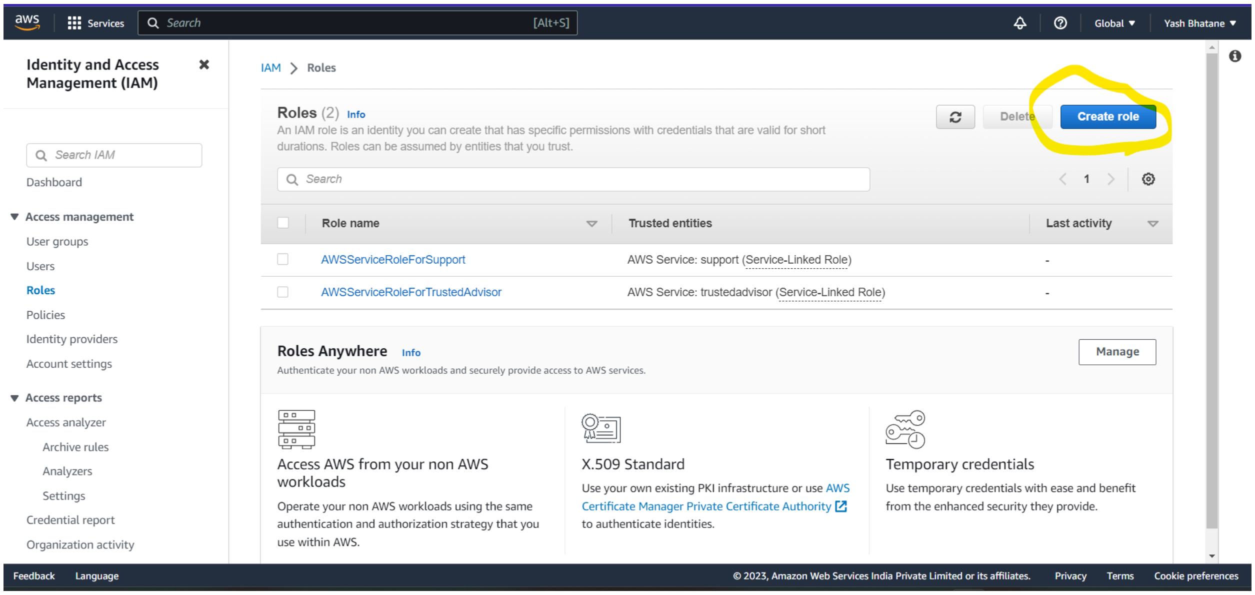
IAM > User groups

User groups (1) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Group name	Users	Permissions	Creation time
HR	1	Defined	10 minutes ago

Click on : **Create role**



Identity and Access Management (IAM)

IAM > Roles

Roles (2) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by identities that you trust.

Role name	Trusted entities	Last activity
AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-

Roles Anywhere Info

Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads

Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.

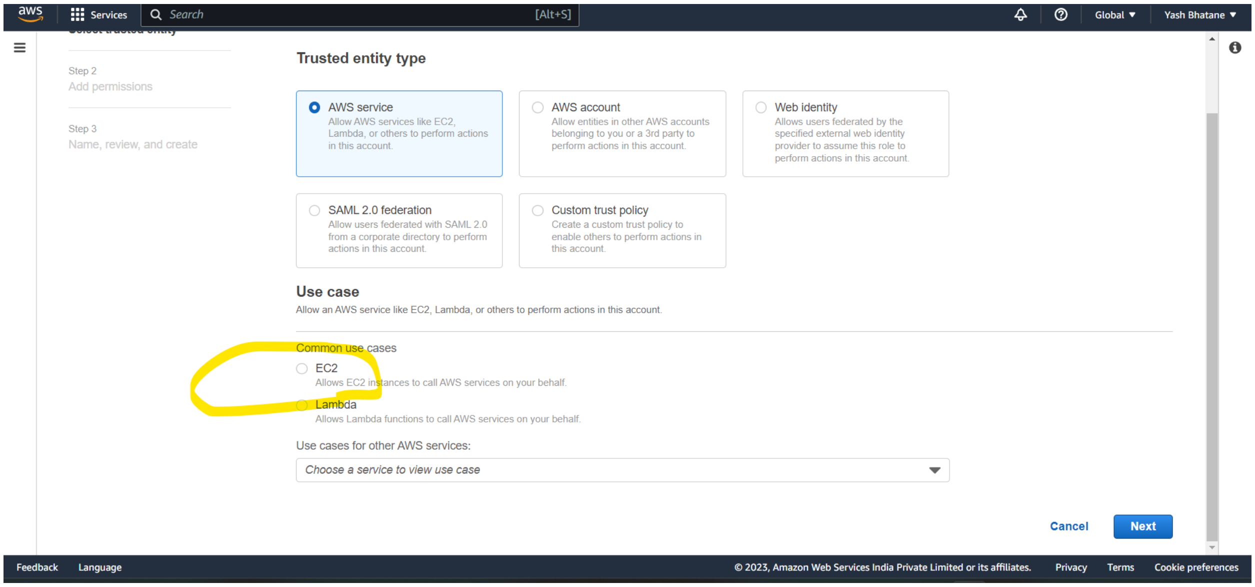
X.509 Standard

Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority to authenticate identities.

Temporary credentials

Use temporary credentials with ease and benefit from the enhanced security they provide.

Select **EC2**



Step 2
Add permissions

Step 3
Name, review, and create

Trusted entity type

● AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Common use cases

○ EC2
Allows EC2 instances to call AWS services on your behalf.

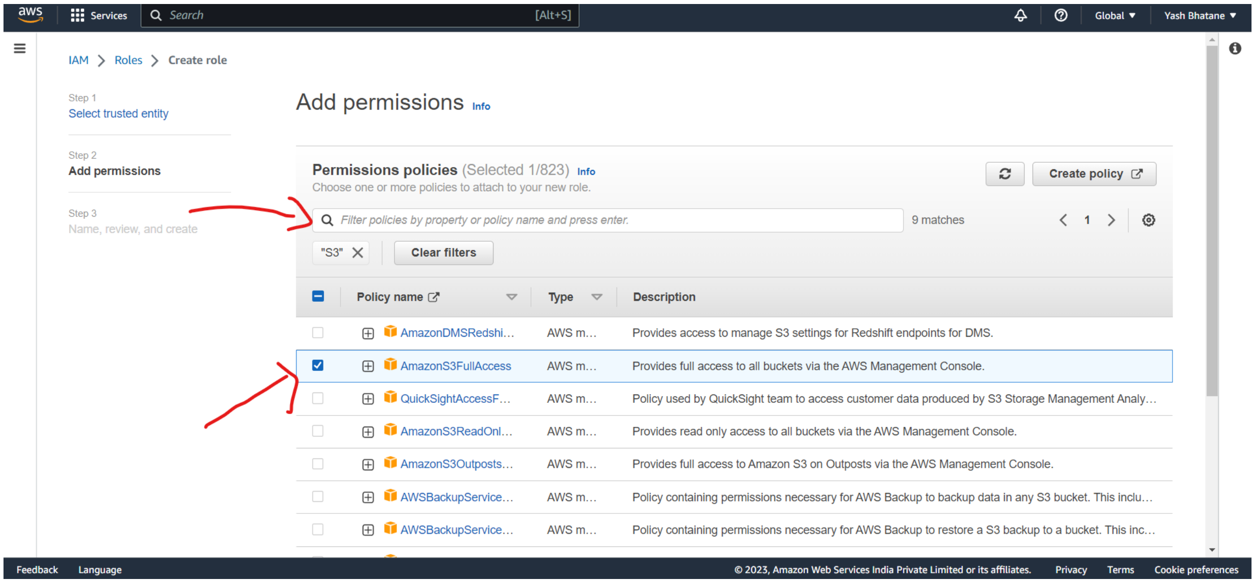
○ Lambda
Allows Lambda functions to call AWS services on your behalf.

Use cases for other AWS services:

Choose a service to view use case

Cancel Next

1) Search **S3**
2) Select 2nd option



IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Add permissions Info

Permissions policies (Selected 1/823) Info

Choose one or more policies to attach to your new role.

Create policy

Filter policies by property or policy name and press enter.

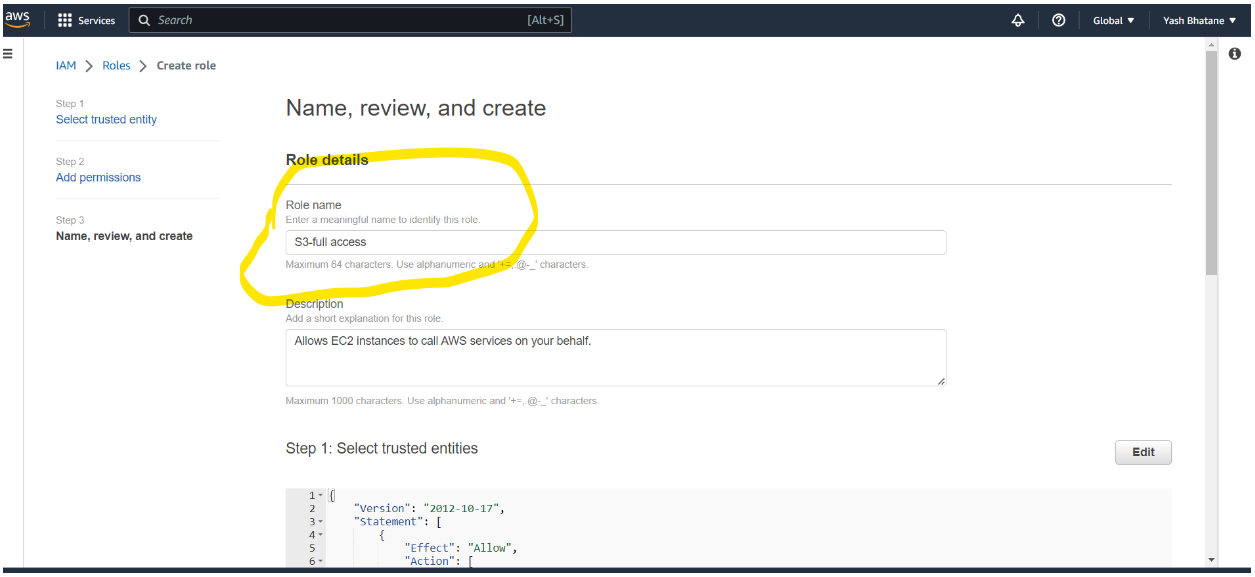
9 matches

< 1 >

"S3" ✕ Clear filters

☐	Policy name	Type	Description
☐	AmazonDMSRedshi...	AWS m...	Provides access to manage S3 settings for Redshift endpoints for DMS.
☑	AmazonS3FullAccess	AWS m...	Provides full access to all buckets via the AWS Management Console.
☐	QuickSightAccessF...	AWS m...	Policy used by QuickSight team to access customer data produced by S3 Storage Management Analy...
☐	AmazonS3ReadOnl...	AWS m...	Provides read only access to all buckets via the AWS Management Console.
☐	AmazonS3Outposts...	AWS m...	Provides full access to Amazon S3 on Outposts via the AWS Management Console.
☐	AWSBackupService...	AWS m...	Policy containing permissions necessary for AWS Backup to backup data in any S3 bucket. This inclu...
☐	AWSBackupService...	AWS m...	Policy containing permissions necessary for AWS Backup to restore a S3 backup to a bucket. This inc...

1) Enter a meaningful name for role
2) Scroll down and click on : **Create role**



Name, review, and create

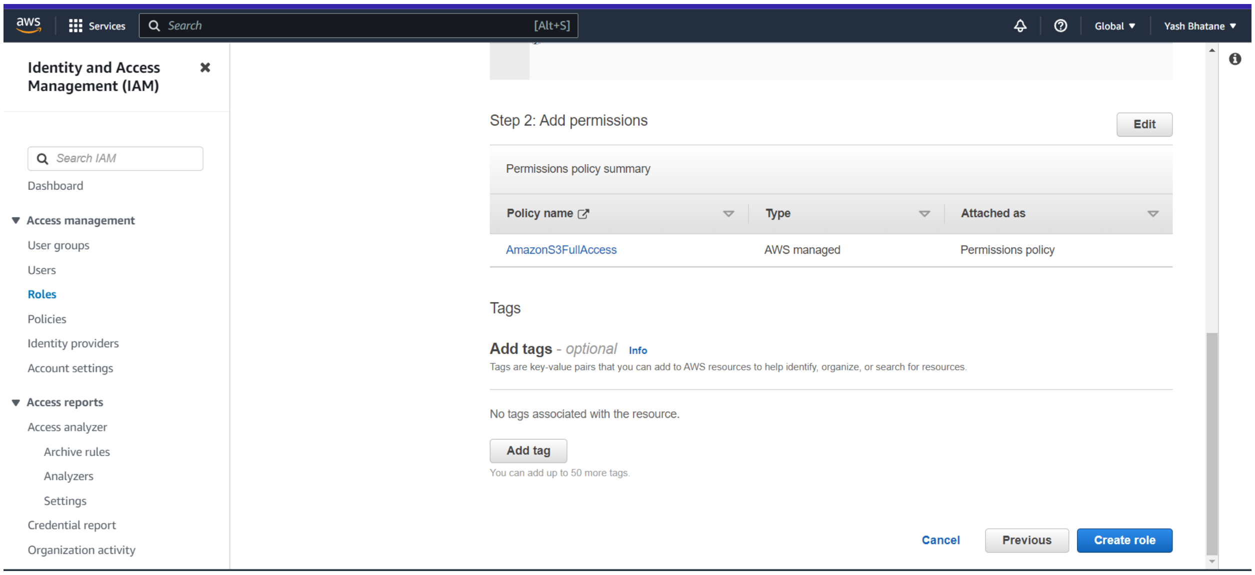
Role details

Role name
Enter a meaningful name to identify this role.
S3-full access
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Step 1: Select trusted entities

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```



Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
AmazonS3FullAccess	AWS managed	Permissions policy

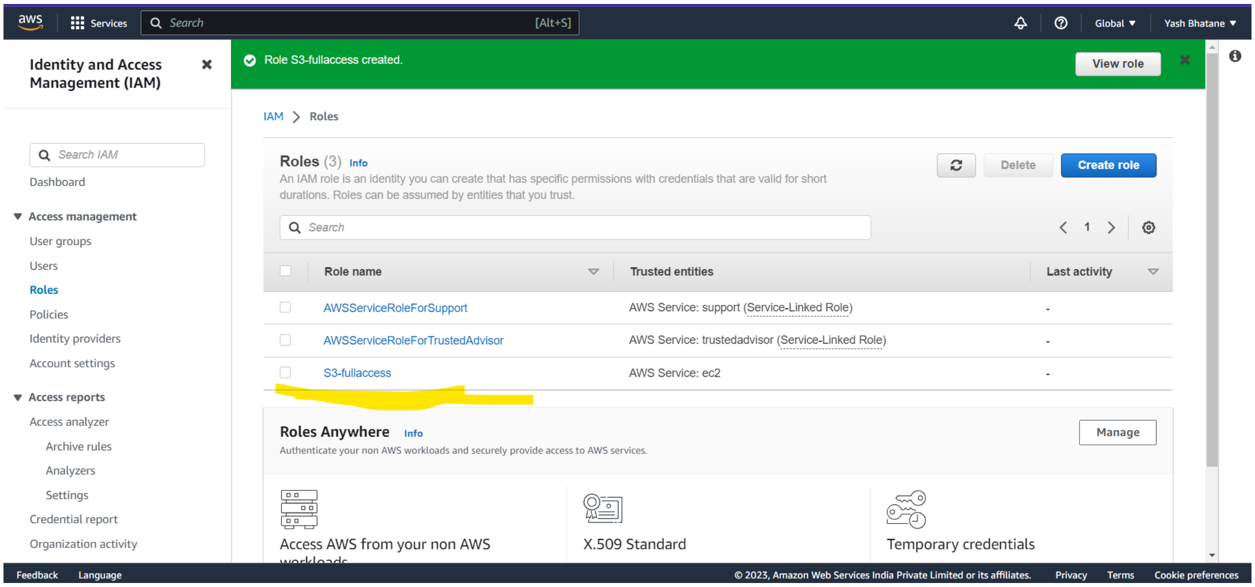
Tags

Add tags - *optional* Info
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

You can add up to 50 more tags.

Your role is created.



Role S3-fullaccess created.

Roles (3) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

□	Role name	Trusted entities	Last activity
□	AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
□	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
□	S3-fullaccess	AWS Service: ec2	-

Roles Anywhere Info

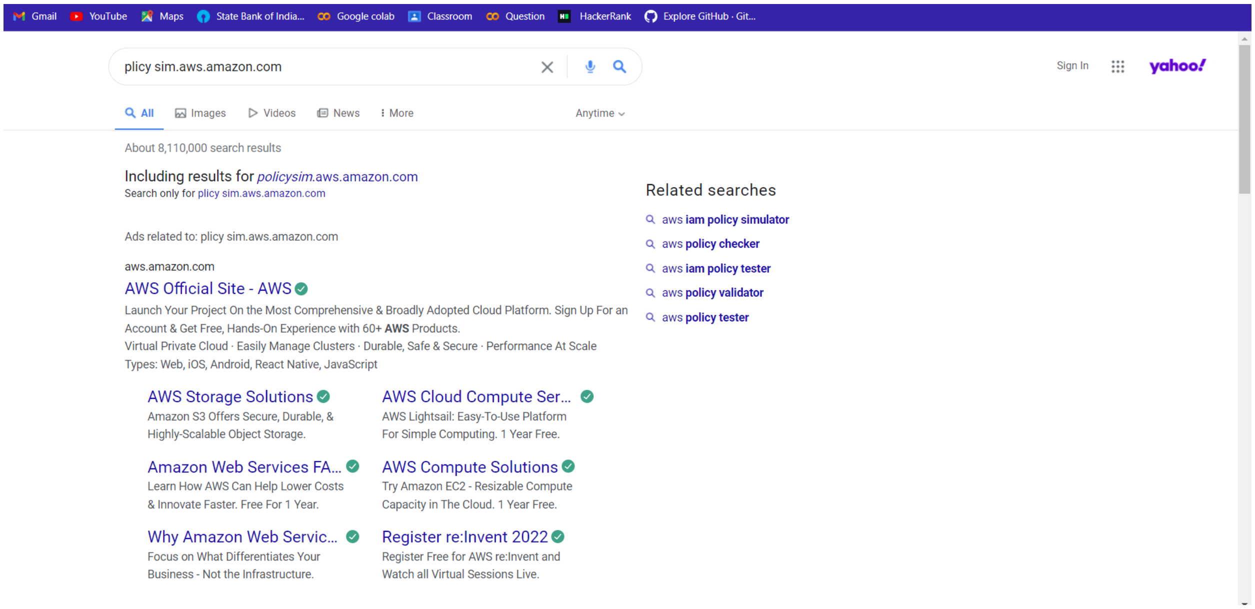
Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads

X.509 Standard

Temporary credentials

IAM : Policy simulator check for authentic users, these users are authorized to run the resources. Test policies that are attached to already existing user groups, is the best way to check any suspected IAM user group or permission.



plicy sim.aws.amazon.com

About 8,110,000 search results

Including results for *policysim*.aws.amazon.com
Search only for plicy sim.aws.amazon.com

Ads related to: plicy sim.aws.amazon.com

aws.amazon.com
AWS Official Site - AWS
Launch Your Project On the Most Comprehensive & Broadly Adopted Cloud Platform. Sign Up For an Account & Get Free, Hands-On Experience with 60+ **AWS** Products.
Virtual Private Cloud · Easily Manage Clusters · Durable, Safe & Secure · Performance At Scale
Types: Web, iOS, Android, React Native, JavaScript

AWS Storage Solutions
Amazon S3 Offers Secure, Durable, & Highly-Scalable Object Storage.

AWS Cloud Compute Ser...
AWS Lightsail: Easy-To-Use Platform For Simple Computing. 1 Year Free.

Amazon Web Services FA...
Learn How AWS Can Help Lower Costs & Innovate Faster. Free For 1 Year.

AWS Compute Solutions
Try Amazon EC2 - Resizable Compute Capacity in The Cloud. 1 Year Free.

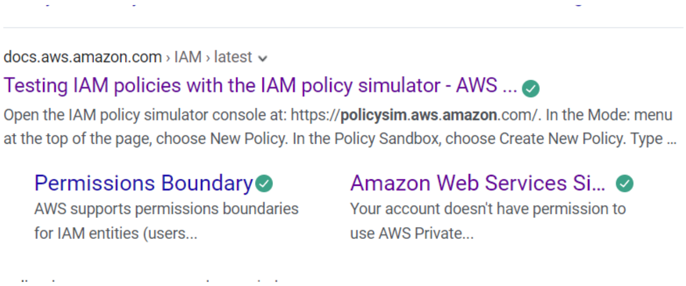
Why Amazon Web Servic...
Focus on What Differentiates Your Business - Not the Infrastructure.

Register re:Invent 2022
Register Free for AWS re:Invent and Watch all Virtual Sessions Live.

Related searches

- aws **iam policy simulator**
- aws **policy checker**
- aws **iam policy tester**
- aws **policy validator**
- aws **policy tester**

Open this site



docs.aws.amazon.com › IAM › latest

Testing IAM policies with the IAM policy simulator - AWS ...

Open the IAM policy simulator console at: https://**policysim.aws.amazon**.com/. In the Mode: menu at the top of the page, choose New Policy. In the Policy Sandbox, choose Create New Policy. Type ...

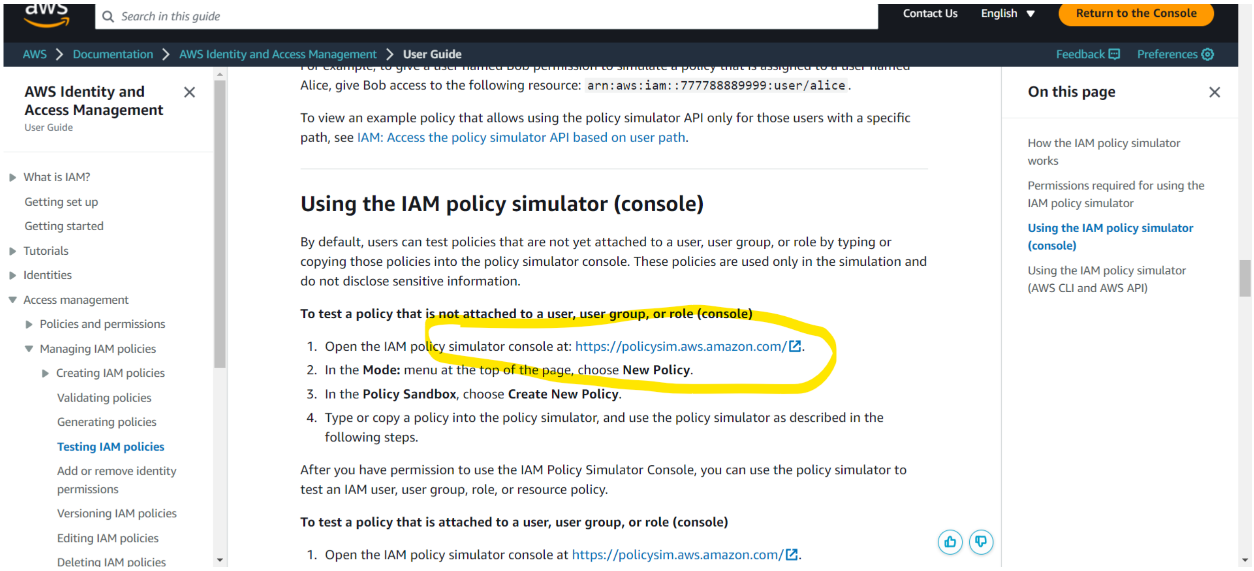
Permissions Boundary

AWS supports permissions boundaries for IAM entities (users...

Amazon Web Services Si...

Your account doesn't have permission to use AWS Private...

Click on site



For example, to give a user named Bob permission to simulate a policy that is assigned to a user named Alice, give Bob access to the following resource: `arn:aws:iam::777788889999:user/alice`.

To view an example policy that allows using the policy simulator API only for those users with a specific path, see IAM: Access the policy simulator API based on user path.

Using the IAM policy simulator (console)

By default, users can test policies that are not yet attached to a user, user group, or role by typing or copying those policies into the policy simulator console. These policies are used only in the simulation and do not disclose sensitive information.

To test a policy that is not attached to a user, user group, or role (console)

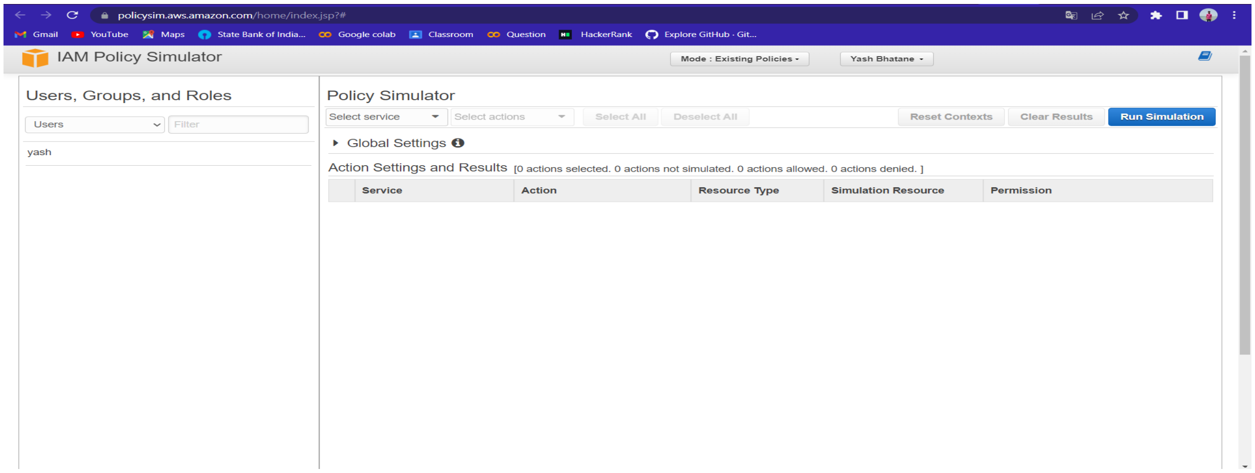
1. Open the IAM policy simulator console at: https://policysim.aws.amazon.com/.
2. In the **Mode:** menu at the top of the page, choose **New Policy**.
3. In the **Policy Sandbox**, choose **Create New Policy**.
4. Type or copy a policy into the policy simulator, and use the policy simulator as described in the following steps.

After you have permission to use the IAM Policy Simulator Console, you can use the policy simulator to test an IAM user, user group, role, or resource policy.

To test a policy that is attached to a user, user group, or role (console)

1. Open the IAM policy simulator console at https://policysim.aws.amazon.com/.

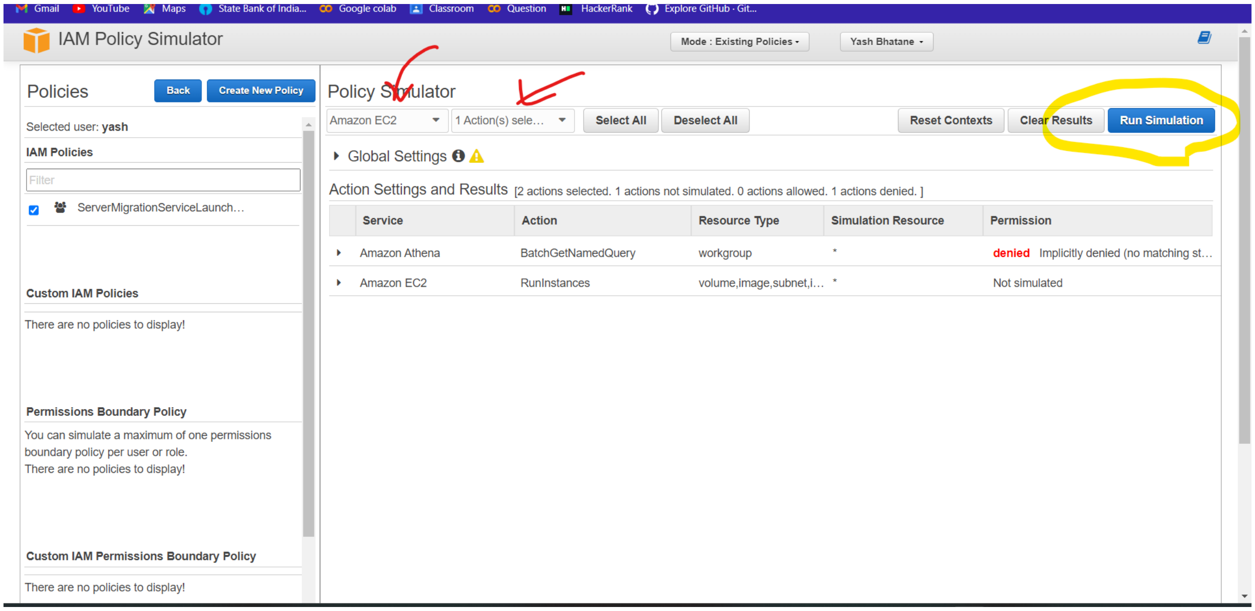
Click on your user :



Action Settings and Results [0 actions selected. 0 actions not simulated. 0 actions allowed. 0 actions denied.]

	Service	Action	Resource Type	Simulation Resource	Permission

1) In select service : **EC2**
2) In action select : **Runinstances**
3) Click on **Run Simulation**



Selected user: yash

IAM Policies

☑ ServerMigrationServiceLaunch...

Custom IAM Policies

There are no policies to display!

Permissions Boundary Policy

You can simulate a maximum of one permissions boundary policy per user or role.
There are no policies to display!

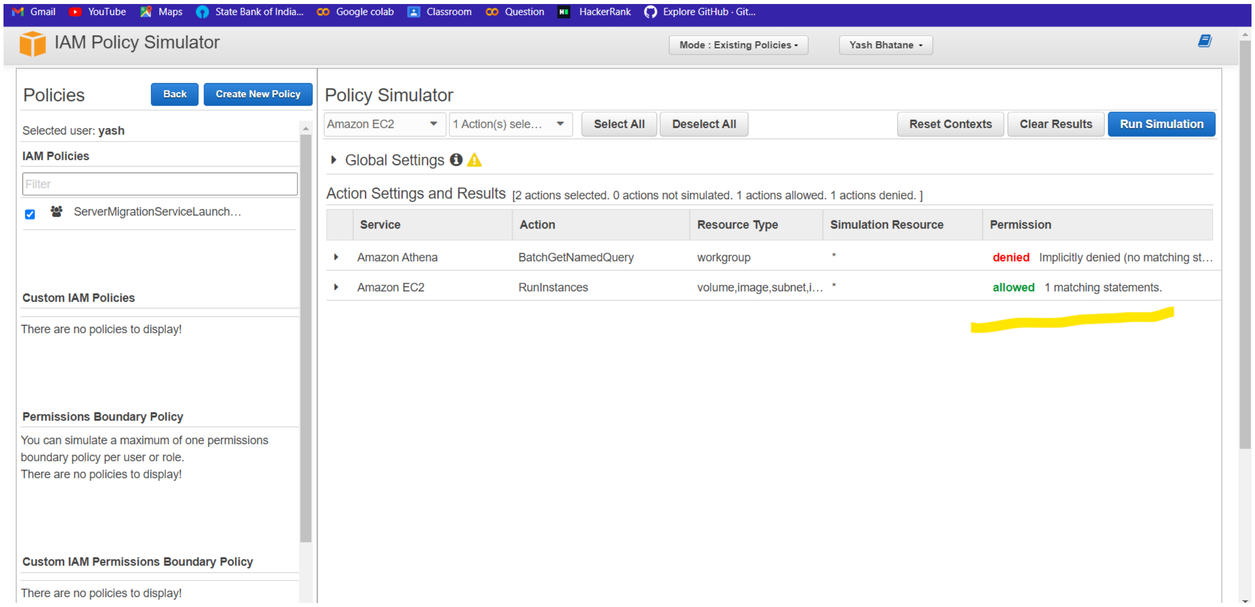
Custom IAM Permissions Boundary Policy

There are no policies to display!

Action Settings and Results [2 actions selected. 1 actions not simulated. 0 actions allowed. 1 actions denied.]

	Service	Action	Resource Type	Simulation Resource	Permission
▸	Amazon Athena	BatchGetNamedQuery	workgroup	*	denied Implicitly denied (no matching st...
▸	Amazon EC2	RunInstances	volume,image,subnet,i...	*	Not simulated

After Run



Selected user: yash

IAM Policies

Filter

☑ ServerMigrationServiceLaunch…

Custom IAM Policies

There are no policies to display!

Permissions Boundary Policy

You can simulate a maximum of one permissions boundary policy per user or role.
There are no policies to display!

Custom IAM Permissions Boundary Policy

There are no policies to display!

Amazon EC2 | 1 Action(s) sele…

Action Settings and Results [2 actions selected. 0 actions not simulated. 1 actions allowed. 1 actions denied.]

Service	Action	Resource Type	Simulation Resource	Permission
Amazon Athena	BatchGetNamedQuery	workgroup	*	denied Implicitly denied (no matching st…
Amazon EC2	RunInstances	volume,image,subnet,i…	*	allowed 1 matching statements.

S3 -

S3 simple storage service is a highly scalable secure cloud base storage provided by AWS. It enables individuals and organizations to store and retrieve data/object/file or any kind of unstructured data over the internet globally.

There are three feature :

1) **Object storage** : provide secure, durable, highly scalable object storage.
2) **Scalable** : It allows the user or organization to store and retrieve data from anywhere and at a very low cost.
3) **Simple** :
   - AWS is a web service interface. Here data is managed as an object rather than a file or block. In this we can upload files of any type like photos, videos, text files,pdf,ppt etc.

- It can not be used to run an operating system or database.
- This provides ultimate storage (the total volume of data and object you can store unlimited)
- As we said everything is stored in object format size of object 0bite to 5 terabyte
- S3 bucket stores files in a bucket similarly like folders.
- When you work with S3 bucket the following things you should need to follow.
    1. Universal namespace : As all AWS account S3 namespace each S3 bucket name should be uniq.
    2. When you upload a file to an s3 bucket you will receive an **http** code 200 if uploaded successfully.

S3 stores anything in key value pair :

- **Key** is name of object eg. file.txt
- **Values data** itself which is made up of sequence of byte
- **Version id** is an important entity for storing versions of the same kind of object.
- **Meta data** stores data about data. Eg. last modified