

## LAB 1: IAM User (Free TIER)

### Foot Print of AWS Datacenters

- **Who is AWS?**

- Amazon Web Services launched in 2006 and today is 2020 and AWS Provide 200+ Services (Network, Compute, Storage, Databases, Developer Tools etc.) and also Include Block Chain, IOT and Serverless as well. In Short AWS Provide Everything.



### AWS Regions

- 22 Regions
- 70 Availability Zone
- <https://infrastructure.aws/>



- 🔍 See AWS Management Console. <https://aws.amazon.com/console/>
- 🔍 See AWS Global infrastructure. <https://aws.amazon.com/about-aws/global-infrastructure/>
- 🔍 Look for AZ and POPs and potential customers.
- 🔍 See Free tier services.
- 🔍 Create your Account.

aws

Contact Sales Support English My Account Sign In to the Console

re:Invent Products Solutions Pricing Documentation Learn Partner Network AWS Marketplace Customer Enablement Explore More

AWS Free Tier Overview FAQs Terms and Conditions

**free tier details**

Filter by:  
Clear all filters

Tier Type

- ☐ Featured
- ☐ 12 Months Free
- ☐ Always Free
- ☐ Trials

Product Categories

- ☐ Analytics
- ☐ Application Integration
- ☐ Business Productivity
- ☐ Compute
- ☐ Customer Engagement
- ☐ Database
- ☐ Developer tools

Search free tier products

COMPUTE	STORAGE	DATABASE
<p>Free Tier 12 MONTHS FREE</p> <p><b>Amazon EC2</b></p> <p><b>750 Hours</b></p> <p>per month</p> <p>Resizable compute capacity in the Cloud.</p> <p><small>*FEC focuses new month of 12,000, 20,000, or 30 EC2</small></p>	<p>Free Tier 12 MONTHS FREE</p> <p><b>Amazon S3</b></p> <p><b>5 GB</b></p> <p>of standard storage</p> <p>Secure, durable, and scalable object storage infrastructure.</p> <p>5 GB of Standard Storage</p> <p>20,000 Get Requests</p> <p>2,000 Put Requests</p>	<p>Free Tier 12 MONTHS FREE</p> <p><b>Amazon RDS</b></p> <p><b>750 Hours</b></p> <p>per month of db.t2.micro database usage (applicable DB engines)</p> <p>Managed Relational Database Service for MySQL, PostgreSQL, MariaDB, Oracle BYOL, or SQL Server.</p>

- Search google for Account Creation: [How do I create and activate amazon account?](#)

aws

Contact Sales Support English My Account Sign In to the Console

re:Invent Products Solutions Pricing Documentation Learn Partner Network AWS Marketplace Customer Enablement Explore More

## How do I create and activate a new AWS account?

Last updated: 2020-10-03


I'm getting started with AWS. How do I create and activate a new AWS account?

### Resolution

#### Create your account

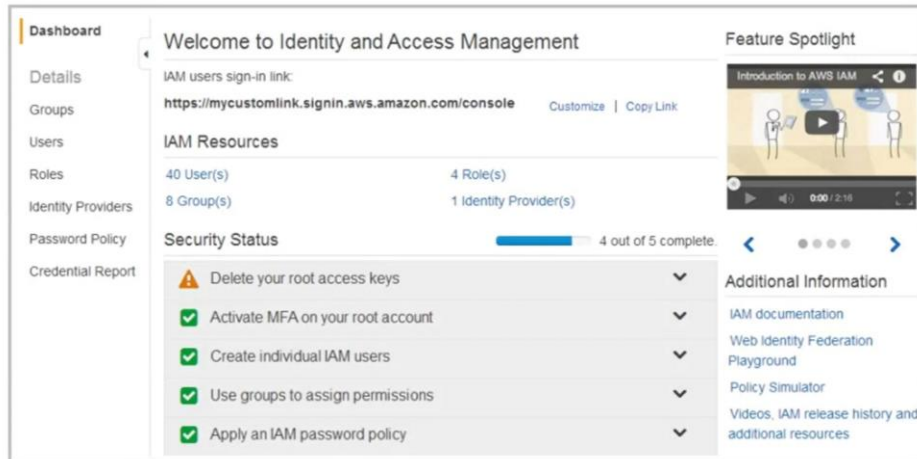
1. Open the Amazon Web Services home page.
2. Choose **Create an AWS Account**.  
**Note:** If you signed in to AWS recently, choose **Sign in to the Console**. If **Create a new AWS account** isn't visible, first choose **Sign in to a different account**, and then choose **Create a new AWS account**.
3. Enter your account information, and then choose **Continue**. Be sure that you enter your account information correctly, especially

#### Related videos



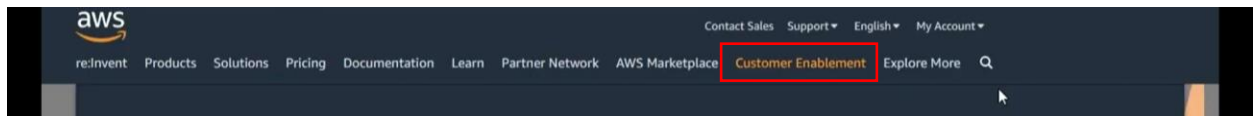
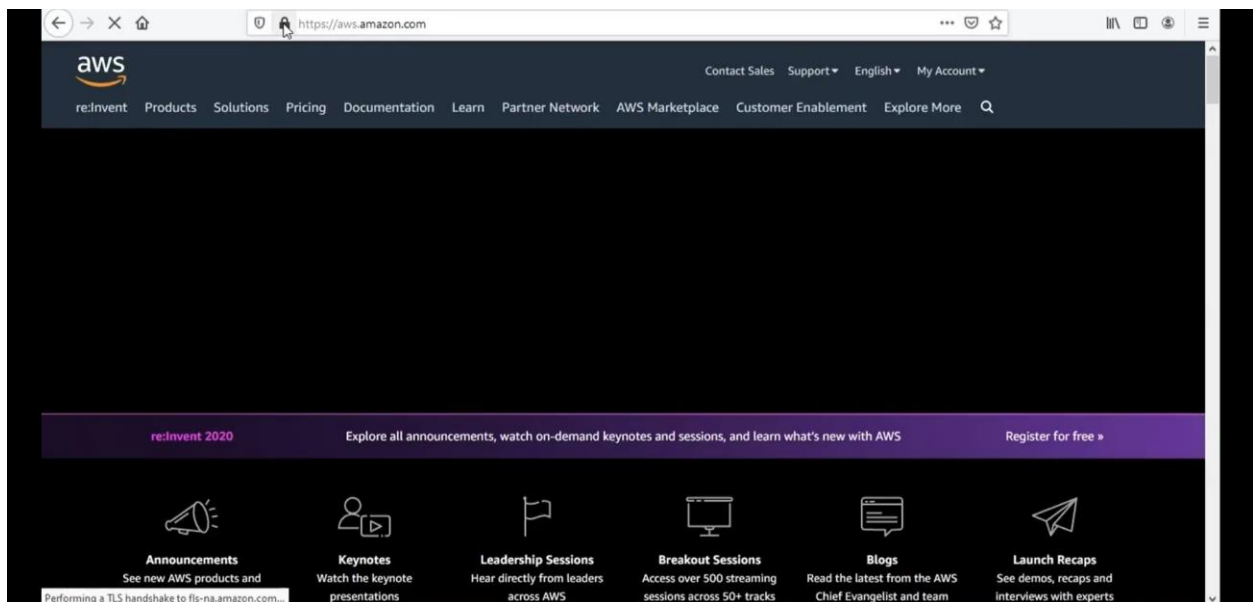
Watch Jamie's video to learn more (4:30)

# IAM Lab Overview



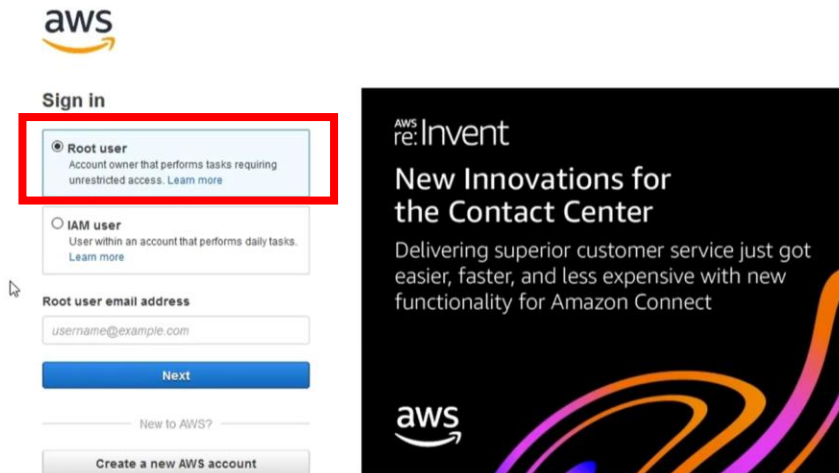
IAM is a regional service.

- Search for IAM service:

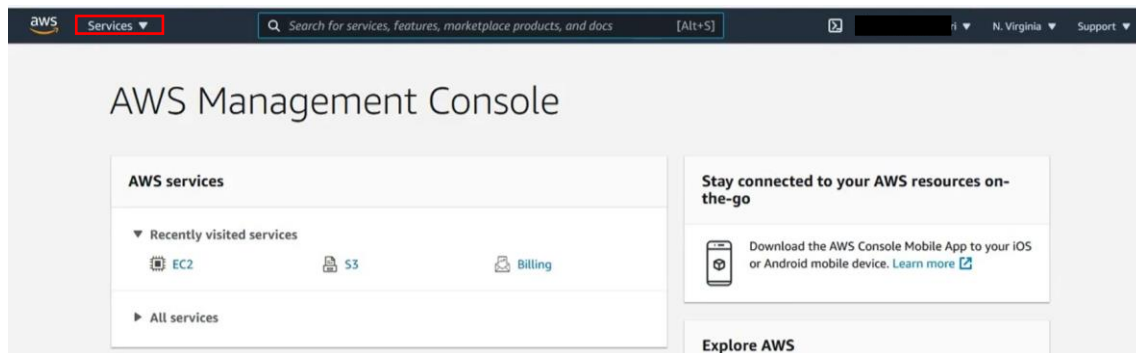


- Click on SignIn to Console and sign in as root user.

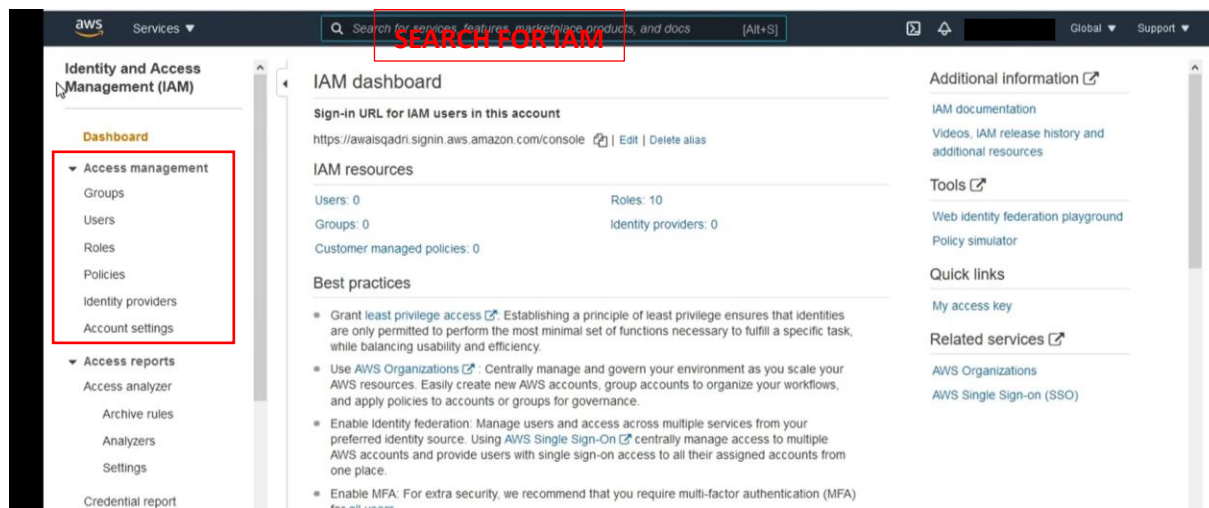




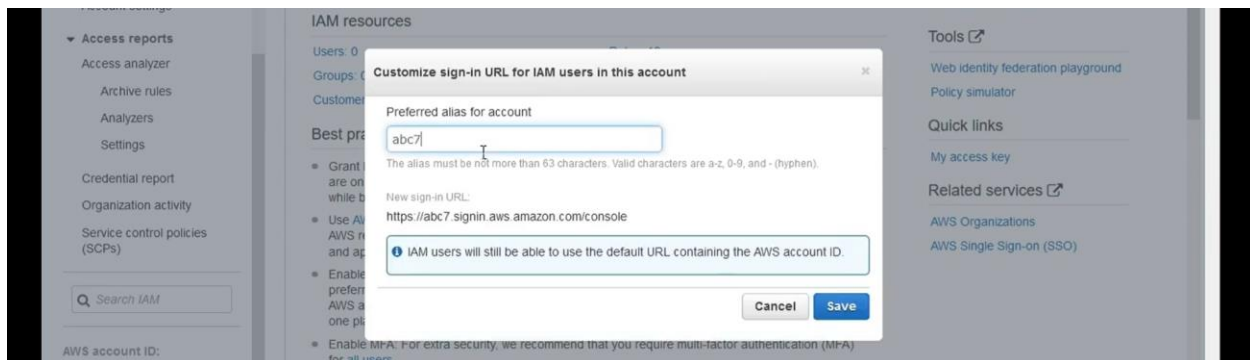
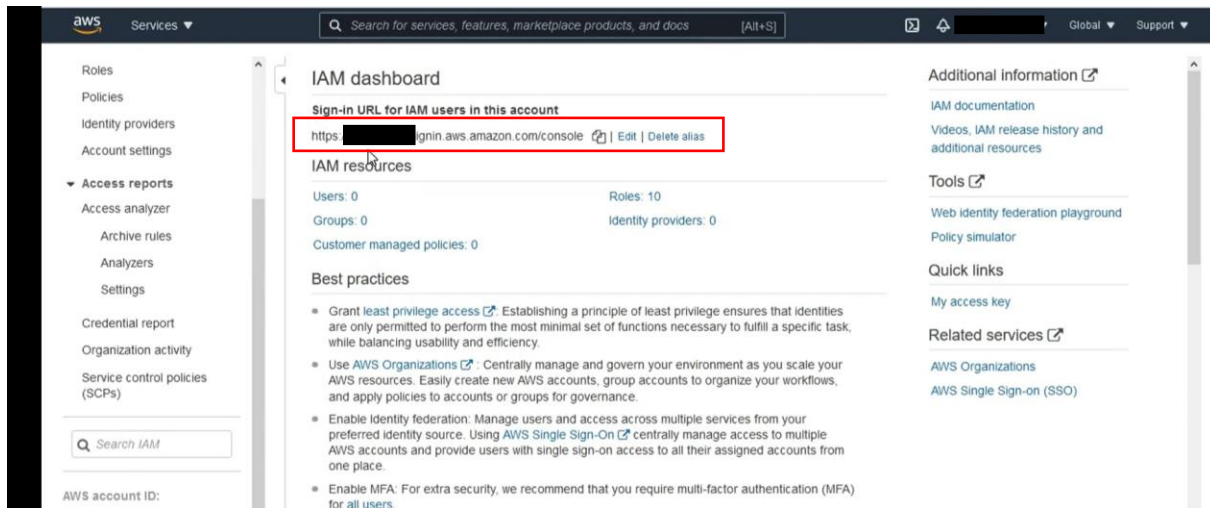
- Search for services.



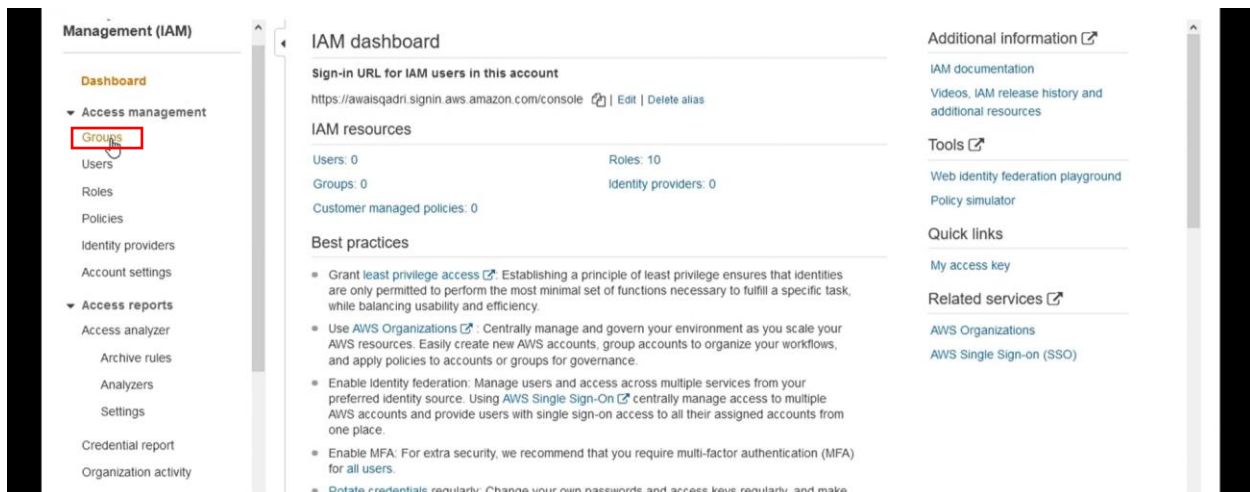
- Look for IAM Service



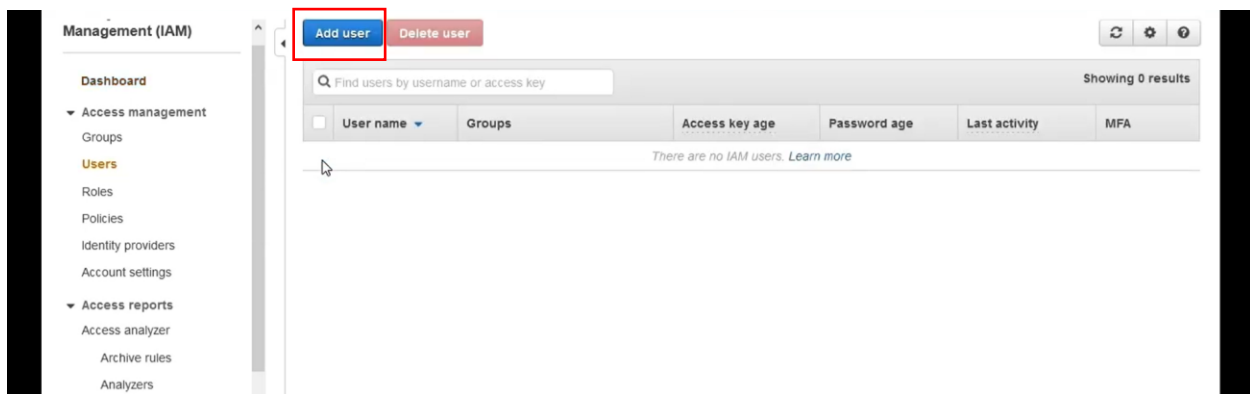
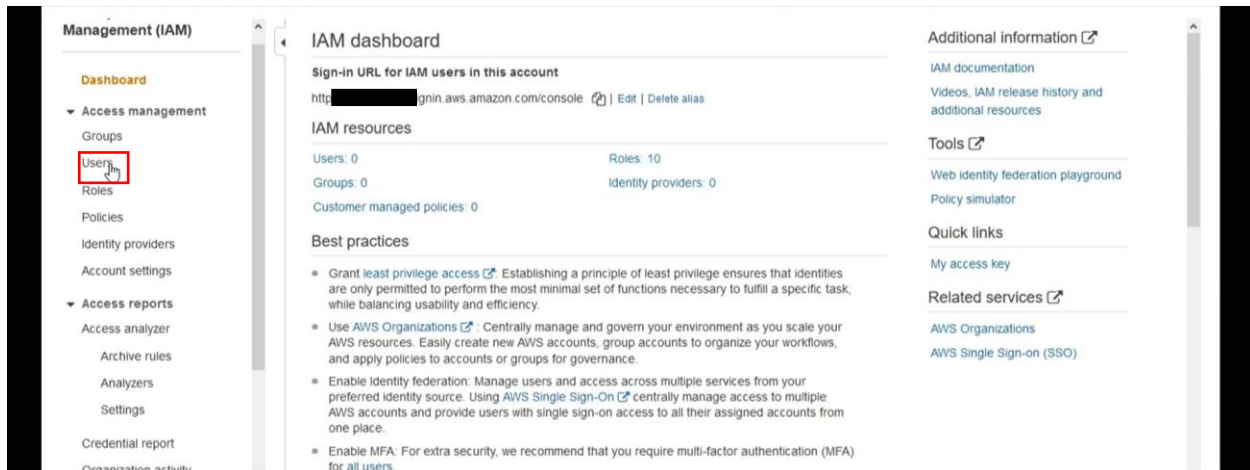
- On IAM dashboard you can see sign in URL and ID against your account. You can aliases or remane by clicking on edit. Alias can be used to login as IAM user.



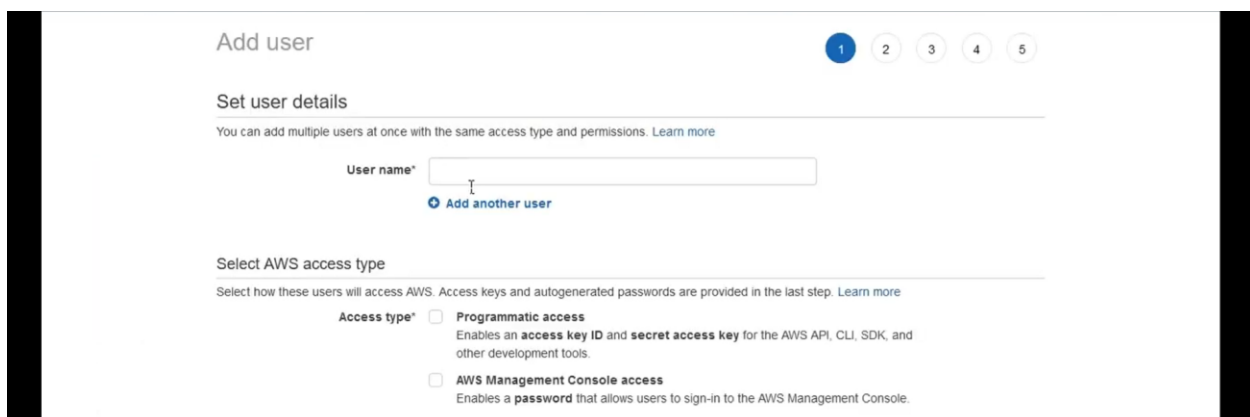
- In IAM you can manage user groups for IAM users created.



- You can add users and also make any user a part of the user group (created). Max 10 users can be added.



- Set the user name and allow the access type for logging in. Programmatic or through console. Both can be given.





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\*

awais

\* Required

Cancel

Next: Permissions

- You have options to add user to a group. Assign user permissions and attach any policy (existing or can be created)

Add user

1
2
3
4
5

Set permissions

Add user to group

Copy permissions from existing user

Attach existing policies directly

Get started with groups

You haven't created any groups yet. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Get started by creating a group. [Learn more](#)

Create group

Add user

1
2
3
4
5

Set permissions

Add user to group

Copy permissions from existing user

Attach existing policies directly

Select an existing user from which to copy policies and group membership.

Copy permissions from existing user

Search

Showing 0 results

User name

Groups

Attached policies

No results

## Add user

1 2 3 4 5

### Set permissions



Add user to group



Copy permissions from existing user



Attach existing policies directly

Create policy



Filter policies

Search

Showing 637 results

	Policy name	Type	Used as
<input type="checkbox"/>	AdministratorAccess	Job function	None
<input type="checkbox"/>	AdministratorAccess-Ampify	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessFullAccess	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	AWS managed	None

- Tags are optional can be used identify particular user.

## 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
Business	Marketing	
Add new key		

You can add 49 more tags.

- Summary of the IAM user created.

## Review

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

### User details

User name	
AWS access type	Programmatic access and AWS Management Console access
Console password type	Autogenerated
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

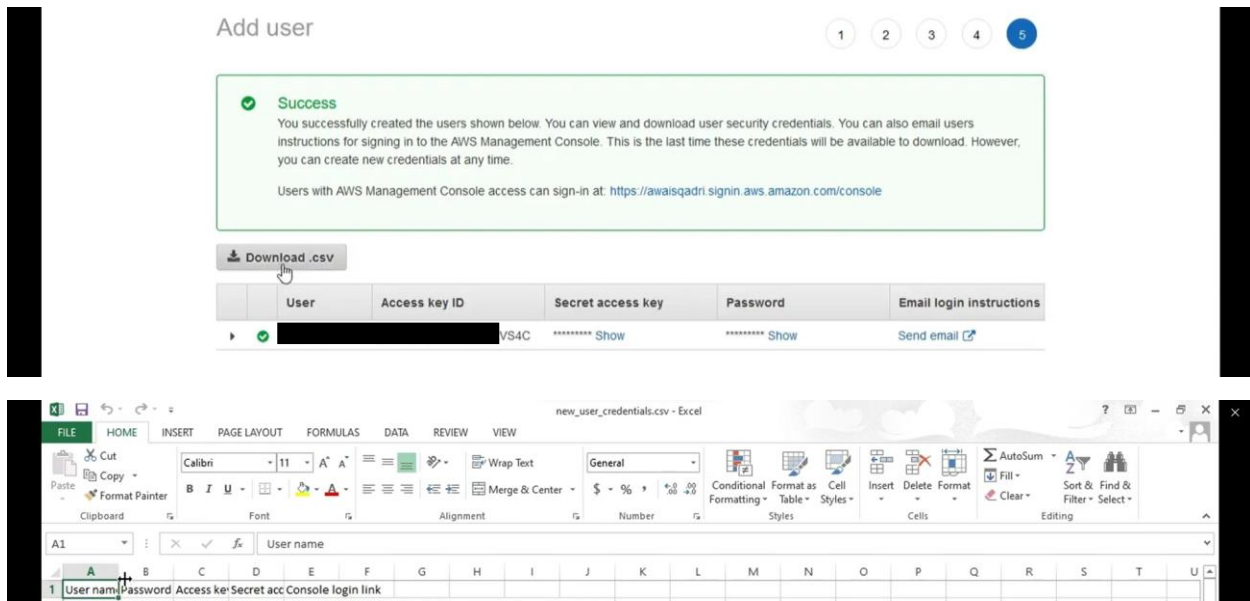
### Permissions summary

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

Type	Name
Managed policy	AmazonS3ReadOnlyAccess
Managed policy	IAMUserChangePassword



- Download the csv file for the record of user credentials.

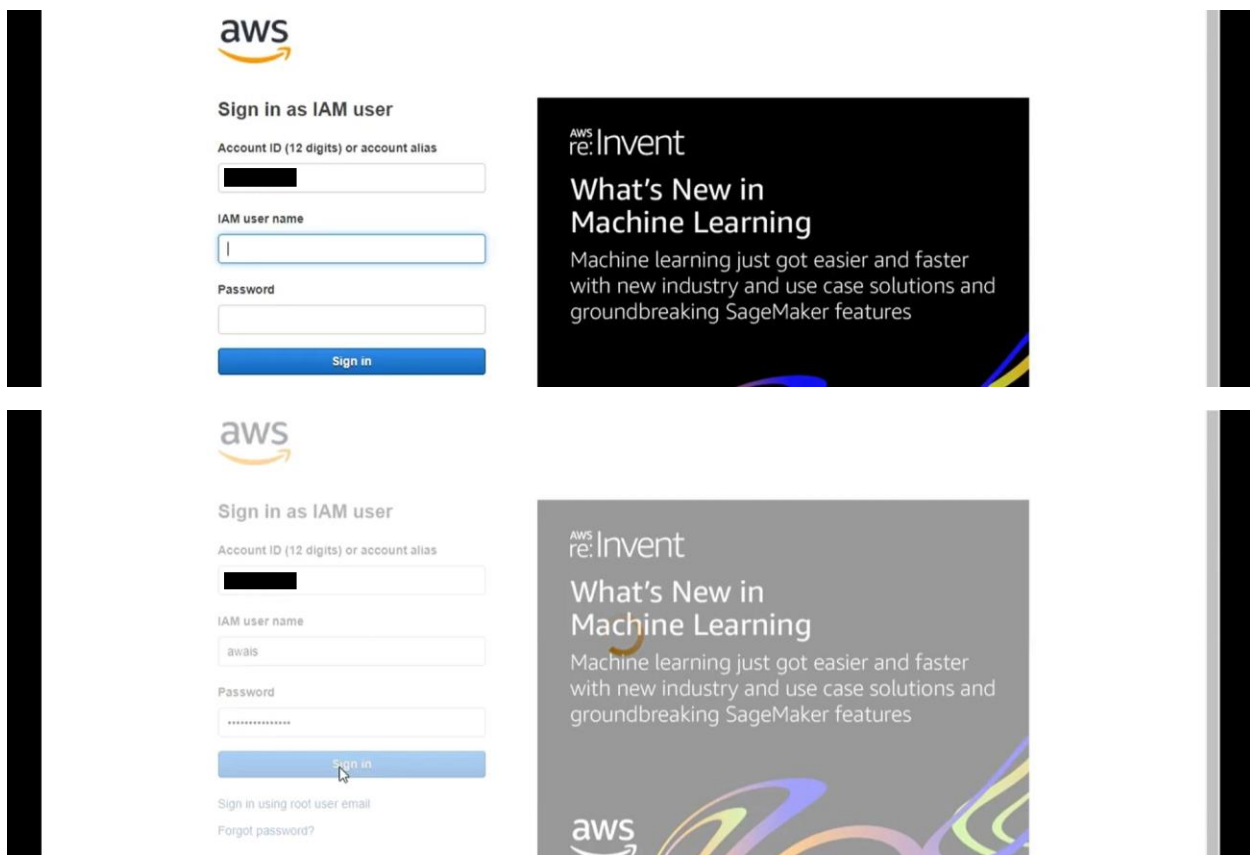


The screenshot shows the 'Add user' page in the AWS IAM console. A success message indicates that users have been created successfully. Below the message is a 'Download .csv' button. A table lists the created users with columns for User, Access key ID, Secret access key, Password, and Email login instructions. The first user is 'VS4C' with a secret access key and password that are partially obscured by asterisks and a 'Show' link.

User	Access key ID	Secret access key	Password	Email login instructions
VS4C		***** Show	***** Show	<a href="#">Send email</a>

Below the table, a preview of the downloaded 'new\_user\_credentials.csv' file is shown in an Excel spreadsheet. The first row contains the following headers: User name, Password, Access key, Secret acc, Console login link.

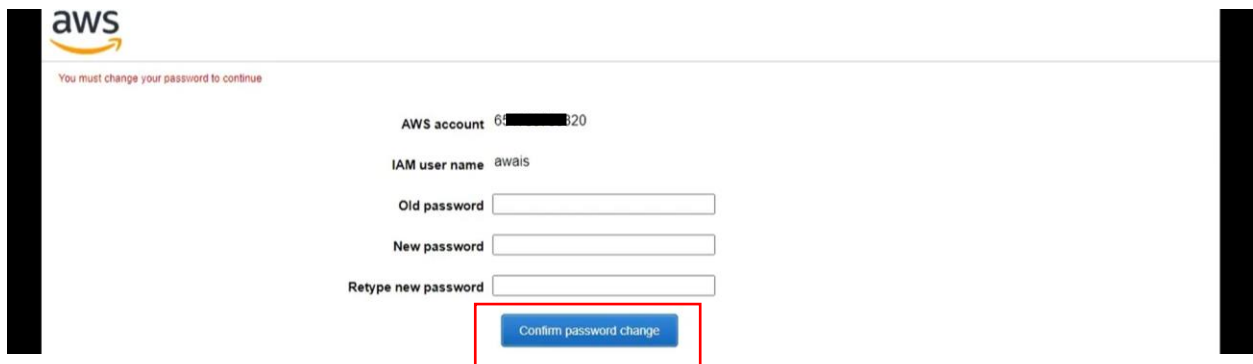
- Use IAM credentials to login as a IAM user



The top section shows the 'Sign in as IAM user' page. The 'Account ID (12 digits) or account alias' field is filled with a redacted value. The 'IAM user name' field is empty. The 'Password' field is filled with a redacted value. The 'Sign in' button is visible.

The bottom section shows the same 'Sign in as IAM user' page, but the 'IAM user name' field is now filled with 'awais'. The 'Sign in' button is highlighted with a mouse cursor. Below the sign-in fields, there are links for 'Sign in using root user email' and 'Forgot password?'. To the right of the sign-in page is an advertisement for AWS re:Invent, titled 'What's New in Machine Learning', which promotes new industry and use case solutions and groundbreaking SageMaker features.

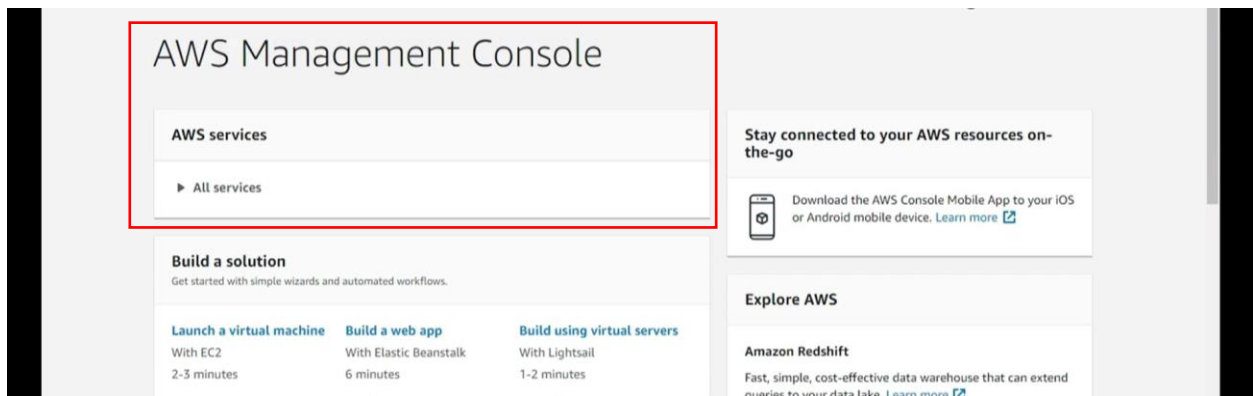
- If password change permission is given you can set your new password.



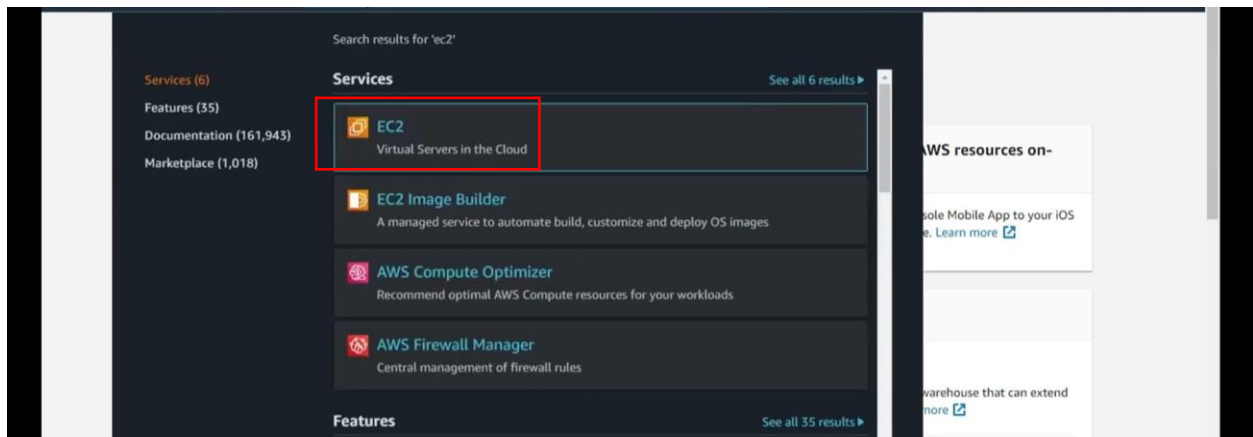
The screenshot shows the AWS password change interface. At the top left is the AWS logo. Below it, a message states: "You must change your password to continue". The form includes the following fields:

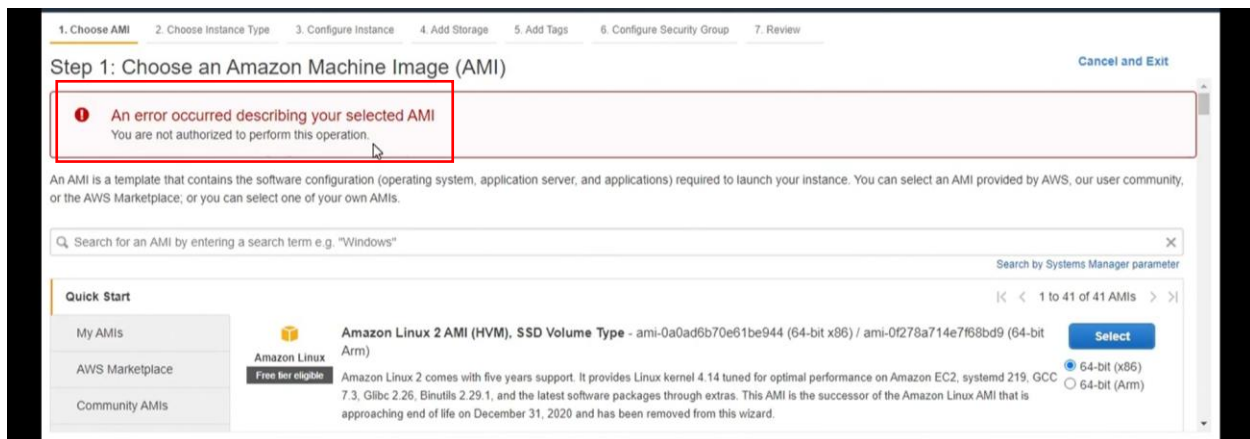
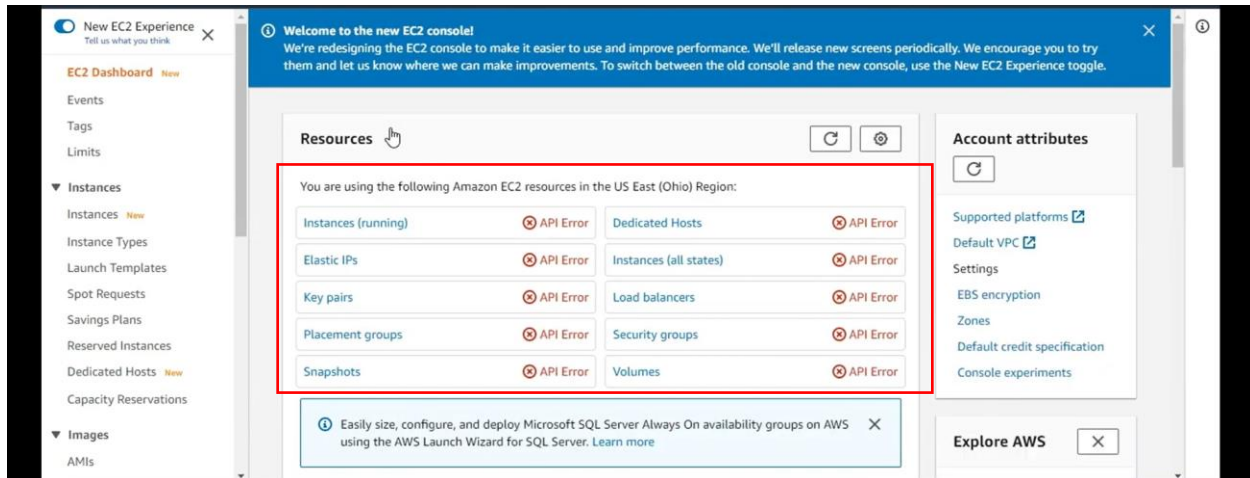
- AWS account: 64 [redacted] 820
- IAM user name: awais
- Old password: [text input field]
- New password: [text input field]
- Retype new password: [text input field]
- A blue button labeled "Confirm password change" is highlighted with a red rectangular box.

- Access the Management console for different services. Only allowed services are accessible.

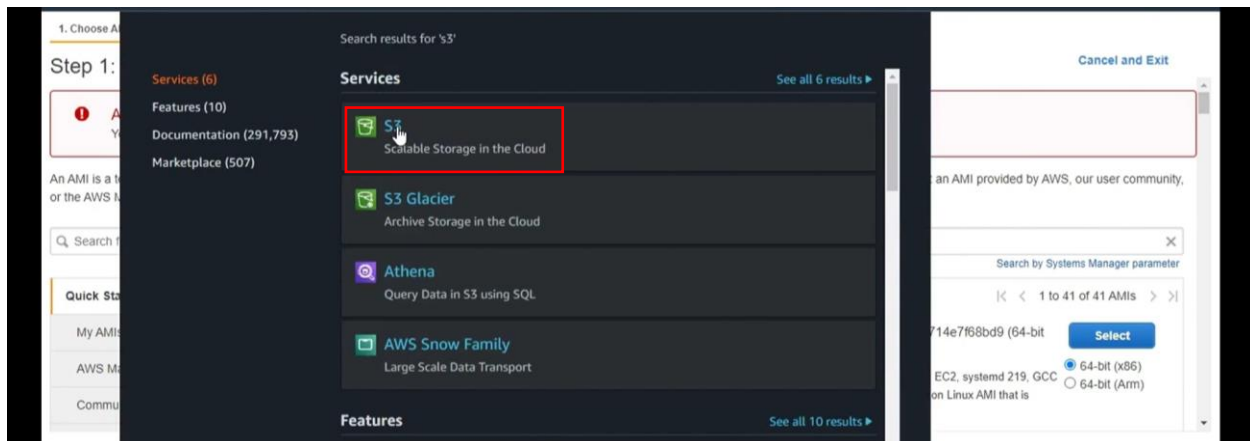


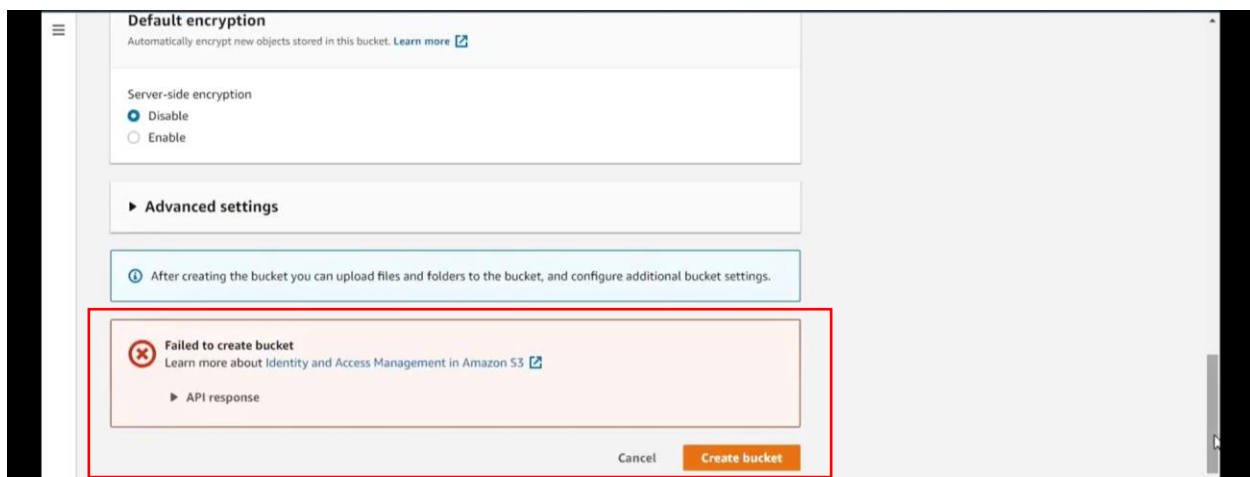
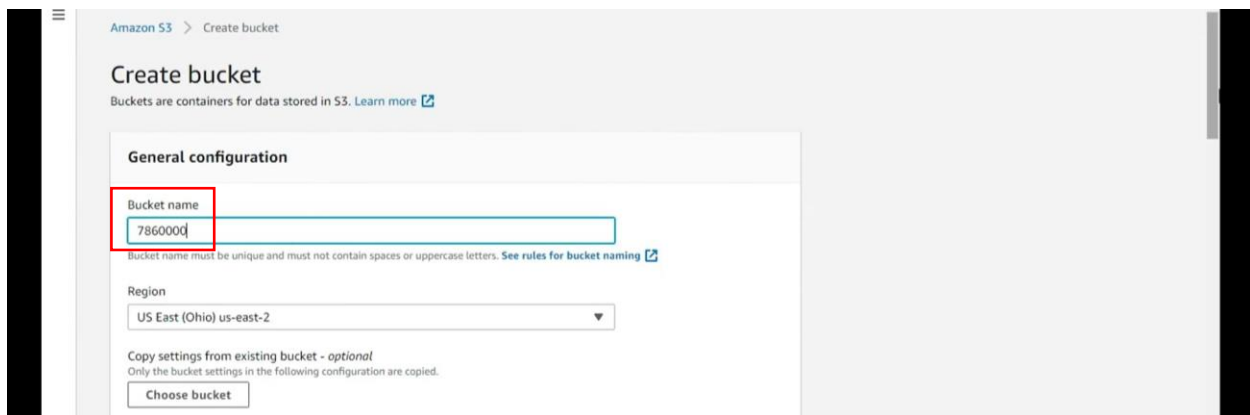
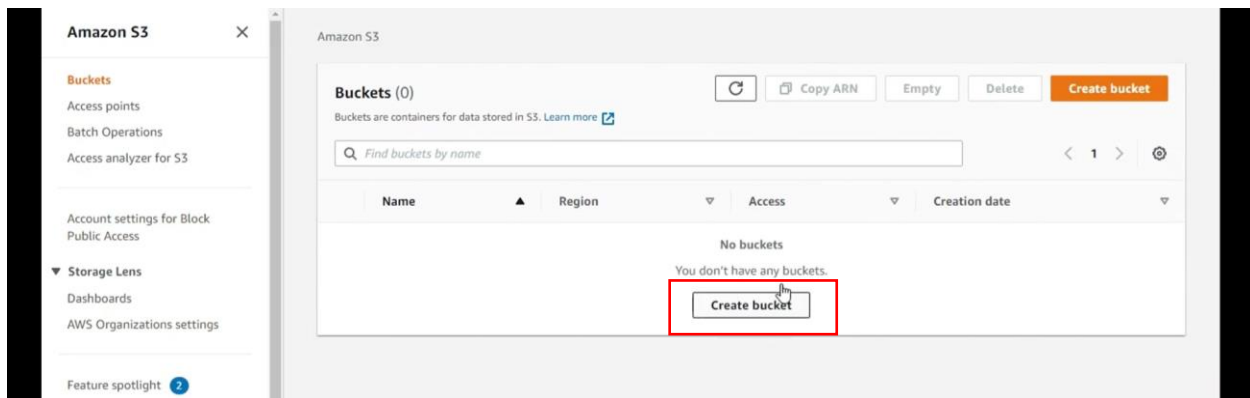
- E.g. EC2 is not accessible as permission is not given.



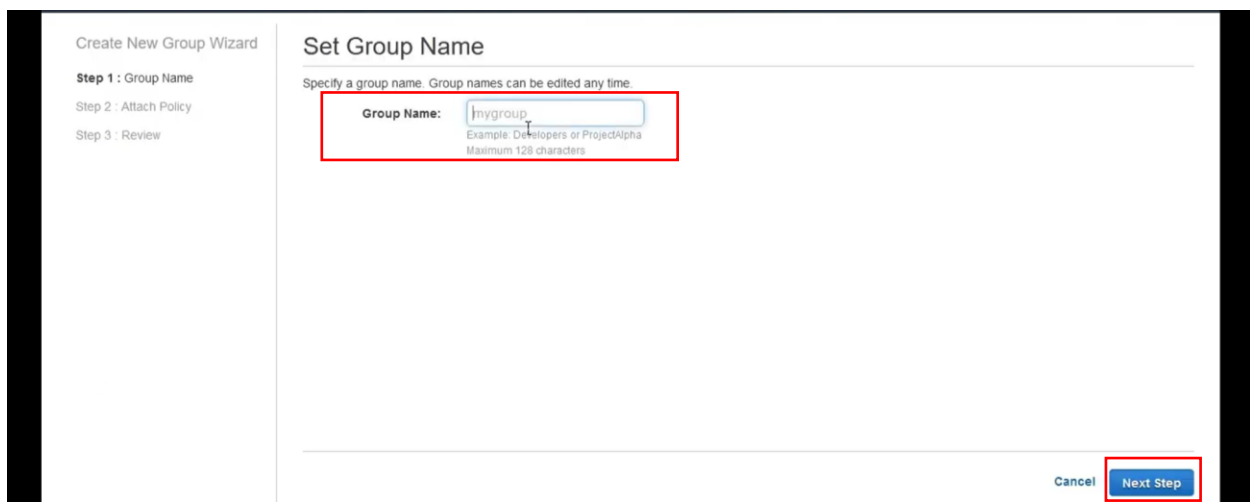
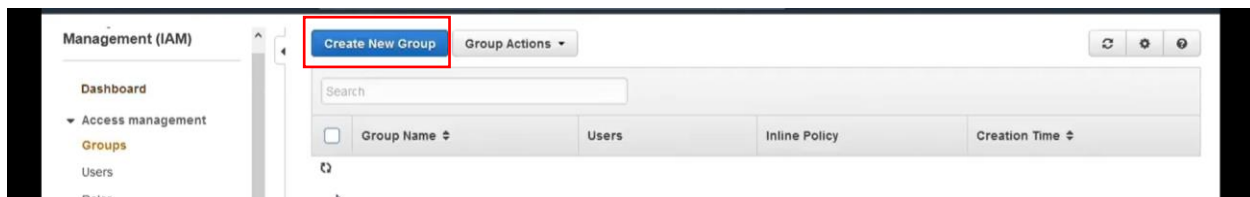
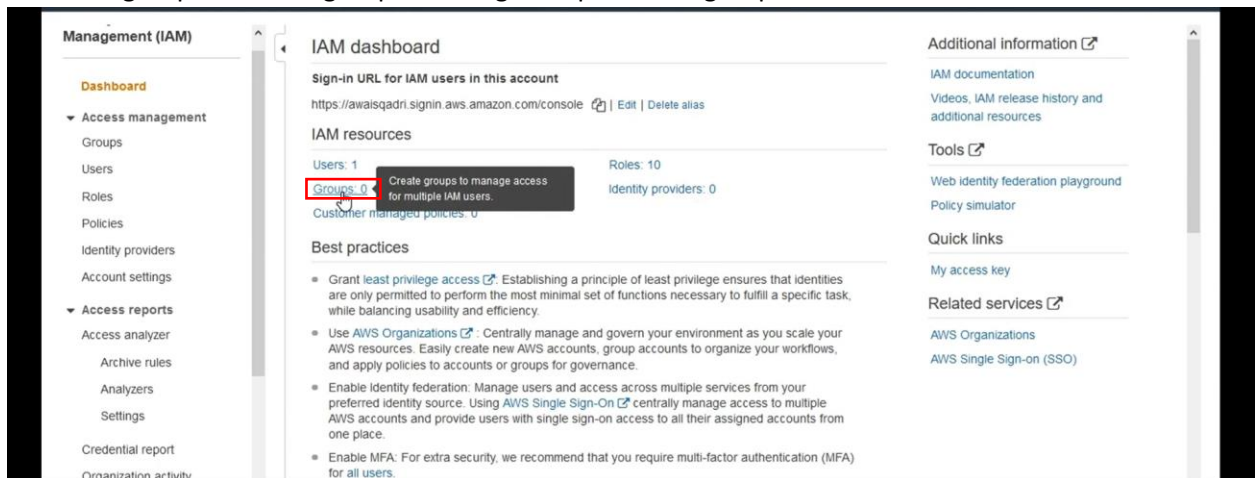


- Access the S3 storage option. You are unable to create a bucket as READONLY permission is attached.





- To create groups: Create a group and assign the policies at group level



## Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

Step 3 : Review

## Attach Policy

Select one or more policies to attach. Each group can have up to 10 policies attached.

Filter: Policy Type <input type="text" value="Search"/>		Showing 637 results		
<input type="checkbox"/>	Policy Name	Attached Entities	Creation Time	
<input type="checkbox"/>	AmazonS3FullAccess	4	2015-02-06 23:40 UTC+...	
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	1	2015-02-06 23:40 UTC+...	
<input type="checkbox"/>	IAMUserChangePassword	1	2016-11-15 05:25 UTC+...	
<input type="checkbox"/>	AdministratorAccess	0	2015-02-06 23:39 UTC+...	
<input type="checkbox"/>	AdministratorAccess-Amplify	0	2020-12-02 00:03 UTC+...	
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	0	2017-11-30 21:47 UTC+...	
<input type="checkbox"/>	AlexaForBusinessFullAccess	0	2017-11-30 21:47 UTC+...	
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	0	2017-11-30 21:47 UTC+...	

## Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

Step 3 : Review

## Attach Policy

Select one or more policies to attach. Each group can have up to 10 policies attached.

Filter: Policy Type <input type="text" value="Search"/>		Showing 637 results		
<input type="checkbox"/>	Policy Name	Attached Entities	Creation Time	
<input checked="" type="checkbox"/>	AmazonS3FullAccess	4	2015-02-06 23:40 UTC+...	
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	1	2015-02-06 23:40 UTC+...	
<input type="checkbox"/>	IAMUserChangePassword	1	2016-11-15 05:25 UTC+...	
<input type="checkbox"/>	AdministratorAccess	0	2015-02-06 23:39 UTC+...	
<input type="checkbox"/>	AdministratorAccess-Amplify	0	2020-12-02 00:03 UTC+...	
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	0	2017-11-30 21:47 UTC+...	
<input type="checkbox"/>	AlexaForBusinessFullAccess	0	2017-11-30 21:47 UTC+...	
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	0	2017-11-30 21:47 UTC+...	

## Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

Step 3 : Review

## Review

Review the following information, then click **Create Group** to proceed.

Group Name	test	<a href="#">Edit Group Name</a>
Policies	arn:aws:iam::aws:policy/AmazonS3FullAccess	<a href="#">Edit Policies</a>

## Management (IAM)

Dashboard

Access management

Groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Create New Group		Group Actions			Showing 1 results	
<input type="checkbox"/>	Group Name	Users	Inline Policy	Creation Time		
<input type="checkbox"/>	test	0		2020-12-26 19:41 UTC+0500		

- You can add users to a group

The first screenshot shows the 'Summary' tab for a group named 'test'. It displays the Group ARN, the number of users (0), the path, and the creation time. A red box highlights a warning message: 'This group does not contain any users.' Below the warning is a blue button labeled 'Add Users to Group'.

The second screenshot shows the 'Permissions' tab for the same group. It displays a table of managed policies. A red box highlights the 'Attach Policy' button. Below the table, there is a list of policies with their names and actions.

Policy Name	Actions
AmazonS3FullAccess	Show Policy   Detach Policy   Simulate Policy

- Policies can be detached.

The screenshot shows the 'Permissions' tab for the 'test' group. A red box highlights a 'Detach Policy' dialog box. The dialog asks: 'Are you sure you want to detach policy AmazonS3FullAccess from group test'. There are 'Cancel' and 'Detach' buttons. The 'Detach' button is highlighted with a mouse cursor.

The screenshot shows the 'Add Users to Group' dialog. It displays a table of users. A red box highlights the first user in the table.

User Name	Groups	Password	Password Last Used	Access Keys	Creation Time
[redacted]	0	✓	2020-12-26 19:36 UTC+0500	1 active	2020-12-26 19:31 U.



- Users can be removed from a group.

The image displays three sequential screenshots of the AWS IAM console, illustrating the process of removing a user from a group.

**Top Screenshot: Group Management**  
The left sidebar shows the 'Management (IAM)' menu with 'Groups' selected. The main content area shows the 'test' group details. The 'Users' tab is active, displaying a table with one user. A red box highlights the 'Remove User from Group' button in the 'Actions' column. Another red box highlights the 'Remove Users from Group' button in the top right corner.

**Middle Screenshot: User Management**  
The left sidebar shows 'Users' selected. The main content area shows the 'Summary' page for a user. The 'Permissions' tab is active, displaying a table of policies. A red box highlights the 'AmazonS3ReadOnlyAccess' and 'IAMUserChangePassword' policies. A 'Delete user' button is visible in the top right corner.

**Bottom Screenshot: User Management**  
The left sidebar shows 'Users' selected. The main content area shows the 'Permissions' page for the same user. The 'Permissions' tab is active, displaying a table of policies. A red box highlights the 'AmazonS3FullAccess' policy under the 'Attached from group' section.

- Roles and policies can be created, will be discussed later.

**Identity and Access Management (IAM)**

**Dashboard**

- Access management
  - Groups
  - Users
  - Roles**
  - Policies
  - Identity providers
  - Account settings
- Access reports
  - Access analyzer
  - Archive rules
  - Analyzers
  - Settings
- Credential report

**Roles**

**What are IAM roles?**

IAM roles are a secure way to grant permissions to entities that you trust. Examples of entities include the following:

- IAM user in another account
- Application code running on an EC2 instance that needs to perform actions on AWS resources
- An AWS service that needs to act on resources in your account to provide its features
- Users from a corporate directory who use identity federation with SAML

IAM roles issue keys that are valid for short durations, making them a more secure way to grant access.

**Additional resources:**

- IAM Roles FAQ
- IAM Roles Documentation
- Tutorial: Setting Up Cross Account Access
- Common Scenarios for Roles

**Create role** Delete role

**Identity and Access Management (IAM)**

**Dashboard**

- Access management
  - Groups
  - Users
  - Roles**
  - Policies
  - Identity providers
  - Account settings
- Access reports
  - Access analyzer
  - Archive rules
  - Analyzers
  - Settings
- Credential report

**Create role** Delete role

Search Showing 10 results

Role name	Trusted entities	Last activity
<input type="checkbox"/> aurangzaibEC2S3	AWS service: ec2	None
<input type="checkbox"/> awaisEc2toS3	AWS service: ec2	15 days
<input type="checkbox"/> AWSServiceRoleForAmazonElasticFileSyst...	AWS service: elasticfilesystem (Service-Link...	303 days
<input type="checkbox"/> AWSServiceRoleForCloudWatchEvents	AWS service: events (Service-Linked role)	303 days
<input type="checkbox"/> AWSServiceRoleForElasticLoadBalancing	AWS service: elasticloadbalancing (Service-...	284 days
<input type="checkbox"/> AWSServiceRoleForRDS	AWS service: rds (Service-Linked role)	284 days
<input type="checkbox"/> AWSServiceRoleForSupport	AWS service: support (Service-Linked role)	None
<input type="checkbox"/> AWSServiceRoleForTrustedAdvisor	AWS service: trustedadvisor (Service-Link...	None
<input type="checkbox"/> S3fullaccesstoEC2	AWS service: ec2	328 days
<input type="checkbox"/> waqarec2toS3	AWS service: ec2	None

**Identity and Access Management (IAM)**

**Dashboard**

- Access management
  - Groups
  - Users
  - Roles
  - Policies**
  - Identity providers
  - Account settings
- Access reports
  - Access analyzer
  - Archive rules
  - Analyzers
  - Settings
- Credential report

**Create policy** Policy actions

Filter policies Search Showing 10 results

Policy name	Type	Used as	Description
<input type="radio"/> AccessAnalyzerServiceRole...	AWS managed	None	Allow Access Analyzer to analyze resource metadata
<input type="radio"/> AdministratorAccess	Job function	None	Provides full access to AWS services and resources.
<input type="radio"/> AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permissions while explicitly...
<input type="radio"/> AlexaForBusinessDeviceSe...	AWS managed	None	Provide device setup access to AlexaForBusiness service...
<input type="radio"/> AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness resources and a...
<input type="radio"/> AlexaForBusinessGateway...	AWS managed	None	Provide gateway execution access to AlexaForBusiness...
<input type="radio"/> AlexaForBusinessLifeseD...	AWS managed	None	Provide access to Lifesize AVS devices
<input type="radio"/> AlexaForBusinessNetworkP...	AWS managed	None	This policy enables Alexa for Business to perform autom...
<input type="radio"/> AlexaForBusinessPolyDele...	AWS managed	None	Provide access to Poly AVS devices
<input type="radio"/> AlexaForBusinessReadOnl...	AWS managed	None	Provide read only access to AlexaForBusiness services

## TASK:

1. You are requested to create accounts on AWS as a root user.
2. Next create an IAM user for your usage and login as an IAM user, try working around with different policies and see how the access is managed.
3. For complete access as an IAM user look for rights or policies. *(May find the hint in the screens)*
4. Add this IAM user (with maximum access) to a user group say Administrator. Then perform next lab EC2 using that account.
5. Share your findings.