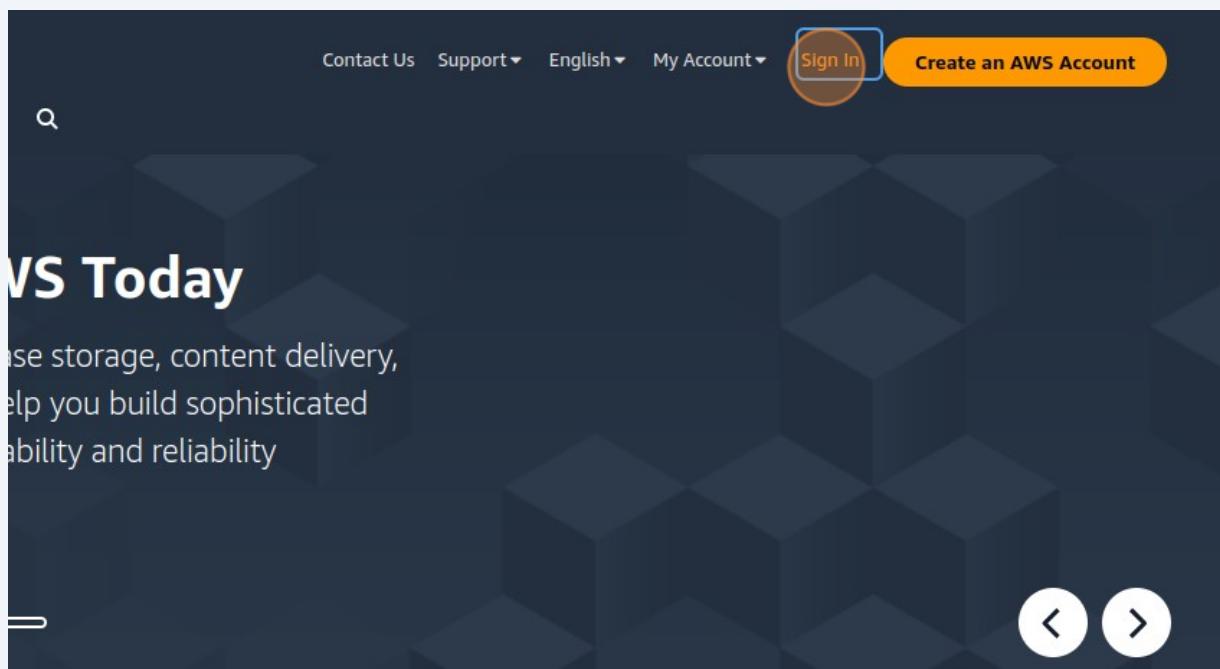


Step-by-Step Guide: Creating an IAM User and Granting Permissions and Creating UsersGroup

Scribe 

- 1 Navigate to <https://aws.amazon.com/>

- 2 Click "Sign In"



3 Enter your root email id

Root user
Account owner that performs tasks requiring unrestricted access. [Learn more](#)

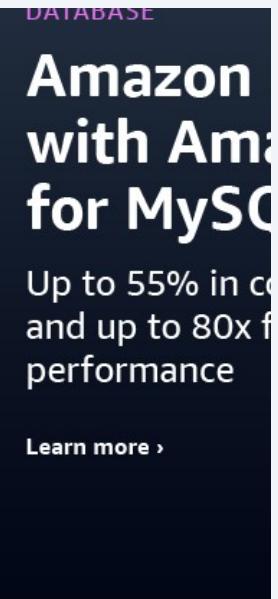
IAM user
User within an account that performs daily tasks. [Learn more](#)

Root user email address

[Next](#)

By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

New to AWS? [Create a new AWS account](#)



4 Click "Next"

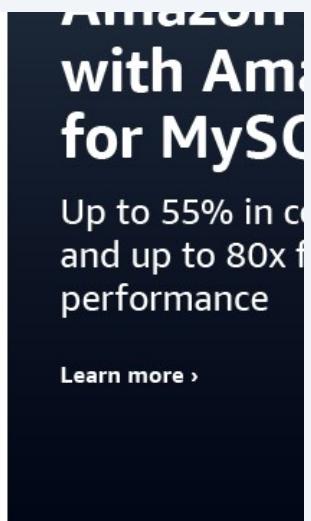
IAM user
User within an account that performs daily tasks. [Learn more](#)

Root user email address

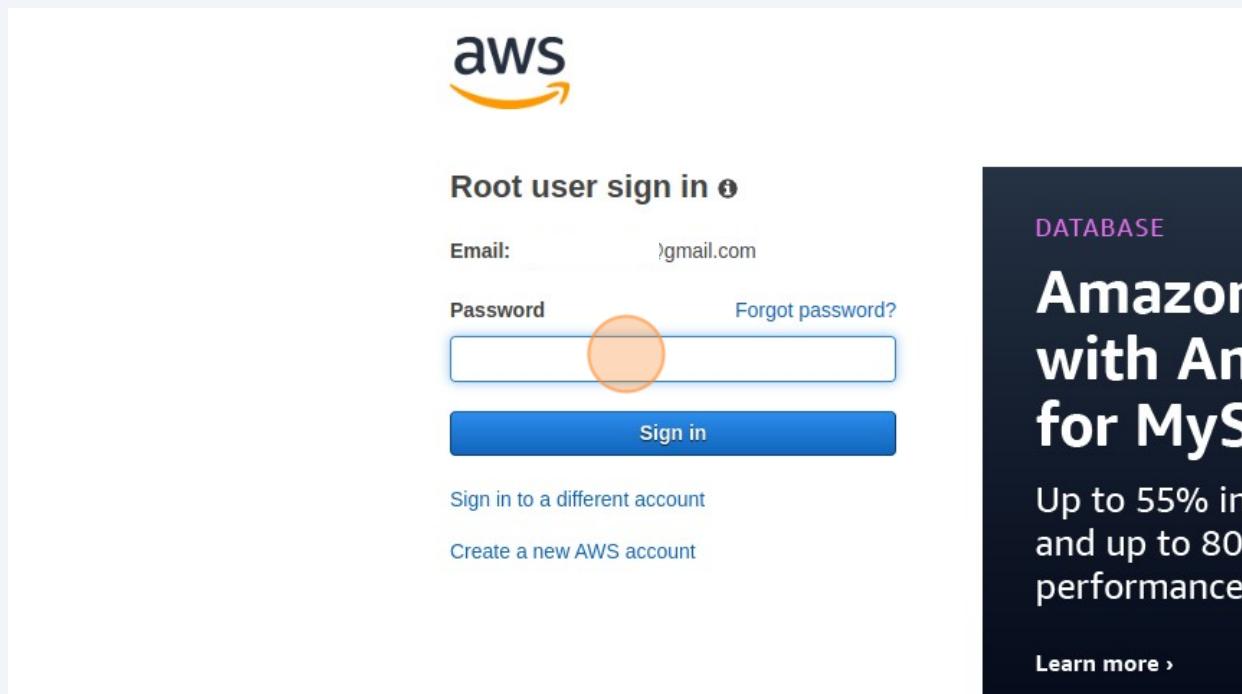
[Next](#)

By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

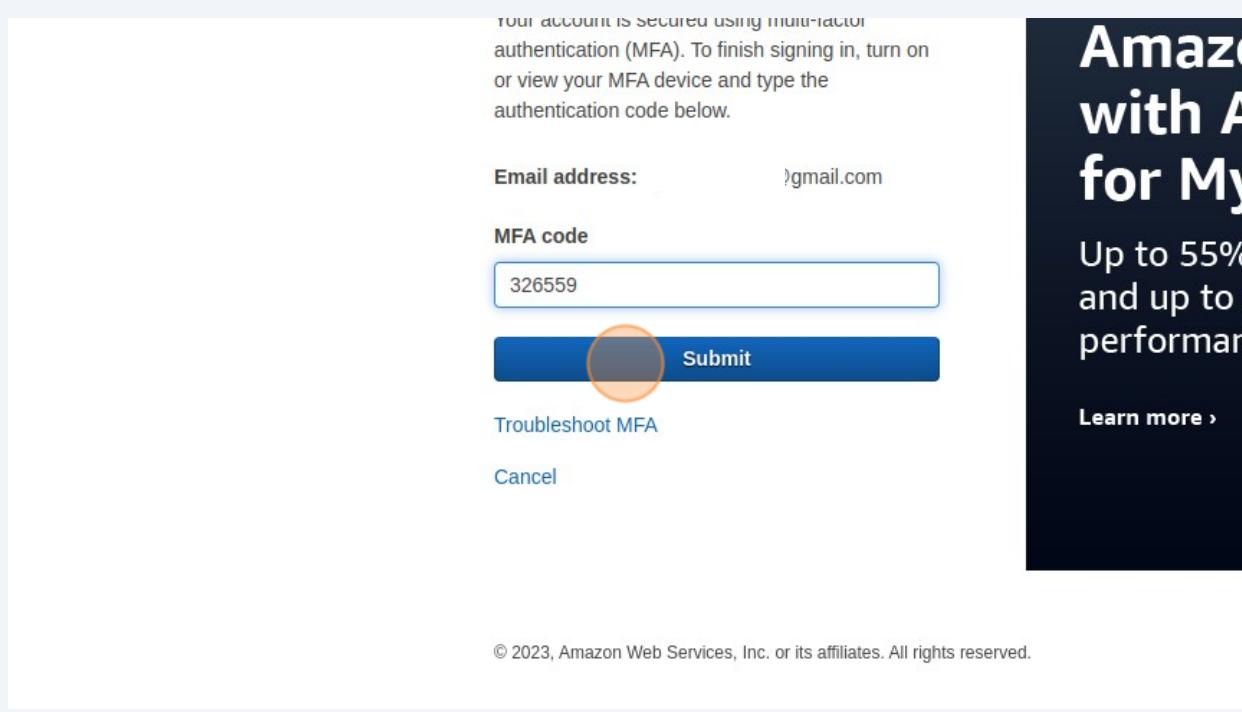
New to AWS? [Create a new AWS account](#)



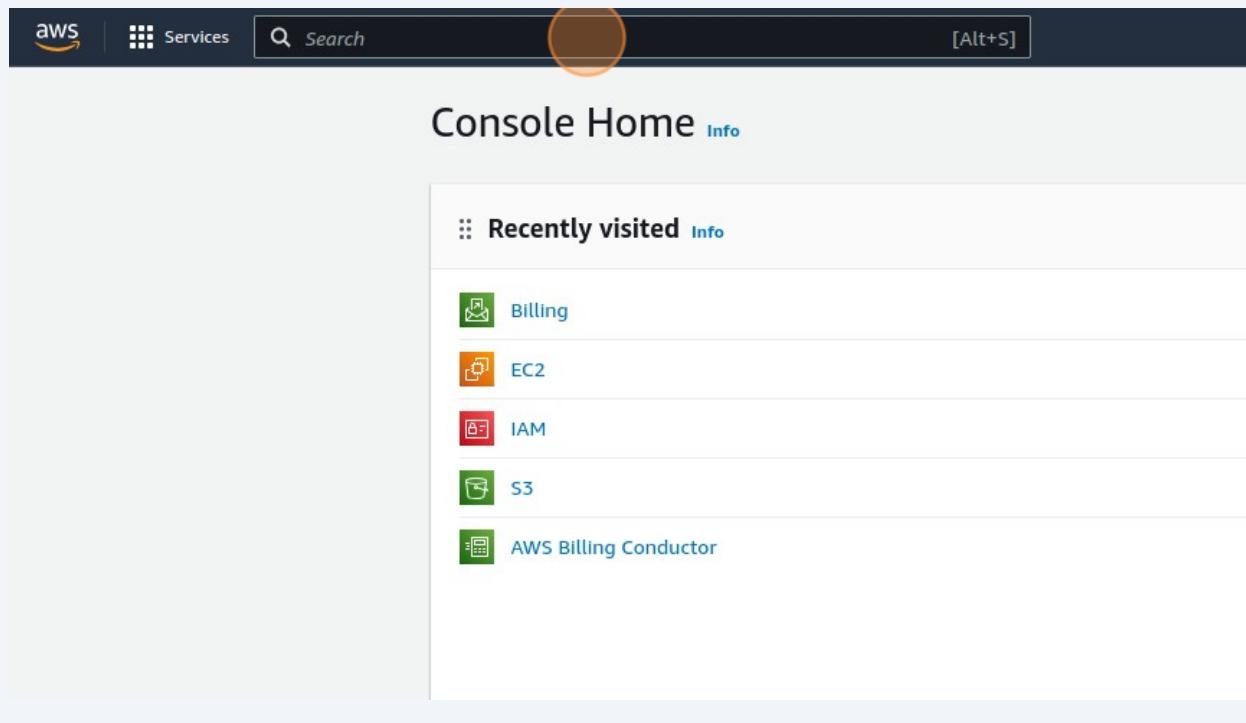
- 5 Click this password field and enter your password



- 6 Enter you MFA Code and Click "Submit"

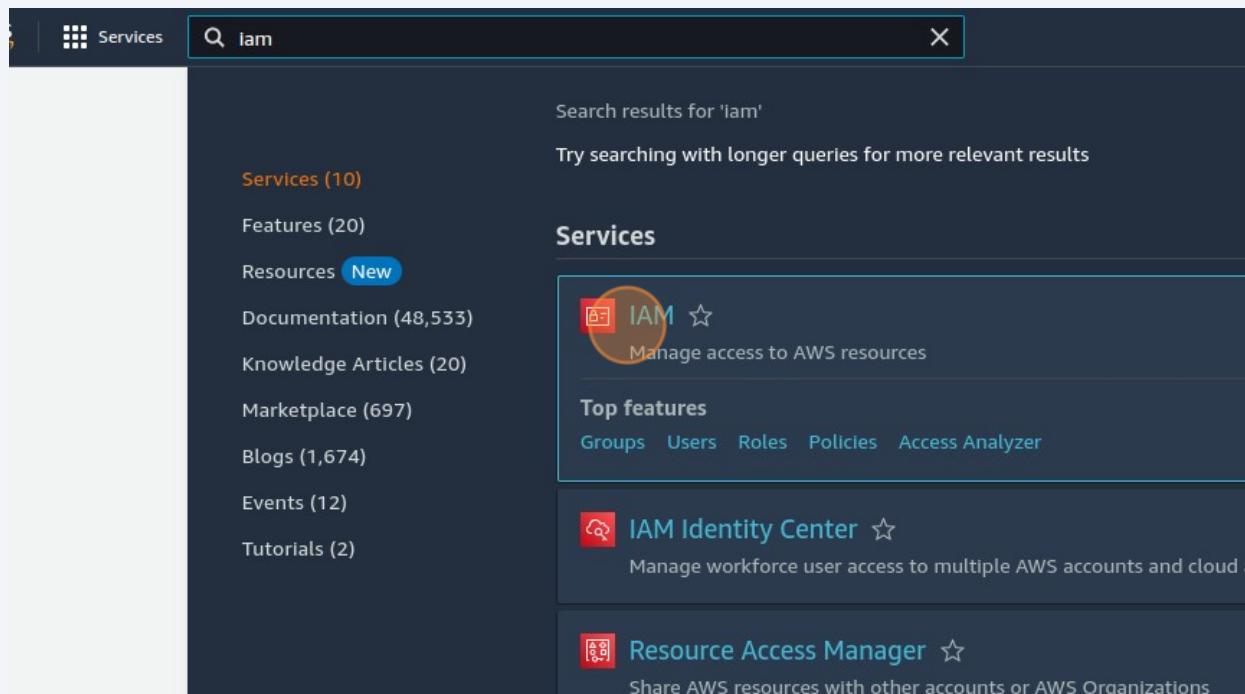


- 7 Click the "Search" field.



- 8 Type "iam"

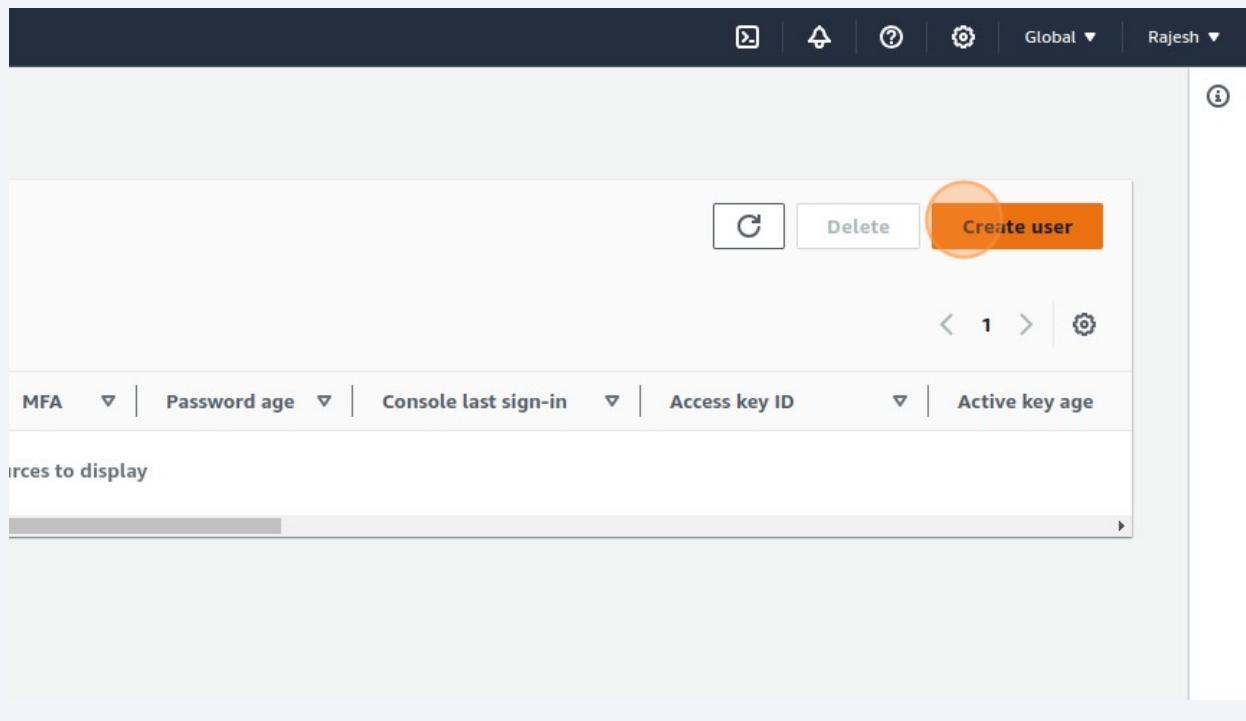
9 Click "IAM"



10 Click "Users"

The screenshot shows the IAM Dashboard. At the top left is a search bar labeled 'Search IAM'. The main content area is titled 'IAM Dashboard'. On the left, there's a sidebar with sections like 'Dashboard', 'Access management' (with 'User groups', 'Users' highlighted with a red circle, and 'Roles'), 'Policies', 'Identity providers', and 'Account settings'. Below that is another section titled 'Access reports' with 'Access analyzer' and 'Archive rules'. The main dashboard area has two main sections: 'Security recommendations' (with a red circle containing the number 1) and 'IAM resources'. The 'Security recommendations' section contains two items: a green checkmark for 'Root user has MFA' and a yellow warning icon for 'Deactivate or delete access keys for root user'. The 'IAM resources' section shows a table with three columns: 'User groups' (0), 'Users' (0), and 'Roles' (2).

11 Click "Create user"



12 Click the "User name" field.

A screenshot of the 'Specify user details' form. At the top, there's a toolbar with a 'Create user' button and other icons. The main form has a section titled 'User details' with a 'User name' input field. The 'User name' field is highlighted with an orange circle. Below it, there's a note about character restrictions and a checkbox for 'Provide user access to the AWS Management Console - optional'. A note at the bottom explains how to generate programmatic access keys.

13 Type "test-user-1" . This is for example only you can type your wished name

14 Click this checkbox. That means you are providing AWS Management console access to our creates user

The screenshot shows the 'Specify user details' step of the AWS IAM User Creation wizard. On the left, a sidebar lists steps: Step 1 (Specify user details), Step 2 (Set permissions), and Step 3 (Review and create). The main area is titled 'User details'. It shows a 'User name' field containing 'test-user-1', which is highlighted with a blue border. Below the field is a note: 'The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @'. To the right of the note is a checkbox labeled 'Provide user access to the AWS Management Console - optional'. A callout bubble points to this checkbox with the text: 'If you're providing console access to a person, it's a best practice [link] to manage their'. At the bottom, there is an information icon with the text: 'If you are creating programmatic access through access keys or service [link]'.

15 Click on "I want to create an IAM user"

The screenshot shows the AWS IAM User Creation process at Step 4: Retrieve password. A checkbox for "Provide user access to the AWS Management Console - optional" is checked. Below it, there are two options for User type: "Specify a user in Identity Center - Recommended" (selected) and "I want to create an IAM user" (highlighted with a red circle). A note below the second option states: "We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific Keypairs, or a backup credential for emergency account access." At the bottom, there is a link: "If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit".

16 choose Autogenerated password ,why? because you are providing a password policy to your new user so that he can reset with new password

The screenshot shows the AWS IAM User Creation process at Step 4: Retrieve password. A checkbox for "Provide user access to the AWS Management Console - optional" is checked. Below it, there are two options for User type: "Specify a user in Identity Center - Recommended" (unselected) and "I want to create an IAM user" (selected). A note below the selected option states: "We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific Keypairs, or a backup credential for emergency account access." In the "Console password" section, the "Autogenerated password" option is selected (highlighted with a red circle), and a note says: "You can view the password after you create the user." Below this, the "Custom password" option is unselected. A note for "Custom password" says: "Enter a custom password for the user." Under "Custom password", there are two bullet points: "Must be at least 8 characters long" and "Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and punctuation symbols (!@#\$%^&*).". There is also a "Show password" checkbox. A checkbox for "Users must create a new password at next sign-in - Recommended" is checked, with a note: "Users automatically get the IAMUserChangePassword policy to allow them to change their own password." At the bottom, there is a link: "If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit".

17 Click "Next"

the AWS Management Console - optional
access to a person, it's a best practice [to manage their access in IAM Identity Center](#).

ng console access to a person?

or in Identity Center - Recommended
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 services.

ate an IAM user
that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Kinesis Data Firehose, or a backup credential for emergency account access.

ord
after you create the user.

or the user.

haracters long
st three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # \$ % ^ & * () _ + - (hyphen) = [] { } | ^

new password at next sign-in - Recommended
e IAMUserChangePassword [policy](#) to allow them to change their own password.

programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keypairs, you can generate them after you create this IAM user. [Learn more](#)

Cancel **Next**

18

We will provide the permissions to our user after creating the user. So, just Click "Next"

Create user

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.

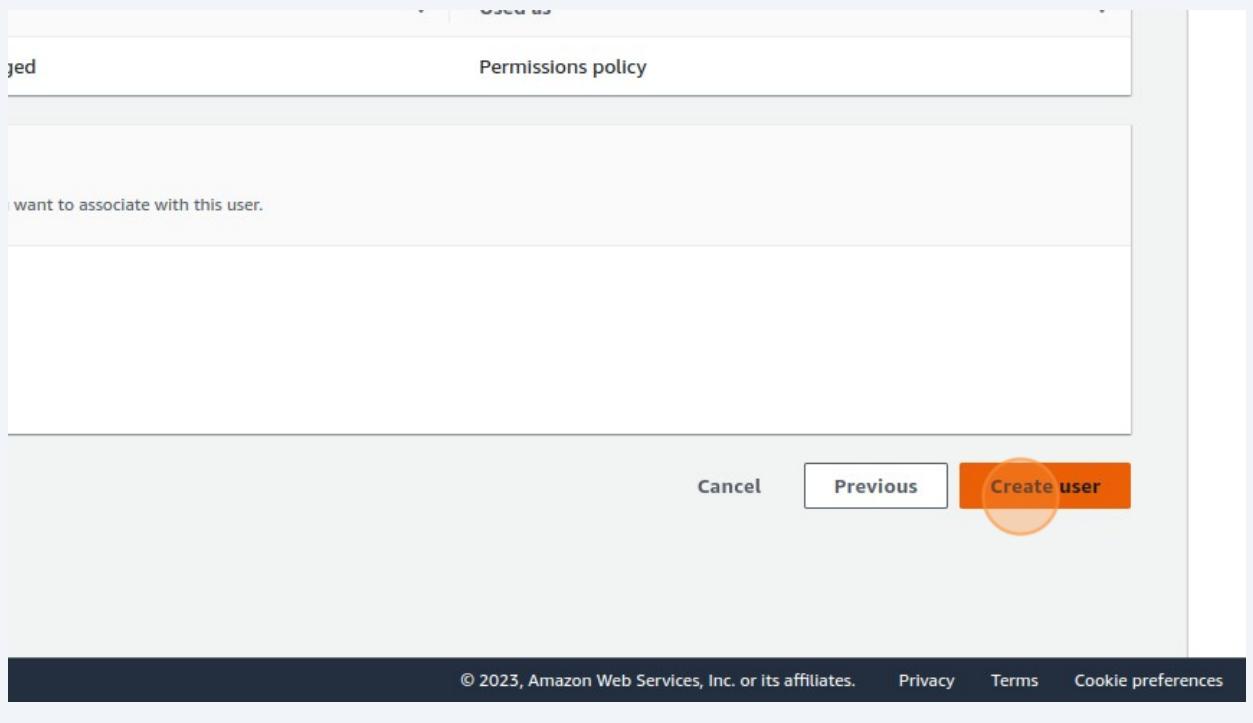
Get started with groups
Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

Create group

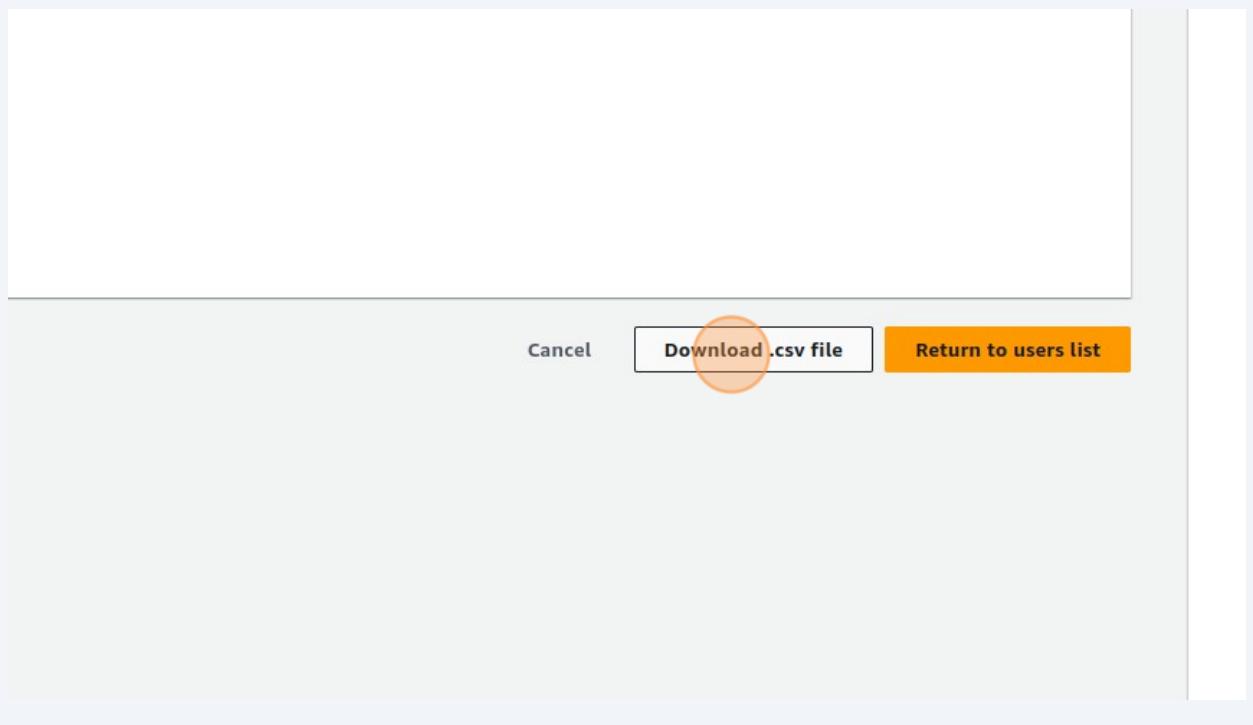
Set permissions boundary - optional

Cancel **Next**

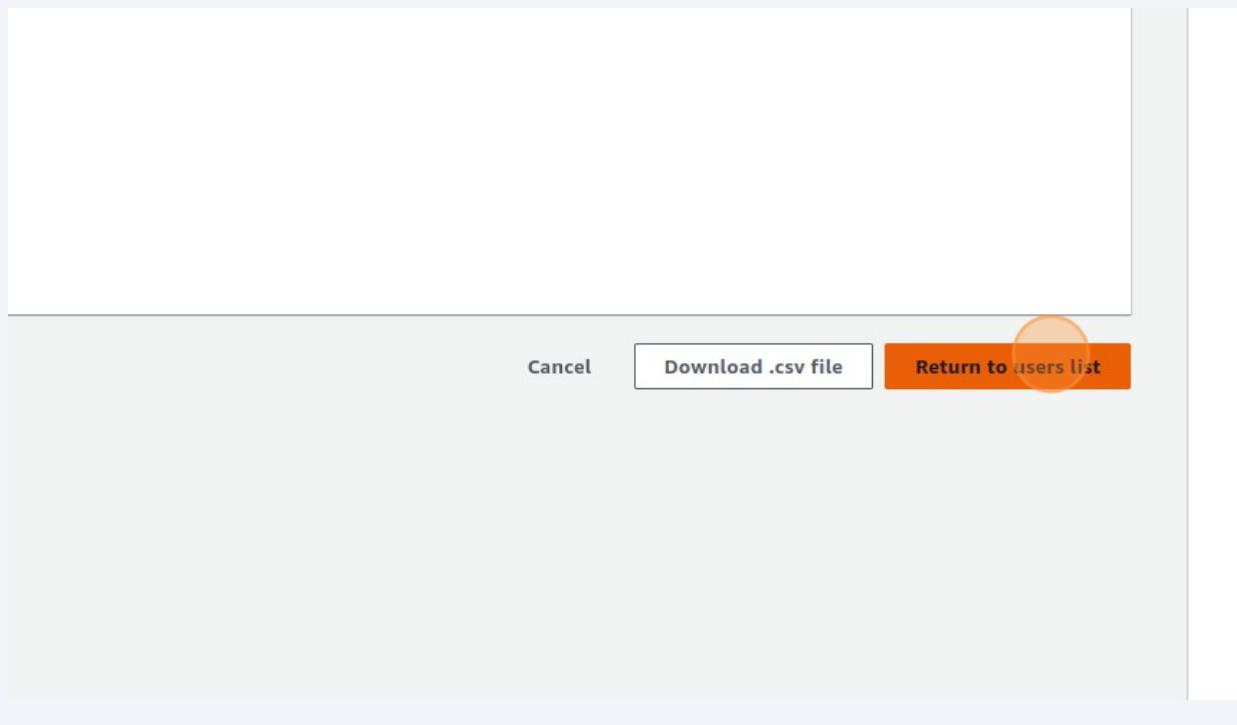
19 Click "Create user"



20 Now you have gotten new user credentials Click "Download .csv file" and make a copy



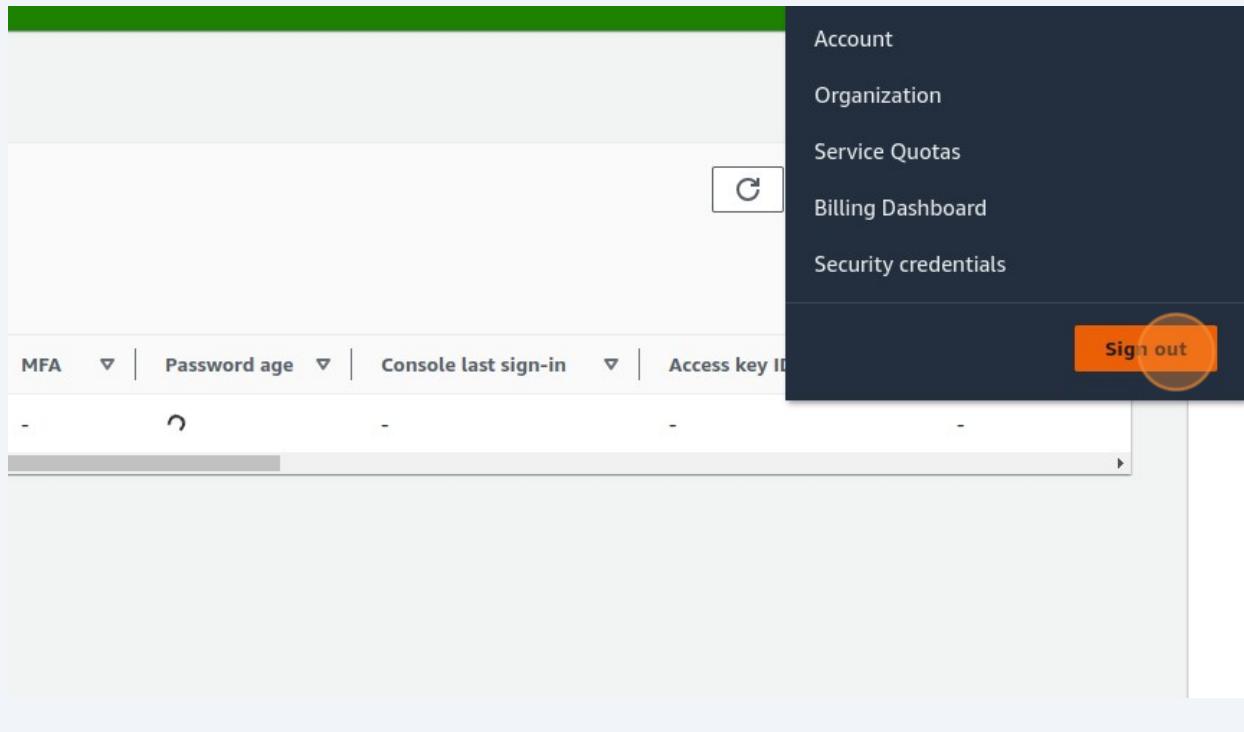
21 Click "Return to users list"



22 Great,you have successfully created a user.Click on your account profile

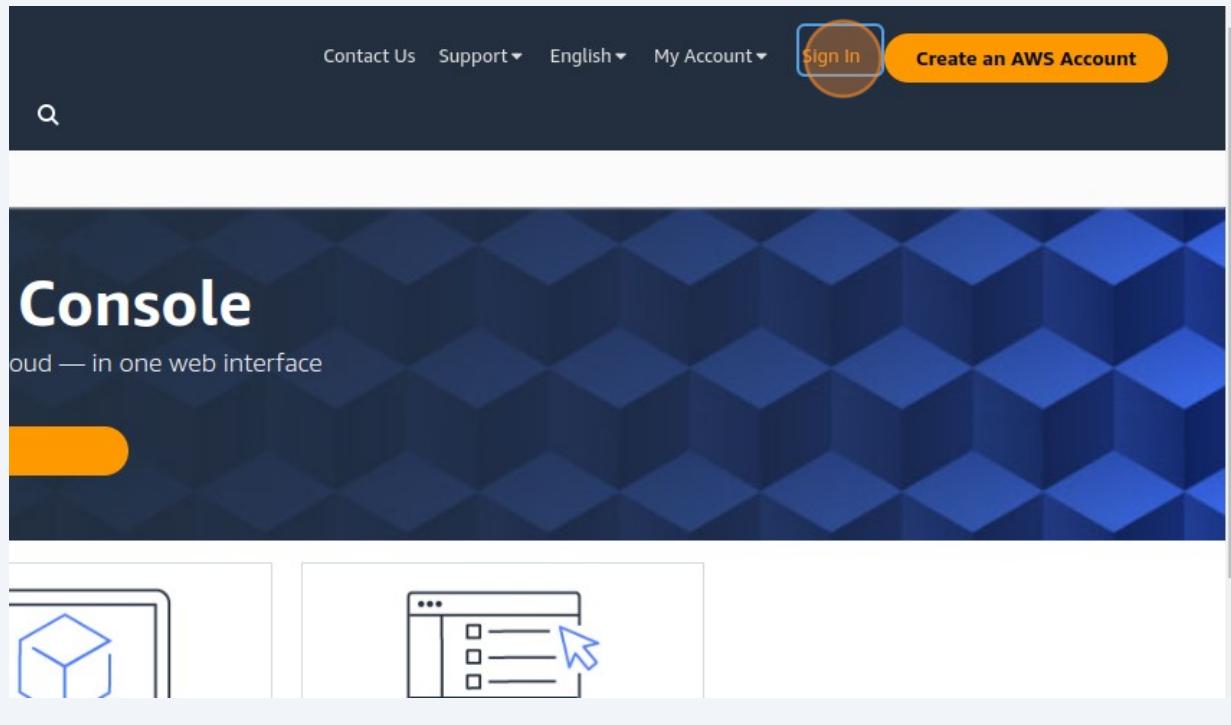
A screenshot of the AWS IAM User Management console. The top navigation bar shows 'Search [Alt+S]' and 'Global Rajesh'. A green success message box says 'User created successfully' with the note 'You can view and download the user's password and email instructions for signing in to the AWS Management Console.' Below it, a 'View user' button is highlighted with a red circle. The main area shows the 'Users (1) Info' section with a table. The table has columns: User name, Path, Groups, Last activity, MFA, Password age, Console last sign-in, Access key ID, and Active key age. One row is visible for 'test-user-1'. At the bottom right of the page, there is an account profile icon with a red circle around it, and the footer includes links for 'Privacy', 'Terms', and 'Cookie preferences'.

23 Click "Sign out"

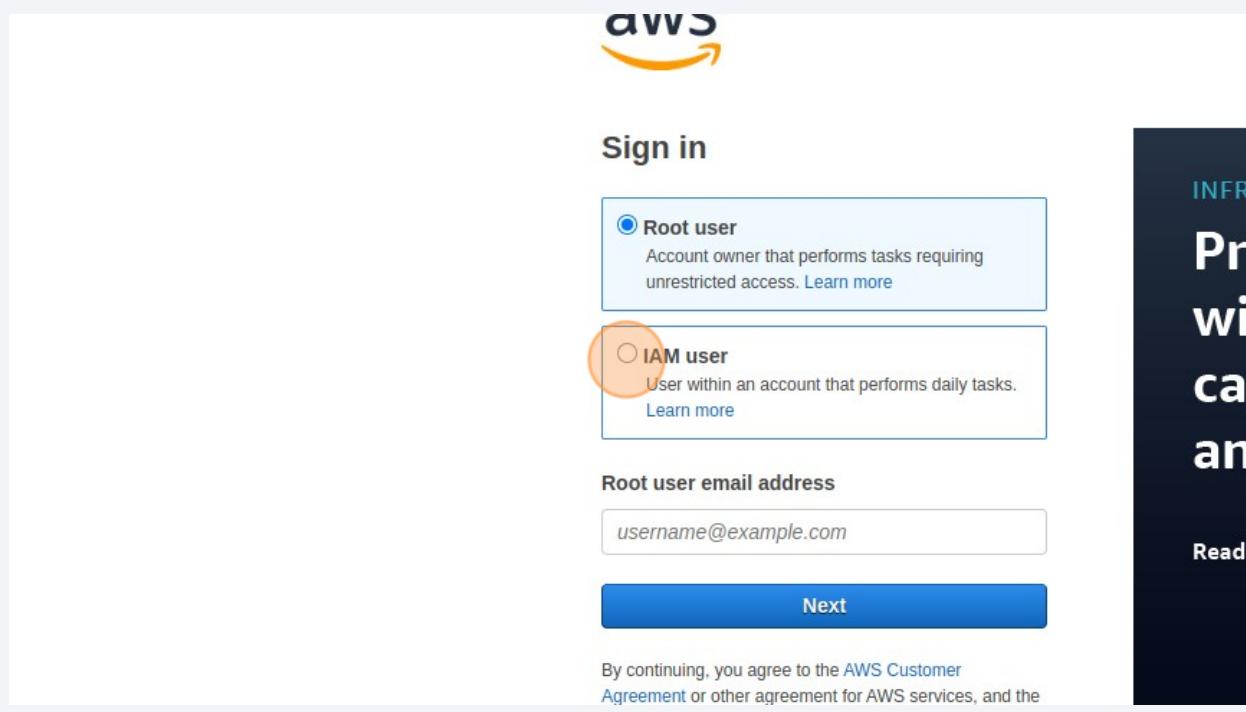


24 Now we are sign in to the user account

25 Click "Sign In"

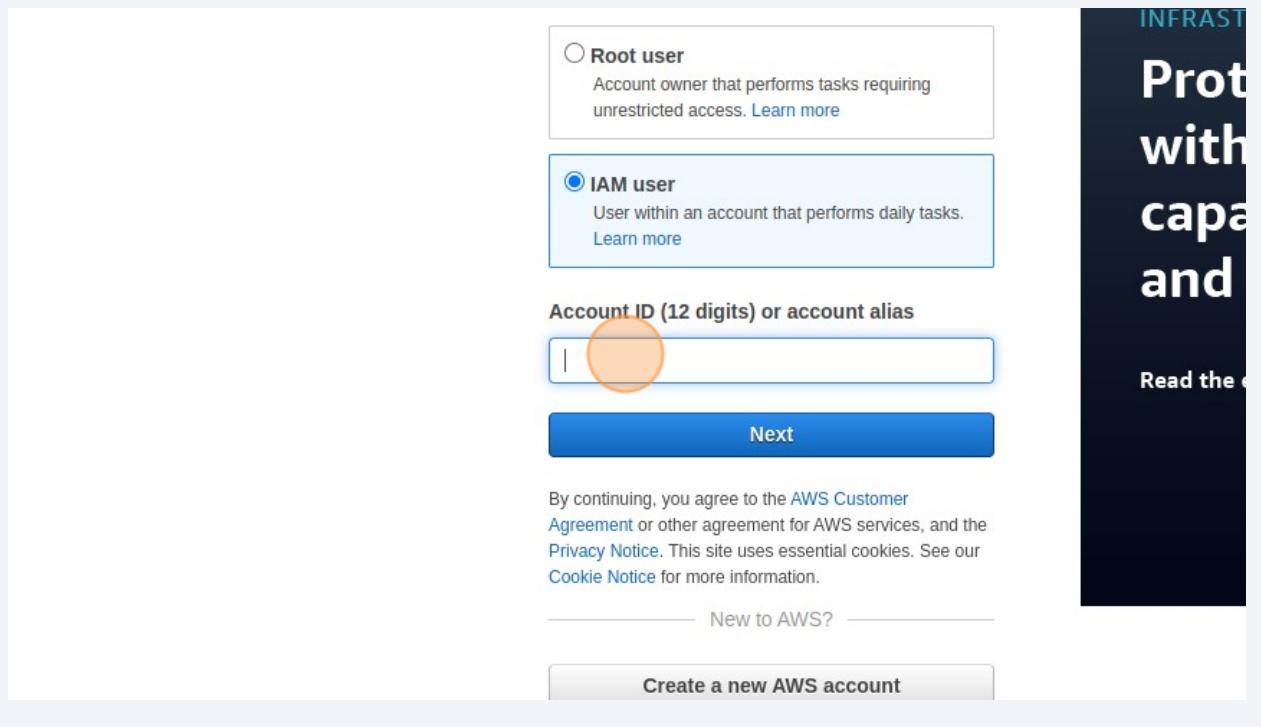


26 Click on IAM user



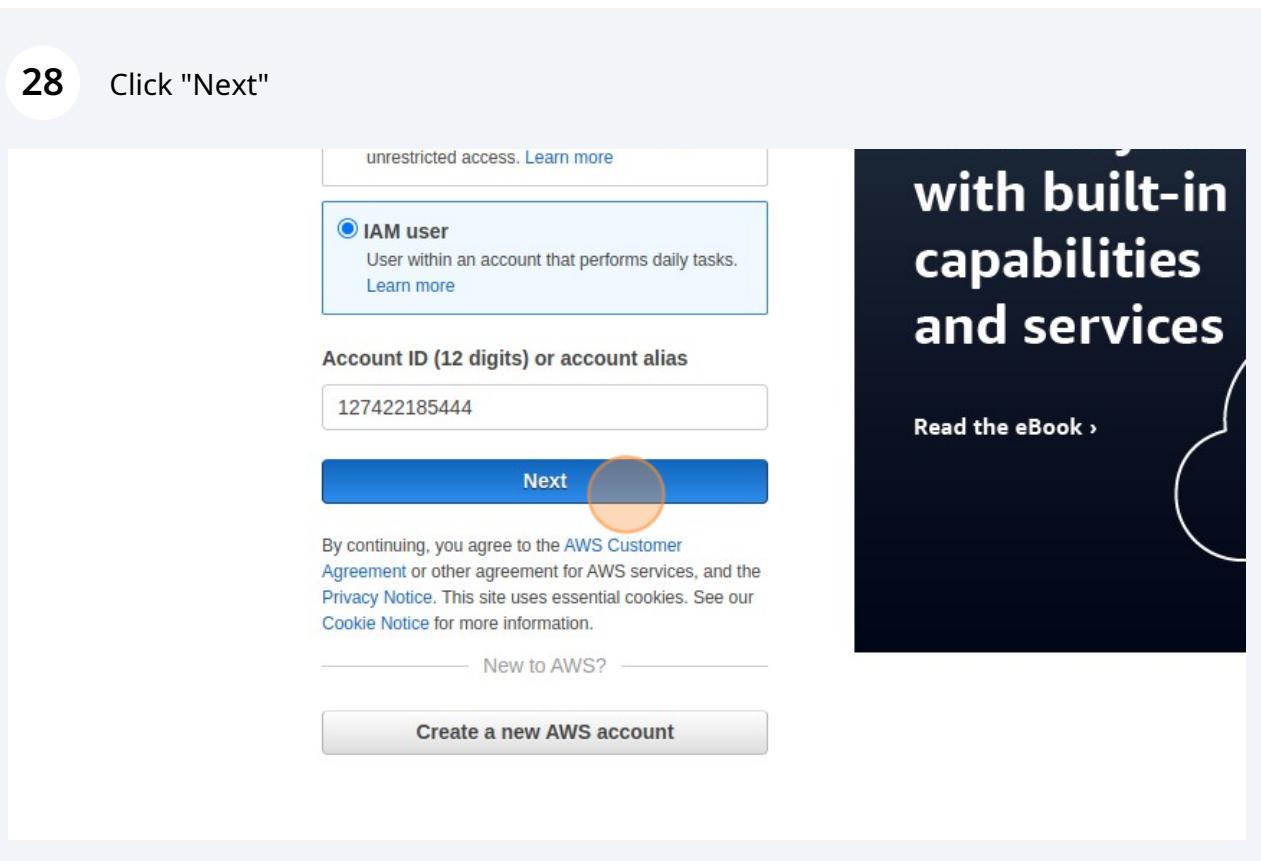
27

Enter your credentials, First enter your user Account ID , you can find in the url



28

Click "Next"



- 29** Click the "IAM user name" field, and enter the user name

The image shows the Amazon IAM sign-in page. At the top left is the Amazon smile logo. Below it, the heading "Sign in as IAM user" is displayed. There are three input fields: "Account ID (12 digits) or account alias" containing "127422185444", "IAM user name" which is empty and has a red circle highlighting its border, and "Password" which is also empty. Below these fields is a checkbox labeled "Remember this account". A large blue "Sign in" button is centered below the password field. At the bottom of the form are links for "Sign in using root user email" and "Forgot password?". To the right of the form is a dark sidebar with the word "INFRASTRUCTURE" at the top, followed by the text "Protect you with built-in capabilities and service", a "Read the eBook >" link, and a small circular icon.

- 30** Click the "Password" field, and enter the password you have received in the .csv file

The image shows the same Amazon IAM sign-in page as the previous screenshot, but with the "Password" field filled in. The "Account ID" field contains "127422185444", the "IAM user name" field contains "test-user-1", and the "Password" field contains a long string of characters. The rest of the page, including the sidebar, remains identical to the first screenshot.

31 Click "Sign in"

The screenshot shows the AWS sign-in page. It has fields for 'IAM user name' (containing 'test-user-1') and 'Password' (containing '*****'). There is a checkbox for 'Remember this account'. A large orange circle highlights the 'Sign in' button. Below the button are links for 'Sign in using root user email' and 'Forgot password?'. To the right, there is a dark sidebar with text and a 'Read the eBook' link, along with language and copyright information at the bottom.

32 Click the "Old password" field. and enter the same password again

The screenshot shows the AWS password change page. It displays the AWS account number '127422185444' and the IAM user name 'test-user-1'. It has four input fields: 'Old password' (highlighted with an orange circle), 'New password', 'Retype new password', and a 'Confirm password change' button. Below the fields is a 'Sign in using root user email' link. At the bottom, there is a language selection dropdown set to 'English'.

- 33** Click the "New password" field. and enter your new password

AWS account 127422185444
IAM user name test-user-1
Old password [REDACTED]
New password [REDACTED]
Retype new password [REDACTED]
Confirm password change
[Sign in using root user email](#)
English ▾
[Terms of Use](#) [Privacy Policy](#) © 1996-2023, Amazon Web Services, Inc. or its affiliates.

- 34** Click the "Retype new password" field. and again enter the new password

AWS account 127422185444
IAM user name test-user-1
Old password [REDACTED]
New password [REDACTED]
Retype new password [REDACTED]
Confirm password change
[Sign in using root user email](#)
English ▾
[Terms of Use](#) [Privacy Policy](#) © 1996-2023, Amazon Web Services, Inc. or its affiliates.

35 Click "Confirm password change"

IAM user name test-user-1

Old password [REDACTED]

New password [REDACTED]

Retype new password [REDACTED]

Confirm password change

Sign in using root user email

English ▾

Terms of Use Privacy Policy © 1996-2023, Amazon Web Services, Inc. or its affiliates.

36 Now you are in new user account Click the "Search" field. Type "s3"

Console Home Info

Recently visited

- AWS Billing Conductor
- S3
- EC2
- Billing
- IAM

View all services

Welcome to AWS

Getting started with AWS

Learn the fundamentals and find valuable information to get the most out of AWS.

Training and certification

Learn from AWS experts and advance your skills and knowledge.

What's new with AWS?

Discover new AWS services, features, and Regions.

AWS Health

No health data

You don't have permissions to access AWS Health.

Go to AWS Health

Cost and usage

No cost and usage

You haven't configured AWS Cost Explorer or you do not have permission.

Build a solution

Start building with simple wizards and automated workflows.

- Launch a virtual machine With EC2 (2 mins)
- Register a domain With Route 53 (3 mins)
- Start a development project With CodeStar (5 mins)
- Build a web app With AWS App Runner (5 mins)
- Start migrating to AWS With AWS MGN (2 mins)
- Host a static web app With AWS Amplify Console (2 mins)
- Build SQL Server on AWS With high availability (HA and FC) (2 mins)
- Deploy SAP on AWS With NetWeaver and HANA (with HA) (10 mins)

CloudShell Feedback

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy

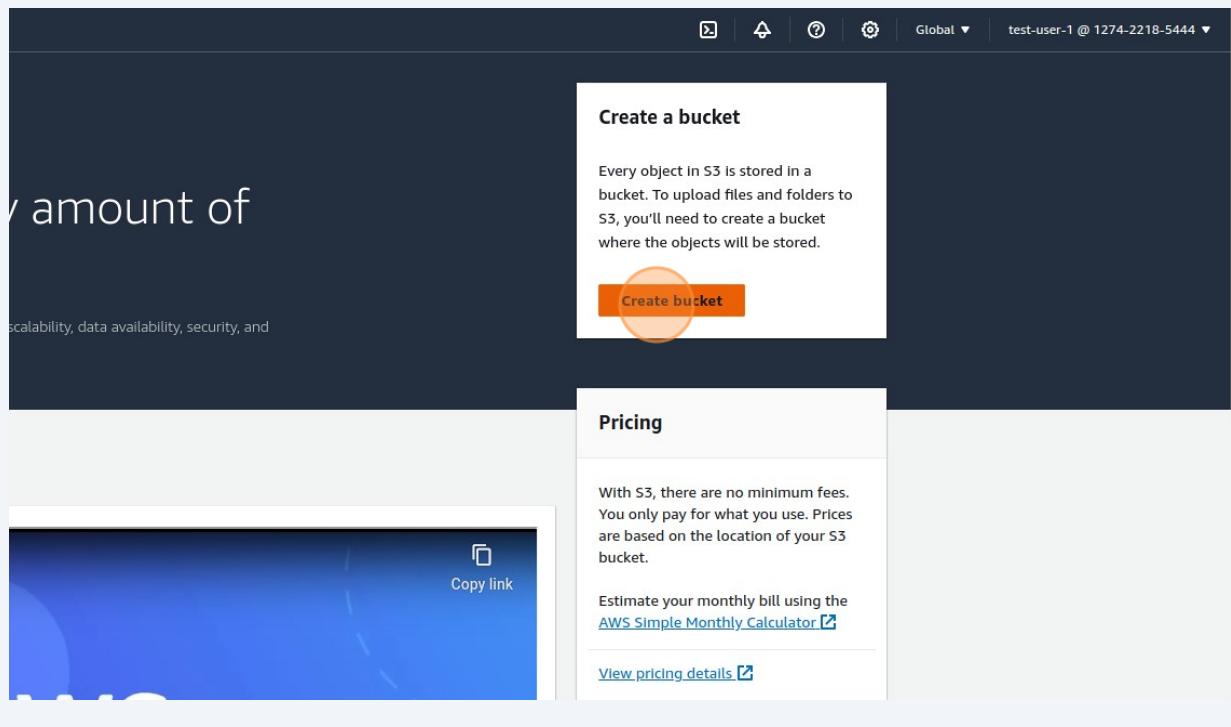
37 Click on s3

The screenshot shows the AWS search interface. The search bar at the top contains the query 's3'. Below the search bar, there is a sidebar with the following categories and their counts: Services (8), Features (26), Resources (New), Documentation (23,547), Knowledge Articles (20), Marketplace (1,490), Blogs (1,310), Events (25), and Tutorials (13). The main content area is titled 'Services' and displays three items: 'S3' (Scalable Storage in the Cloud), 'S3 Glacier' (Archive Storage in the Cloud), and 'AWS Snow Family' (Large Scale Data Transport). The 'S3' item is highlighted with a red circle.

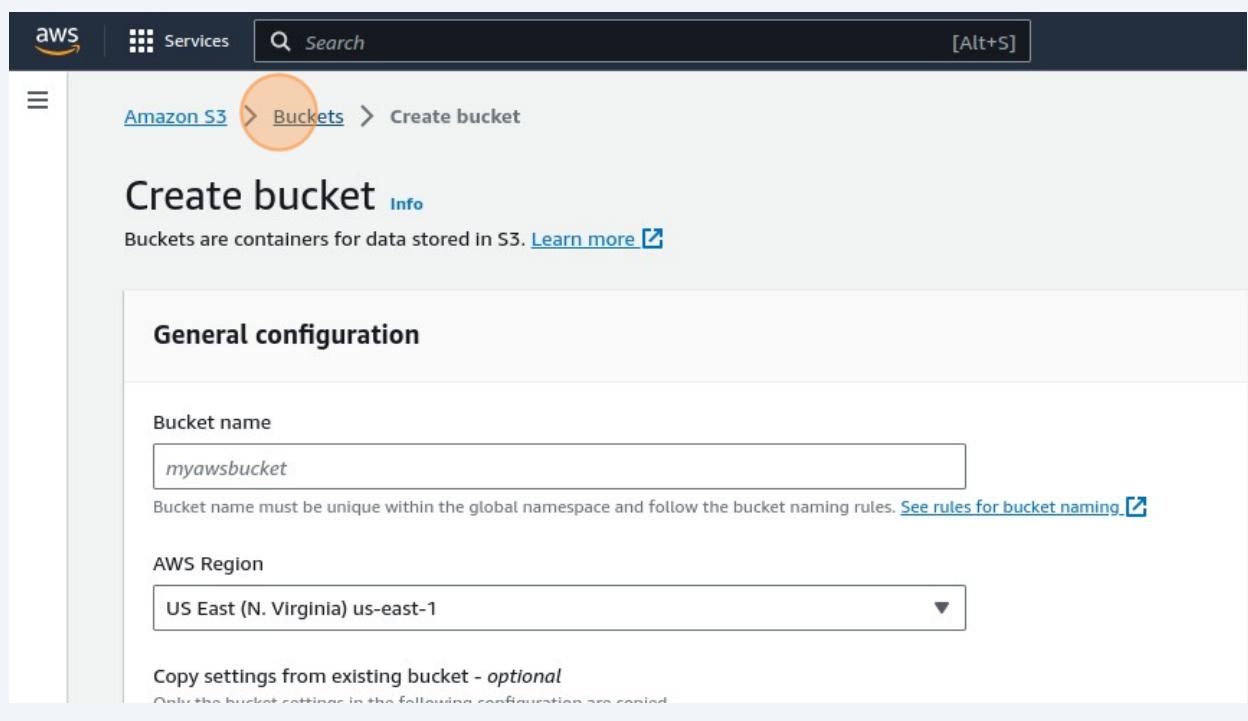
38 Click "S3"

This screenshot is identical to the one above, showing the AWS search results for 's3'. The sidebar and main content area are the same, but the 'S3' service card is now explicitly highlighted with a red circle around its icon and title.

39 Click "Create bucket"



40 Click "Buckets"



- 41 Observe here the new user don't have any s3 policy

The screenshot shows the AWS S3 Buckets page. At the top, there is a search bar labeled "Find buckets by name". Below it, a table header includes columns for "Name" and "AWS Region". A prominent error message is displayed in a red-bordered box: "You don't have permissions to list buckets. After you or your AWS administrator has updated your permissions to allow the s3>ListAllMyBuckets action, ref". The entire error message box is highlighted with an orange oval.

- 42 Click the "Search" field. Type "ec2"

The screenshot shows the AWS S3 Buckets page. At the top, there is a navigation bar with the AWS logo, "Services", and a search bar containing the text "Search" which is highlighted with a brown oval. Below the search bar, the URL "Amazon S3 > Buckets" is visible. A section titled "Account snapshot" is present, followed by the "Buckets" table. The table header includes columns for "Name" and "AWS Region". A red-bordered error message box is shown again: "You don't have permissions to list buckets. After you or your AWS administrator has updated your permissions to allow the s3>ListAllMyBuckets action, ref". The search input field is also highlighted with an orange oval.

43 Click "EC2"

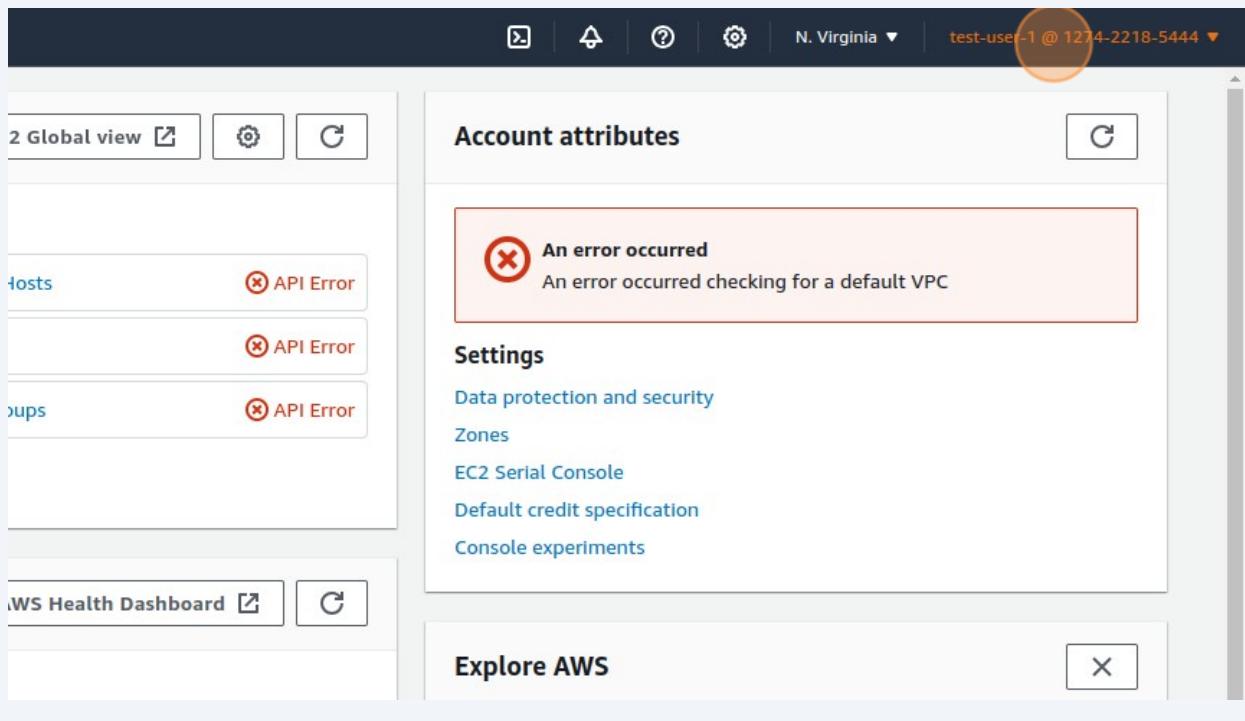
The screenshot shows the AWS Management Console search results for the query 'ec2'. The search bar at the top contains 'ec2'. Below it, a sidebar on the left lists services like Amazon S3, Account, Storage, Buckets, and Tutorials. The main content area is titled 'Services' and shows the EC2 service card. The EC2 card features the EC2 logo, the text 'Virtual Servers in the Cloud', and a 'Top features' section with links to Dashboard, Launch templates, Instances, Spot Instance requests, Savings plans, and more. Other cards visible include 'EC2 Image Builder' and 'Recycle Bin'.

44 You can understand that our new user don't have a permission to ec2 also

The screenshot shows the AWS EC2 Dashboard. On the left, a sidebar lists EC2 Global View, Events, Instances (with sub-options like Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, and New), and Images (with sub-options like AMIs and AMI Catalog). The main content area is titled 'Resources' and displays a message: 'You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:'. It lists resources with their counts and API error status: Instances (running) [0], Auto Scaling Groups [0] (API Error), Elastic IPs [0] (API Error), Instances [0] (API Error), Load balancers [0] (API Error), Placement groups [0] (API Error), Snapshots [0] (API Error), and Volumes [0]. Below this is a 'Launch instance' section with a large orange 'Launch instance' button and a 'Migrate a server' link. To the right is a 'Service health' section showing the Region as US East (N. Virginia).

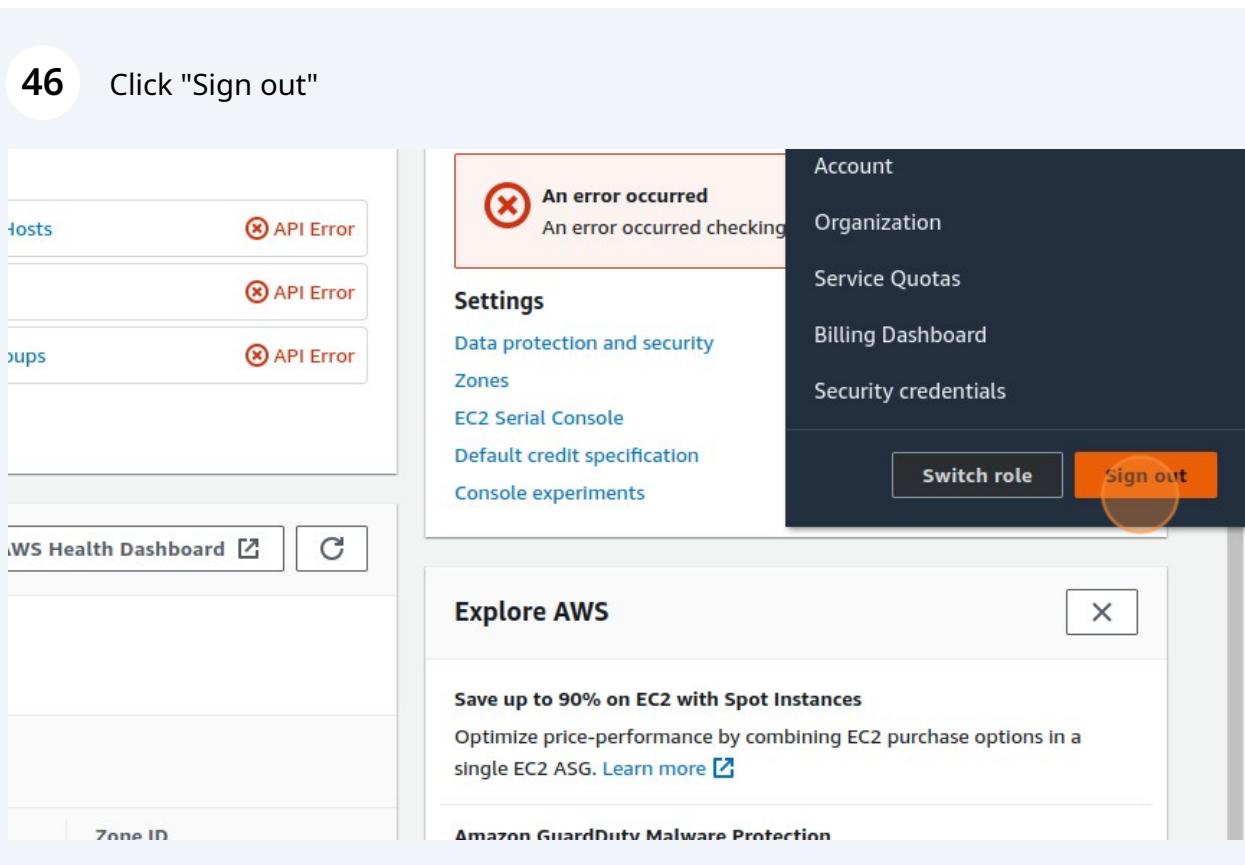
45

Our new user don't have any permissions .Now we will provide a permission.Click "test-user-1 @ 1274-2218-5444"(account profile)

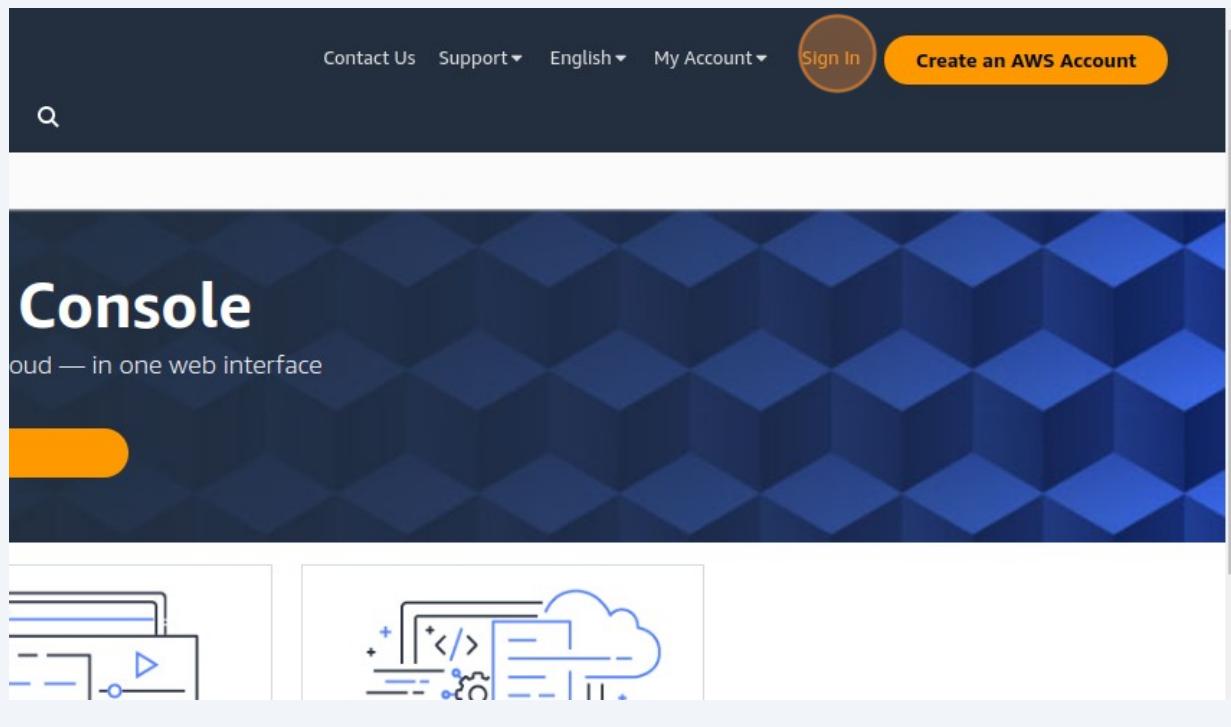


46

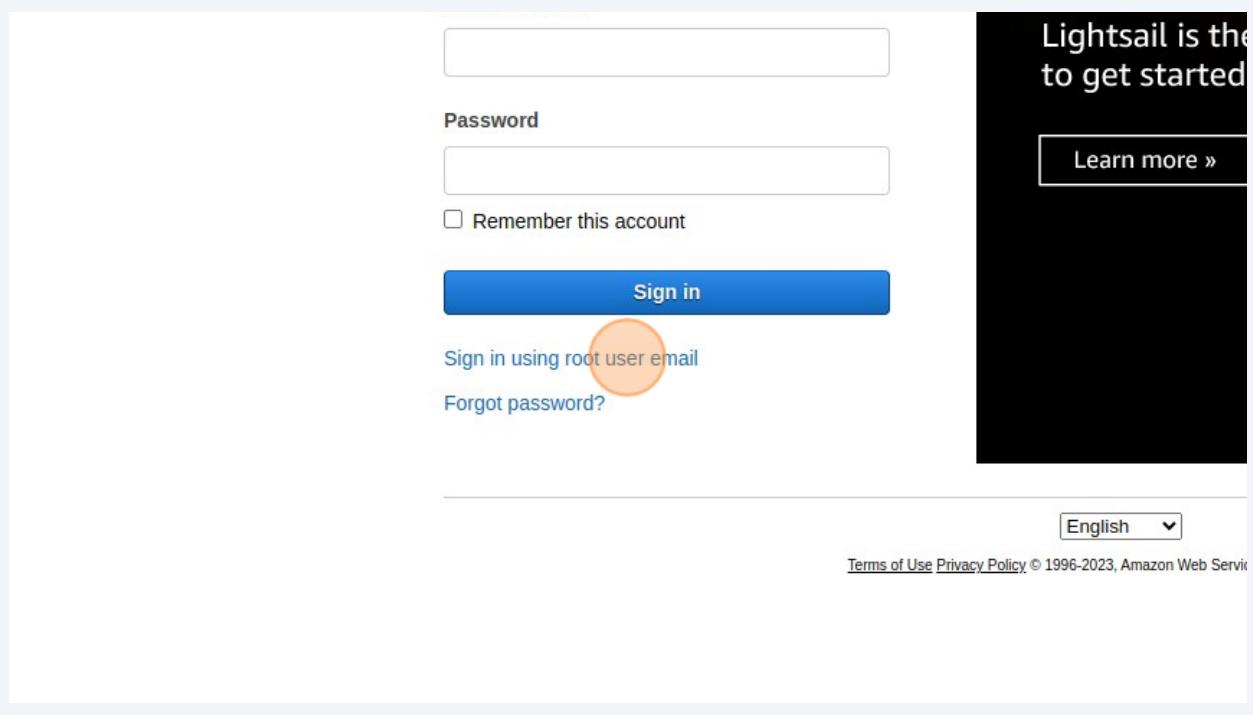
Click "Sign out"



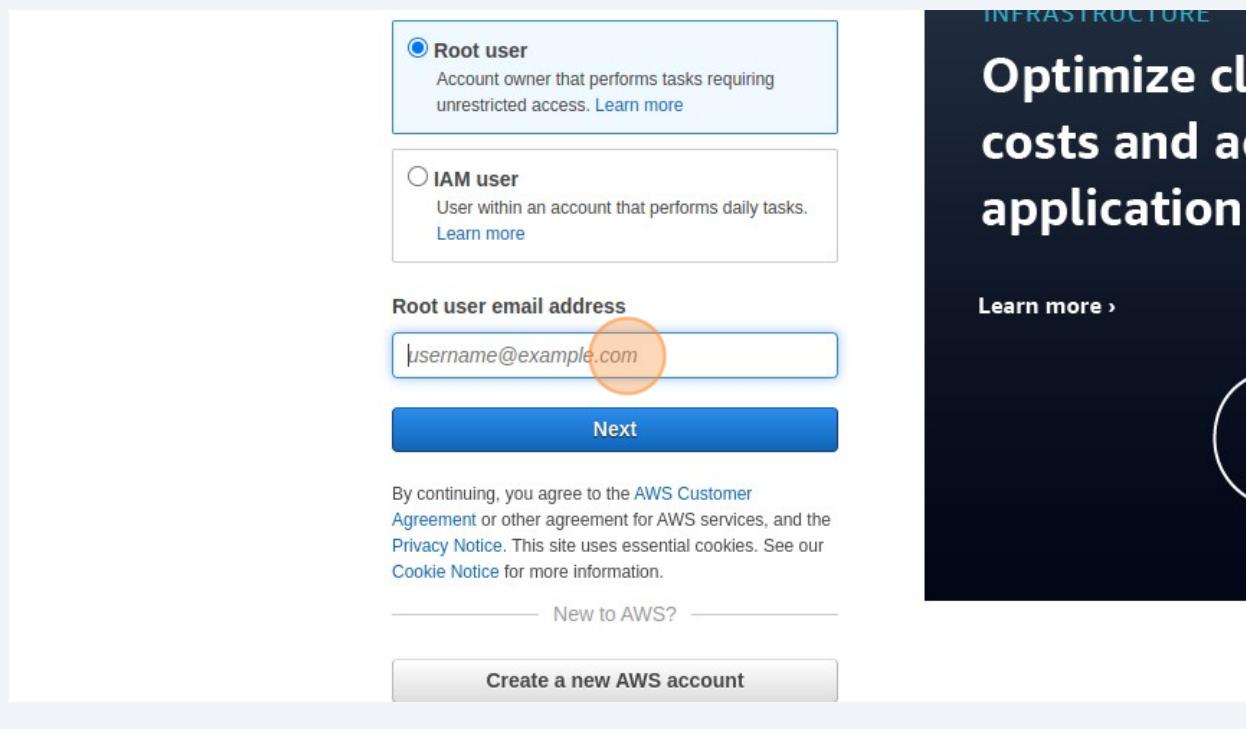
47 Click "Sign In"



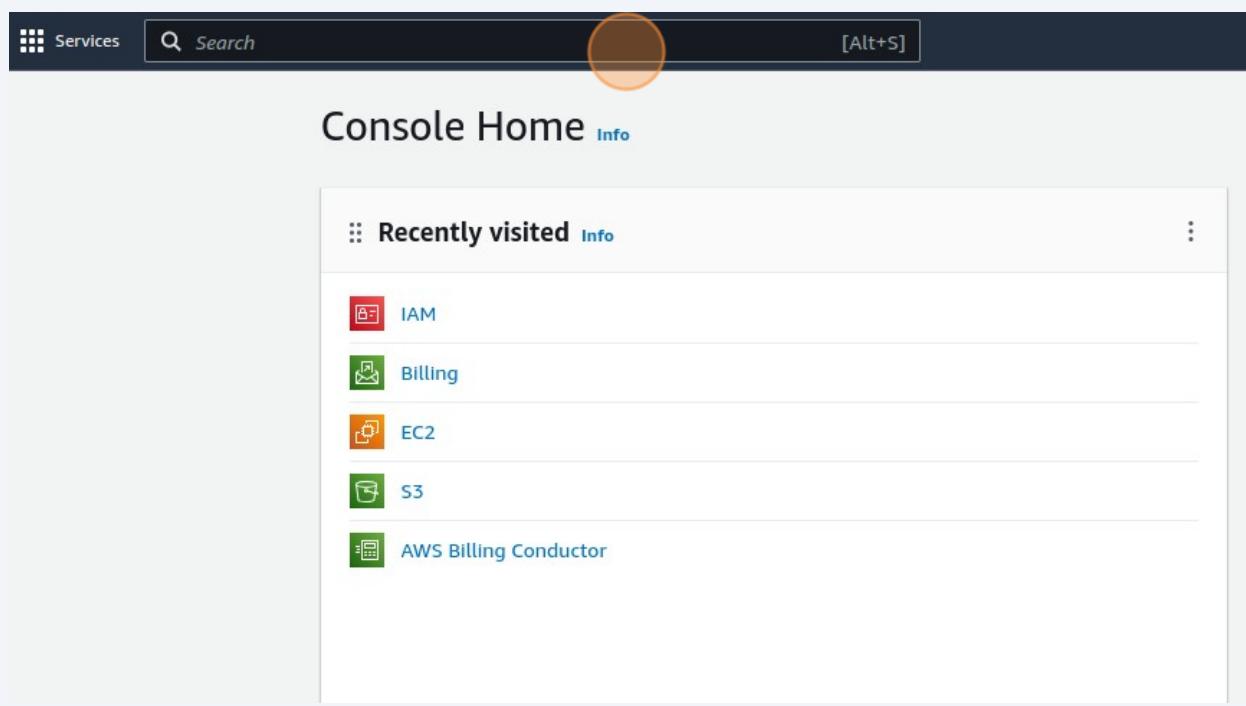
48 Click "Sign in using root user email"



49 Enter into your Root AWS Account



50 Click the "Search" field.



51 Type "iam"

52 Click "IAM"

The screenshot shows the AWS search interface. In the top navigation bar, there is a 'Services' button, a search bar containing the text 'iam', and a close button ('X'). Below the search bar, a message says 'Search results for 'iam'' and 'Try searching with longer queries for more relevant results'. On the left, there is a sidebar with categories: 'Services (10)', 'Features (20)', 'Resources New', 'Documentation (48,533)', 'Knowledge Articles (20)', 'Marketplace (697)', 'Blogs (1,674)', 'Events (12)', and 'Tutorials (2)'. The main content area is titled 'Services' and lists three items: 'IAM' (Manage access to AWS resources), 'IAM Identity Center' (Manage workforce user access to multiple AWS accounts and cloud apps), and 'Resource Access Manager' (Share AWS resources with other accounts or AWS Organizations). The 'IAM' item has a yellow circle highlighting it.

53 Click "Users"

The screenshot shows the AWS IAM Dashboard. On the left sidebar, under the 'Access management' section, the 'Users' link is highlighted with an orange circle. The main content area is titled 'IAM Dashboard' and contains a 'Security recommendations' section with two items: 'Root user has MFA' (green checkmark) and 'Deactivate or delete access keys for root user' (yellow warning icon). Below that is an 'IAM resources' section showing 0 User groups, 1 User, and 2 Roles.

54 Click "test-user-1"

The screenshot shows the 'Management (IAM)' interface. On the left sidebar, under the 'Access management' section, the 'Users' link is highlighted with an orange circle. The main content area is titled 'Users (1) Info' and shows a table with one row for 'test-user-1'. The 'User name' column contains 'test-user-1', which is also highlighted with an orange circle.

55 our new user had only one policy . we already utilise it for reset password

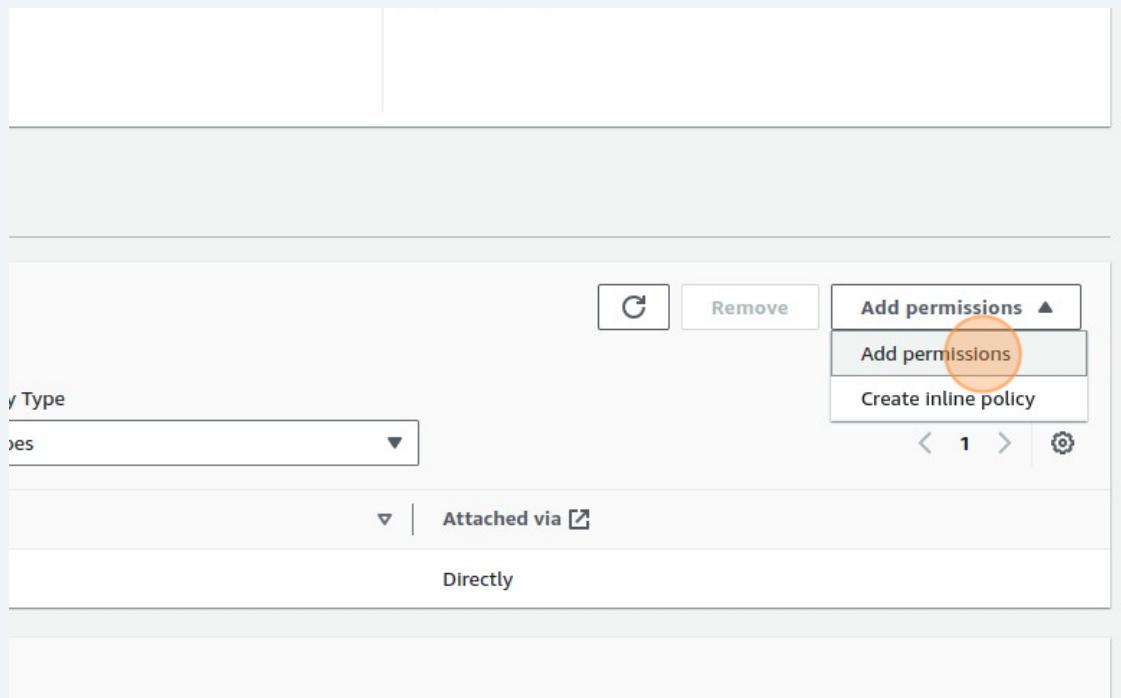
The screenshot shows the 'Permissions policies' section of the AWS IAM console. It displays a single policy named 'IAMUserChangePassword'. The policy is categorized as 'AWS managed'. A search bar and a filter button ('All types') are visible at the top. Below the table, there are sections for 'Permissions boundary' (not set) and 'Generate policy based on CloudTrail events'.

Policy name	Type
IAMUserChangePassword	AWS managed

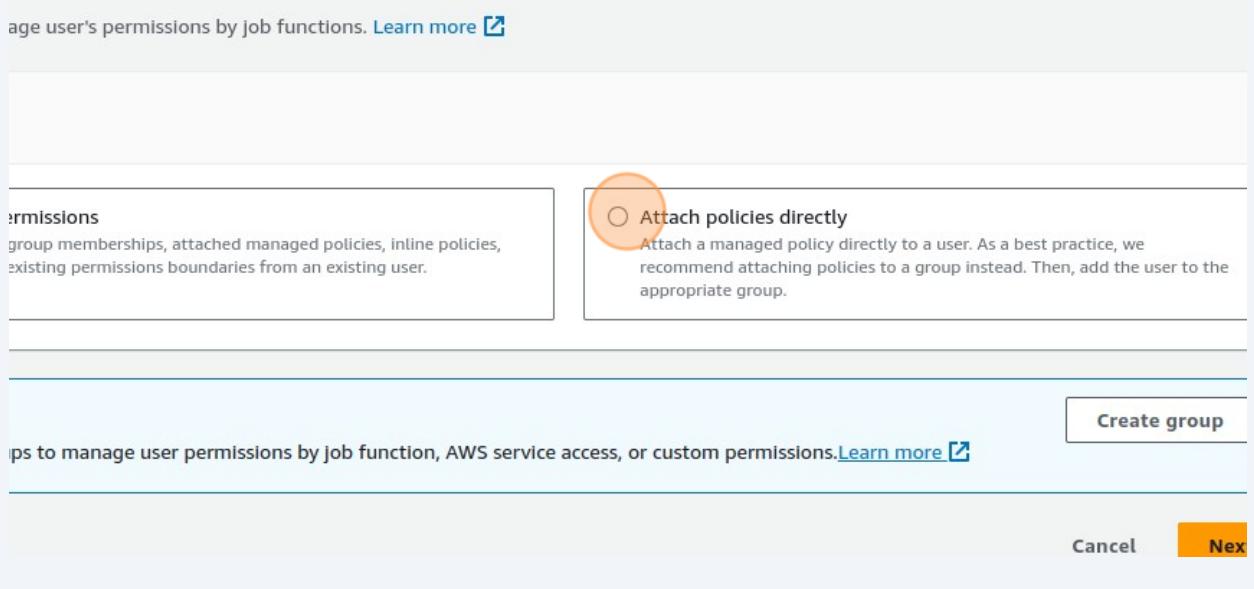
56 Click "Add permissions"

The screenshot shows the 'Permissions' tab of the AWS IAM User configuration page. It includes a 'Create access key' button, a 'Type' dropdown set to 'Yes', and a 'Remove' button. The 'Add permissions' button is highlighted with an orange circle. Below these are sections for 'Attached via' (set to 'Directly') and navigation controls.

57 Click "Add permissions"



58 Click on "Attach policies directly"



59 Click the "Search" field. Type "s3"

- 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 any existing permissions boundaries from an existing group.

Permissions policies (1134)

 Search

Filter by Type

All types ▾

<input type="checkbox"/>	Policy name 	Type
<input type="checkbox"/>	 AccessAnalyzerServiceRolePolicy	AWS managed
<input type="checkbox"/>	 AdministratorAccess	AWS managed - job function
<input type="checkbox"/>	 AdministratorAccess-Amplify	AWS managed
<input type="checkbox"/>	 AdministratorAccess-AWSElasticBeanstalk	AWS managed

60 Click this checkbox. That means you are providing s3 services full access to our test user

Permissions policies (1134)

 s3

Policy name 

 [AmazonDMSRedshiftS3Role](#)

 [AmazonS3FullAccess](#)

 [AmazonS3ObjectLambdaExecutionRolePolicy](#)

 [AmazonS3OutpostsFullAccess](#)

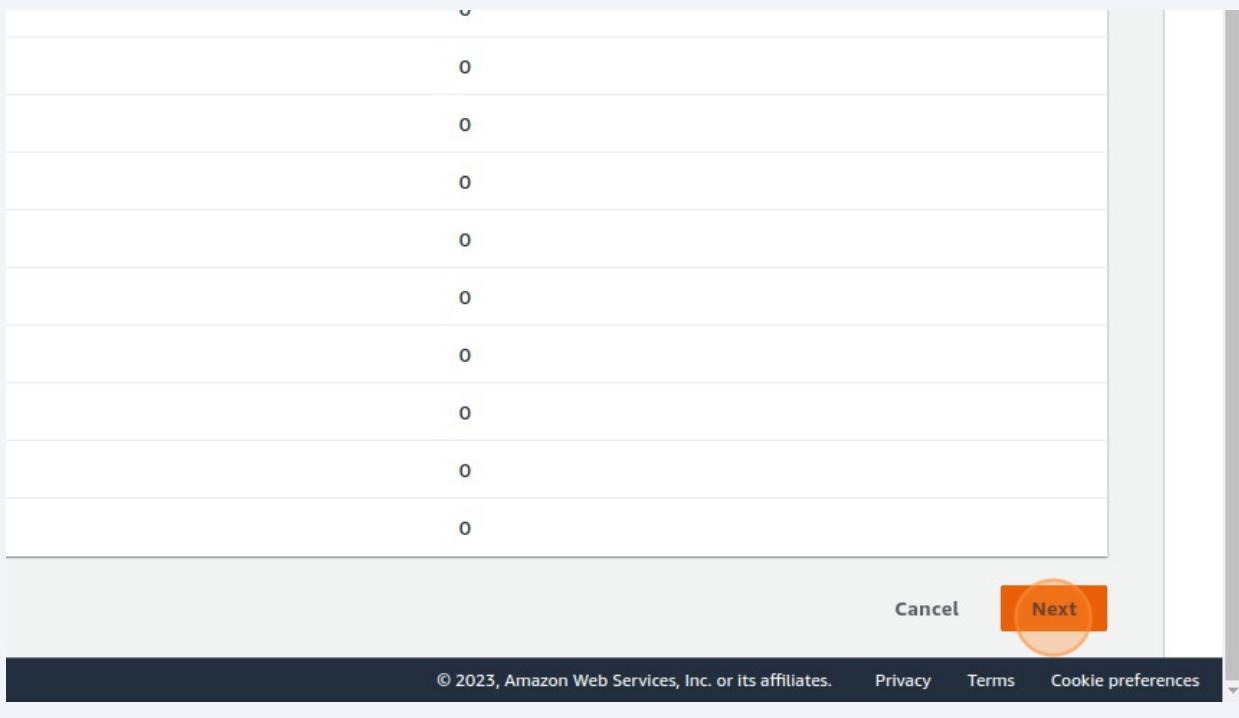
 [AmazonS3OutpostsReadOnlyAccess](#)

 [AmazonS3ReadOnlyAccess](#)

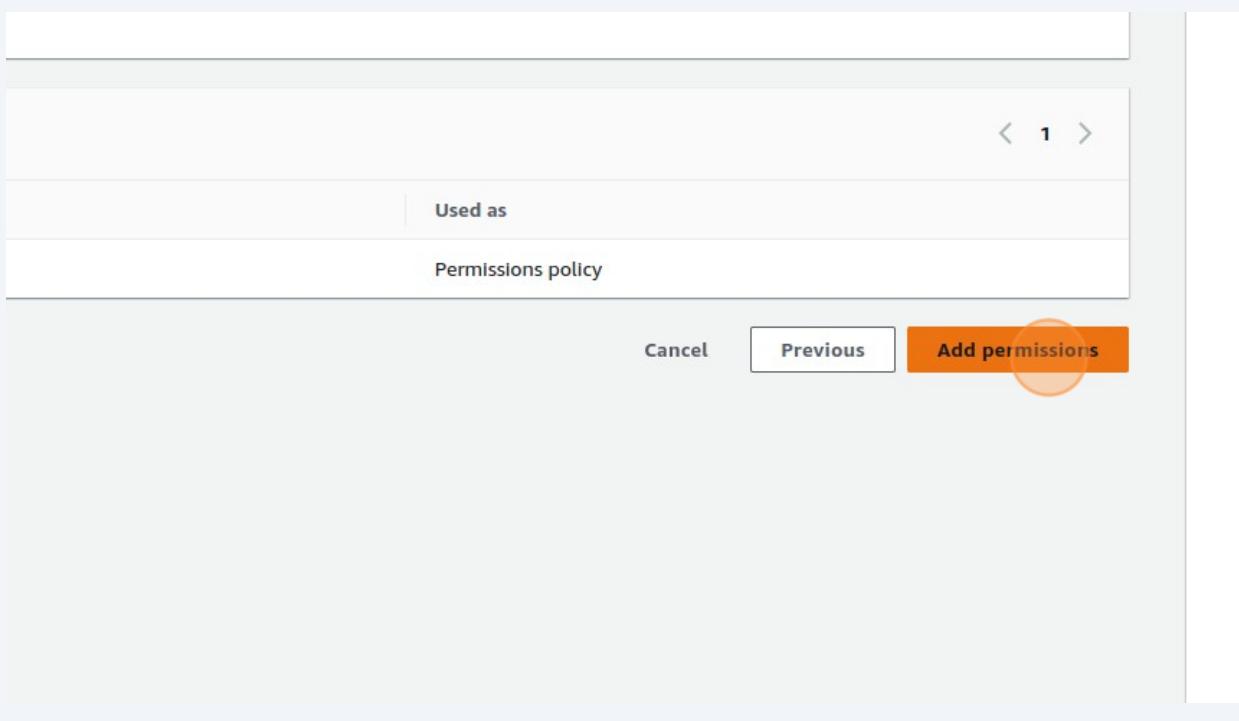
 [AWSBackupServiceRolePolicyForS3Backup](#)

 [AWSBackupServiceRolePolicyForS3Restore](#)

61 Click "Next"



62 Click "Add permissions"



63 Now, you can see here, our new test user has got a new policy (s3)

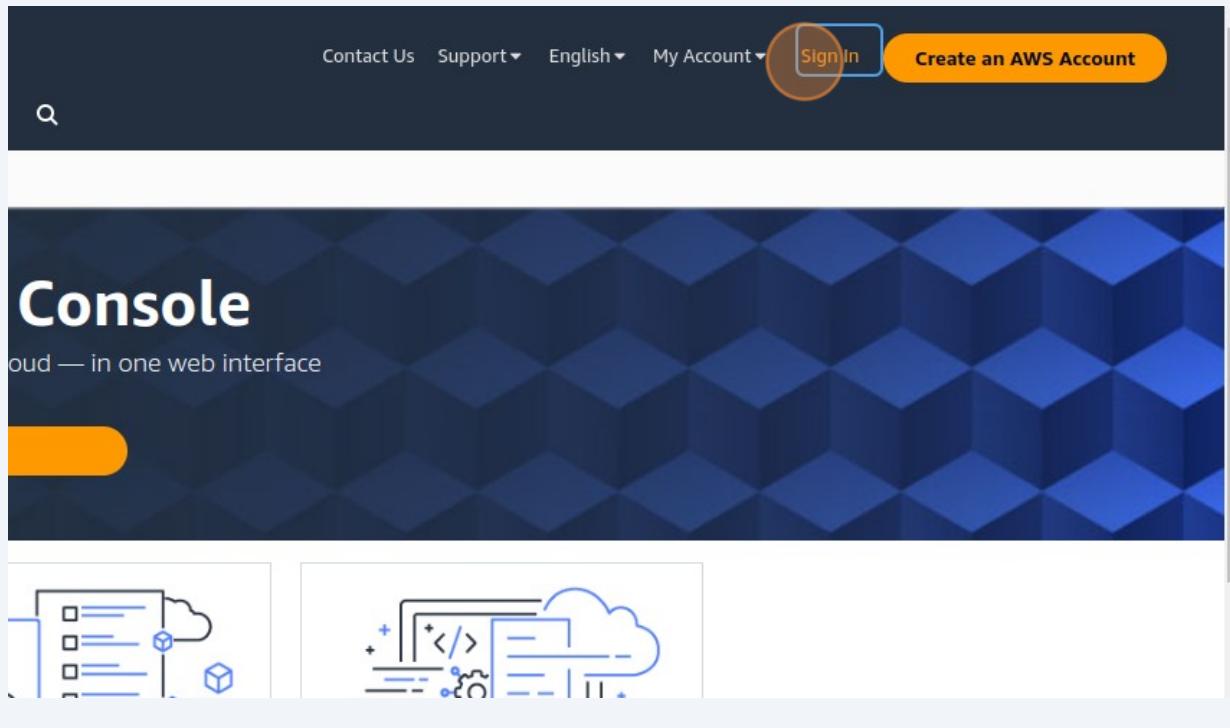
The screenshot shows the AWS IAM Policies page. At the top, a message says "Permissions are defined by policies attached to the user directly or through groups." Below this is a search bar and a table header with columns for "Policy name" and "Type". Two policies are listed: "AmazonS3FullAccess" (AWS managed) and "IAMUserChangePassword" (AWS managed). The second policy is highlighted with an orange circle. Below the table, there's a section titled "Permissions boundary (not set)" and another titled "Generate policy based on CloudTrail events" with a "more" link.

Policy name	Type
AmazonS3FullAccess	AWS managed
IAMUserChangePassword	AWS managed

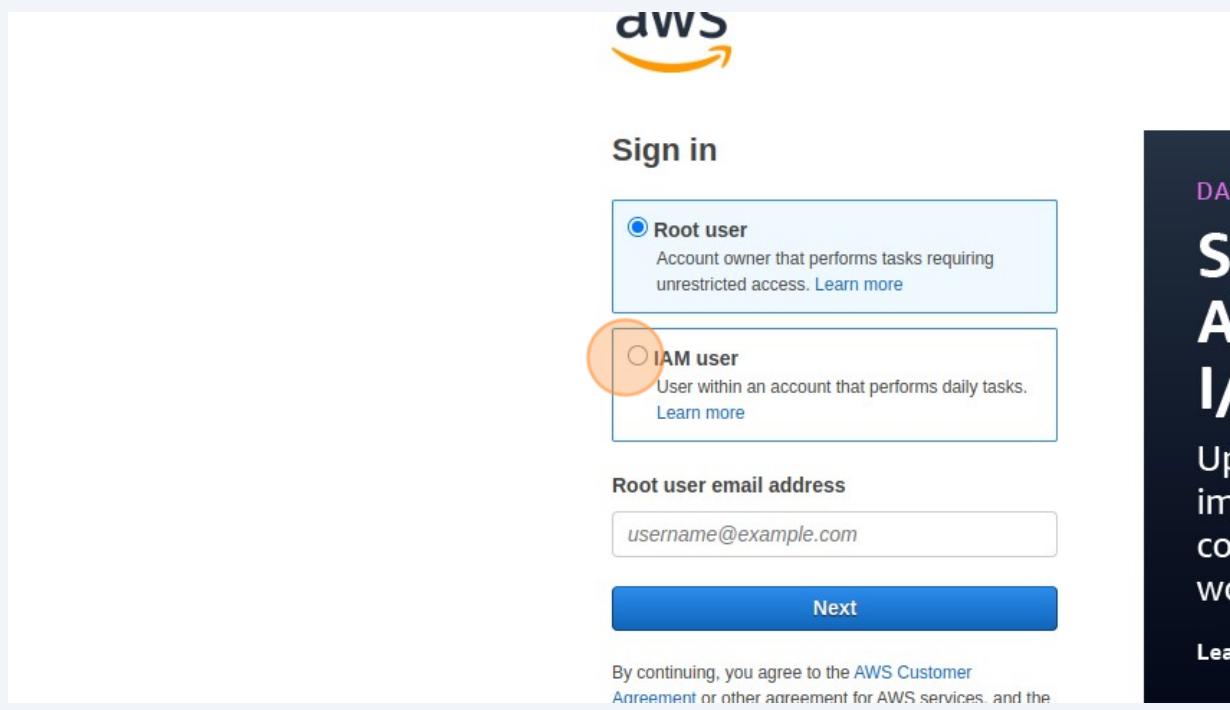
64 Now click on your Root account profile and Click "Sign out"

The screenshot shows the AWS Root account profile page. On the right, a sidebar menu includes "Account", "Organization", "Service Quotas", "Billing Dashboard", and "Security credentials". At the bottom of the sidebar is a "Sign out" button, which is highlighted with an orange circle. The main content area shows "Access key 1" and a "Create access key" link.

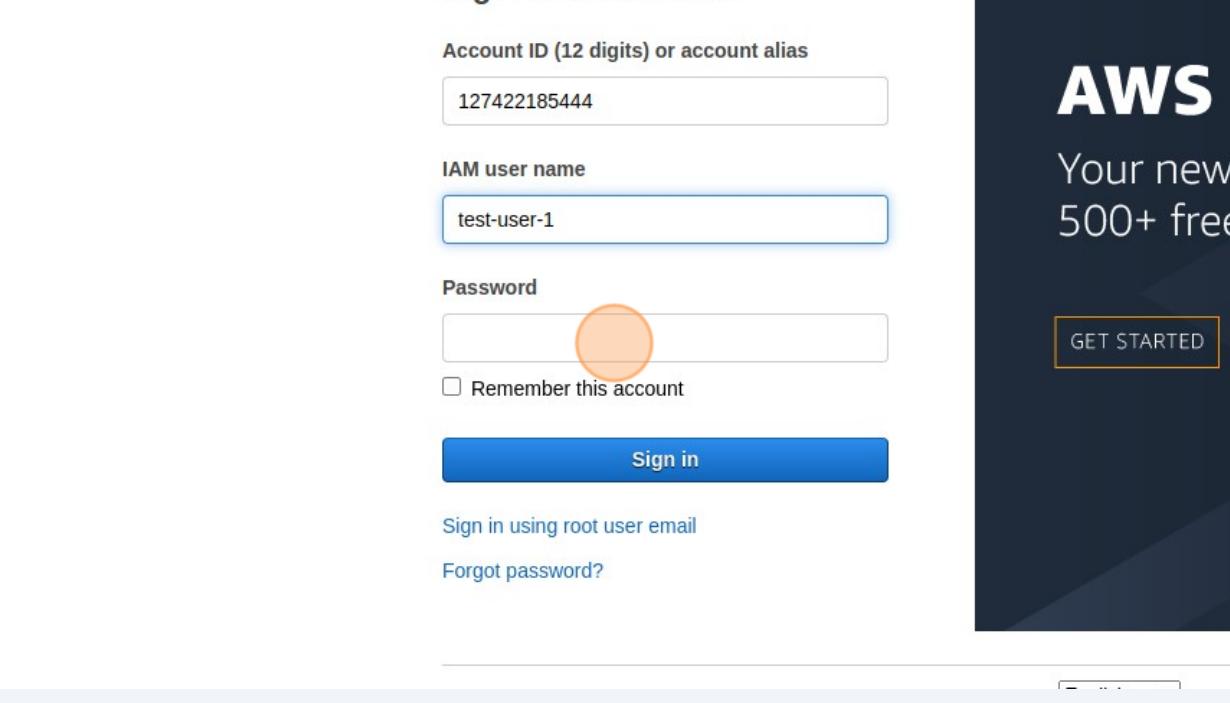
65 let's go to our test user account Click "Sign In"



66 Click IAM user



67 Enter your user account credentials



The image shows the AWS sign-in interface. It has a light gray header bar with the AWS logo and a dark blue sidebar on the right. The main form area contains fields for Account ID (12 digits) or account alias (filled with '127422185444'), IAM user name ('test-user-1'), and Password (redacted). There is a 'Remember this account' checkbox and a large blue 'Sign in' button. Below the form are links for 'Sign in using root user email' and 'Forgot password?'. The sidebar on the right displays the AWS logo, a promotional message 'Your new free tier includes 500+ free services', and a 'GET STARTED' button.

Account ID (12 digits) or account alias
127422185444

IAM user name
test-user-1

Password

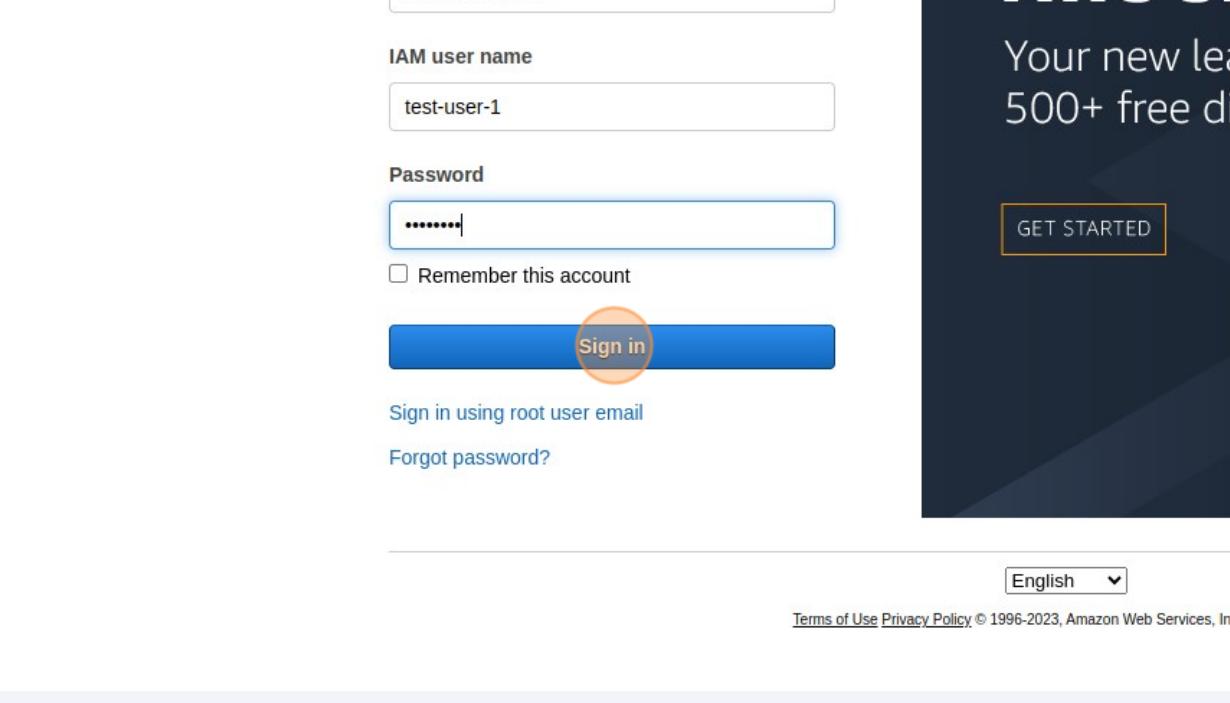
Remember this account

Sign in

[Sign in using root user email](#)
[Forgot password?](#)

AWS
Your new free tier includes 500+ free services
GET STARTED

68 Click "Sign in"



The image shows the same AWS sign-in interface as the previous screenshot, but with the 'Sign in' button highlighted by a large orange circle. The rest of the interface is identical to the first screenshot.

IAM user name
test-user-1

Password

Remember this account

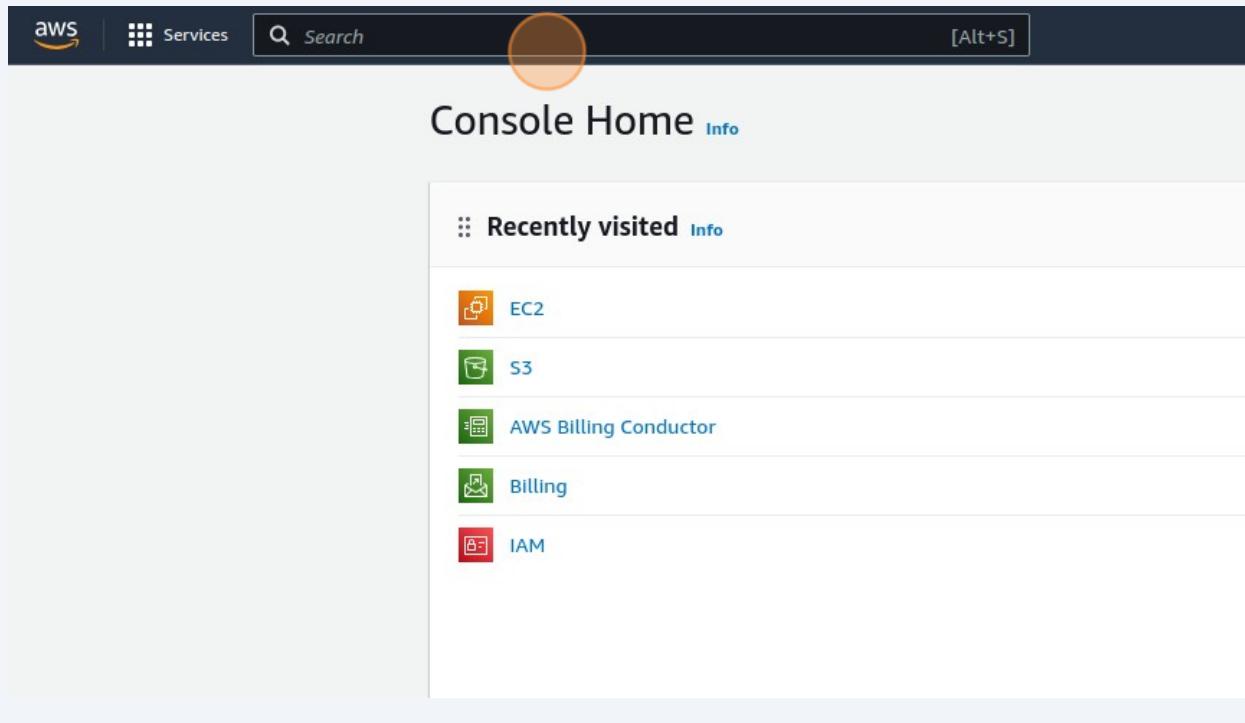
Sign in

[Sign in using root user email](#)
[Forgot password?](#)

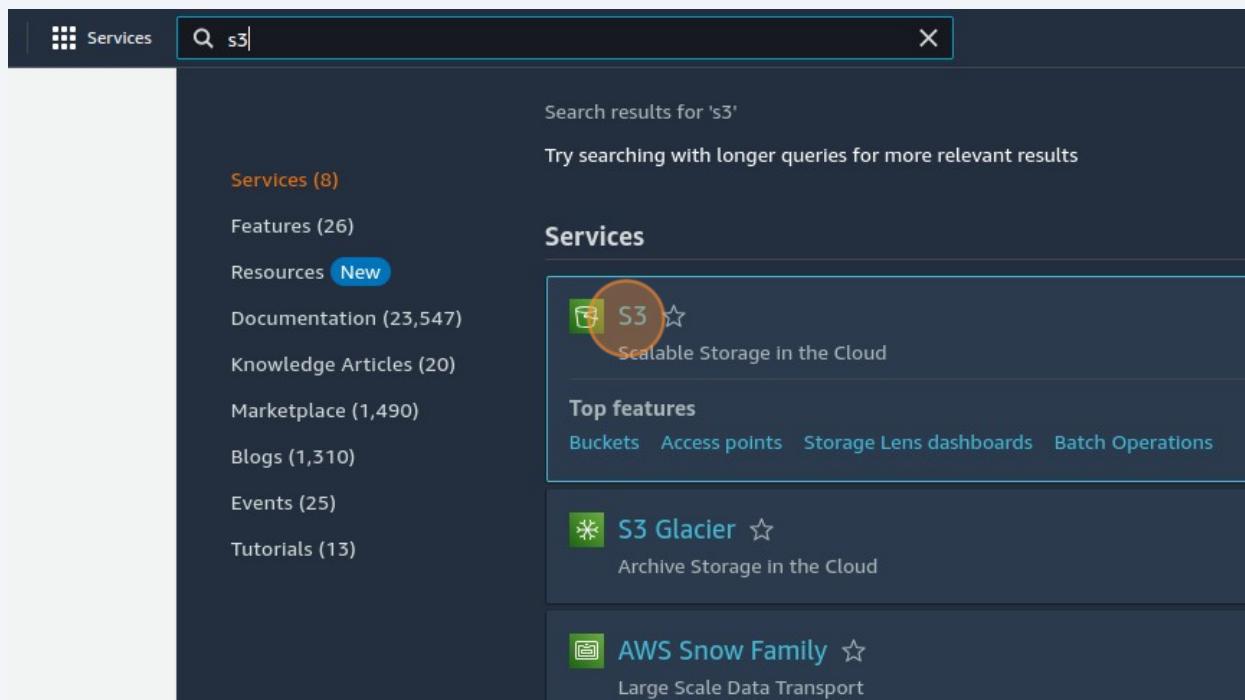
Your new free tier includes 500+ free services
GET STARTED

English ▾
[Terms of Use](#) [Privacy Policy](#) © 1996-2023, Amazon Web Services, Inc.

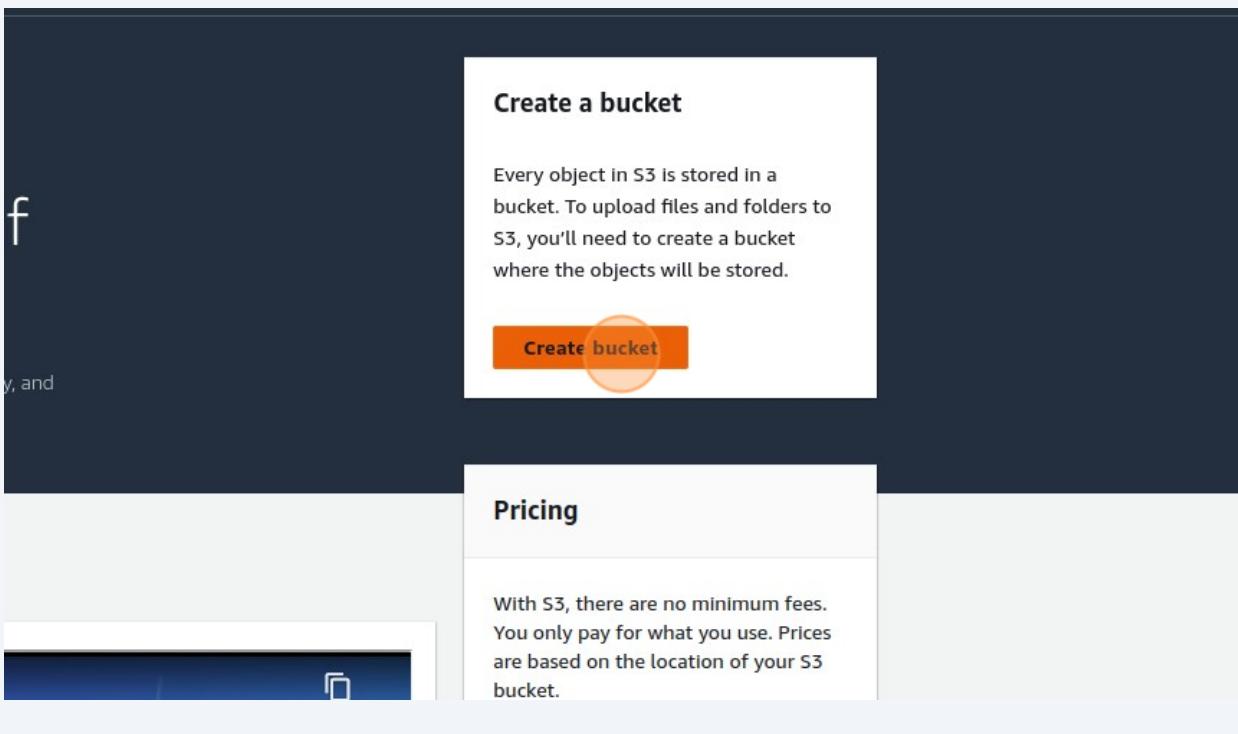
69 Click the "Search" field.Type "s3"



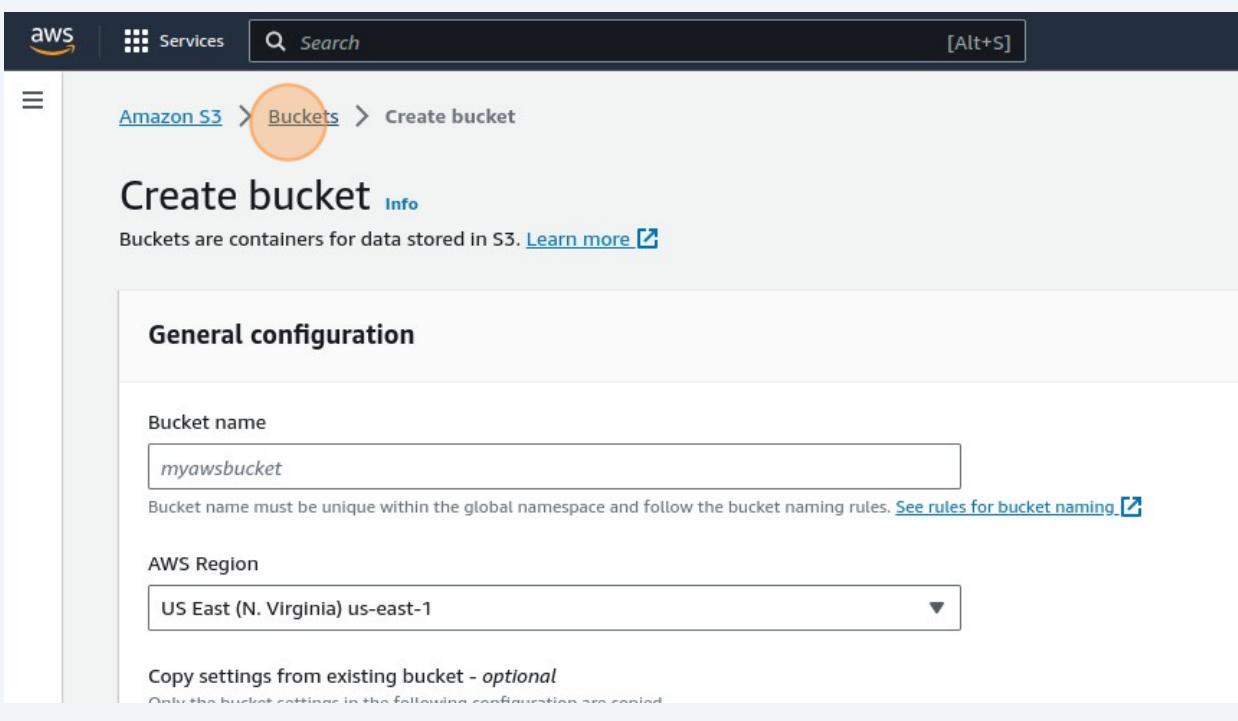
70 Click "S3"



71 Click "Create bucket"

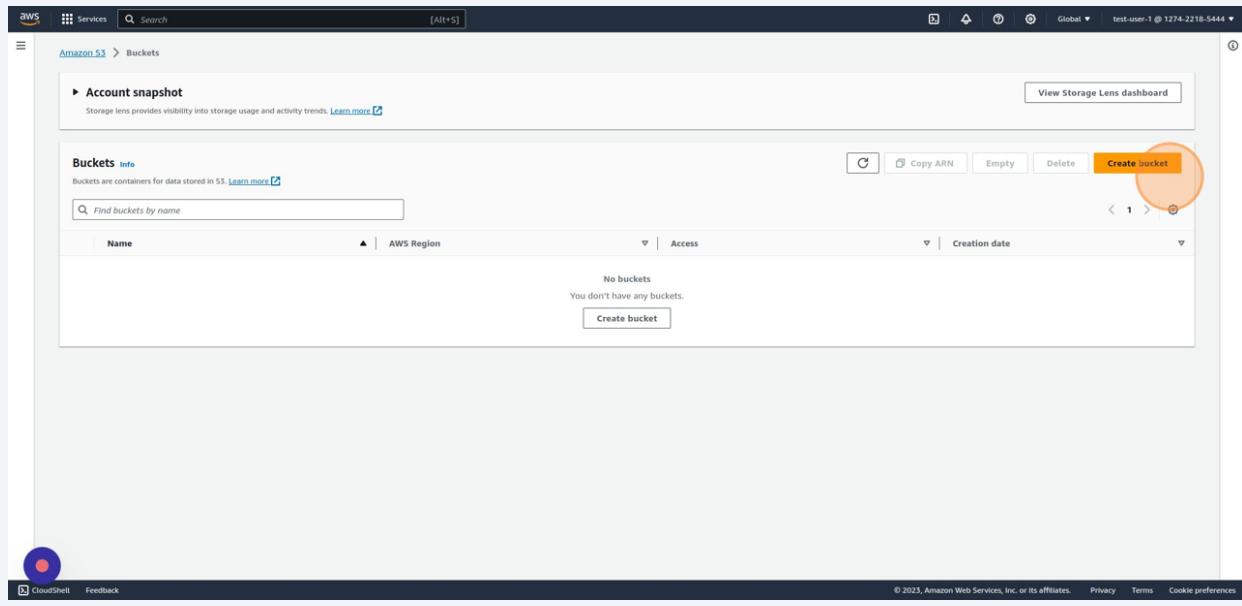


72 Click "Buckets"



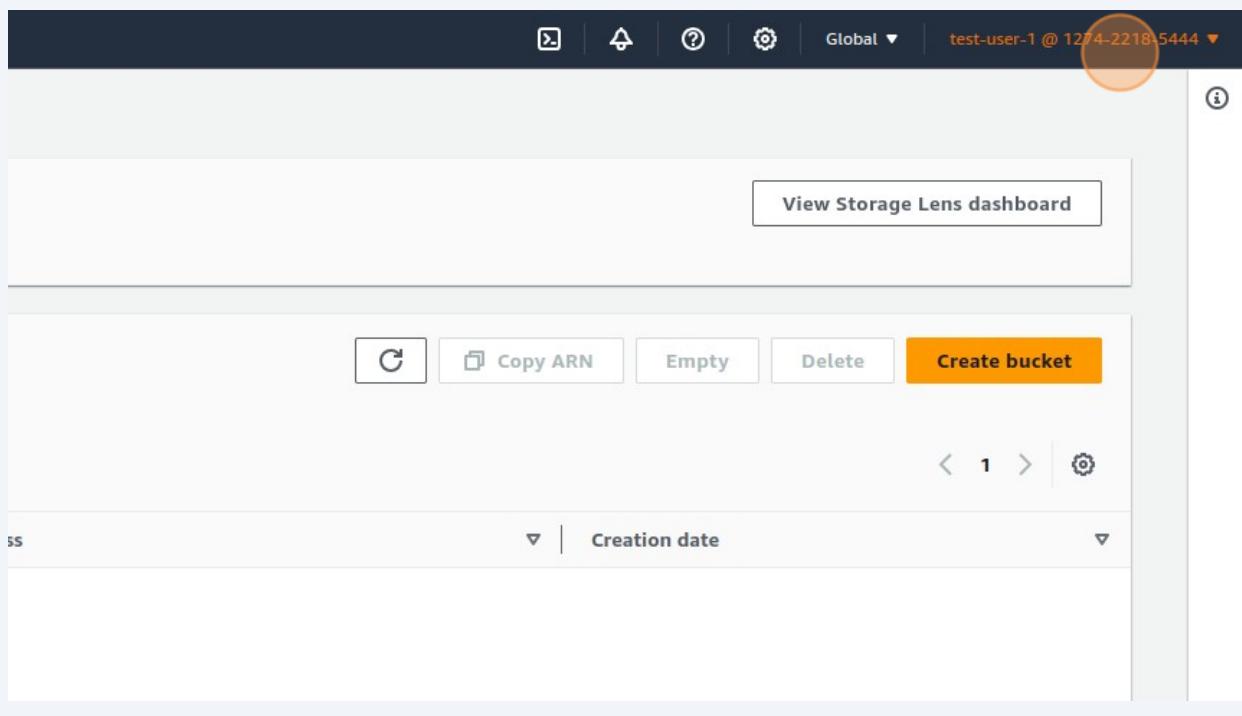
73

Now you can observe ,the test-user have full access to s3.Now the user can perform any action on s3 service.

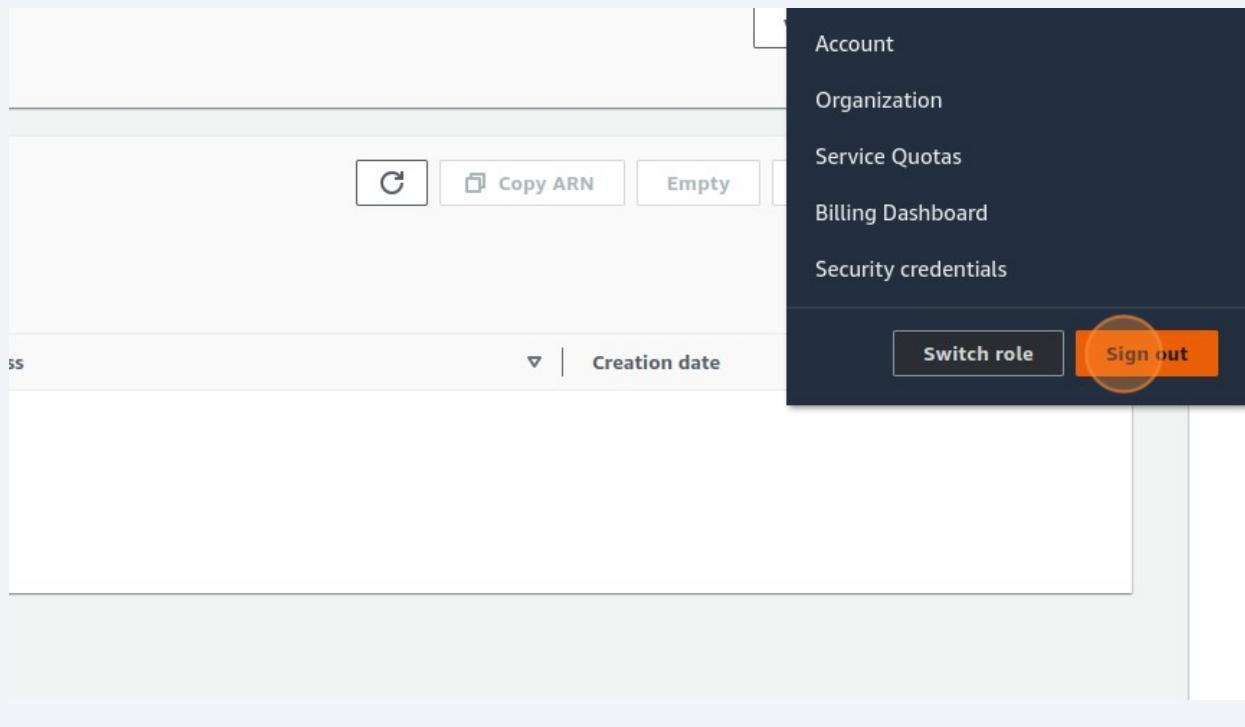


74

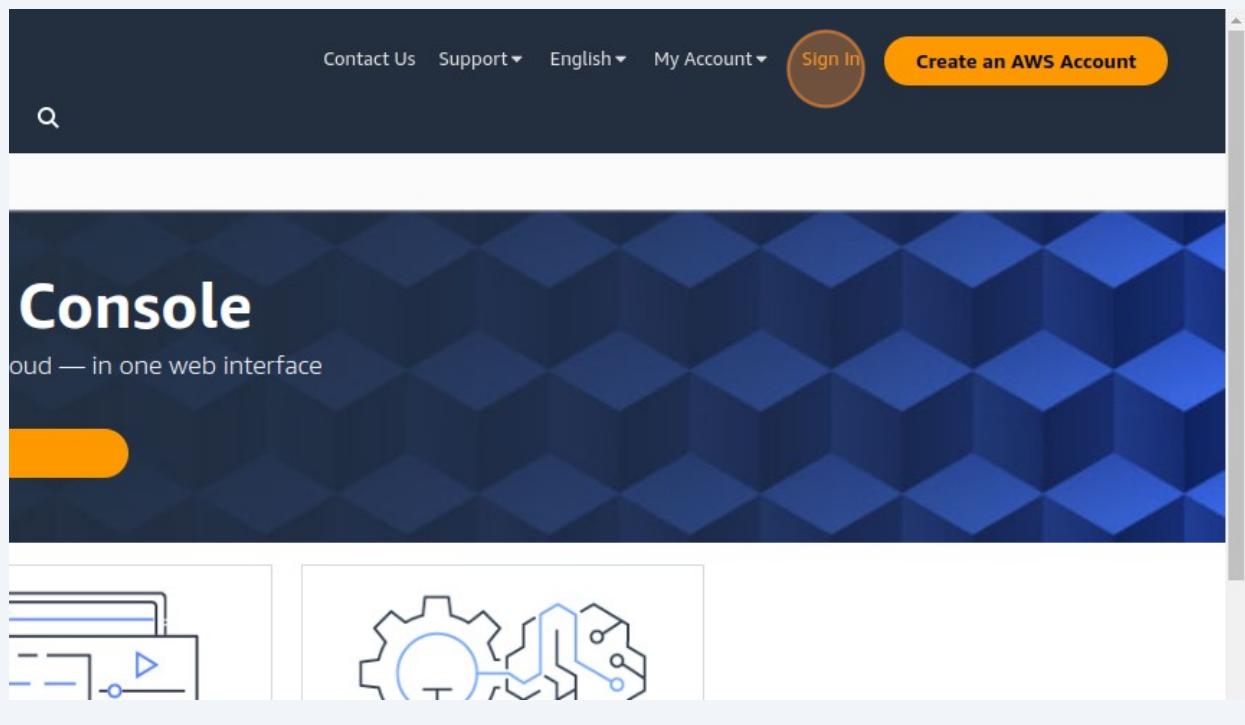
Click "test-user-1 @ 1274-2218-5444" (profile account)



75 Click "Sign out"

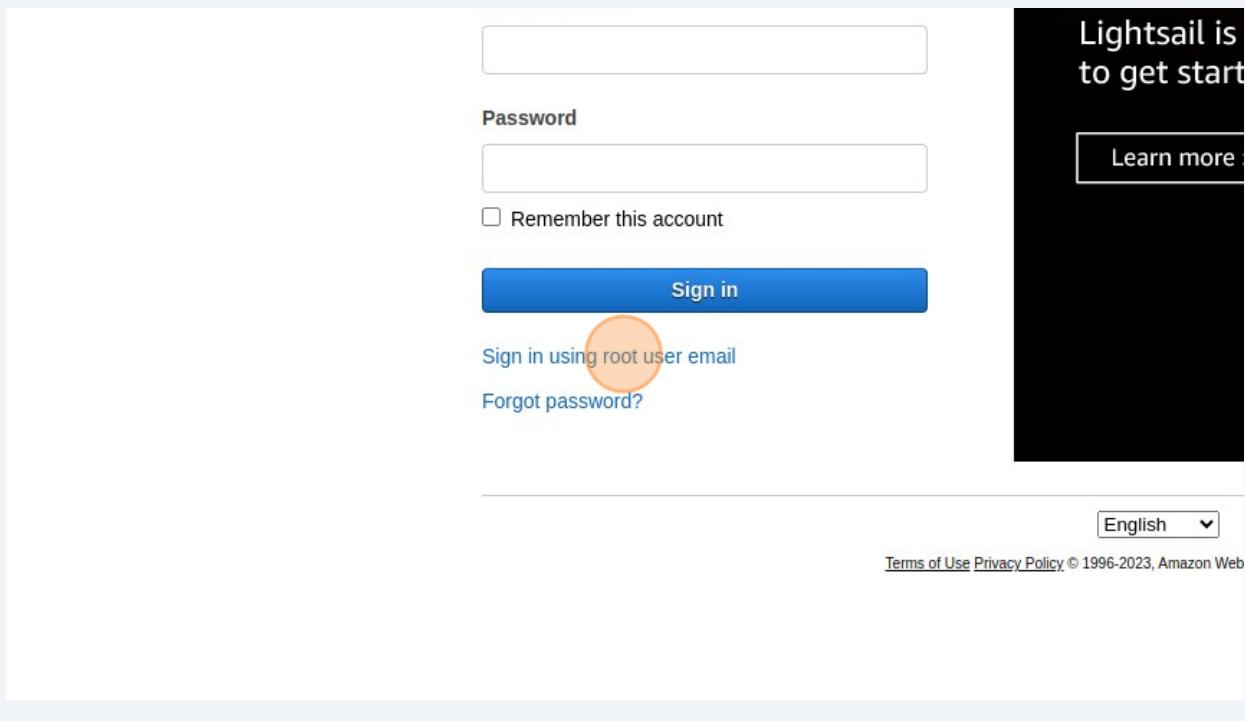


76 Click "Sign In"



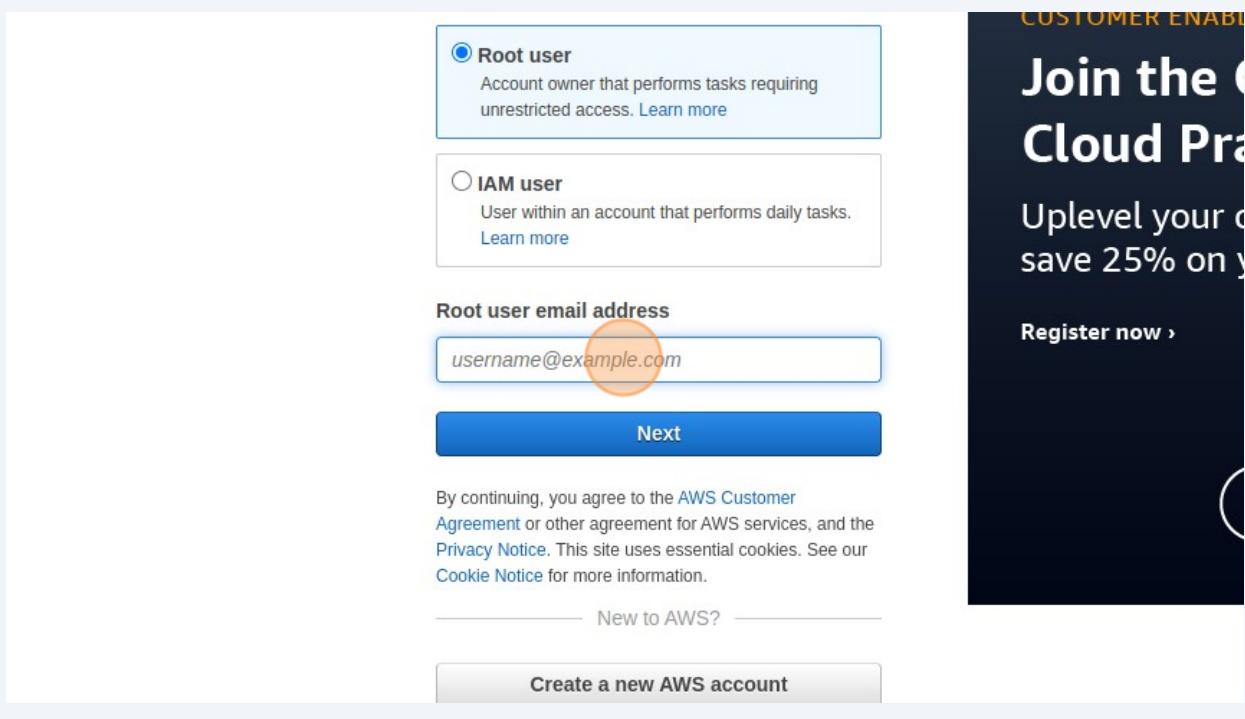
77

Click "Sign in using root user email"

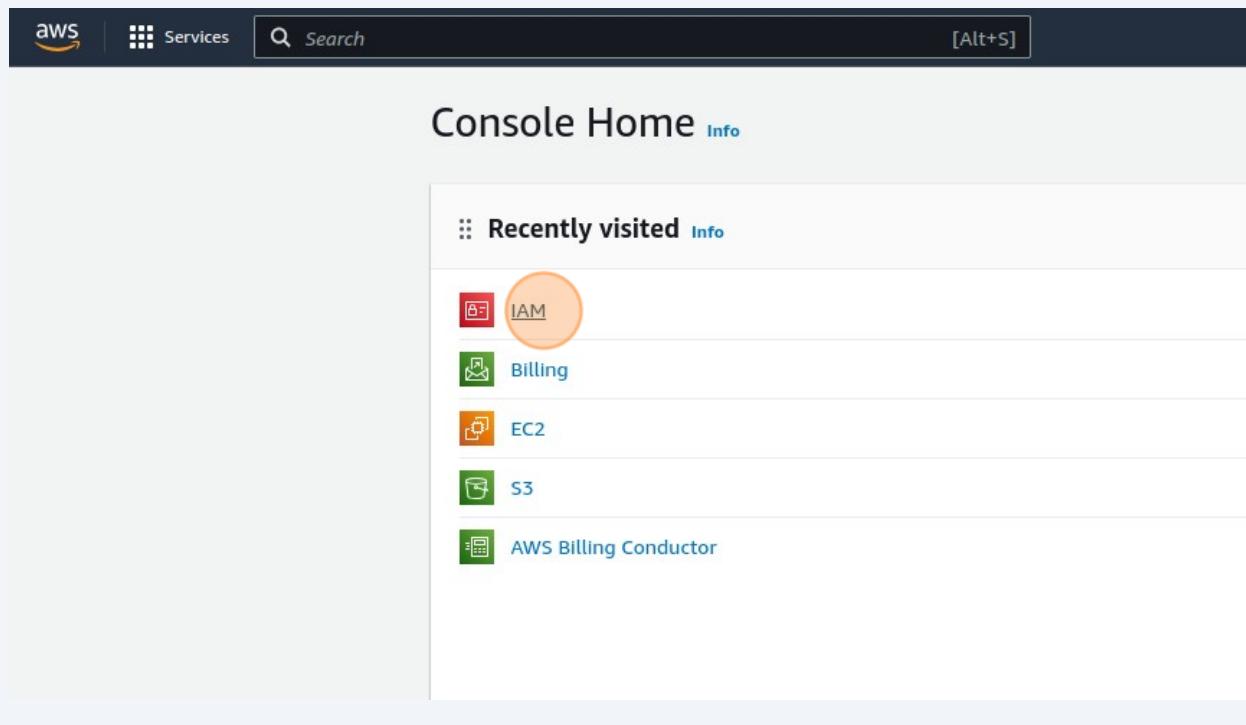


78

Enter into your Root Account, Now we are going to see that how we can create a users group



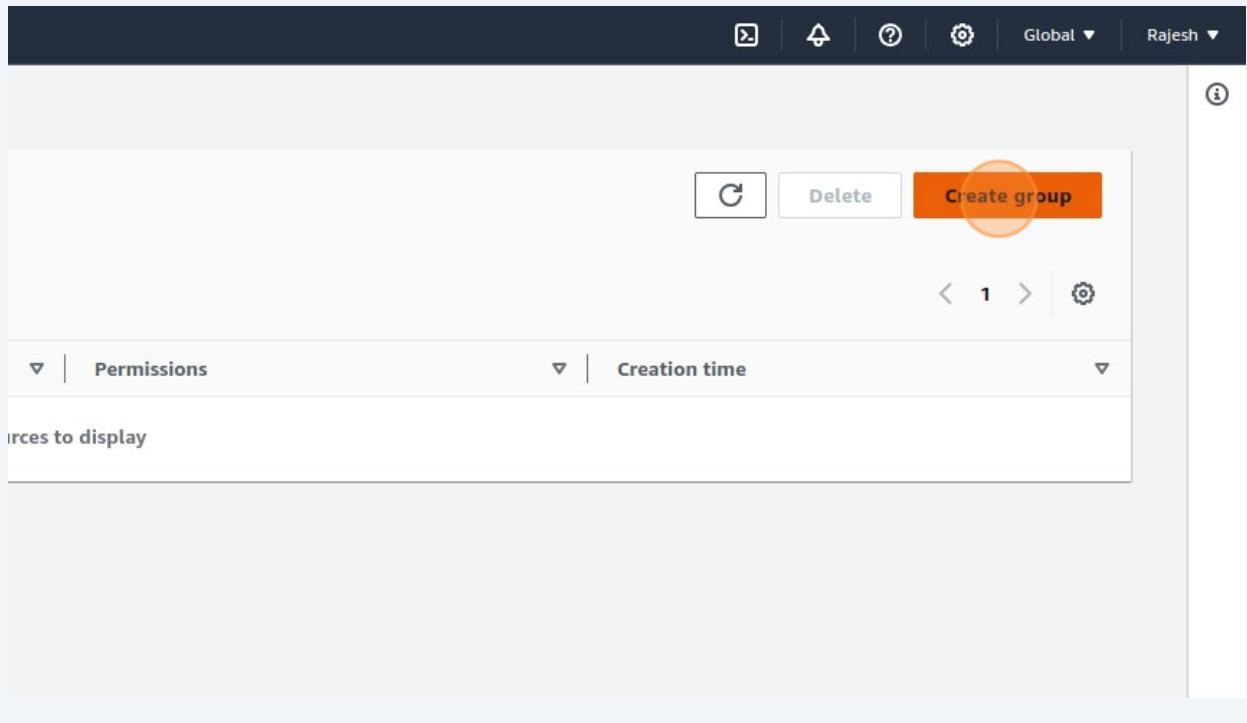
79 Click "IAM"



80 Click "User groups"

The screenshot shows the IAM Dashboard. On the left, a sidebar menu is open under 'Identity and Access Management (IAM)'. The 'Access management' section is expanded, showing 'User groups' (which is highlighted with an orange circle), 'Users', 'Roles', 'Policies', 'Identity providers', and 'Account settings'. Below that, the 'Access reports' section includes 'Access analyzer'. The main content area is titled 'IAM Dashboard' and contains a 'Security recommendations' section with two items: 'Root user has MFA' (green checkmark) and 'Deactivate or delete access keys for root user' (yellow warning icon). It also features an 'IAM resources' section with tabs for 'User groups', 'Users', and 'Roles'.

81 Click "Create group"



82 Click the "User group name" field. Enter your group name and skip adding users to group . we will add users after creating the group.

IAM > [User groups](#) > Create user group

Create user group

Name the group

User group name

Enter a meaningful name to identify this group.

A text input field for entering the user group name. It has a red circle highlighting its right side.

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

Add users to the group - *Optional (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 search bar for finding IAM users.

User name [Edit](#)

- 83** Click the "Search" field. Here you can add permissions policies to our group . It will be applied to all our group users

The screenshot shows the AWS IAM User Groups interface. On the left, there's a sidebar with navigation links: User groups, Users, Roles, Policies, Identity providers, and Account settings. Below that is a section for Access reports with links to Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, and Service control policies (SCPs). The main content area is titled 'Attach permissions policies - Optional (884)'. It includes a search bar with the placeholder 'Search' and a filter button 'Filter by Type' set to 'All types'. A list of policies is displayed with columns for Policy name, Type, and Description. The policies listed are: AdministratorAccess (AWS managed - job function), AdministratorAccess-Amplify (AWS managed), AdministratorAccess-AWSElasticBeanstalk (AWS managed), and AlexaForBusinessDeviceSetup (AWS managed). The 'AdministratorAccess' policy is highlighted with an orange circle.

Policy name	Type
AdministratorAccess	AWS managed - job function
AdministratorAccess-Amplify	AWS managed
AdministratorAccess-AWSElasticBeanstalk	AWS managed
AlexaForBusinessDeviceSetup	AWS managed

- 84** Type "s3". Click this checkbox.

The screenshot shows the AWS IAM User Groups interface. The sidebar and main content area are identical to the previous screenshot, but the search bar now contains the text 's3'. The results list shows several AWS managed policies related to S3, with the 'AmazonS3FullAccess' policy highlighted with an orange circle. This indicates it is the selected policy for attachment.

Policy name	Type
AmazonDMSRedshiftS3Role	AWS managed
AmazonS3FullAccess	AWS managed
AmazonS3ObjectLambdaExecutionRolePo...	AWS managed
AmazonS3OutpostsFullAccess	AWS managed
AmazonS3OutpostsReadOnlyAccess	AWS managed
AmazonS3ReadOnlyAccess	AWS managed
AWSBackupServiceRolePolicyForS3Backup	AWS managed
AWSBackupServiceRolePolicyForS3Restore	AWS managed

85 Type "ec2" Click this checkbox.

The screenshot shows the AWS IAM Policies list. On the left, there's a sidebar with navigation links like Account settings, Access reports, and Related consoles. The main area lists policies with columns for Policy name, Description, and Type. One policy, 'AmazonEC2FullAccess', has its checkbox highlighted with a red circle, indicating it should be selected.

	Policy name	Type
<input type="checkbox"/>	AmazonEC2ContainerRegistryFullAccess	AWS managed
<input type="checkbox"/>	AmazonEC2ContainerRegistryPowerUser	AWS managed
<input type="checkbox"/>	AmazonEC2ContainerRegistryReadOnly	AWS managed
<input type="checkbox"/>	AmazonEC2ContainerServiceAutoscaleRole	AWS managed
<input type="checkbox"/>	AmazonEC2ContainerServiceEventsRole	AWS managed
<input type="checkbox"/>	AmazonEC2ContainerServiceforEC2Role	AWS managed
<input type="checkbox"/>	AmazonEC2ContainerServiceRole	AWS managed
<input checked="" type="checkbox"/>	AmazonEC2FullAccess	AWS managed
<input type="checkbox"/>	AmazonEC2ReadOnlyAccess	AWS managed
<input type="checkbox"/>	AmazonEC2RoleforAWSCodeDeploy	AWS managed
<input type="checkbox"/>	AmazonEC2RoleforAWSCodeDeployLimited	AWS managed

86 Click "Create group"

The screenshot shows the 'Create group' dialog box. It lists several policies under the 'NOTICE' column and their descriptions in the 'PROVIDES EC2 UNLIMITED ACCESS TO S3 BUCK...' column. At the bottom right, there are 'Cancel' and 'Create group' buttons, with the 'Create group' button highlighted with a red circle.

NOTICE	PROVIDES EC2 UNLIMITED ACCESS TO S3 BUCK...
None	Default policy for the Amazon EC2 Rol...
None	This policy will soon be deprecated. Pl...
None	Managed policy for the Amazon Launc...
None	Policy to enable Autoscaling for Amaz...
None	Allows EC2 Spot Fleet to request, term...
None	Default policy for the Amazon Elastic ...
None	This policy enables AWS Systems Man...
None	This policy provides Amazon EC2 oper...
None	This policy allows installing and using ...

Create group

87 A new user group is created .Click "database-group"

The screenshot shows the AWS IAM User Groups page. On the left, there's a sidebar with a search bar and links for Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), and Access reports (Access analyzer, Archive rules). The main area shows a table titled "User groups (1) Info". The table has one row with a checkbox, the header "Group name", and the value "database-group". An orange circle highlights the "database-group" text. The table also includes a "Users" column with a triangle icon.

88 Click "Add users"

The screenshot shows the same AWS IAM User Groups page as above, but with a different view. It shows a table with one row: "arn:aws:iam::127422185444:group/database-group". Below the table is a control panel with a "C" icon, a "Remove" button, and an "Add users" button, which is highlighted with an orange circle. There are also navigation arrows and a refresh icon. At the bottom, there are sorting options for "Groups", "Last activity", and "Creation time".

89 we will select our test-user-1

Add users to database-group Info

Other users in this account (1)

Search

User name Filter

[test-user-1](#)

90 Click "Add users"

Groups	Last activity	Creation time
0	5 minutes ago	19 minutes ago

91 Click "User groups"

The screenshot shows the AWS Identity and Access Management (IAM) console. The left sidebar is titled 'Identity and Access Management (IAM)' and includes a search bar. Under 'Access management', the 'User groups' option is selected and highlighted in blue. The main content area shows a green banner at the top stating '1 user added to this group.' Below it, the breadcrumb navigation shows 'IAM > User groups > database-group'. The 'database-group' name is displayed in large bold letters. A 'Summary' section shows the 'User group name' as 'database-group'. At the bottom, there are tabs for 'Users (1)', 'Permissions', and 'Access Advisor', with 'Users (1)' being the active tab.

92 Click "database-group"

The screenshot shows the 'User groups' list page in the AWS IAM console. The left sidebar includes a search bar and a list of navigation items under 'Access management': 'User groups' (selected), 'Users', 'Roles', 'Policies', 'Identity providers', and 'Account settings'. The main content area shows the breadcrumb navigation 'IAM > User groups' and the title 'User groups (1) [Info](#)'. A descriptive text states 'A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.' Below this is a table with one row, showing a checkbox, the 'Group name' 'database-group', and a 'Users' link. The 'database-group' name is highlighted with an orange circle.

93 Click "Permissions"

The screenshot shows the AWS IAM User Groups interface. On the left, there's a sidebar with various navigation options like Dashboard, Access management, User groups, Users, Roles, Policies, Entity providers, Account settings, Access reports, Access analyzer, Archive rules, and Analyzers. The 'User groups' option is highlighted. The main area has a 'Summary' section with details: User group name is 'database-group', Creation date is 'November 1, 2023'. Below this, there are three tabs: 'Users (1)', 'Permissions' (which is highlighted with an orange circle), and 'Access Advisor'. Under the 'Users' tab, it says 'Users in this group (1)'. A search bar is present, followed by a table with one row: 'User name' is 'test-user-1'. The entire screenshot is enclosed in a light gray rounded rectangle.

94 here you can find out what permissions ,we have provided to our users in the group

The screenshot shows the 'Permissions' tab of the AWS IAM User Groups interface. At the top, there are tabs for 'Users (1)', 'Permissions' (highlighted with an orange circle), and 'Access Advisor'. Below this, it says 'Permissions policies (2) Info'. It states that you can attach up to 10 managed policies. A search bar and a 'Filter by Type' dropdown set to 'All types' are shown. A table lists two policies: 'AmazonEC2FullAccess' and 'AmazonS3FullAccess', both categorized as 'AWS managed'. The entire screenshot is enclosed in a light gray rounded rectangle.

95

If you want to add a new permission. Instead of going to every user and providing permission you can provide the permission easily in this group. Click "Add permissions"

This screenshot shows the 'Permissions' tab of the AWS IAM Groups page. At the top, there are buttons for 'ARN' and a copy icon. Below these are buttons for 'C' (Create), 'Simulate', 'Remove', and 'Add permissions' (which is highlighted with a red circle). A dropdown menu labeled 'Copy Type' is open, showing 'Attached policies'. The main area displays a table titled 'Attached entities' with two entries: '1' and '2'. Navigation arrows and a refresh icon are at the bottom right.

96

Click "Attach policies"

This screenshot shows the 'Permissions' tab of the AWS IAM Groups page. The interface is identical to the previous screenshot, but the 'Attach policies' button in the dropdown menu is highlighted with a red circle. The rest of the page, including the table of attached entities, remains the same.

97

Click the "Search" field. Type "rds" .Now we are going to provide RDS service access to the users

▶ Current permissions policies (2)

Other permission policies (882)

You can attach up to 10 managed policies to this user group. All of the users in this group inherit the attached permissions.

Filter by Type

All types

<input type="checkbox"/>	Policy name	Type
<input type="checkbox"/>	AdministratorAccess	AWS managed - job function
<input type="checkbox"/>	AdministratorAccess-Amplify	AWS managed
<input type="checkbox"/>	AdministratorAccess-AWSElasticBeanstalk	AWS managed
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	AWS managed
<input type="checkbox"/>	AmazonDynamoDBFullAccess	AWS managed
<input type="checkbox"/>	AmazonKinesisFullAccess	AWS managed
<input type="checkbox"/>	AmazonS3FullAccess	AWS managed
<input type="checkbox"/>	AmazonSQSFullAccess	AWS managed
<input type="checkbox"/>	AmazonSNSFullAccess	AWS managed
<input type="checkbox"/>	AmazonSSRFullAccess	AWS managed
<input type="checkbox"/>	AmazonVPCFullAccess	AWS managed

98

Click "Select data for AmazonRDSDDataFullAccess"

Other permission policies (882)

You can attach up to 10 managed policies to this user group. All of the users in this group inherit the attached permissions.

rds

<input type="checkbox"/>	Policy name	Type
<input type="checkbox"/>	AmazonRDSDDataFullAccess	AWS managed
<input type="checkbox"/>	AmazonRDSDirectoryServiceAccess	AWS managed
<input type="checkbox"/>	AmazonRDSEnhancedMonitoringRole	AWS managed
<input type="checkbox"/>	AmazonRDSFullAccess	AWS managed
<input type="checkbox"/>	AmazonRDSPerformanceInsightsFullAccess	AWS managed
<input type="checkbox"/>	AmazonRDSPerformanceInsightsReadOnly	AWS managed
<input type="checkbox"/>	AmazonRDSReadOnlyAccess	AWS managed

99 Click "Attach policies"

The screenshot shows a list of AWS IAM policies on the left and their descriptions on the right. At the bottom right are 'Cancel' and 'Attach policies' buttons, with 'Attach policies' highlighted by a yellow circle.

Name	Description
None	Provides full access to Amazon RDS via...
None	Provides full access to RDS Performan...
None	Read-Only policy for RDS Performance...
None	Provides read only access to Amazon R...
None	(Elastic Beanstalk operations role) Allo...
None	This policy grants the Fault Injection Si...
None	Allow QuickSight to describe the RDS r...
None	Provides access to the non-CloudWatc...
None	Default policy for the Amazon RDS ser...

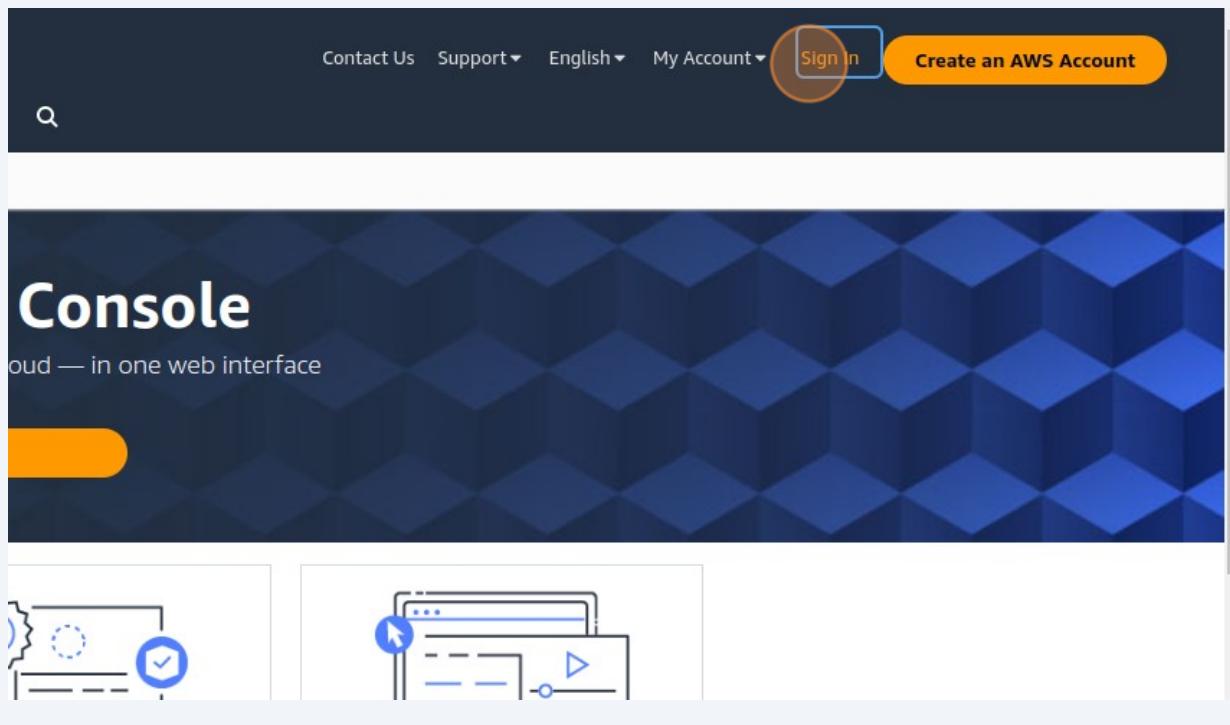
Cancel **Attach policies**

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

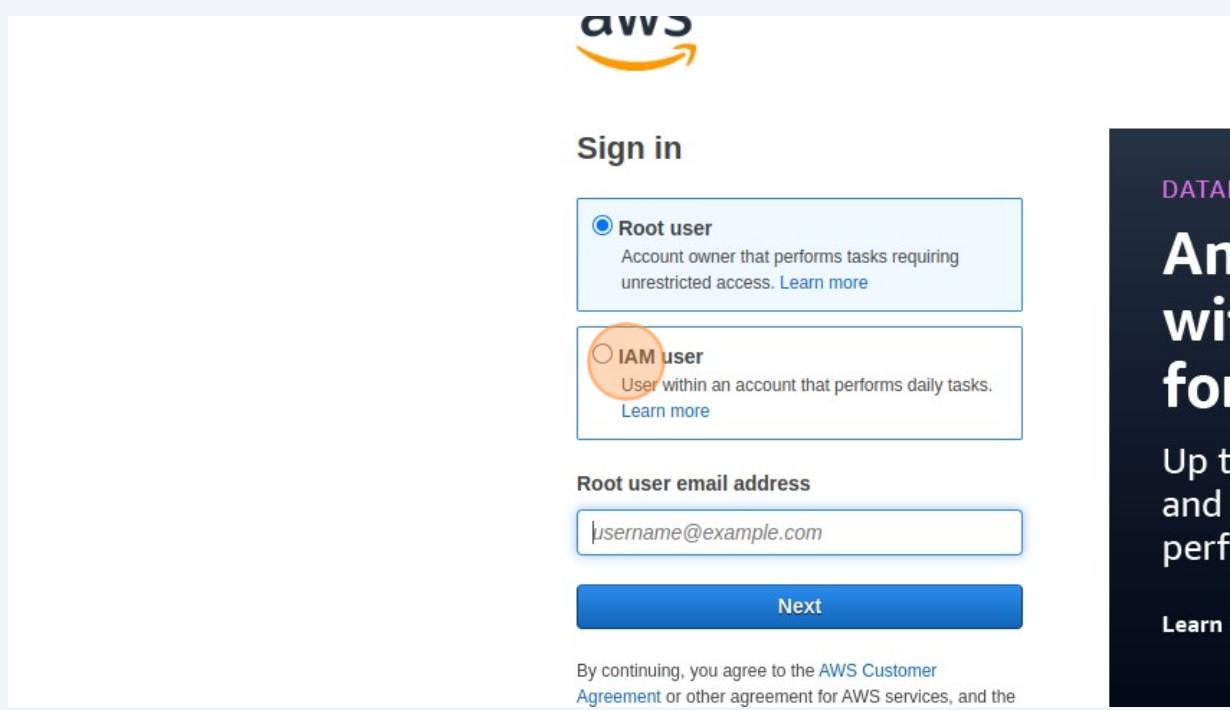
100 Good you have successfully updated the users group permissions.Click "Sign out"

The screenshot shows the AWS IAM Groups page. On the right, a navigation menu is open, showing 'Account', 'Organization', 'Service Quotas', 'Billing Dashboard', and 'Security credentials'. At the bottom right of the menu is a 'Sign out' button, which is highlighted by a yellow circle. Below the menu, there are buttons for 'C' (Copy), 'Simulate', 'Remove', and 'Add permissions'. A search bar at the bottom left contains the placeholder 'Type'.

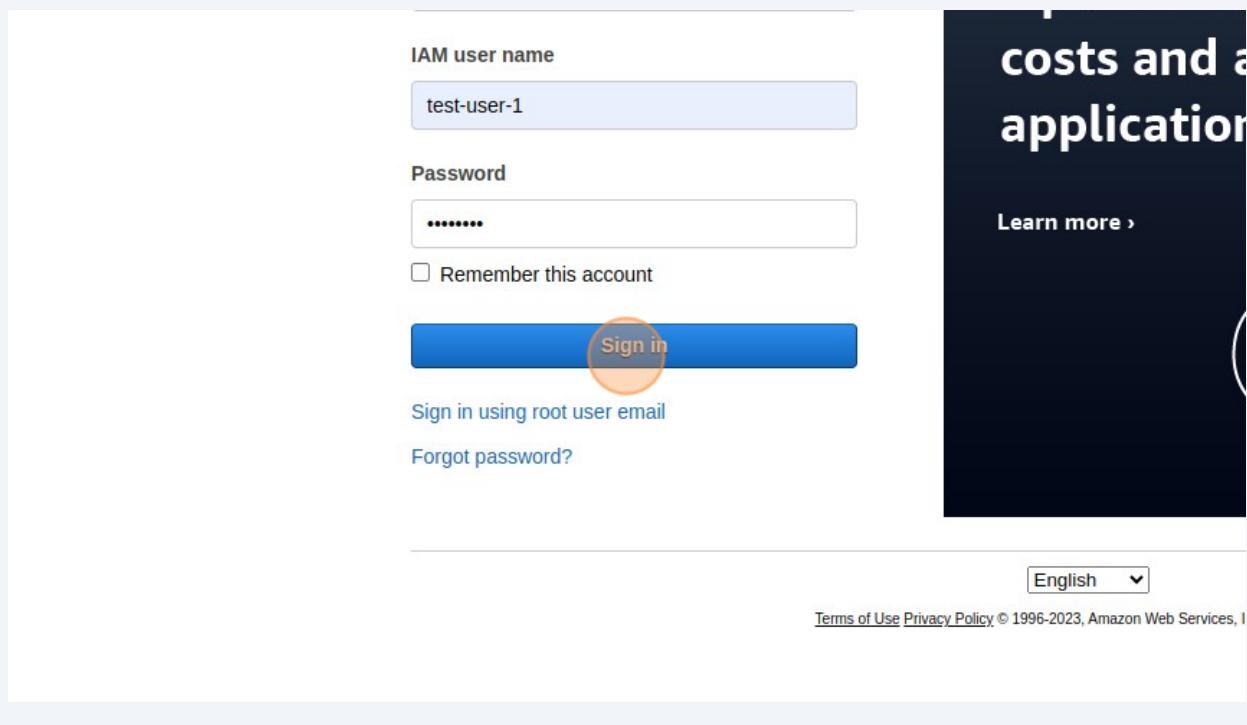
101 Click "Sign In" and enter into your test-user account



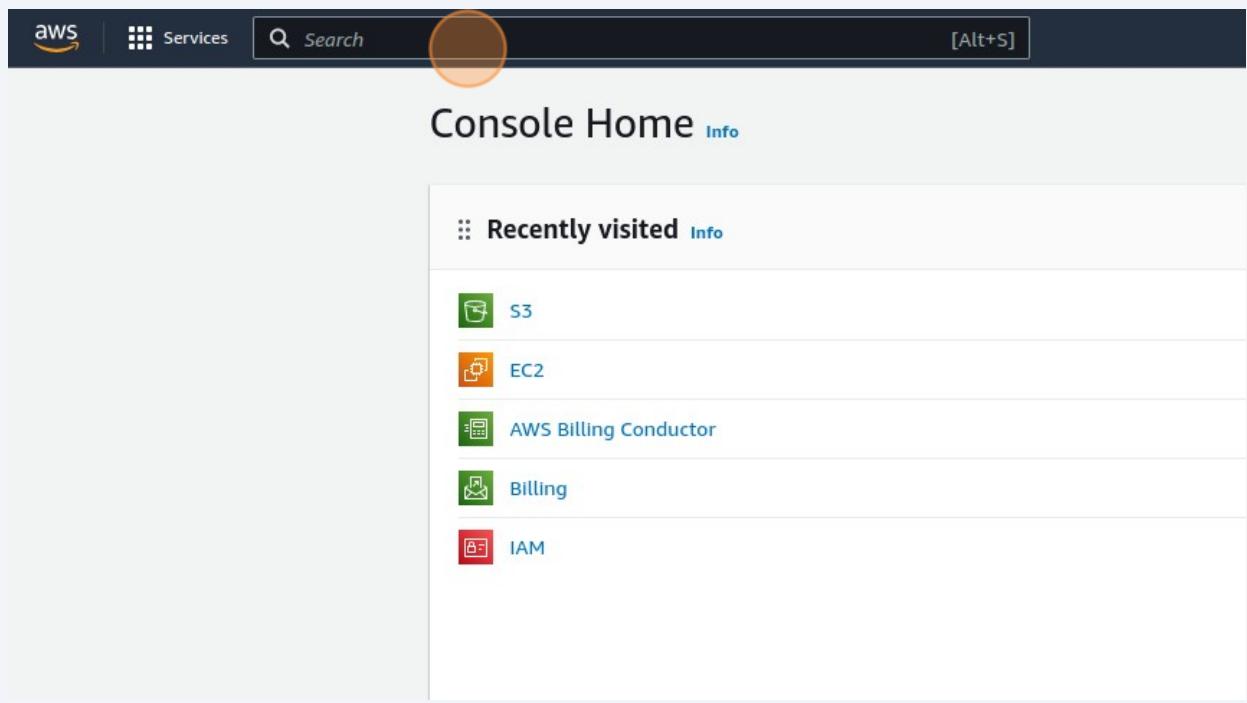
102 Click "IAM user"



103 Click "Sign in"



104 Click the "Search" field.



105 Type "ec2".Click "EC2"

The screenshot shows the AWS search interface with the query 'ec2' entered in the search bar. The search results page displays various services and features related to 'ec2'. On the left, there's a sidebar with links like 'Services (13)', 'Features (54)', 'Resources New', 'Documentation (33,750)', 'Knowledge Articles (20)', 'Marketplace (3,179)', 'Blogs (2,066)', 'Events (30)', and 'Tutorials (21)'. The main area is titled 'Services' and features a prominent card for 'EC2' with the subtext 'Virtual Servers in the Cloud'. Below this, there are sections for 'Top features' (Dashboard, Launch templates, Instances, Spot Instance requests, Savings plans) and other cards for 'EC2 Image Builder' and 'Recycle Bin'.

106 now you can see that our new user had gotten ec2 access ,we gave it our group and group users will automatically get the permissions.

The screenshot shows the AWS EC2 Service Health dashboard. It includes a summary table with counts for Auto Scaling Groups (0), Instances (0), Placement groups (0), Volumes (0), Dedicated Hosts (0), Key pairs (1), and Security groups (2). A large orange circle highlights the 'Security groups' row. To the right, there's a sidebar with 'Default VF' (vpc-0045de), 'Settings' (Data protection, Zones, EC2 Serial C, Default cred, Console exp), and 'Explore A' (Amazon GuardDuty, EC2 container). At the bottom, there's a section for '10 Things You'.