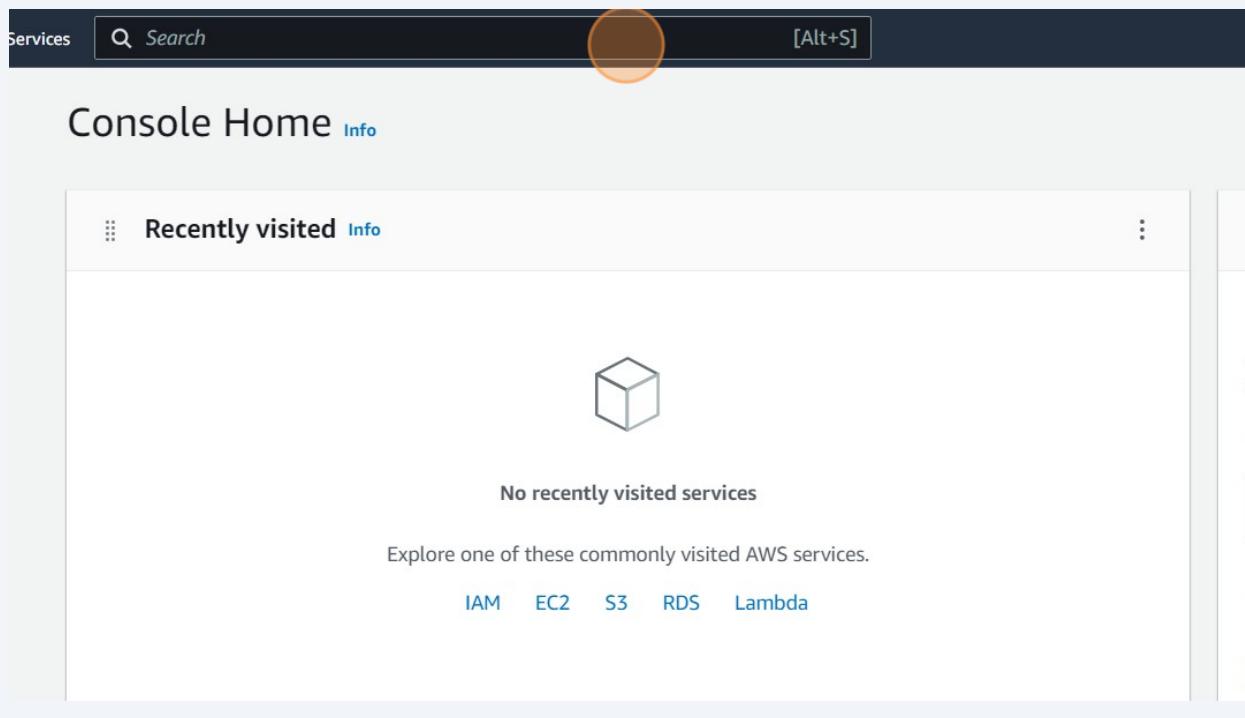


# How to Add Permissions to an IAM User in AWS

Scribe

- 1 Click the "Search" field.



- 2 Type "iam"

### 3 Click "IAM"

The screenshot shows the AWS search interface with the query 'iam' entered in the search bar. The results page has a sidebar on the left with categories like Services (10), Features (20), Resources (New), Documentation (48,333), Knowledge Articles (20), Marketplace (598), Blogs (1,623), Events (12), and Tutorials (2). The main content area displays the 'Services' section, which includes a card for 'IAM' (Manage access to AWS resources) and another for 'IAM Identity Center (successor to AWS Single Sign-On)' (Manage workforce user access to multiple AWS accounts and cloud app). Below these are cards for 'Resource Access Manager' (Share AWS resources with other accounts or AWS Organizations).

### 4 Click "Users"

The screenshot shows the IAM Dashboard. On the left, there's a sidebar with 'Dashboard', 'Access management' (User groups, **Users**, Roles), 'Policies', 'Identity providers', and 'Account settings'. Under 'Access reports', there are 'Access analyzer' and 'Archive rules'. The main content area is titled 'IAM Dashboard' and features a 'Security recommendations' section with three items: 'Add MFA for root user' (warning icon), 'Add MFA for yourself' (warning icon), and 'Your user, vipuldemoadmin, does not have any active access keys that have been used in the last year.' (checkmark icon). At the bottom, there's a 'IAM resources' section with the subtext 'Resources in this AWS Account'.

## 5 Select user you want to "give access" or "attach policy"

The screenshot shows the AWS Identity and Access Management (IAM) console. On the left, there's a sidebar with options like Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), and Access reports. The main area is titled 'Users (2) Info' and shows two IAM users: 'vipuladmin01' and 'vipuldemoadmin'. The user 'vipuladmin01' is circled in orange.

## 6 On "Permissions policies" Section

The screenshot shows the detailed view for the user 'vipuladmin01'. It includes information like ARN (arn:aws:iam::927599844895:user/vipuladmin01), Creation date (September 04, 2023, 01:00 (UTC+05:30)), and Console access status (Enabled without MFA). The 'Permissions' tab is selected, showing 'Permissions policies (0)' and a note that permissions are defined by policies attached directly or through groups. There's also a search bar and a 'Filter by Type' dropdown set to 'All types'.

- 7 Click "Add permissions" to dropdown

The screenshot shows the AWS IAM 'Access Advisor' section. At the top, there are two sections: 'Console access' (Enabled without MFA) and 'Access key 1' (Create access key). Below these are sections for 'Last console sign-in' (Today) and 'credentials' (Access Advisor). A dropdown menu is open at the top right, with the 'Add permissions' option highlighted by a red circle. The menu also includes 'Remove' and a 'C' icon. Below the dropdown, there's a 'Filter by Type' dropdown set to 'All types', and a table header with columns for 'Type' and 'Attached via'. The message 'No resources to display' is shown below the table.

- 8 Click "Add permissions" to attach policy. If you want to make/ customize your own policy then choose another option.

This screenshot is similar to the previous one, showing the 'Access Advisor' section. The 'Add permissions' dropdown is now fully expanded, showing three options: 'Add permissions ▲', 'Add permissions', and 'Create inline policy'. The 'Add permissions ▲' option is highlighted by a red circle. The rest of the interface is identical to the previous screenshot, including the 'Last console sign-in' section, the 'credentials' tab, the 'Filter by Type' dropdown, and the 'No resources to display' message.

## 9 Click "Attach policies directly"

Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Copy permissions  
Copy all group memberships, attached managed policies, inline policies, and any existing permissions boundaries 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.

[Create group](#)

Each to the group. We recommend using groups to manage user permissions by job function, ns.[Learn more](#)

## 10 Search which permission you want to give to your user

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, inline policies, and any existing permissions boundaries from an existing user.

### Permissions policies (1125)

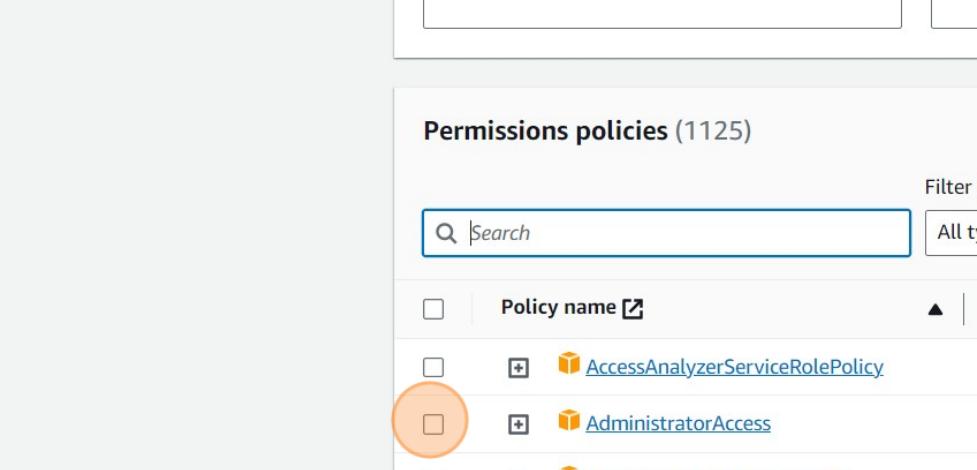
Filter by Type

Search

Policy name	Type
<a href="#">AccessAnalyzerServiceRolePolicy</a>	AWS managed
<a href="#">AdministratorAccess</a>	AWS managed - job function
<a href="#">AdministratorAccess-Amplify</a>	AWS managed
<a href="#">AdministratorAccess-AWSElasticBea...</a>	AWS managed

11

Select the permission you want to give to your user. give permission wisely .



The screenshot shows the AWS IAM console with the 'Permissions policies' page. At the top, there is a note about adding users to existing groups or creating new ones. Below the note, the title 'Permissions policies (1125)' is displayed, followed by a search bar and a 'Filter by Type' dropdown set to 'All types'. The main table lists 1125 policies, with columns for a checkbox, policy name, type, and ARN. One specific policy, 'AdministratorAccess', is highlighted with an orange circle around its checkbox and row.

	Policy name	Type
<input type="checkbox"/>	<a href="#">AccessAnalyzerServiceRolePolicy</a>	AWS managed
<input checked="" type="checkbox"/>	<a href="#">AdministratorAccess</a>	AWS managed
<input type="checkbox"/>	<a href="#">AdministratorAccess-Amplify</a>	AWS managed
<input type="checkbox"/>	<a href="#">AdministratorAccess-AWSElasticBea...</a>	AWS managed

12

Click "Next"

<u>cess</u>	AWS managed	0
<u>rator</u>	AWS managed	0
<u>llAccess</u>	AWS managed	0
<u>loudW...</u>	AWS managed	0
	AWS managed	0
<u>cess</u>	AWS managed	0
<u>s</u>	AWS managed	0
<u>s</u>	AWS managed	0
<u>Access</u>	AWS managed	0
<u>cess</u>	AWS managed	0

[Cancel](#) [Next](#)

**13** You can cross check here then Click "Add permissions"

The screenshot shows the 'Review' step of adding permissions for a user named 'vipuladmin01'. It displays the 'User details' section with the user name 'vipuladmin01'. Below it is the 'Permissions summary (1)' table:

Name	Type	Used as
<a href="#">AdministratorAccess</a>	AWS managed - job function	Permissions policy

At the bottom right of the table, there are buttons for 'Cancel', 'Previous', and 'Add permissions'. The 'Add permissions' button is highlighted with an orange circle.

**14** then "Sign In to the Console" with the user you given permission to it

The screenshot shows the AWS Management Console sign-in page. At the top, there is a dark header bar with links for 'Contact Us', 'Support', 'English', 'My Account', and a prominent orange 'Sign In to the Console' button. Below the header, there is a message about Maui wildfires. The main area features the 'Management Console' logo and the text 'and manage the AWS Cloud — in one web interface'. A large orange 'Log back in' button is visible. At the bottom, there are three small decorative icons.

**15** Enter your credential

The screenshot shows the AWS sign-in interface. At the top, it says "IAM user name" followed by a text input field containing "vipuladmin01". Below that is a "Password" field with a placeholder "Password" and a red circle highlighting the password character input area. Underneath the password field is a checkbox labeled "Remember this account". A large blue "Sign in" button is centered below the password field. At the bottom left, there is a link "Sign in using root user email".

**16** Click the "Search" field.

The screenshot shows the AWS Console Home page. At the top, there is a navigation bar with the AWS logo, "Services" (with a grid icon), a search bar containing "Search" with a red circle highlighting the search input area, and a keyboard shortcut "[Alt+S]". Below the navigation bar is the "Console Home" header with an "Info" link. A "Recently visited" section follows, featuring a thumbnail for "EC2" with a red circle highlighting the thumbnail area.

17 Type "s3"

18 Click "S3"

The screenshot shows the AWS search interface. In the top navigation bar, there is a 'Services' icon and a search bar containing the text 's3'. Below the search bar, a message says 'Search results for 's3'' and 'Try searching with longer queries for more relevant results'. On the left, a sidebar lists various categories: Services (7), Features (22), Resources (New), Documentation (23,172), Knowledge Articles (20), Marketplace (1,287), Blogs (1,282), Events (25), and Tutorials (13). The main content area is titled 'Services' and contains three cards. The first card, 'S3', is highlighted with a red circle and has a sub-section titled 'Top features' with links to Buckets, Access points, Storage Lens dashboards, and Batch Operations. The second card is 'S3 Glacier' and the third is 'AWS Snow Family'.

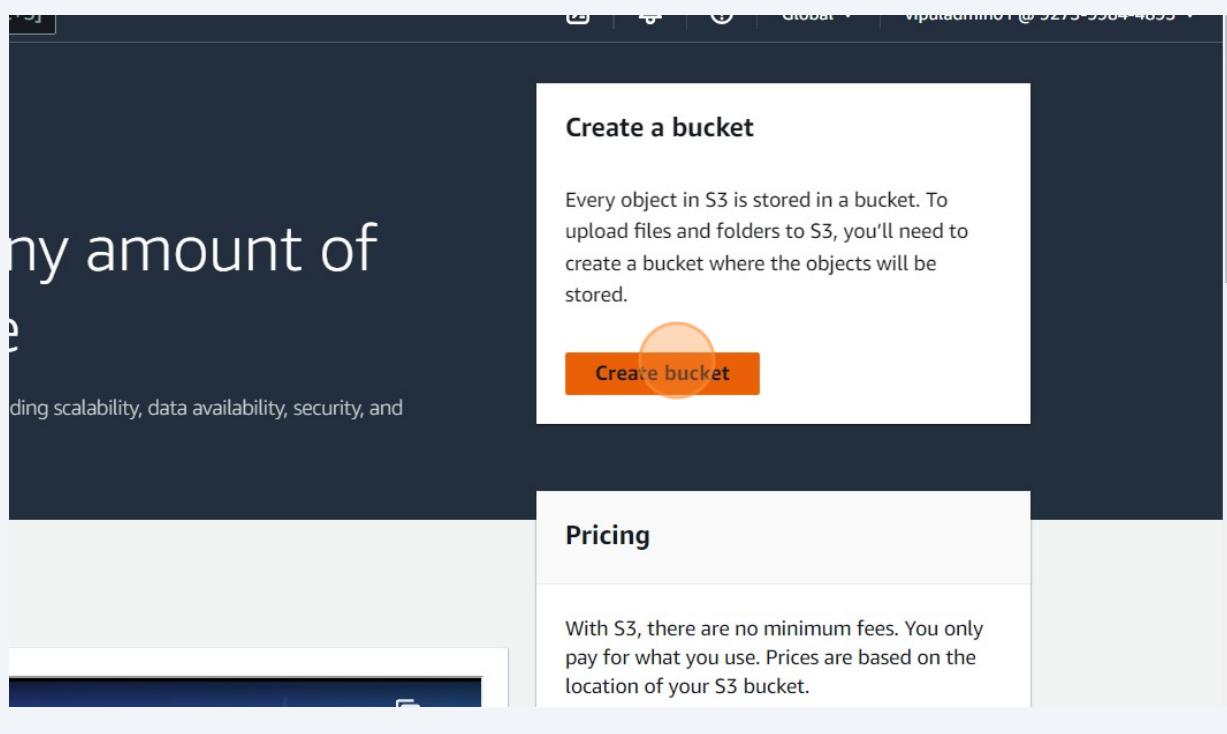
Category	Count
Services	7
Features	22
Resources	New
Documentation	23,172
Knowledge Articles	20
Marketplace	1,287
Blogs	1,282
Events	25
Tutorials	13

**S3**  
Scalable Storage in the Cloud  
Buckets Access points Storage Lens dashboards Batch Operations

**S3 Glacier**  
Archive Storage in the Cloud

**AWS Snow Family**  
Large Scale Data Transport

**19** Click "Create bucket"



**20** Click the "Bucket name" field.

The screenshot shows the 'General configuration' step of the 'Create bucket' wizard. It includes fields for 'Bucket name' (containing 'myawsbucket'), 'AWS Region' (set to 'Europe (Stockholm) eu-north-1'), and an optional 'Copy settings from existing bucket' section with a 'Choose bucket' button. A yellow circle highlights the 'Bucket name' input field.

**21** Type "demobuck01"

**22** Click "Create bucket"

Management Service keys (SSE-KMS)

or AWS Key Management Service keys (DSSE-KMS)

of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the [Storage](#) tab of the

Encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-

Cancel

Create bucket

© 2023, Amazon Web Services India Private Limited or its affil

**23** You can see here bucket is created

The screenshot shows the AWS S3 Buckets page. At the top, there are three status indicators labeled "Pending". Below them, the heading "Buckets (1) [Info](#)" is displayed. A sub-instruction "Buckets are containers for data stored in S3. [Learn more](#)" follows. A search bar with the placeholder "Find buckets by name" is present. The main table has columns for "Name", "AWS Region", and "Actions". One row is shown, representing a bucket named "demobuck01" located in "Europe (Stockholm) eu-north-1". The "Name" column contains a link "demobuck01" which is highlighted with an orange circle. The bottom navigation bar includes links for "CloudShell", "Feedback", and "Language".

Name	AWS Region	Actions
<a href="#">demobuck01</a>	Europe (Stockholm) eu-north-1	<a href="#">... Bucket</a>