

# How to Grant Permissions in AWS IAM

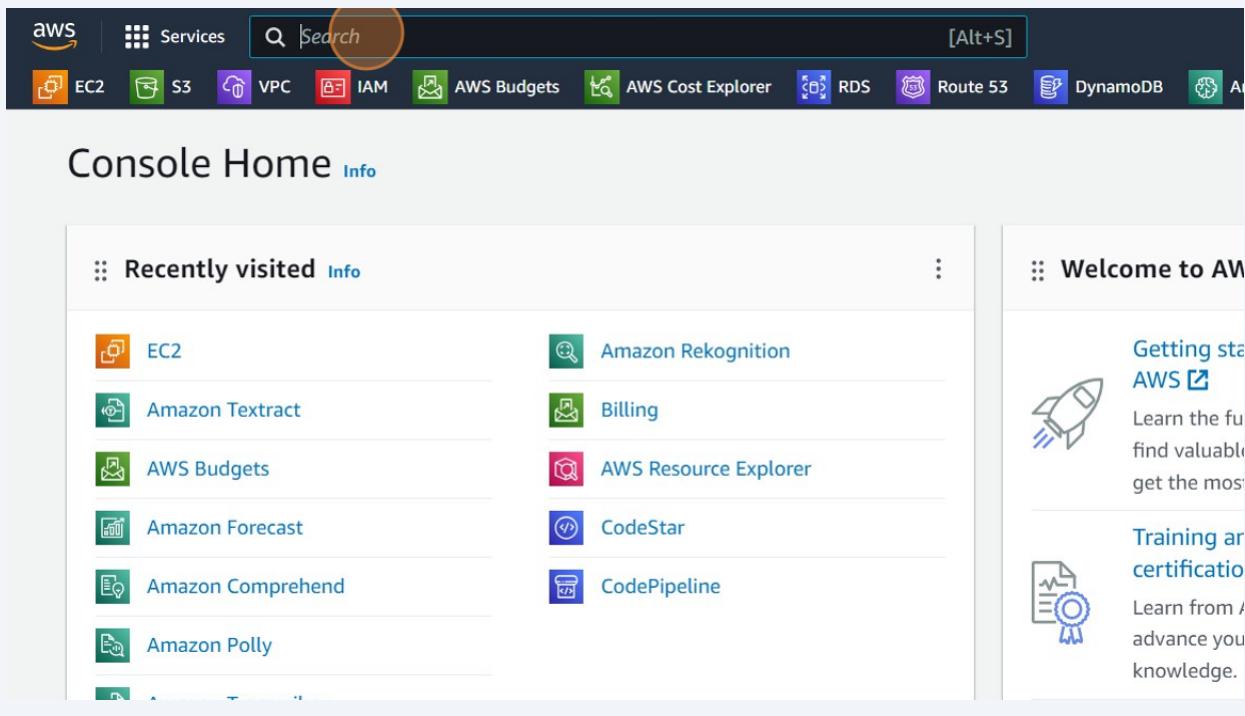
This guide provides step-by-step instructions on how to grant group administrator permissions in AWS IAM. It covers checking user permissions, attaching policies directly to users, adding permissions to groups, and creating custom policies using both visual and JSON formats. Viewing this guide will help someone understand and navigate the process of granting group administrator permissions in AWS IAM.

This guide was created by Nijat Hajiyev

## Check User permissions

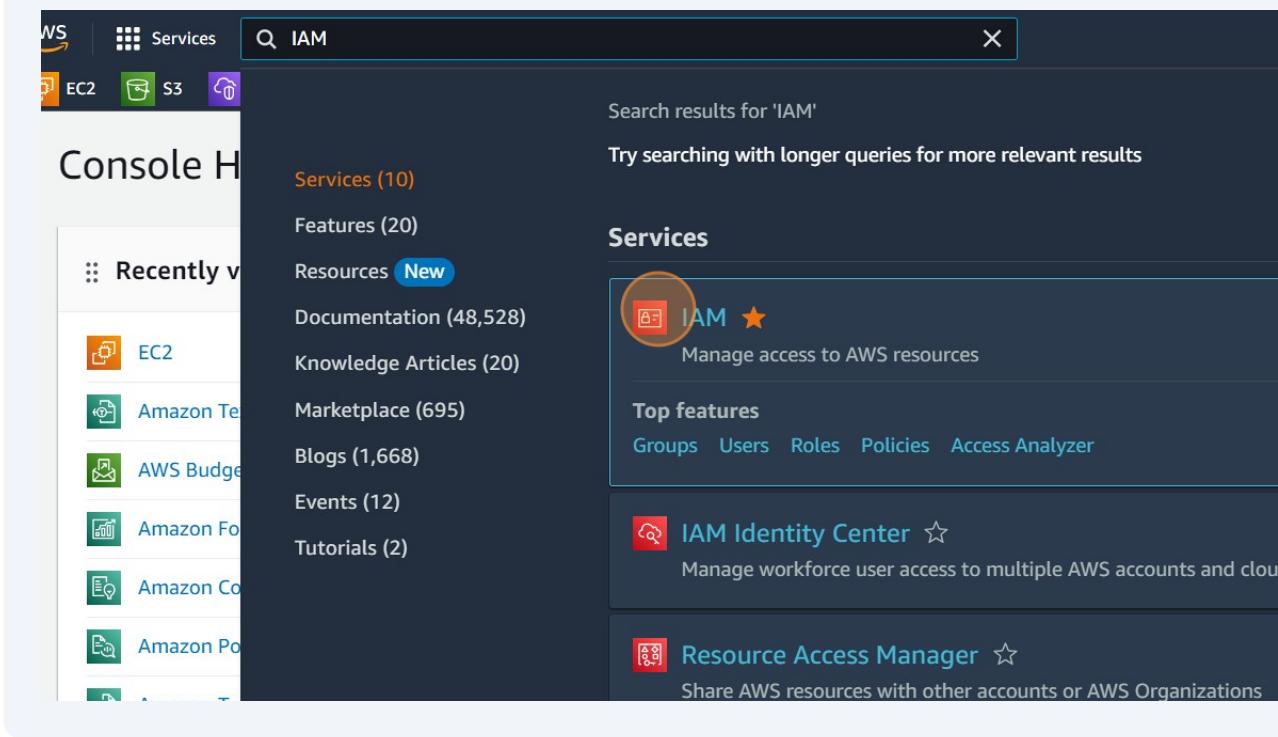
- 1 Navigate to [aws.amazon.com](https://aws.amazon.com)

- 2 Click the "Search" field.

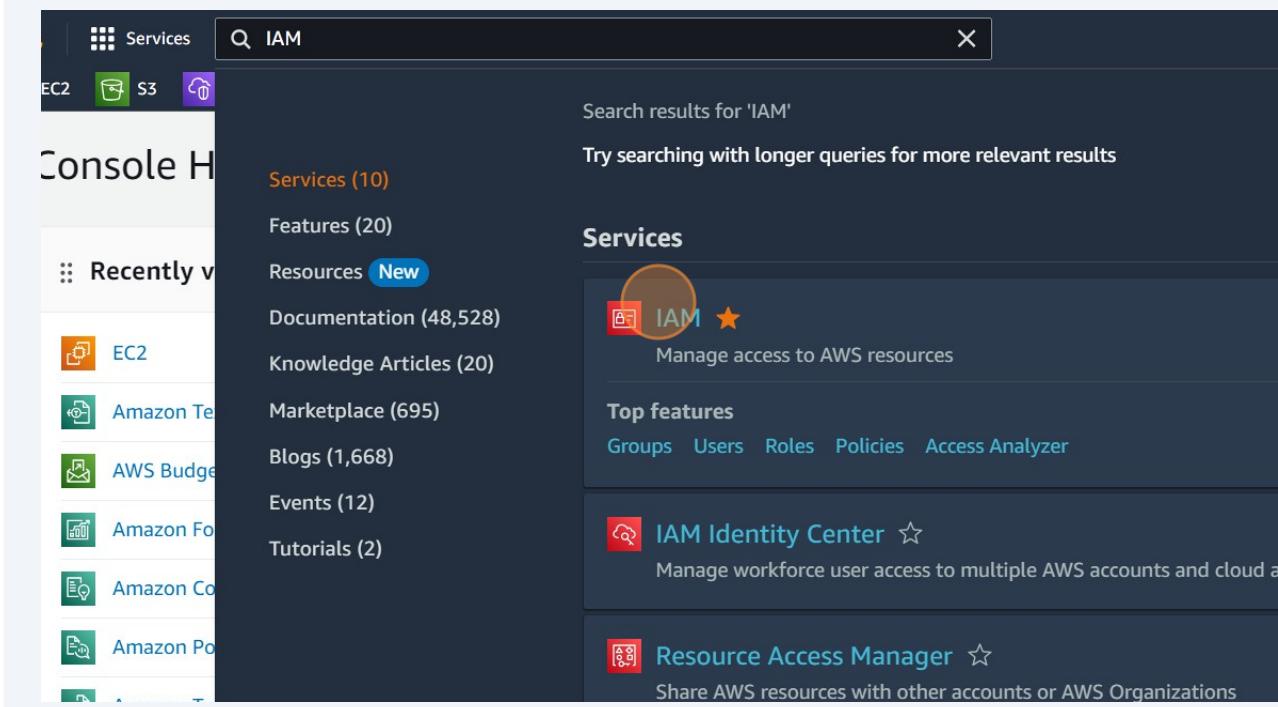


- 3 Type "IAM"

4 Click this image.



5 Click "IAM"



**6** 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: 'Add MFA for root user' (warning icon) and 'Root user has no active access keys' (checkmark icon). Below this is an 'IAM resources' section with tabs for User groups, Users, Roles, and Policies.

**7** Click "DemoUser"

The screenshot shows the 'Identity and Access Management (IAM)' service page. The 'Users' link in the sidebar is highlighted with an orange circle. The main content area is titled 'Users (1) Info' and shows a single user entry: 'DemoUser'. This entry is also highlighted with an orange circle. The table columns are 'User name', 'Path', and 'Groups'.

8 Click "Permissions". Here you can find User permissions

The screenshot shows the AWS Identity and Access Management (IAM) console. The left sidebar has a tree view with 'Access management' expanded, showing 'User groups', 'Users' (which is selected), 'Roles', 'Policies', and 'Identity providers'. The main area is titled 'Permissions' and displays 'Permissions policies (2)'. It lists two policies: 'AdministratorAccess' (AWS managed - job function) and 'IAMUserChangePassword' (AWS managed). Both policies have checkboxes next to them and small orange plus icons.

Policy name	Type
<a href="#">AdministratorAccess</a>	AWS managed - job function
<a href="#">IAMUserChangePassword</a>	AWS managed

## Attach policy directly

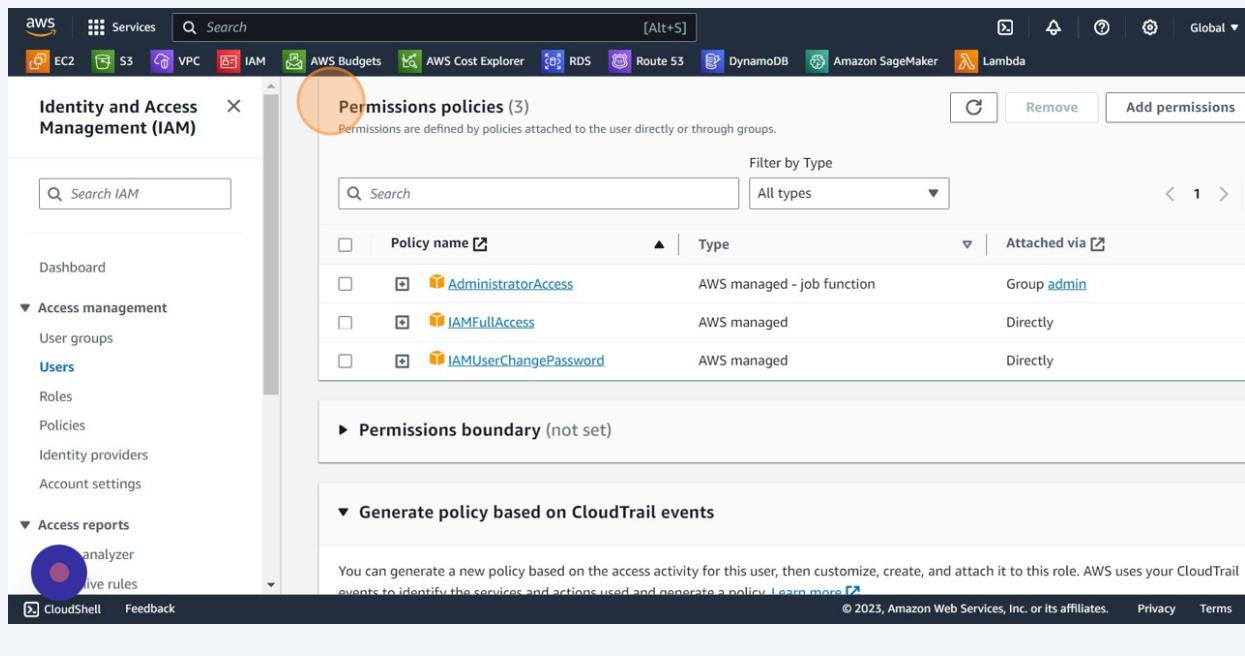
## 9 Click "Users"

The screenshot shows the AWS Identity and Access Management (IAM) dashboard. On the left, there's a sidebar with options like User groups, Users (which is selected and highlighted with an orange circle), Roles, Policies, Identity providers, and Account settings. The main area has a green banner at the top stating "1 policy added" and "Root user has no active access keys". Below this is a section titled "IAM resources" with counts: 1 User group, 1 User, 34 Roles, 10 Policies, and 0 Identity providers. There's also a "What's new" section with two items: "IAM Roles Anywhere is now available in the AWS GovCloud (US) Regions." and "AWS Identity and Access Management provides action last accessed information for more than 140 services." At the bottom right, it says "© 2023, Amazon Web Services".

## 10 Click "DemoUser"

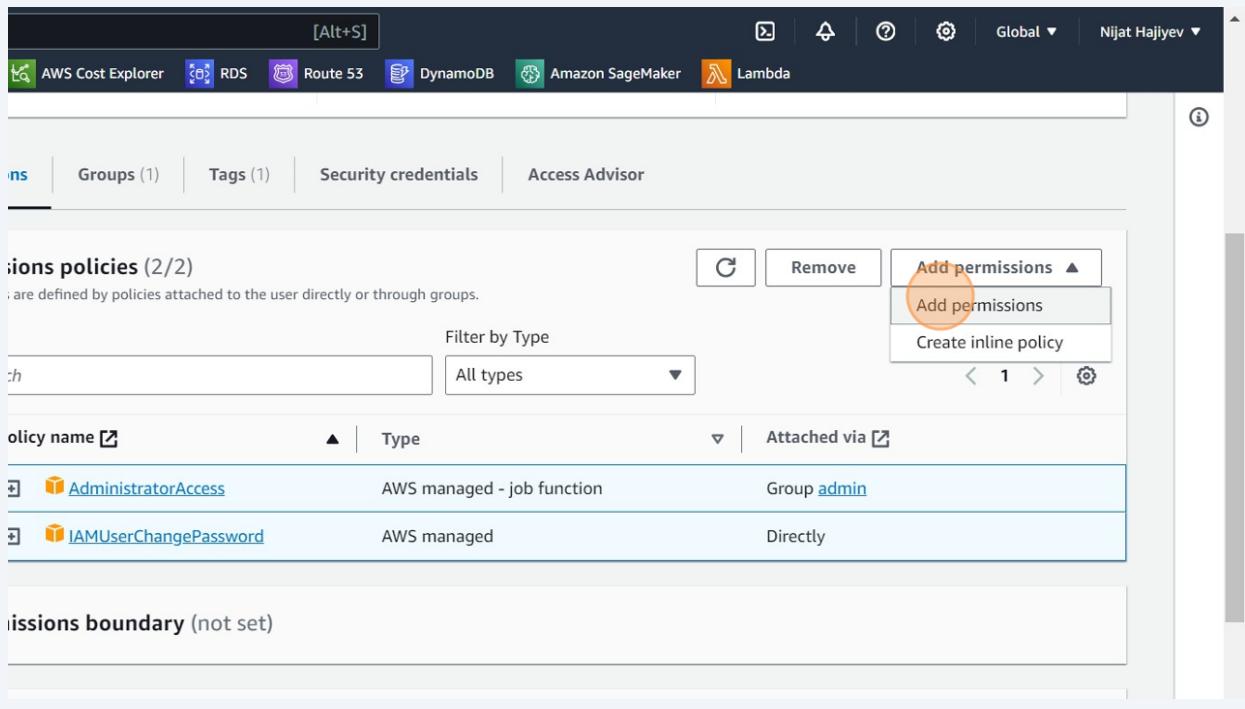
The screenshot shows the "Users" page under the IAM service. The sidebar on the left includes "User groups", "Users" (selected and highlighted with an orange circle), "Roles", "Policies", "Identity providers", and "Account settings". The main content area shows a table titled "Users (1) Info" with one entry: "DemoUser". The table columns include "User name", "Path", "Group", "Last activity", "MFA", and "Password age". The "DemoUser" row is highlighted with an orange circle. At the top right of the table, there are "Delete" and "Create" buttons.

## 11 Go to "Permissions policies"



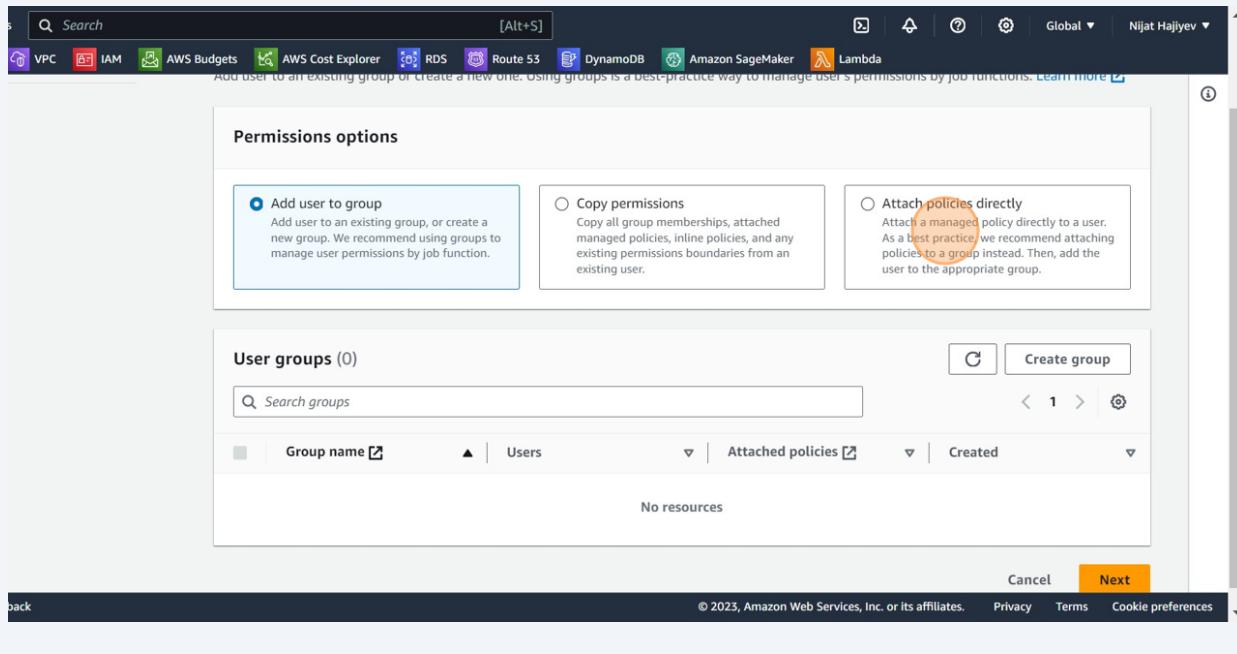
The screenshot shows the AWS IAM console. On the left, there's a sidebar with 'Identity and Access Management (IAM)'. In the main area, under 'Access management', there's a 'Users' section. A red circle highlights the 'Permissions policies (3)' section, which contains three entries: 'AdministratorAccess' (AWS managed - job function, Group 'admin'), 'IAMFullAccess' (AWS managed), and 'IAMUserChangePassword' (AWS managed). Below this, there are sections for 'Permissions boundary (not set)' and 'Generate policy based on CloudTrail events'.

## 12 Click "Add permissions" inside User

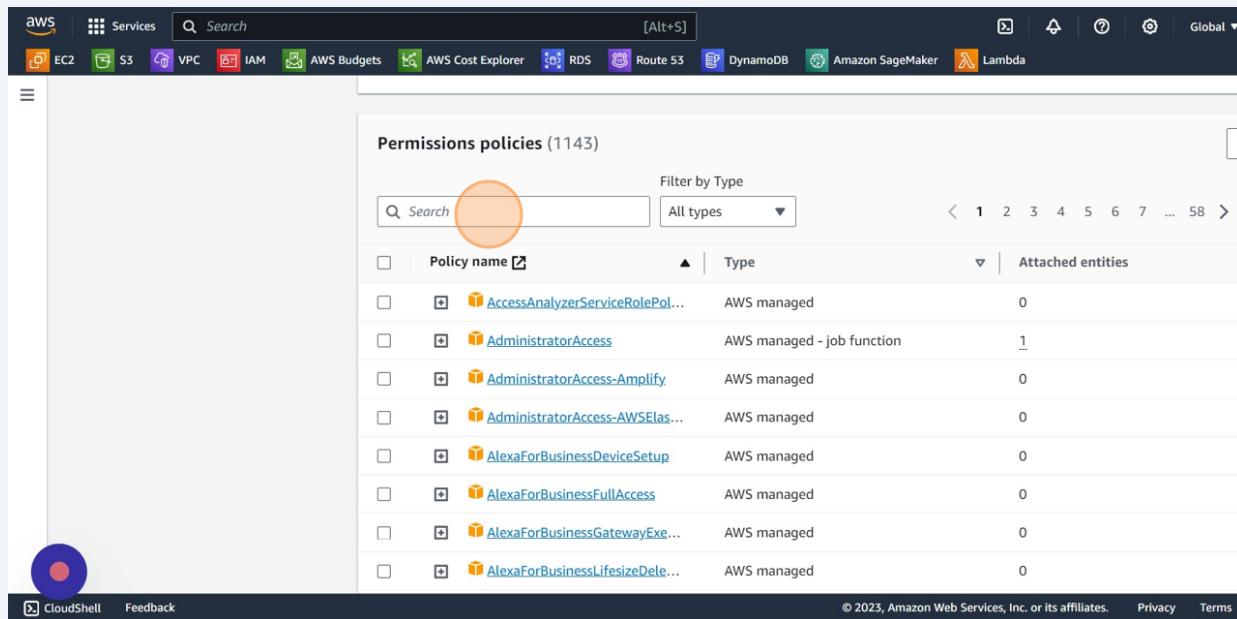


The screenshot shows the AWS IAM User permissions page. At the top, it says 'Permissions policies (2/2)'. A red circle highlights the 'Add permissions' button in the top right corner of the policy list. The list shows two policies: 'AdministratorAccess' (AWS managed - job function, Group 'admin') and 'IAMUserChangePassword' (AWS managed). Below the policy list, there's a section for 'Permissions boundary (not set)'.

## 13 Click "Attach a managed policy directly"



## 14 Click the "Search" field to search Policy



**15** Click this checkbox.

The screenshot shows the AWS IAM service interface. In the top navigation bar, the 'Services' tab is selected. Below it, the 'Permissions policies' section is displayed with a total count of 1143. A search bar at the top right contains the text 'IAM'. A filter bar below it shows 'All types' and '8 matches'. The main table lists various IAM policies, with one row highlighted and circled in orange. This row corresponds to the 'IAMFullAccess' policy, which is also highlighted with a blue selection bar at the bottom of the list. The table columns include 'Policy name', 'Type', and 'Attached entities'. The 'Attached entities' column shows values such as 0, 0, 0, 0, 1, 0, and 0. At the bottom of the page, there are links for 'CloudShell', 'Feedback', and the copyright notice '© 2023, Amazon Web Services, Inc. or its affiliates.' followed by 'Privacy' and 'Terms'.

**16** After selecting Policy, Click "Next"

This screenshot shows the same AWS IAM interface as the previous one, but with a different focus. The 'IAMFullAccess' policy has been selected, indicated by a checked checkbox and a blue highlight bar. The 'Next' button at the bottom right of the list is also highlighted with an orange circle. The rest of the interface is identical to the previous screenshot, including the search bar, filter bar, and the list of other IAM policies.

## 17 Click "Add permissions"

The screenshot shows the 'Review' step of creating a new IAM user. The user details section shows 'User name: DemoUser'. The 'Permissions summary' table lists one policy: 'IAMFullAccess' (AWS managed, used as a 'Permissions policy'). At the bottom right, there are buttons for 'Cancel', 'Previous', and 'Add permissions' (which is highlighted with a red circle).

Name	Type	Used as
IAMFullAccess	AWS managed	Permissions policy

## 18 Check if policy under "Permission policies"

The screenshot shows the 'Permissions' tab in the IAM console. A green banner at the top indicates '1 policy added'. The 'Permissions policies' section lists three policies: 'AdministratorAccess' (selected, highlighted with a red circle), 'IAMFullAccess', and 'IAMUserChangePassword'. The 'AdministratorAccess' policy is described as 'AWS managed - job function'. The 'Permissions boundary' section below is '(not set)'.

Policy name	Type
AdministratorAccess	AWS managed - job function
IAMFullAccess	AWS managed
IAMUserChangePassword	AWS managed

Add permission to Group.

## 19 Click "User groups"

The screenshot shows the AWS IAM Dashboard. On the left sidebar, under 'Access management', the 'User groups' option is highlighted with a red circle. The main content area displays 'Security recommendations' with one item: 'Add MFA for root user'. Below that is a section titled 'IAM resources' with tabs for User groups, Users, Roles, Policies, and Identity providers. The 'User groups' tab is selected.

## 20 Click "admin"

The screenshot shows the 'User groups' page within the AWS IAM service. The 'User groups' section header has '(1)' next to it. A table lists one user group: 'admin', which is highlighted with a red circle. The table includes columns for Group name, Users, and Permissions. The 'Defined' checkbox for the admin group is checked.

## 21 Click "Permissions"

The screenshot shows the AWS Identity and Access Management (IAM) console. On the left, the navigation pane is open, showing the 'Access management' section with 'User groups' selected. The main content area displays the 'Summary' for the 'admin' user group. The 'Users (1)' tab is selected, showing one user named 'admin'. The 'Permissions' tab is highlighted with an orange circle, indicating it is the next step. Below the tabs, there is a section titled 'Users in this group (1)' with a search bar and a table header 'User name'. The bottom right corner of the screen shows the copyright notice '© 2023, Amazon Web Service'.

## 22 Click "Add permissions"

The screenshot shows the same AWS IAM User Groups page as the previous step, but now the 'Permissions' tab is selected. In the 'Permissions policies' section, there are two managed policies listed: 'AdministratorAccess' and 'IAMFullAccess'. The 'Add permissions' button, located at the top right of this section, is highlighted with an orange circle. The bottom right corner of the screen shows the copyright notice '© 2023, Amazon Web Services, Inc. or its affiliates.' and links for 'Privacy', 'Terms', and 'Cookie preferences'.

## 23 Click "Attach policies"

The screenshot shows the AWS IAM Groups page. At the top, there's a group named 'admin' with a creation time of October 29, 2023, and an ARN. Below this, the 'Permissions' tab is selected, showing two attached policies: 'AdministratorAccess' and 'IAMFullAccess'. A context menu is open over the 'AdministratorAccess' policy, with the 'Attach policies' option highlighted and circled.

## 24 Click the "Search" field to search Policy

The screenshot shows the AWS IAM Policies page. It displays a list of other permission policies. The 'Search' field at the top of the list is highlighted and circled. The list includes policies like 'AdministratorAccess-Amplify', 'AdministratorAccess-AWSEla...', 'AlexaForBusinessDeviceSetup', 'AlexaForBusinessFullAccess', 'AlexaForBusinessGatewayEx...', 'AlexaForBusinessLifesizeDelega...', and 'AlexaForBusinessPolyDelega...'. The page also includes navigation links for CloudShell and Feedback, and standard footer links for Privacy and Terms.

## 25 Type "s3" (name of policy want to attach)

**26** Click this checkbox.

Current permissions policies (2)

Other permission policies (891)  
You can attach up to 10 managed policies to this user group. All of the users in this group inherit the attached permissions.

Policy name	Type	Used as
AmazonDMSRedshiftS3Role	AWS managed	None
AmazonS3FullAccess	AWS managed	None
AmazonS3ObjectLambdaExe...	AWS managed	None
AmazonS3OutpostsFullAccess	AWS managed	None
AmazonS3OutpostsReadOnl...	AWS managed	None
AmazonS3ReadOnlyAccess	AWS managed	None
AWSBackupServiceRolePolic...	AWS managed	None

Filter by Type  
All types 14 matches

CloudShell Feedback © 2023, Amazon Web Service

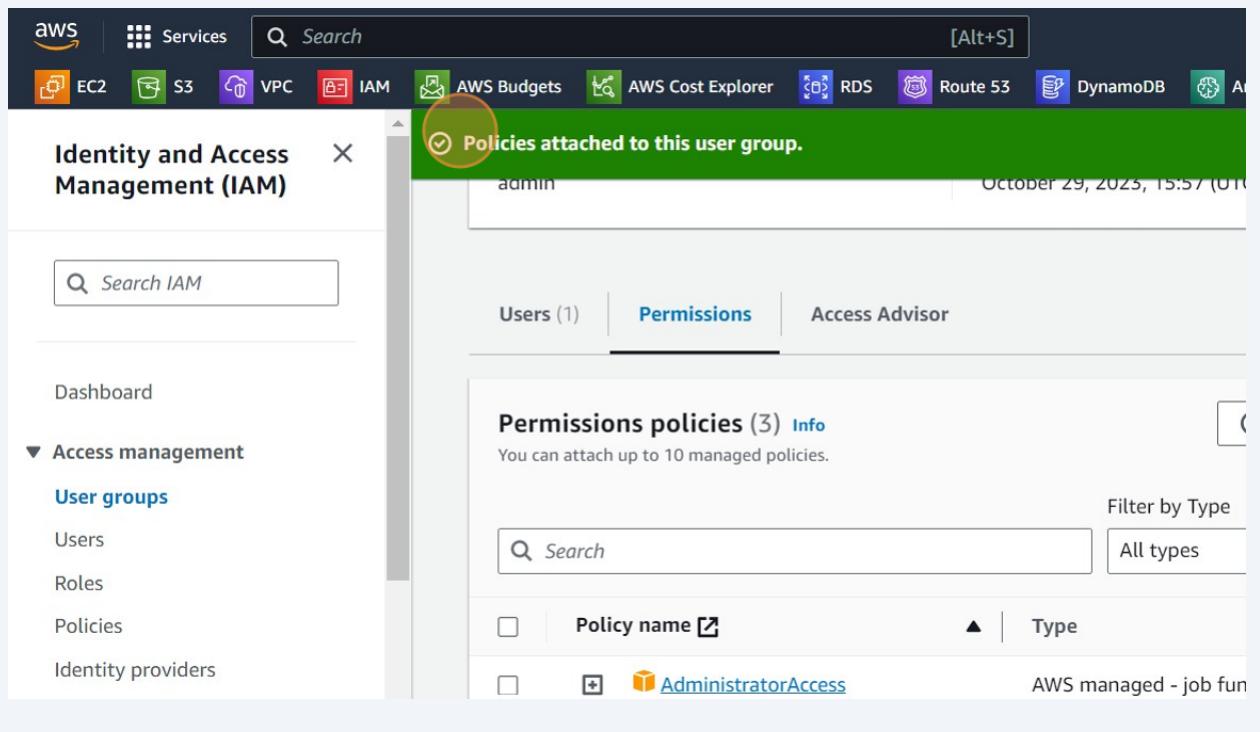
**27** Click "Attach policies"

None	Provides read only access to Amazon S...
None	Provides read only access to all bucket...
None	Policy containing permissions necessar...
None	Policy containing permissions necessar...
None	Policy used by QuickSight team to acc...
ed	Permissions policy (1)

Cancel Attach policies

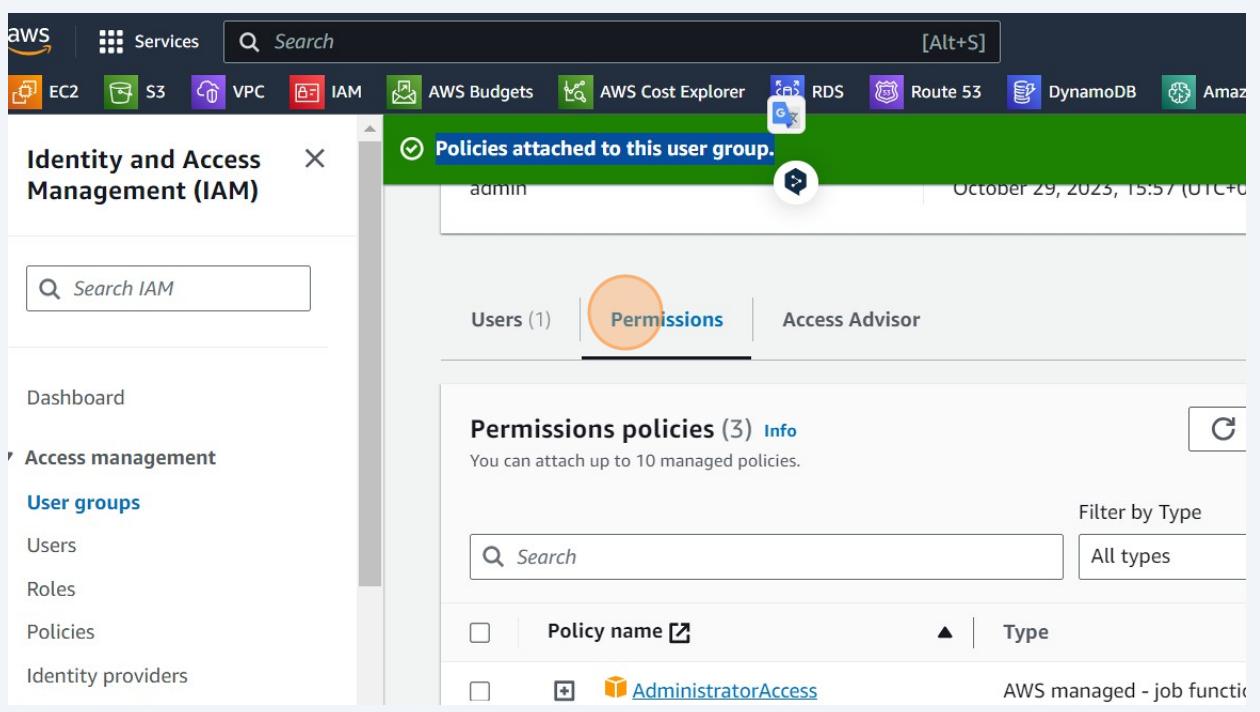
© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

## 28 Check "Policies attached to this user group." notification



The screenshot shows the AWS Identity and Access Management (IAM) service in the AWS Management Console. The navigation bar at the top includes links for EC2, S3, VPC, IAM, AWS Budgets, AWS Cost Explorer, RDS, Route 53, DynamoDB, and other services. The main title is "Identity and Access Management (IAM)". On the left, there's a sidebar with "Access management" expanded, showing "User groups", "Users", "Roles", "Policies", and "Identity providers". The main content area is titled "Permissions policies (3) Info" and states "You can attach up to 10 managed policies." It includes a search bar, a filter button for "All types", and a table with one item: "AdministratorAccess" (AWS managed - job function). A green banner at the top of the content area says "Policies attached to this user group." with a circled checkmark icon.

## 29 Check "Permissions"



This screenshot is nearly identical to the previous one, showing the AWS IAM console. The main difference is the color of the banner at the top, which is blue instead of green. The blue banner also contains a circled blue arrow icon. The rest of the interface, including the sidebar, the "Permissions policies" table, and the overall layout, remains the same.

## 30 Check permission

The screenshot shows the AWS IAM console. On the left, there's a sidebar with a search bar and navigation links like Dashboard, Access management, User groups, Roles, Policies, Identity providers, and Account settings. Under Access management, 'User groups' is selected. On the right, the main area has tabs for Users (1), Permissions (selected), and Access Advisor. The Permissions section shows 'Permissions policies (3)'. It includes a search bar, a filter for 'All types', and a table with three rows:

	Policy name	Type
<input type="checkbox"/>	<a href="#">AdministratorAccess</a>	AWS managed - job fun
<input type="checkbox"/>	<a href="#">AmazonS3FullAccess</a>	AWS managed
<input type="checkbox"/>	<a href="#">IAMFullAccess</a>	AWS managed

The row for 'AmazonS3FullAccess' is circled in red.

## Check ready policies

### 31 Click "Policies"

The screenshot shows the AWS IAM Dashboard. On the left, there's a sidebar with a search bar at the top. Below it, under 'Access management', the 'Policies' option is highlighted with an orange circle. Other options like 'User groups', 'Users', 'Roles', and 'Identity providers' are also listed. Under 'Access reports', there are 'Access analyzer' and 'Archive rules'. At the bottom of the sidebar are 'CloudShell' and 'Feedback' buttons. The main area has a header 'IAM DASHBOARD'. It features a 'Security recommendations' section with one item: 'Add MFA for root user' (warning icon) and 'Root user has no active access keys' (green checkmark icon). Below that is a 'IAM resources' section with tabs for 'User groups', 'Users', 'Roles', and 'Policies', where 'Policies' is also highlighted with an orange circle.

### 32 Click the "Search" field to search policy

The screenshot shows the 'Policies' page within the AWS IAM service. At the top, there's a navigation bar with 'Services' and a search bar containing 'Search [Alt+S]'. Below the search bar are links for S3, VPC, IAM, AWS Budgets, AWS Cost Explorer, RDS, Route 53, DynamoDB, and Amazon SageMaker. The main content area shows the title 'Policies (1142) Info' with a note that a policy defines permissions. A 'Filter by Type' section includes a search input field and a dropdown set to 'All types'. The main table lists policies with columns for 'Policy name', 'Type', and 'Used as'. The first few rows show policies like 'AccessAnalyzerServiceRolePolicy', 'AdministratorAccess', and 'AdministratorAccess'. The 'Search' input field in the filter section is highlighted with an orange circle.

33 Type "iam"

34 Click "IAMFullAccess"

The screenshot shows the AWS IAM Policies list. A search bar at the top contains the text "iam". Below the search bar, a table lists several AWS managed policies. The "IAMFullAccess" policy is highlighted with a red circle around its name. The table columns are "Policy name", "Type", and "Used as".

Policy name	Type	Used as
AWSQuickSightList...	AWS managed	None
IAMAccessAdvisorR...	AWS managed	None
IAMAccessAnalyzer...	AWS managed	None
IAMAccessAnalyzer...	AWS managed	None
IAMFullAccess	AWS managed	Permissions: [redacted]
IAMReadOnlyAccess	AWS managed	Permissions: [redacted]
IAMSelfManageSer...	AWS managed	None

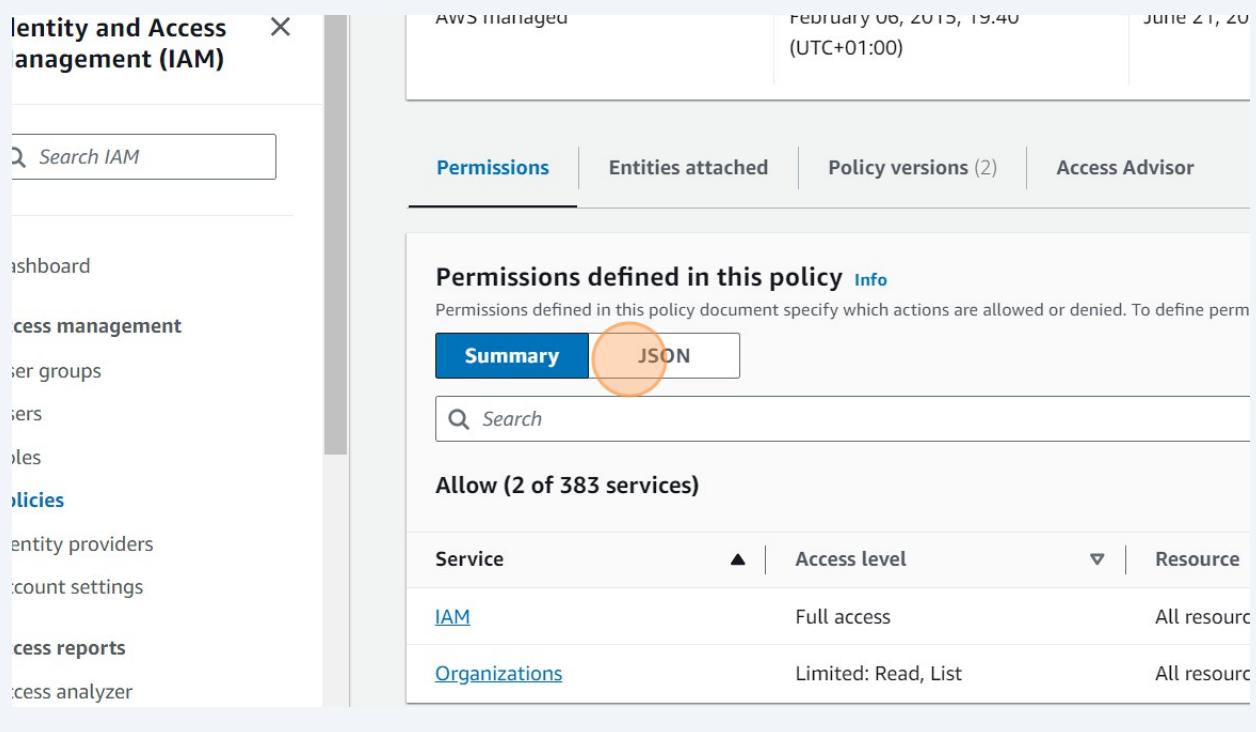
### 35 Click "Summary"

The screenshot shows the AWS Identity and Access Management (IAM) console. On the left, there's a navigation sidebar with links like Dashboard, Access management, Policies, and Access reports. The main area is titled 'Identity and Access Management (IAM)' and shows a summary card for a policy named 'AWS managed'. The card displays the creation date ('February 06, 2015, 19:40 (UTC+01:00)'), last updated date ('June 21, 2019, 21:40 (UTC+02:00)'), and version count ('(UTC+01:00)'). Below the card, there are tabs for Permissions, Entities attached, Policy versions (2), and Access Advisor. The 'Permissions' tab is selected. A sub-section titled 'Permissions defined in this policy' contains two buttons: 'Summary' (which is highlighted with a yellow circle) and 'JSON'. A search bar is also present. The main content area shows a table titled 'Allow (2 of 383 services)' with columns for Service, Access level, Resource, and Request condition. The table lists two entries: 'IAM' with 'Full access' and 'All resources' and 'Request condition' set to 'None', and 'Organizations' with 'Limited: Read, List' and 'All resources'.

### 36 Check permissions

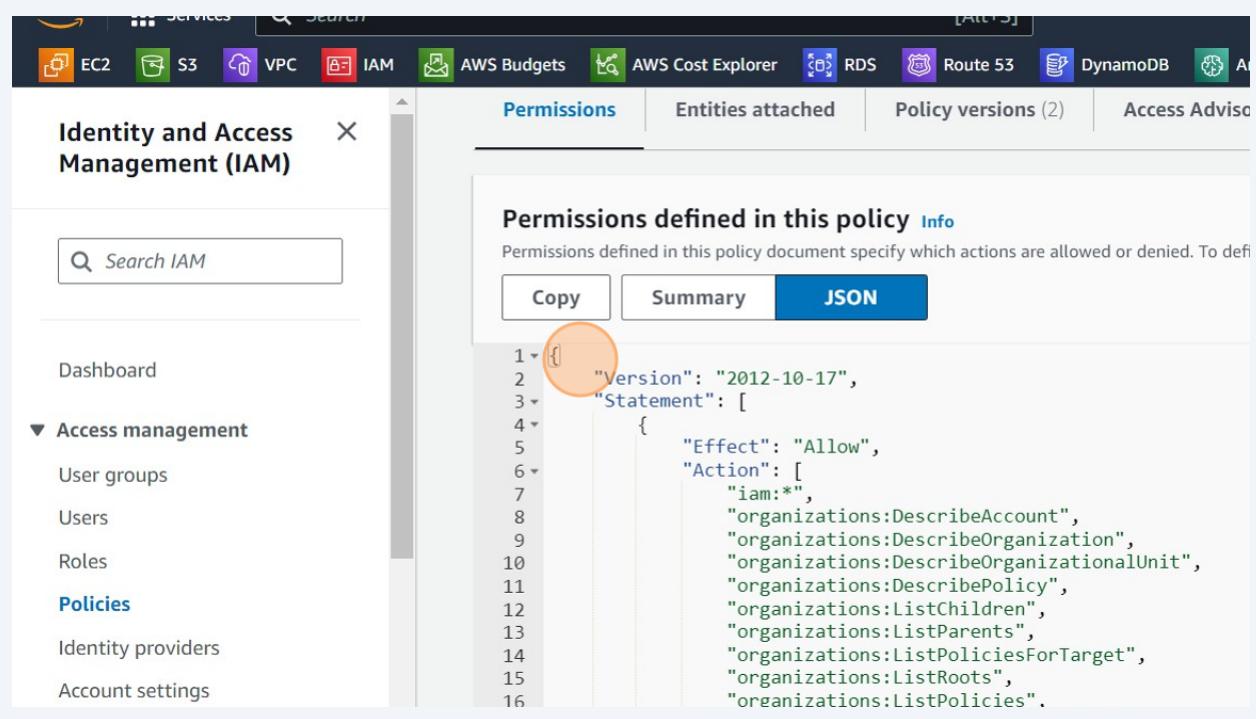
This screenshot is similar to the previous one but shows a different policy. The summary card for 'AWS managed' now shows the last update date as 'June 21, 2019, 21:40 (UTC+02:00)'. The 'Permissions' section is again selected, and the 'Summary' button is highlighted with a yellow circle. The 'Allow (2 of 383 services)' table shows the same two entries as before: 'IAM' with 'Full access' and 'All resources' and 'Request condition' set to 'None', and 'Organizations' with 'Limited: Read, List' and 'All resources'.

### 37 Click "JSON"



The screenshot shows the AWS IAM console. On the left, there's a sidebar with navigation links like Dashboard, Access management, User groups, Users, Roles, Policies, Identity providers, Account settings, Access reports, and Access analyzer. The main area is titled "Identity and Access Management (IAM)". It shows a policy named "AWS Managed". The "Permissions" tab is selected, showing "Allow (2 of 383 services)" for the IAM service. Below this, there's a table with columns for Service, Access level, and Resource. The table shows "IAM" with "Full access" and "Organizations" with "Limited: Read, List". At the bottom of the "Permissions defined in this policy" section, there are tabs for "Summary" and "JSON". The "JSON" tab is highlighted with a yellow circle.

### 38 Check JSON format



The screenshot shows the same AWS IAM console as the previous one, but the "JSON" tab is now active. The JSON code for the policy is displayed:

```
1 { "Version": "2012-10-17", "Statement": [ 2 { "Effect": "Allow", "Action": [ 3 "iam:*", "organizations:DescribeAccount", "organizations:DescribeOrganization", "organizations:DescribeOrganizationalUnit", "organizations:DescribePolicy", "organizations>ListChildren", "organizations>ListParents", "organizations>ListPoliciesForTarget", "organizations>ListRoots", "organizations>ListPolicies" ] } ] }
```

## 39 Check JSON format

The screenshot shows the AWS IAM Policies page. On the left, there's a sidebar with navigation links like 'Management', 'Providers', 'Settings', 'Ports', 'Analyzer', and 'rules'. The main area has a title 'Permissions defined in this policy' with an 'Info' link. Below it are three tabs: 'Copy', 'Summary', and 'JSON' (which is highlighted). The JSON code area contains numbered lines from 3 to 22, representing a policy document. A large orange circle highlights the entire JSON code area. At the bottom, there's a 'Feedback' button and a copyright notice '© 2023, Amazon Web Services'.

## Create own policy VISUAL

## 40 Click "Policies"

The screenshot shows the AWS IAM Dashboard. On the left, there's a sidebar with 'Dashboard', 'Access management' (which is expanded, showing 'User groups', 'Users', 'Roles', and 'Policies'), 'Identity providers', 'Account settings', and 'Access reports' (which is expanded, showing 'Access analyzer' and 'Archive rules'). The 'Policies' link under 'Access management' is highlighted with an orange circle. The main area has a title 'IAM Dashboard' and a 'Security recommendations' section with one item ('Add MFA for root user') and an 'IAM resources' section listing 'User groups', 'Users', 'Roles', and 'Policies'. At the bottom, there's a 'CloudShell' button and a 'Feedback' button.

## 41 Click "Create policy"

The screenshot shows the AWS IAM Policies page. At the top, there is a navigation bar with various service icons like RDS, Route 53, DynamoDB, Amazon SageMaker, and Lambda. Below the navigation bar is a search bar with the placeholder "[Alt+S]". The main area contains a table of existing policies. The table has columns for Type, Used as, and Description. The 'Create policy' button is located at the top right of the table area, highlighted with a yellow circle.

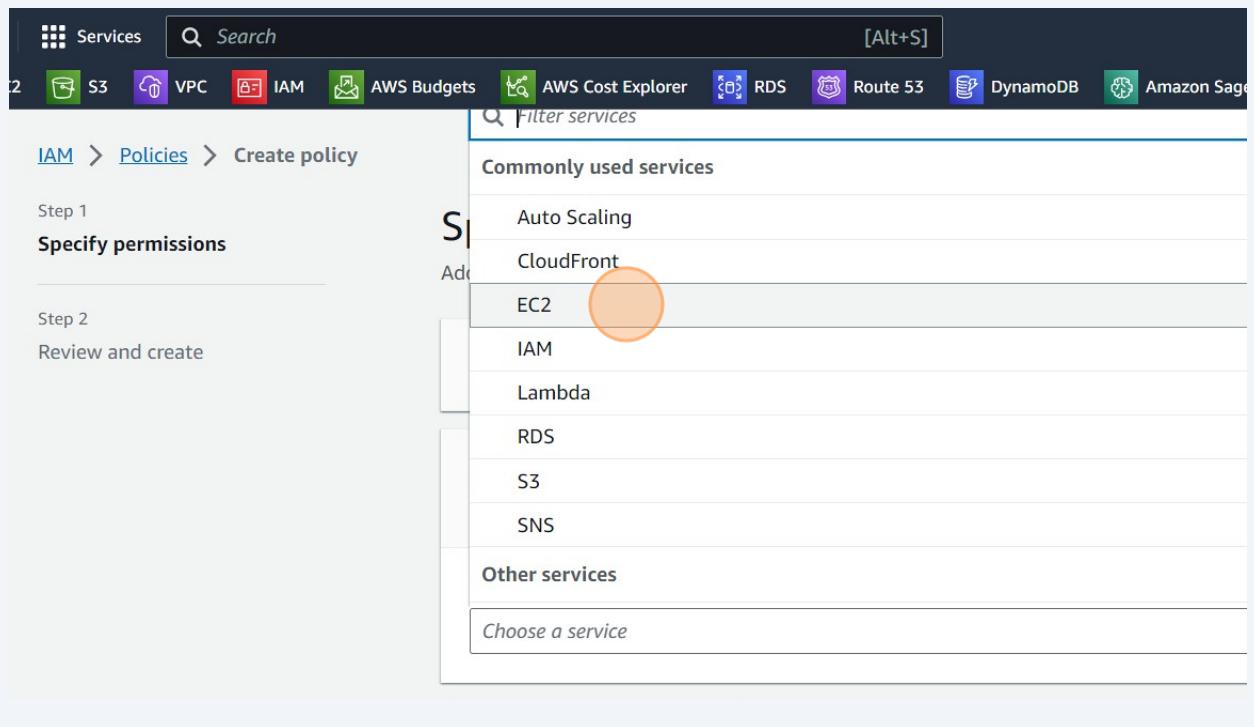
Type	Used as	Description
AWS managed	None	
AWS managed - job funct...	Permissions policy (1)	
AWS managed	None	
AWS managed	None	

## 42 Create Policy from Visual

Click "Choose a service"

The screenshot shows the 'Specify permissions' step of the 'Create policy' wizard. The left sidebar shows the navigation path: IAM > Policies > Create policy. The main area is titled 'Specify permissions' with a sub-instruction: 'Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.' A 'Policy editor' section is present, with tabs for 'Visual' (which is selected), 'JSON', and 'Actions'. Below the tabs is a section titled 'Select a service' with a sub-instruction: 'Specify what actions can be performed on specific resources in a service.' A dropdown menu labeled 'Choose a service' is highlighted with a yellow circle. At the bottom of the editor is a button '+ Add more permissions'.

**43** Click "EC2"



**44** Type "rea"

**45** Click the "Filter Actions" field.

The screenshot shows the AWS IAM Actions allowed page. At the top, there's a navigation bar with links for S3, VPC, IAM, AWS Budgets, AWS Cost Explorer, RDS, Route 53, DynamoDB, and Amazon SageMaker. A search bar is at the top right with the placeholder "[Alt+S]". Below the navigation bar, a heading says "Specify what actions can be performed on specific resources in EC2.". Underneath, a section titled "Actions allowed" has a sub-section "Access level" with four items: "List (168)", "Read (32)", "Write (407)", and "Permissions management (5)". To the left of the "Access level" section, there's a "Manual actions | Add actions" link and a checkbox for "All EC2 actions (ec2:\*)". At the very bottom of this section is a search bar with the placeholder "Filter Actions", which is highlighted with a red circle. The entire interface is set against a light gray background.

**46** Type "create"

47

Click this checkbox.

Specify actions from the service to be allowed.

Search: create

**Write**

<input type="checkbox"/> CreateCapacityReservation	Info	<input type="checkbox"/> CreateCapacityReservationFleet	Info	<input type="checkbox"/> CreateCarrierGateway
<input type="checkbox"/> CreateClientVpnEndpoint	Info	<input type="checkbox"/> CreateClientVpnRoute	Info	<input type="checkbox"/> CreateCoipCidr
<input type="checkbox"/> CreateCoipPool	Info	<input type="checkbox"/> CreateCoipPoolPermission	Info	<input type="checkbox"/> CreateCustomerGateway
<input type="checkbox"/> CreateDefaultSubnet	Info	<input type="checkbox"/> CreateDefaultVpc	Info	<input type="checkbox"/> CreateDhcpOption
<input type="checkbox"/> CreateEgressOnlyInternetGateway	Info	<input type="checkbox"/> CreateFleet	Info	<input type="checkbox"/> CreateFlowLogs
<input type="checkbox"/> CreateFpgalmage	Info	<input checked="" type="checkbox"/> CreateImage	Info	<input type="checkbox"/> CreateInstanceConnect
<input type="checkbox"/> CreateInstanceEventWindow	Info	<input type="checkbox"/> CreateInstanceExportTask	Info	<input type="checkbox"/> CreateInternetGateway
<input type="checkbox"/> CreateIpam	Info	<input type="checkbox"/> CreateIpamPool	Info	<input type="checkbox"/> CreateIpamResource
<input type="checkbox"/> CreateIpamScope	Info	<input type="checkbox"/> CreateKeyPair	Info	<input type="checkbox"/> CreateLaunchTemplate
<input type="checkbox"/> CreateLaunchTemplateVersion	Info	<input type="checkbox"/> CreateLocalGatewayRoute	Info	<input type="checkbox"/> CreateLocalGateway

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

48

Click ALLOW or DENY

[Alt+S]

RDS Route 53 DynamoDB Amazon SageMaker Lambda

Global ▾ Nijat Hajiyev ▾

performed on specific resources in EC2.

ce to be allowed.

Effect

Allow  Deny

<input type="checkbox"/> CreateCapacityReservationFleet	Info	<input type="checkbox"/> CreateCarrierGateway	Info
<input type="checkbox"/> CreateClientVpnRoute	Info	<input type="checkbox"/> CreateCoipCidr	Info
<input type="checkbox"/> CreateCoipPoolPermission	Info	<input type="checkbox"/> CreateCustomerGateway	Info
<input type="checkbox"/> CreateDefaultVpc	Info	<input type="checkbox"/> CreateDhcpOptions	Info
<input type="checkbox"/> CreateFleet	Info	<input type="checkbox"/> CreateFlowLogs	Info
<input checked="" type="checkbox"/> CreateImage	Info	<input type="checkbox"/> CreateInstanceConnectEndpoint	Info

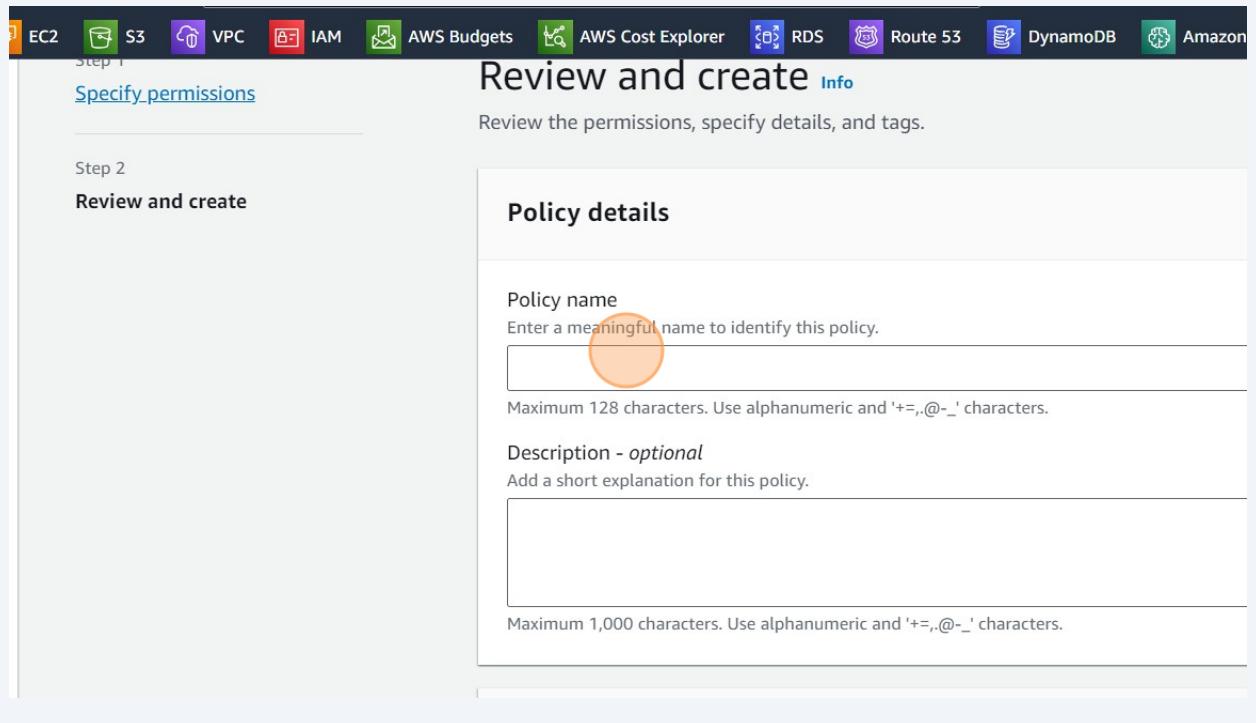
49 Click this radio button.

The screenshot shows the AWS IAM Policy Editor interface. In the 'Resources' section, there is a note: 'Specify resource ARNs for these actions.' Below it are two radio buttons: 'All' (unchecked) and 'Specific' (checked). The 'All' button is highlighted with an orange circle. To the right of the radio buttons are three resource types: 'image', 'instance', and 'snapshot', each with an 'Info' link. Each resource has a note indicating a specified ARN and a link to add more ARNs. Below these resources is a section titled 'Request conditions - optional' with a note about actions being allowed or denied only when certain conditions are met.

50 Click "Next"

The screenshot shows the AWS IAM Policy Editor interface. In the 'Resources' section, there is a note: 'To grant permissions for the selected resource actions, you must include additional required actions'. Below it is a list: 'ec2:CreateImage requires [1.more](#) action.'. The 'Specific' radio button is selected. There is also a note: 'The all wildcard '\*' may be overly permissive for the selected actions. Allowing specific ARNs for these service resources can improve security.' Below the resources is a 'Request conditions - optional' section with a note about actions being allowed or denied only when certain conditions are met. At the bottom of the page, there is a 'Cancel' button, an orange 'Next' button highlighted with an orange circle, and a blue circular profile picture.

**51** Click the "Policy name" field.



**52** Type "DemoPolicy"

**53** Click "Create policy"

The screenshot shows the 'Create policy' wizard on the AWS IAM service. The first step, 'Set permissions', is displayed. The configuration includes:

- Access level:** Limited: Write
- Resource:** All resources
- Request condition:** None

Below the configuration, there is a note: "You can add to AWS resources to help identify, organize, or search for resources." At the bottom of the page, the navigation buttons are visible: Cancel, Previous, Create policy (which is highlighted with a blue circle), and Next Step.

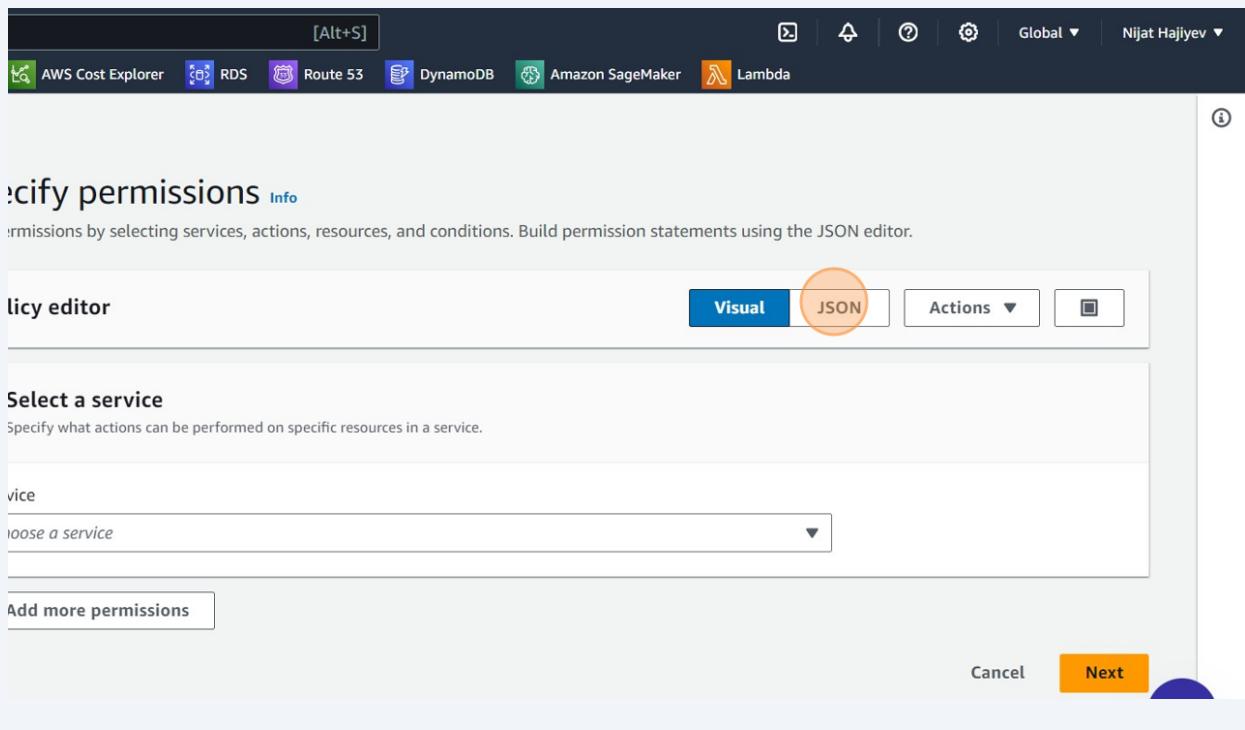
## Create own policy JSON

**54** Click "Create policy"

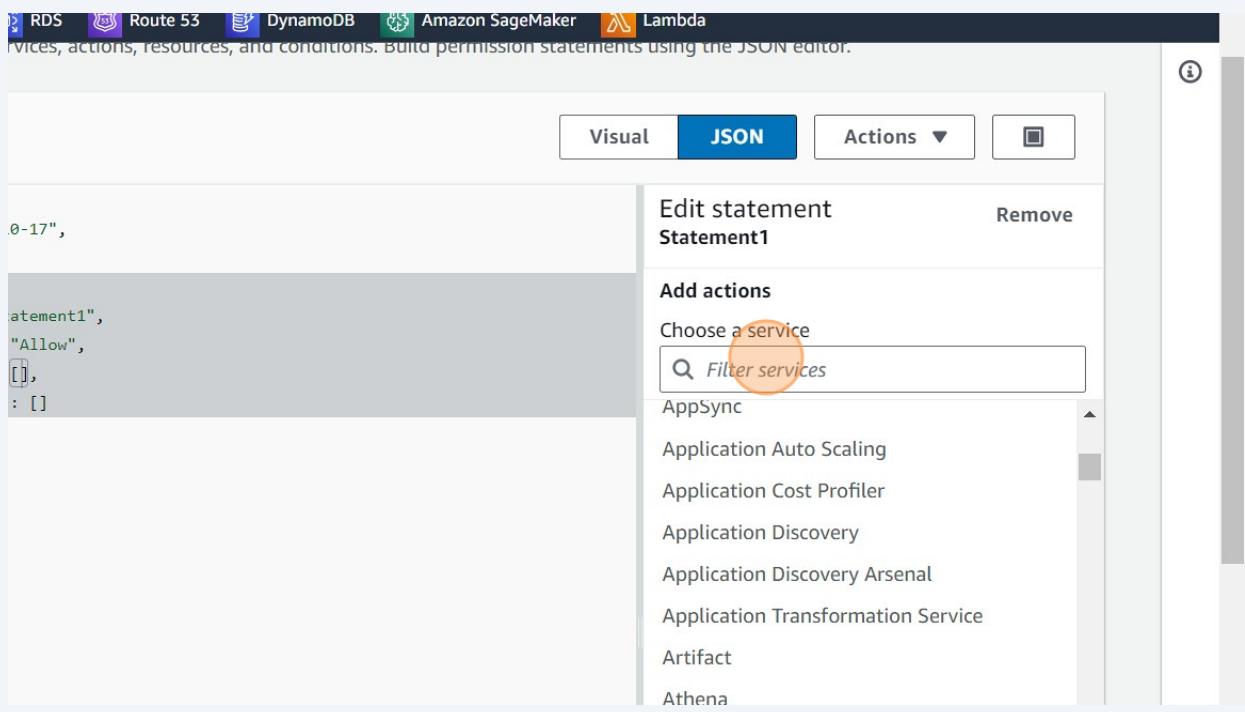
The screenshot shows the 'Policies' page on the AWS IAM service. The 'Create policy' button is highlighted with a blue circle. The page includes:

- A toolbar at the top with various AWS services like RDS, Route 53, DynamoDB, Amazon SageMaker, and Lambda.
- A header with a search bar, notifications, and user information (Nijat Hajiyev).
- A main table listing policies, with one row selected.
- Buttons for Actions, Delete, and Create policy.
- A 'Filter by Type' dropdown set to 'All types'.
- Pagination controls showing page 1 of 58.
- A table at the bottom showing policy details: Type (AWS managed), Used as (None or Permissions policy), and Description (Allow Access Analyzer to analyze resources, Provides full access to AWS services, Grants account administrative permissions).

## 55 Click "JSON"



## 56 Choose service



**57** Type "ec2"

**58** Click "EC2"

The screenshot shows the AWS IAM Policy Editor interface. On the left, there is a code editor window containing JSON policy code. On the right, a modal dialog is open for editing a policy statement named "Statement1". The "Add actions" section contains a search bar with "ec2" typed into it. Below the search bar, a list of services is shown, with "EC2" highlighted by a red circle. Other listed services include EC2 Auto Scaling, EC2 Image Builder, EC2 Instance Connect, and EC2 Messages. At the bottom of the dialog, there is a "Remove" button.

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

## 59 Select actions

Visual JSON Actions ▾

.0-17",  
atement1",  
"Allow",  
[],  
: []

Edit statement Statement1 Remove

Add actions All services > EC2

Filter actions

All actions (ec2:\*)

Access level - list

DescribeAccountAttributes Info  
 DescribeAddresses Info  
 DescribeAddressesAttribute Info  
 DescribeAddressTransfers Info  
 DescribeAggregateIdFormat Info  
 DescribeAvailabilityZones Info

## 60 Click "Add"

DescribeFastSnapshotRestores Info  
 DescribeFleetHistory Info  
 DescribeFleetInstances Info  
 DescribeFleets Info  
 DescribeFlowLogs Info  
 DescribeFpgaImageAttribute Info  
 DescribeFpgaImages Info

Add a resource

Add a condition (optional)

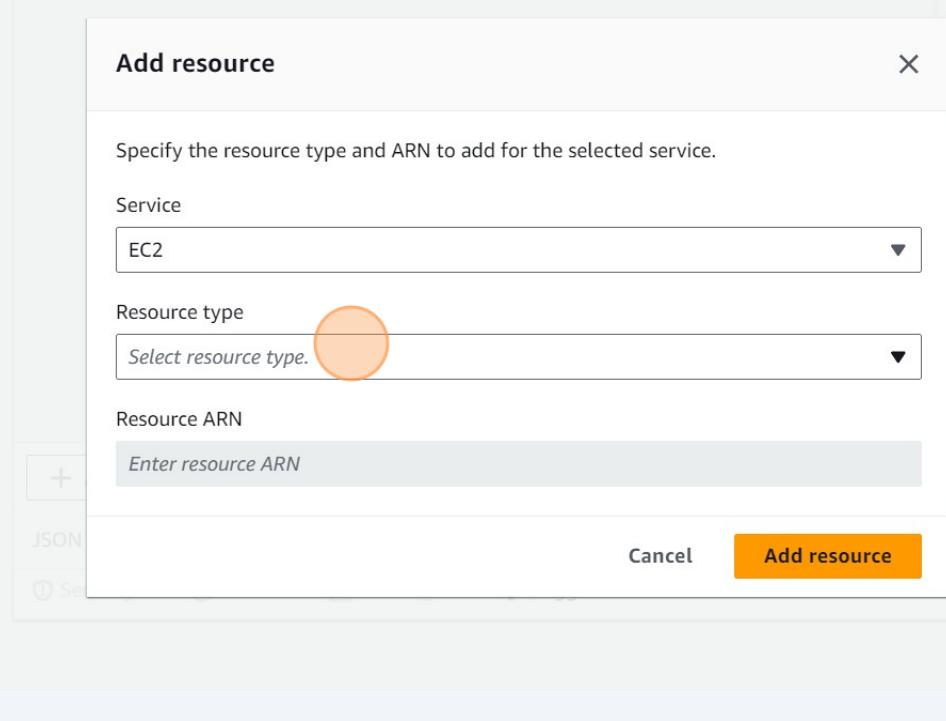
6035 of 6144 characters remaining

⚠ Warnings: 0 ⚡ Suggestions: 1

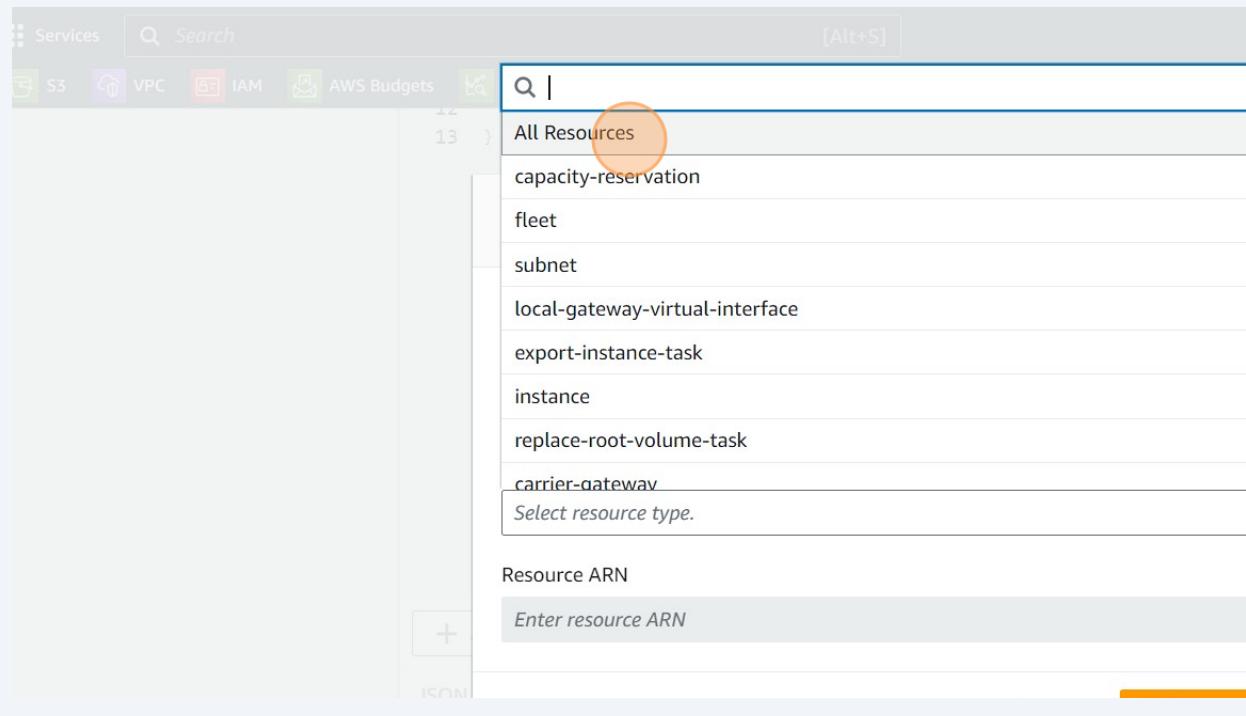
Cancel

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

**61** Click "Select resource type."



**62** Click "All Resources"



**63** Click "Add resource"

The screenshot shows the AWS Lambda function configuration interface. A modal window titled "Add resource" is open, prompting the user to select a resource type and ARN. The "Resource type" dropdown is set to "Lambda function". The "ARN" input field contains a placeholder "arn:aws:lambda:us-east-1:123456789012:function:my-function". Below the input fields are two buttons: "Cancel" and "Add resource", with "Add resource" being highlighted with a red circle. To the right of the modal, a sidebar lists several AWS services with their corresponding API actions: DescribeFleetHistory Info, DescribeFleetInstances Info, DescribeFleets Info, DescribeFlowLogs Info, DescribeFpgaImageAttribute Info, and DescribeFpgaImages Info. Below the sidebar are two "Add" buttons and a character count indicator "6035 of 6144 characters remaining". At the bottom of the page, there are links for "Cancel", "Next", "© 2023, Amazon Web Services, Inc. or its affiliates.", "Privacy", "Terms", and "Cookie preferences".

**64** Click "Next"

The screenshot shows the AWS Lambda function configuration interface after the "Add resource" step has been completed. The modal window now displays a list of selected resources: DescribeFleetHistory Info, DescribeFleetInstances Info, DescribeFleets Info, DescribeFlowLogs Info, DescribeFpgaImageAttribute Info, and DescribeFpgaImages Info. Each item is preceded by a checked checkbox. Below the list are two "Add" buttons and a character count indicator "6032 of 6144 characters remaining". At the bottom of the page, there are links for "Cancel", "Next", "© 2023, Amazon Web Services, Inc. or its affiliates.", "Privacy", "Terms", and "Cookie preferences". The "Next" button is highlighted with a red circle.

**65** Click the "Policy name" field.

Step 1  
[Specify permissions](#)

Step 2  
**Review and create**

## Review and create Info

Review the permissions, specify details, and tags.

### Policy details

#### Policy name

Enter a meaningful name to identify this policy.

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

#### Description - *optional*

Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+=.,@-\_' characters.

**66** Type "DemoPolicy2"

67

Click "Create policy"

The screenshot shows the 'Create policy' wizard on the AWS IAM service. The current step is 'Set permissions'. The configuration table has three columns: 'Access level', 'Resource', and 'Request condition'. A single row is selected with the values 'Full access', 'All resources', and 'None'. Below the table, there is a note about adding tags to resources. At the bottom of the page, there are navigation buttons: 'Cancel', 'Previous', 'Create policy' (which is highlighted with a red oval), and links for 'Privacy', 'Terms', and 'Cookie preferences'. A small circular profile icon is also visible.

Access level	Resource	Request condition
Full access	All resources	None

can add to AWS resources to help identify, organize, or search for resources.

resource.

Cancel Previous Create policy Privacy Terms Cookie preferences



Check created policy

**68** Click the "Search" field.

The screenshot shows the AWS IAM Policies page. At the top, a green banner displays the message "Policy DemoPolicy2 created." Below the banner, the navigation path is "IAM > Policies". The main title is "Policies (1144) Info" with a subtitle "A policy is an object in AWS that defines permissions." A search bar labeled "Search" is highlighted with an orange circle. To the right of the search bar is a dropdown menu set to "All types". The table below has columns: "Policy name", "Type", and "Used as". The data in the table includes:

Policy name	Type	Used as
AccessAnalyzerServiceRole	AWS managed	None
AdministratorAccess	AWS managed - job funct...	Permissions policy (
AdministratorAccess	AWS managed	None
AdministratorAccess	AWS managed	None

**69** Type "Demopolicy2"

## 70 Click "DemoPolicy2"

The screenshot shows the AWS IAM Policies page. A search bar at the top contains the text "Demopol". Below it is a table with columns for Policy name, Type, and Used as. Two rows are visible:

	Policy name	Type	Used as
○	<a href="#">DemoPolicy</a>	Customer managed	None
○	<a href="#">DemoPolicy2</a>	Customer managed	None

A red circle highlights the "DemoPolicy2" row.

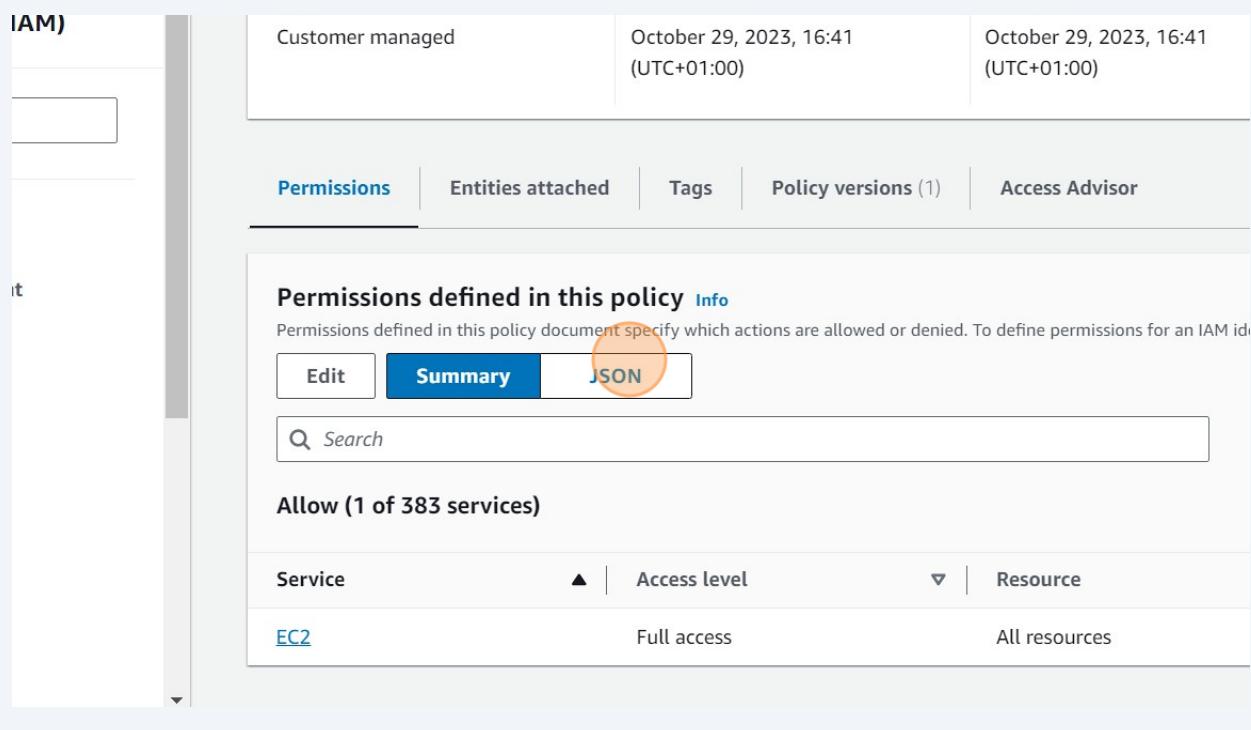
## 71 Click "Permissions"

The screenshot shows the AWS IAM Policy details page for "DemoPolicy2". The left sidebar shows "Access management" with "Policies" selected. The main area displays policy details and the "Permissions" tab, which is highlighted with a red circle.

Type	Creation time	Editor
Customer managed	October 29, 2023, 16:41 (UTC+01:00)	Octo (UTC)

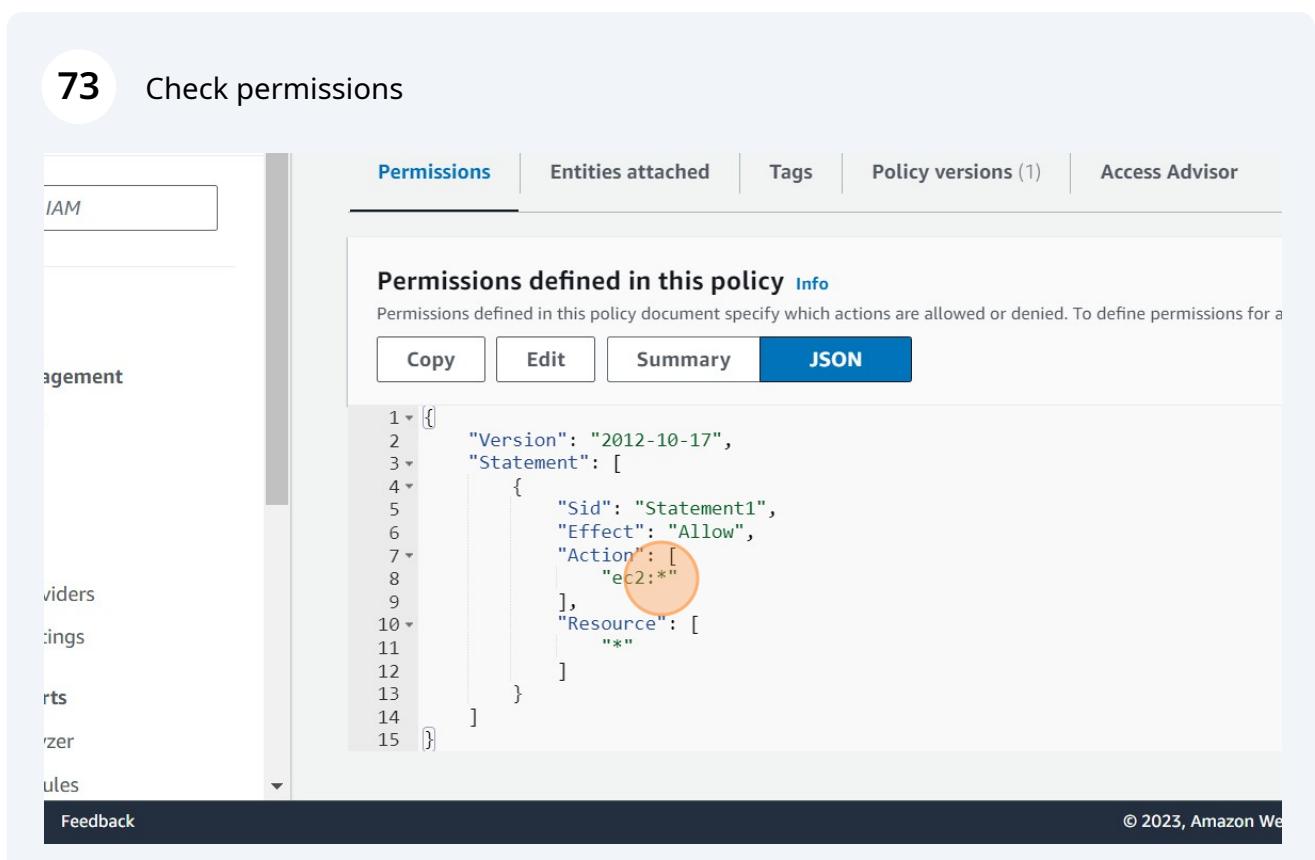
Below the table, the "Permissions" tab is active, showing a summary of permissions defined in the policy. It includes tabs for "Edit", "Summary" (which is selected), and "JSON". A search bar and a link to "Allow (1 of 383 services)" are also present.

## 72 Click "JSON"



A screenshot of the AWS IAM Policy JSON view. At the top, there's a navigation bar with tabs: Permissions, Entities attached, Tags, Policy versions (1), and Access Advisor. The 'Permissions' tab is active. Below the navigation bar, the title 'Permissions defined in this policy' is followed by a link 'Info'. A note states: 'Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM id...'. There are three buttons below the note: 'Edit', 'Summary' (which is highlighted in blue), and 'JSON'. A search bar labeled 'Search' is also present. The main content area shows a table titled 'Allow (1 of 383 services)'. The table has columns: Service, Access level, and Resource. One row is shown: EC2, Full access, All resources. The entire screenshot is framed by a light gray border.

## 73 Check permissions



A screenshot of the AWS IAM Policy JSON view. The interface is similar to the previous one, with a navigation bar and a note about permissions. The 'JSON' button is highlighted. Below the note, the JSON code for the policy is displayed:

```
1 {  
2     "Version": "2012-10-17",  
3     "Statement": [  
4         {  
5             "Sid": "Statement1",  
6             "Effect": "Allow",  
7             "Action": [  
8                 "ec2:*"  
9             ],  
10            "Resource": [  
11                "*"  
12            ]  
13        }  
14    ]  
15}
```

The line 'Action": ["ec2:\*"]' is circled in orange. The bottom of the screen shows a footer with 'Feedback' and '© 2023, Amazon Web Services'.