

IAM-Policies-Assignment---2

Problem Statement:

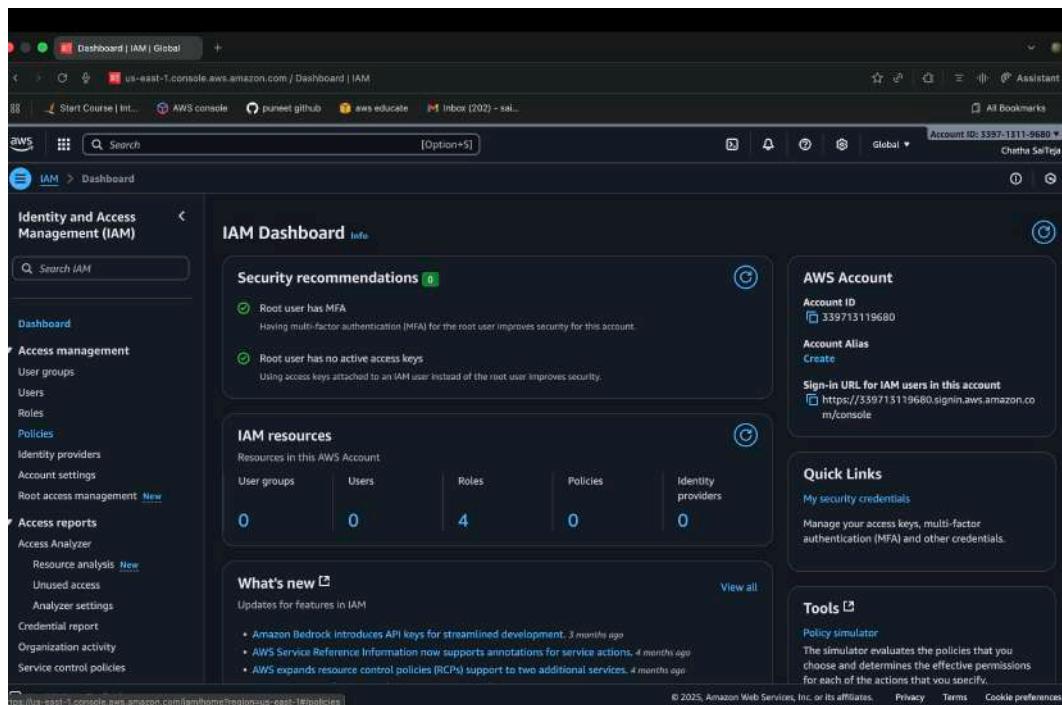
You work for XYZ Corporation. To maintain the security of the AWS account and the resources you have been asked to implement a solution that can help easily recognize and monitor the different users.

Tasks To Be Performed:

1. Create policy number 1 which lets the users to:
 - a. Access S3 completely
 - b. Only create EC2 instances
 - c. Full access to RDS
2. Create a policy number 2 which allows the users to:
 - a. Access CloudWatch and billing completely
 - b. Can only list EC2 and S3 resources
3. Attach policy number 1 to the Dev Team from task 1
4. Attach policy number 2 to Ops Team from task 1

Step-By-Step Procedure:-

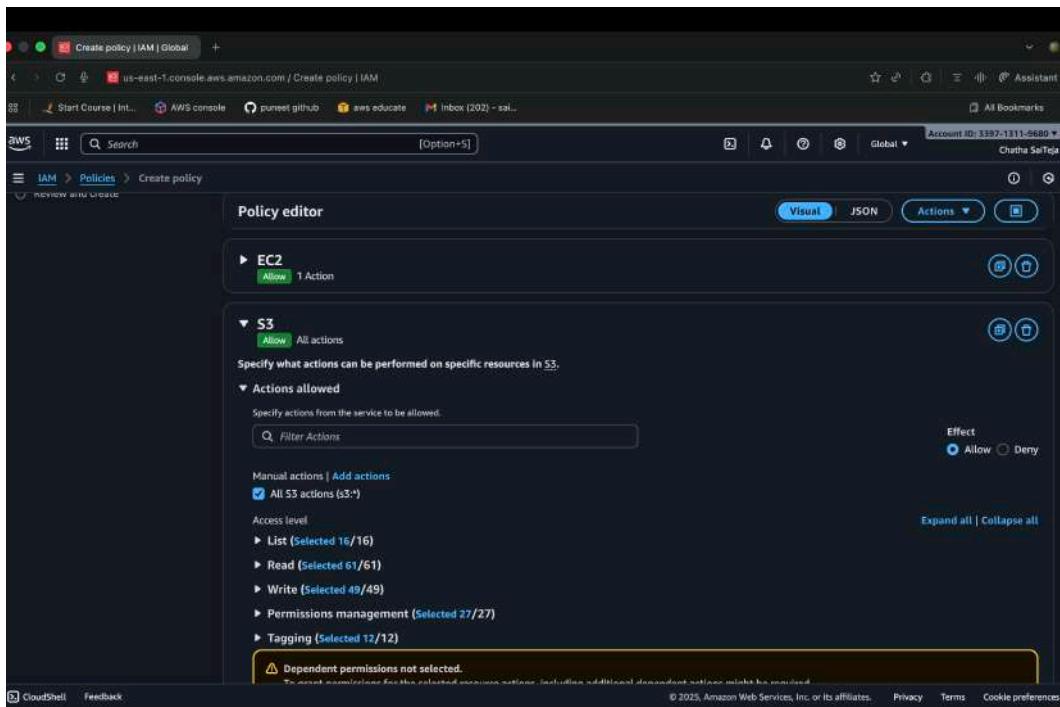
Step1:- Go to AWS and Search for IAM Service we can see a dashboard go to policies.



IAM Dashboard click on policy

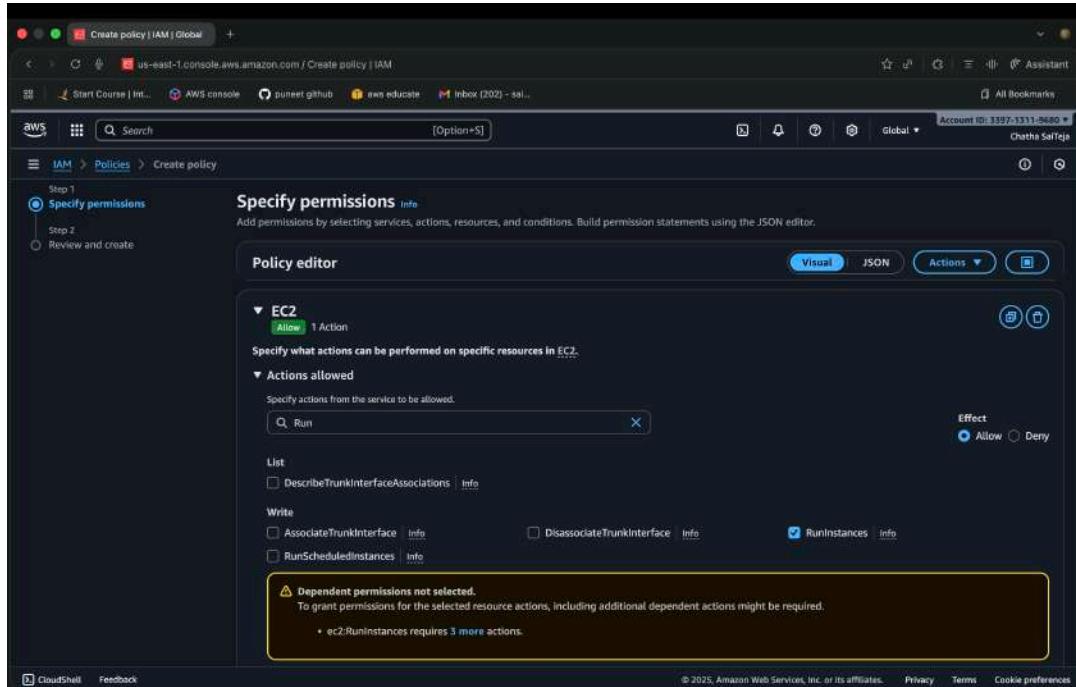
Step 2:- Click on Create Policy the first step to create policy is by specify the permissions , we can add more permissions by clicking on add more now we have to create Policy1 with Access S3 completely, Only create EC2 instances, Full access to RDS.

A) Access S3 completely :- we have to add permission to the policy in permissions by selecting the service (S3) and allow the effect and allow all actions to give S3 Full Access.



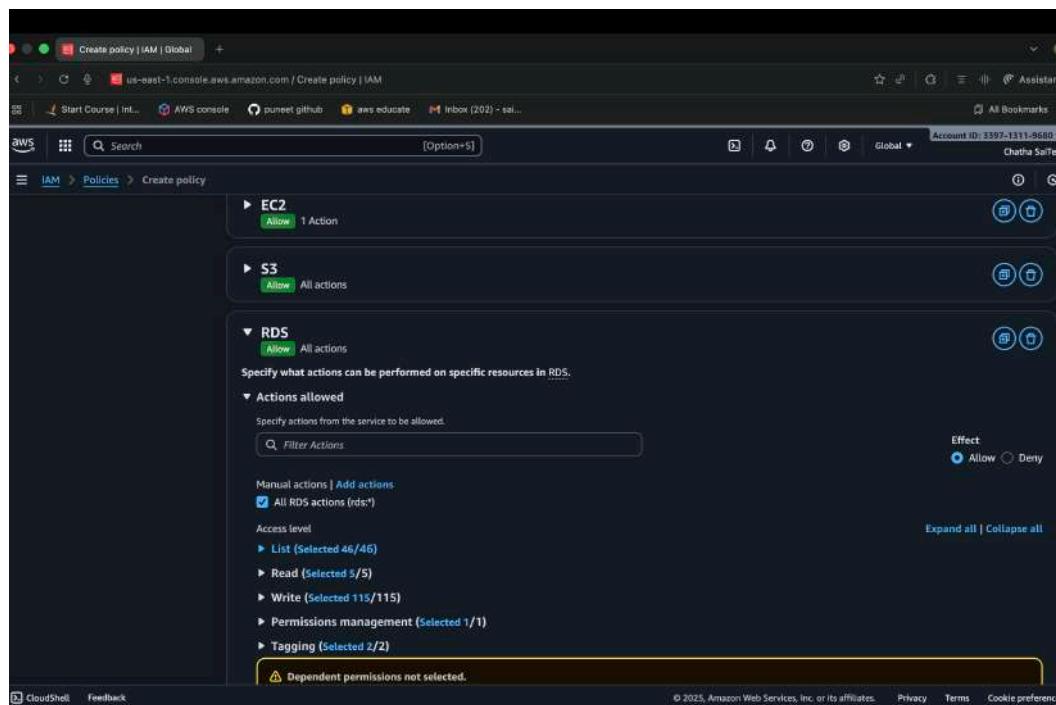
Full access to S3

B) Only create EC2 instances:- Now we have to add the permissions to only create Ec2 Instances, so select the service in visual editor and go to actions and enable “RunInstances”(write) .



Only create EC2 instances

C) Full access to RDS :- we have to give Full access to RDS ,select the service RDS in visual editor and go to actions and enable to all Actions to give full access to the policy.



The screenshot shows the AWS IAM console with the policy 'Policy1' selected. The left sidebar shows navigation options like Identity and Access Management (IAM), User groups, Users, Roles, Policies, and more. The main content area displays the 'Policy details' section with creation and editing information. Below this is the 'Permissions' tab, which lists three services with their access levels: EC2 (Limited: Write), RDS (Full access), and S3 (Full access). A search bar and a link to 'Show remaining 445 services' are also present.

Policy1 summary

Step 3:- Now we have to create another policy - policy 2 which allows users to access cloud watch, billing completely and users can only list EC2 and S3 resources

A)Access CloudWatch and billing completely:- By clicking create policy we have to specify the permissions of cloud watch and billing completely so in visual editor select cloud watch and enable all actions , click on add permission and select Billing then enable all actions .

The screenshot shows the 'Create policy | IAM | Global' interface. The 'Specify permissions' step is selected. In the 'Policy editor', under the 'CloudWatch' section, the 'Actions allowed' tab is active, showing 'Allow' selected. Under 'Access level', several actions are listed: 'List (Selected 7/7)', 'Read (Selected 21/21)', 'Write (Selected 25/25)', and 'Tagging (Selected 2/2)'. The 'Effect' is set to 'Allow'. A note at the top right says 'Specify what actions can be performed on specific resources in CloudWatch.'

Giving Full access to CloudWatch

The screenshot shows the 'Create policy | IAM | Global' interface. The 'Specify permissions' step is selected. In the 'Policy editor', under the 'Billing' section, the 'Actions allowed' tab is active, showing 'Allow' selected. Under 'Access level', several actions are listed: 'List (Selected 1/1)', 'Read (Selected 13/13)', 'Write (Selected 9/9)', 'Permissions management (Selected 5/3)', and 'Tagging (Selected 2/2)'. A note at the top right says 'Specify what actions can be performed on specific resources in Billing.'

Giving Full access to Billing

B) Can only list EC2 and S3 resources:- to provide these permissions we have to specify the service Ec2 and enable actions “DescribeInstance” to list all instances for s3 we have to enable “ListAllMyBuckets”

EC2
Allow 1 Action

Specify what actions can be performed on specific resources in EC2.

Actions allowed

Specify actions from the service to be allowed:

Q: describen

Effect
Allow

List

<input type="checkbox"/> DescribeInstances	Info
<input type="checkbox"/> DescribeInstanceAttribute	Info
<input type="checkbox"/> DescribeInstanceEventNotificationAttribute	Info
<input checked="" type="checkbox"/> DescribeInstances	Info
<input type="checkbox"/> DescribeInstanceEventWindows	Info
<input type="checkbox"/> DescribeInstanceConnectEndpoints	Info
<input type="checkbox"/> DescribeInstanceCreditSpecifications	Info
<input type="checkbox"/> DescribeInstanceImageMetadata	Info
<input type="checkbox"/> DescribeInstanceTypeOfferings	Info
<input type="checkbox"/> DescribeInstanceStatus	Info
<input type="checkbox"/> DescribeInstanceTypes	Info
<input type="checkbox"/> DescribeInstanceTopology	Info
<input type="checkbox"/> DescribeInternetGateways	Info

Resources

Specified resource ARNs for these actions.

All resources

Request conditions - optional

Actions on resources are allowed or denied only when these conditions are met.

+ Add more permissions

List Ec2 Instances

S3
Allow 1 Action

Specify what actions can be performed on specific resources in S3.

Actions allowed

Specify actions from the service to be allowed:

Q: Filter Actions

Effect
Allow

Manual actions | Add actions
 All S3 actions (s3:*)

Access level

List (Selected 1/16)

<input type="checkbox"/> All list actions	<input type="checkbox"/> ListAccessGrants	Info	
<input type="checkbox"/> ListAccessPoints	Info	<input type="checkbox"/> ListAccessGrantsInstances	Info
<input type="checkbox"/> ListBucket	Info	<input type="checkbox"/> ListAccessPointsForObjectLambda	Info
<input type="checkbox"/> ListCallerAccessGrants	Info	<input type="checkbox"/> ListBucketMultipartUploads	Info
<input type="checkbox"/> ListMultiRegionAccessPoints	Info	<input type="checkbox"/> ListJobs	Info
<input type="checkbox"/> ListTagsForResource	Info	<input type="checkbox"/> ListStorageLensConfigurations	Info
		<input checked="" type="checkbox"/> ListAllMyBuckets	Info
		<input type="checkbox"/> ListBucketVersions	Info
		<input type="checkbox"/> ListMultipartUploadParts	Info
		<input type="checkbox"/> ListStorageLensGroups	Info

Read (61)
Write (49)

Expand all | Collapse all

List S3 resources

The screenshot shows the 'Create policy' page in the AWS IAM console. The policy is titled 'Create policy' and is set to 'Global'. The 'Permissions defined in this policy' section lists four services with their access levels and resources:

Service	Access level	Resource	Request condition
Billing	Full access	All resources	None
CloudWatch	Full access	All resources	None
EC2	Limited: List	All resources	None
S3	Limited: List	All resources	None

Below this, there is a section for 'Add tags - optional' which is currently empty. At the bottom right, there are 'Cancel', 'Previous', and 'Create policy' buttons.

Policy 2 summary

Step 4:- Now we have to attach the policy 1 to DevTeam which we created in previous assignment ,now we select the policy 1, go to actions then click on attach then we can see the user group we created.

The screenshot shows the AWS IAM Policies page. On the left, there's a navigation sidebar with options like Dashboard, Access management, Policies, Access reports, and more. The main area displays a table titled "Policies (1/1398)". The table has columns for Policy name, Type, Used as, and Description. It lists two entries: "Policy1" and "Policy2", both of which are "Customer managed" and have "None" listed under "Used as". At the top right of the table, there are buttons for Actions (with Attach highlighted), Delete, and Create policy. Below the table, there are search and filter options.

Go to Actions click on attach

The screenshot shows the "Attach as a permissions policy" page. The URL is "us-east-1.console.aws.amazon.com/Attach policy | IAM". The page title is "Attach policy | IAM | Global". The sub-navigation shows "IAM > Policies > Policy1 > Attach policy". The main content area is titled "Attach as a permissions policy" with the sub-instruction "To define permissions for an IAM identity (user, user group, or role), attach a policy to it." Below this, there's a section titled "IAM Entities (1/6)" with the sub-instruction "Entities are IAM users, user groups and roles.". A table lists entities: Dev1, Dev2, DevTeam (which is selected and highlighted), OpsTeam, Test1, and Test2. The table includes columns for Entity name, Entity type, and a checkbox column. At the bottom right are "Cancel" and "Attach policy" buttons.

Selecting Dev Team

The screenshot shows the AWS IAM User Groups page. On the left, there's a navigation sidebar with options like Dashboard, Access management (User groups, Roles, Policies, Identity providers, Account settings, Root access management), Access reports (Resource analysis, Unused access, Analyzer settings, Credential report, Organization activity, Service control policies), and CloudShell/Feedback. The main content area is titled 'DevTeam' and shows the 'Summary' tab. It displays the user group name 'DevTeam', creation time 'October 12, 2025, 12:44 (UTC+05:30)', and ARN 'arn:aws:iam::339713119680:group/DevTeam'. Below this, there are tabs for 'Users' (2), 'Permissions' (selected), and 'Access Advisor'. Under 'Permissions', it says 'Permissions policies (1) Info' and shows a table with one policy named 'Policy1' (Customer managed). There are buttons for 'Simulate', 'Remove', and 'Add permissions'.

Policy1 added to DevTeam

Step 5:- now we have to attach the policy2 to OpsTeam ,select the policy2 click on action then attach it.

The screenshot shows the AWS IAM Policies page. The left sidebar is identical to the previous screenshot. The main content area is titled 'Policies (1/1398) Info' and describes a policy as an object in AWS that defines permissions. It shows a table with two entries: 'Policy1' (Customer managed, Used as 'Permissions policy (1)'), and 'Policy2' (Customer managed, Used as 'None'). Above the table, there are buttons for 'Actions' (with 'Attach' highlighted in orange), 'Delete', and 'Create policy'. A 'Filter by Type' dropdown is set to 'Customer managed'.

Go to Actions click on attach

The screenshot shows the 'Attach as a permissions policy' step in the AWS IAM console. The 'Entity name' dropdown is set to 'All types'. The 'OpsTeam' user group is selected and highlighted with a blue border. At the bottom right are 'Cancel' and 'Attach policy' buttons.

Selecting OpsTeam

The screenshot shows the 'OpsTeam | IAM | Global' page. The 'Permissions' tab is selected under the 'User groups' section. A table lists one managed policy: 'Policy2' (Customer managed). The ARN of the user group is also visible.

Policy 2 added to OpsTeam