

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 resource
3. Attach policy number 1 to the Dev Team from task 1
4. Attach policy number 2 to Ops Team for task 1

*Policy 1

The screenshot shows the AWS IAM console 'Create policy' page. The 'Policy name' field is filled with 'policies1'. The 'Permissions defined in this policy' section shows a table with three services: EC2, RDS, and S3, all with 'Full access' and 'All resources'.

Service	Access level	Resource	Request condition
EC2	Limited: Write	All resources	None
RDS	Full access	All resources	None
S3	Full access	All resources	None

policy 2

The screenshot shows the 'Create policy' page in the AWS IAM console. The policy name is 'Policy2'. The description field is empty. The 'Permissions defined in this policy' section shows a table with 4 services: Billing Console, CloudWatch, EC2, and S3. The table has columns for Service, Access level, Resource, and Request condition.

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

Add policy 1 in Dev

The screenshot shows the 'Policies attached to this user group' page in the AWS IAM console. The user group is 'Dev'. The 'Permissions policies (1)' section shows a table with 1 policy: policies1. The table has columns for Policy name, Type, and Attached entities.

Policy name	Type	Attached entities
policies1	Customer managed	1

Add policy 2 in ops

The screenshot shows the AWS IAM console interface. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, User groups, Users, Roles, Policies, Identity providers, Account settings, Access reports, Access Analyzer, External access, Unused access, Analyzer settings, and Credential report. The main content area is titled 'Ops' and shows the 'Permissions' tab. A green banner at the top indicates 'Policies attached to this user group.' The 'Summary' section shows the user group name 'Ops', creation time 'April 17, 2024, 18:17 (UTC+05:30)', and ARN 'arn:aws:iam::851725268382:group/Ops'. The 'Permissions policies (1)' section shows a table with one policy attached: 'Policy2' (Customer managed) with 1 attached entity. The table has columns for Policy name, Type, and Attached entities.

Ops [info](#) [Delete](#)

Summary [Edit](#)

User group name: Ops
Creation time: April 17, 2024, 18:17 (UTC+05:30)
ARN: arn:aws:iam::851725268382:group/Ops

Users (2) **Permissions** Access Advisor

Permissions policies (1) [info](#) [Refresh](#) [Simulate](#) [Remove](#) [Add permissions](#)

You can attach up to 10 managed policies.

Filter by Type: All types

<input type="checkbox"/>	Policy name ?	Type	Attached entities
<input type="checkbox"/>	Policy2	Customer managed	1

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)