

Module-8: IAM Assignment - 2

You have been asked to:

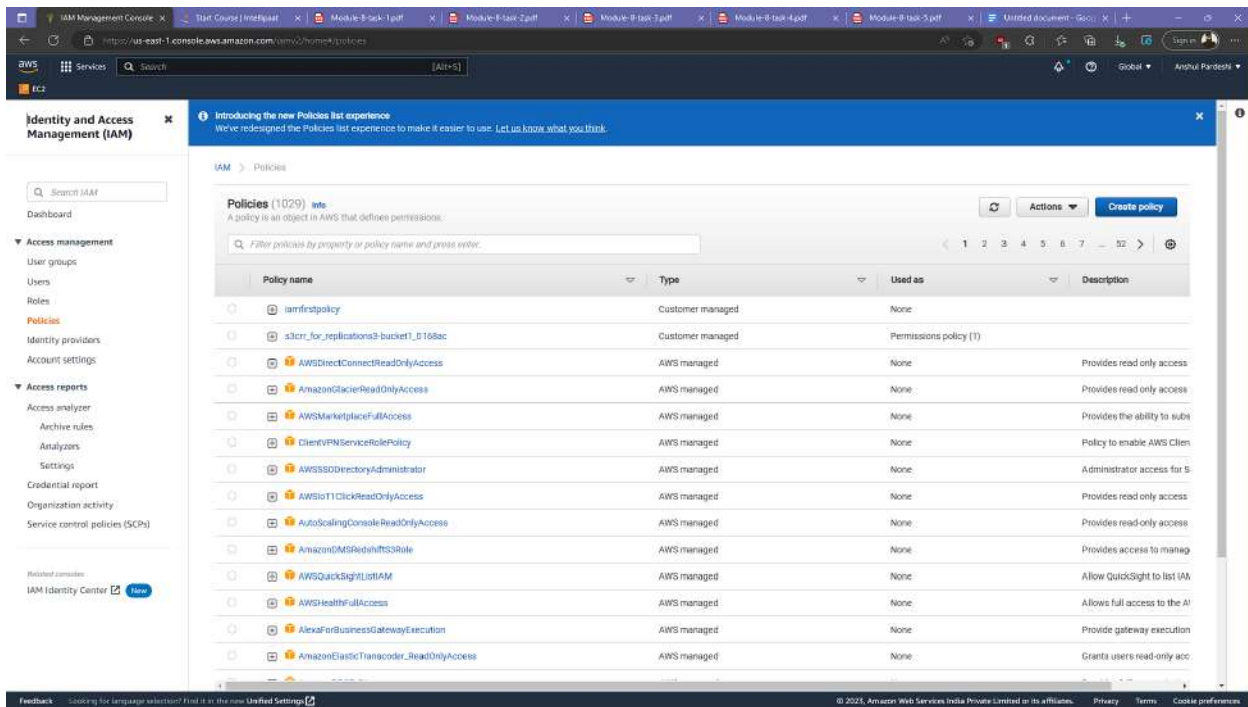
1. Create a policy number 1 which lets the users to:
 - a. Access S3 completely.
 - b. Only create EC2 instances.
 - c. And full access to RDS.
2. Create a policy number 2 which allows the users to:
 - a. Access CloudWatch and Billing completely.
 - b. And can only list EC2 and S3 resources.
3. Attach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

Go to the IAM dashboard first.

The screenshot displays the AWS IAM dashboard in a web browser. The left sidebar shows the navigation menu with options like Dashboard, Access management, Access reports, and Related services. The main content area is titled 'IAM dashboard' and includes a 'Security recommendations' section with a warning to 'Add MFA for root user'. Below this, a 'What's new' section lists recent updates. The 'IAM resources' section provides a summary of current resources: 2 user groups, 4 users, 19 roles, 2 policies, and 0 identity providers. On the right, the 'AWS Account' section shows the account ID and alias. The bottom of the page features a footer with copyright information and links to privacy, terms, and cookie preferences.

Resource Type	Count
User groups	2
Users	4
Roles	19
Policies	2
Identity providers	0

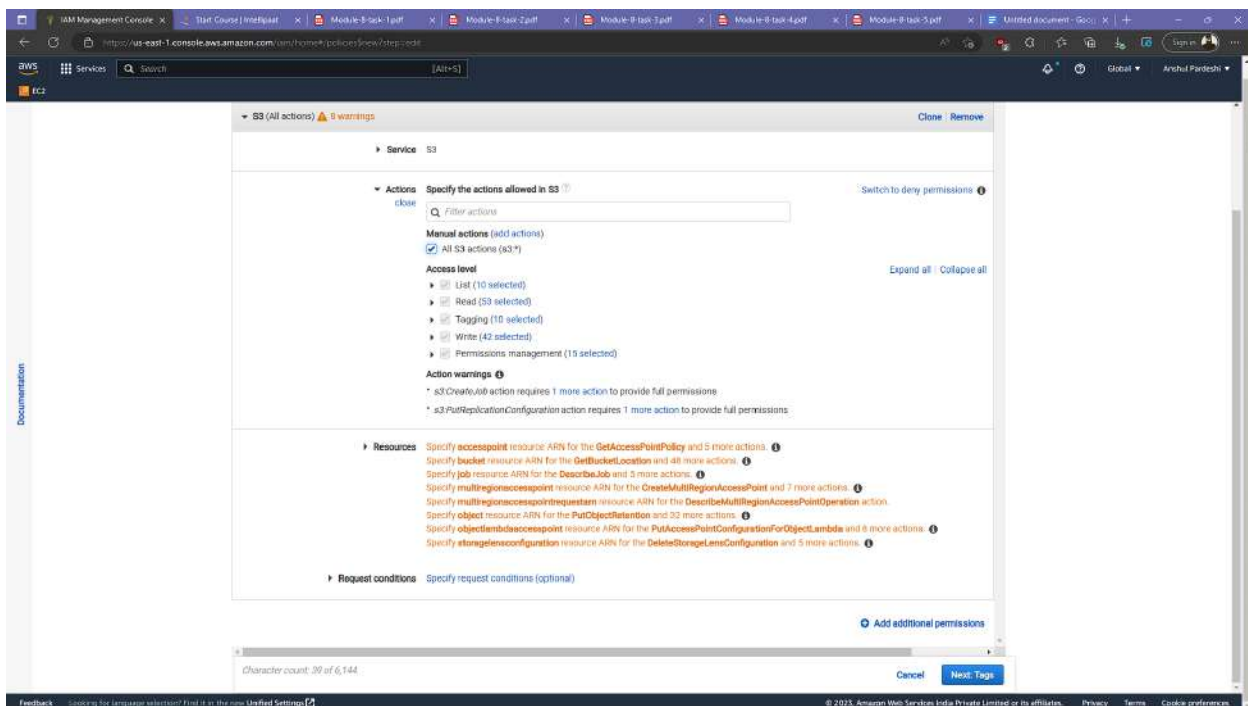
Click on create policy.



The screenshot shows the AWS IAM console's 'Policies' page. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and Related services. The main content area displays a list of 1029 policies. A 'Create policy' button is visible in the top right corner of the policies list.

Policy name	Type	Used as	Description
iamfirstpolicy	Customer managed	None	
s3cm_for_replications3_bucket1_0168ac	Customer managed	Permissions policy (1)	
AWSDirectConnectReadOnlyAccess	AWS managed	None	Provides read only access
AmazonGlacierReadOnlyAccess	AWS managed	None	Provides read only access
AWSMarketplaceFullAccess	AWS managed	None	Provides the ability to sub
ClientVPMServiceRolePolicy	AWS managed	None	Policy to enable AWS Clie
AWSSSODirectoryAdministrator	AWS managed	None	Administrator access for S
AWSIoT1ClickReadOnlyAccess	AWS managed	None	Provides read only access
AutoScalingConsoleReadOnlyAccess	AWS managed	None	Provides read-only access
AmazonOMSGatewayFullAccess	AWS managed	None	Provides access to manag
AWSQuickSightIAM	AWS managed	None	Allow QuickSight to list IA
AWSHealthFullAccess	AWS managed	None	Allows full access to the A
AlexaForBusinessGatewayExecution	AWS managed	None	Provide gateway execution
AmazonElasticTranscoder_ReadOnlyAccess	AWS managed	None	Grants users read-only acc

Choose service as S3, Allow all actions and resources.



The screenshot shows the 'Create policy' wizard in the AWS IAM console. The 'Service' is set to S3. Under 'Actions', 'All S3 actions (s3*)' is selected. The 'Resources' section is also visible, showing a list of resource ARNs and their associated actions. The 'Request conditions' section is optional.

Service: S3

Actions: Specify the actions allowed in S3. [Switch to deny permissions](#)

Manual actions (add actions): ☒ All S3 actions (s3*)

Access level:

- ☒ List (10 selected)
- ☒ Read (53 selected)
- ☒ Tagging (10 selected)
- ☒ Write (42 selected)
- ☒ Permissions management (15 selected)

Action warnings:

- * s3:CreateJob action requires 1 more action to provide full permissions
- * s3:PutReplicationConfiguration action requires 1 more action to provide full permissions

Resources: Specify **accesspoint** resource ARN for the **GetAccessPointPolicy** and 5 more actions. [1](#)

- Specify **bucket** resource ARN for the **GetBucketLocation** and 48 more actions. [1](#)
- Specify **job** resource ARN for the **DescribeJob** and 3 more actions. [1](#)
- Specify **multiregionaccesspoint** resource ARN for the **CreateMultiRegionAccessPoint** and 7 more actions. [1](#)
- Specify **multiregionaccesspointrequestarn** resource ARN for the **DescribeMultiRegionAccessPointOperation** action. [1](#)
- Specify **object** resource ARN for the **PutObjectRetention** and 33 more actions. [1](#)
- Specify **objectlambdasaccesspoint** resource ARN for the **PutAccessPointConfigurationForObjectLambda** and 6 more actions. [1](#)
- Specify **storageglassconfiguration** resource ARN for the **DeleteStorageGlassConfiguration** and 5 more actions. [1](#)

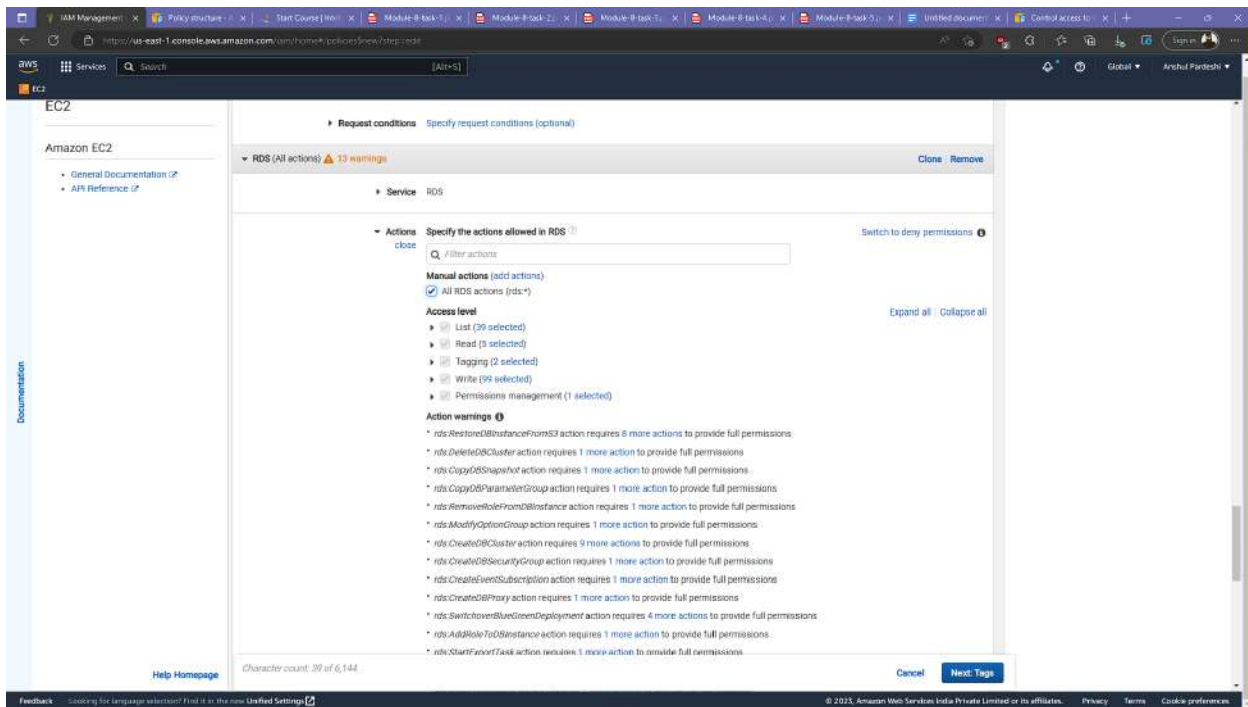
Request conditions: Specify request conditions (optional)

[Add additional permissions](#)

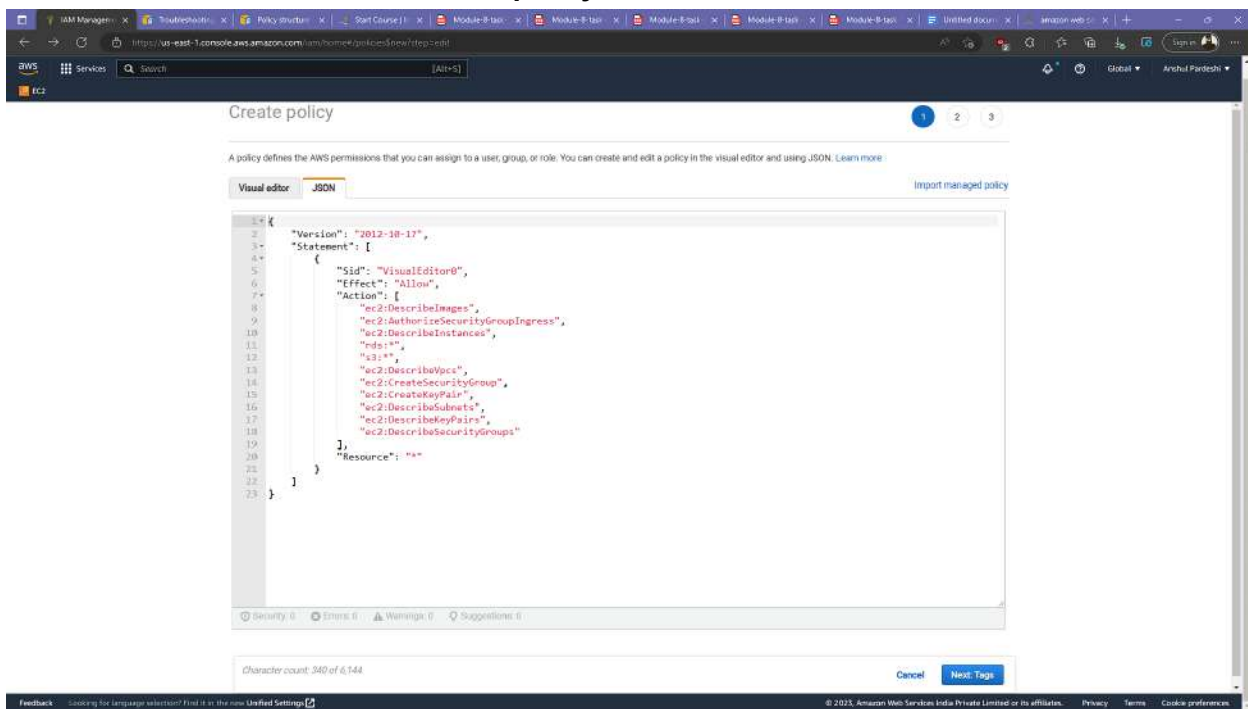
Character count: 39 of 6,144

[Cancel](#) [Next: Tags](#)

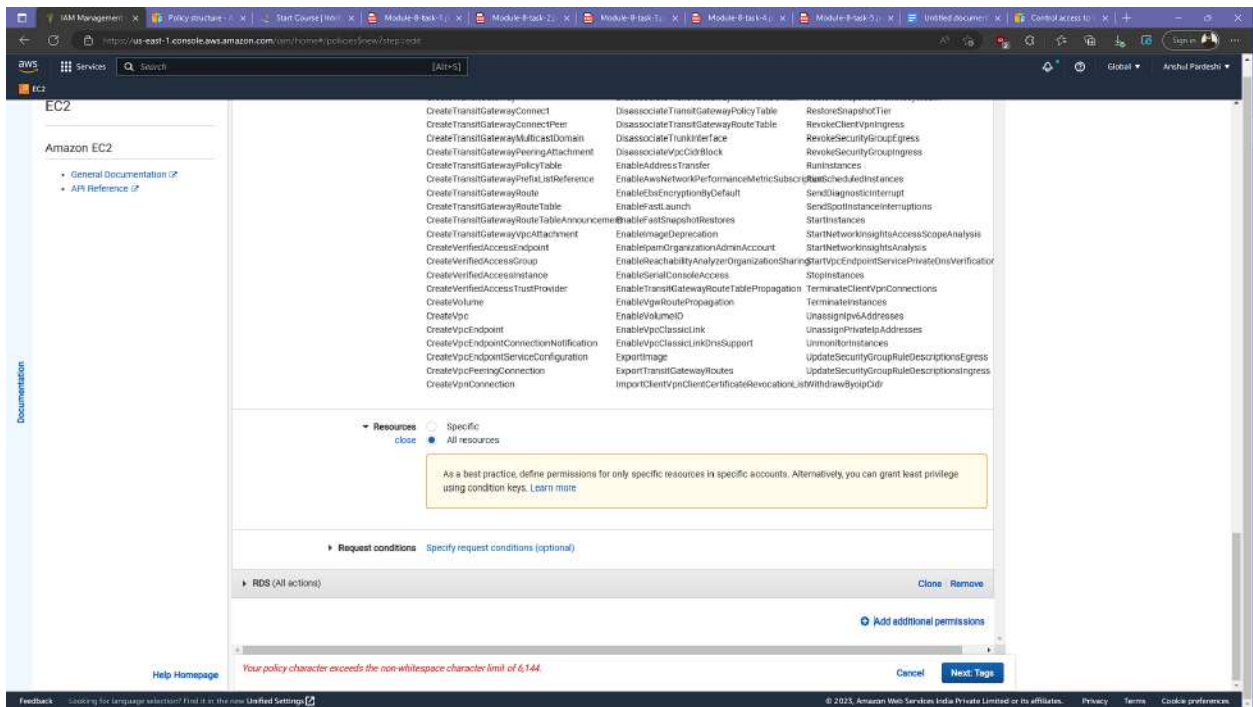
Select service as RDS and allow all actions and resources.



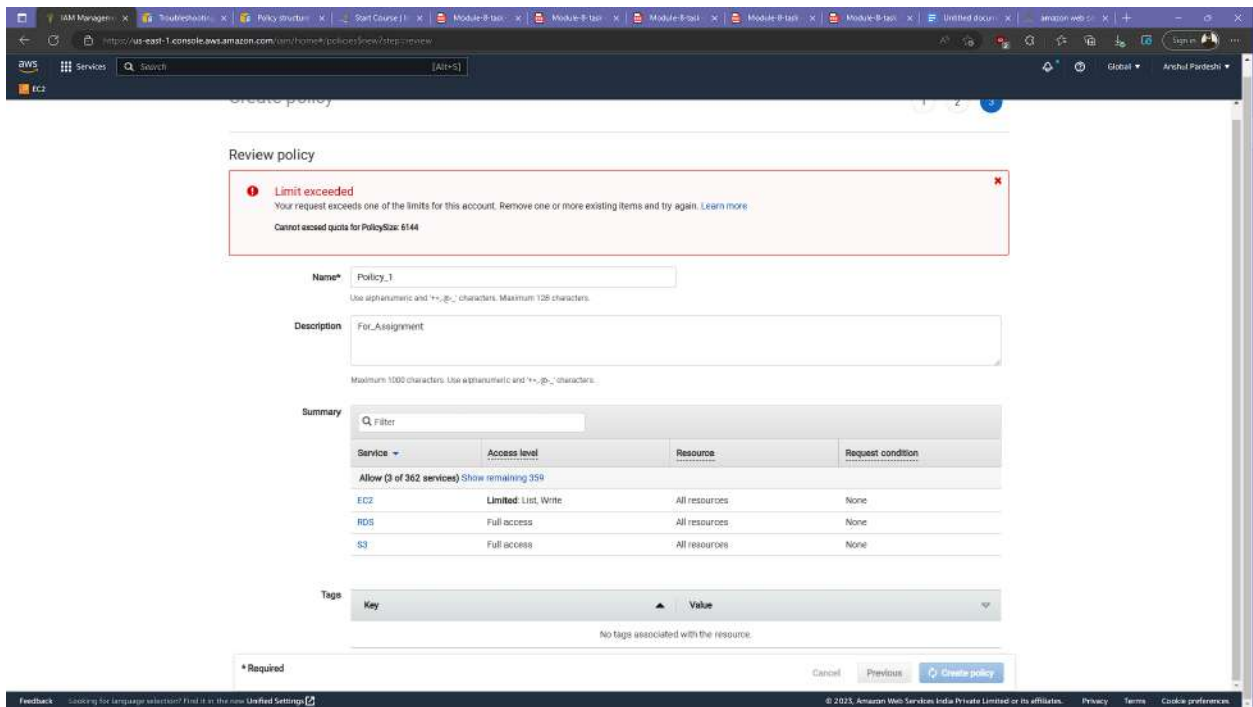
This is JSON policy to create EC2 instance.



Click on next.



This is the policy that is being created.



Let's create policy 2.

The screenshot shows the AWS IAM console's 'Policies' page. A green banner at the top states 'The policy Policy_1 has been created.' Below this, a table lists various policies. The 'Policy_1' policy is highlighted, showing it is a 'Customer managed' policy with no 'Used as' value and a description of 'For_Assignment'.

Policy name	Type	Used as	Description
iamfirstpolicy	Customer managed	None	
Policy_1	Customer managed	None	For_Assignment
x3cm_for_replications3-bucket1_0160ac	Customer managed	Permissions policy (1)	
AWSDirectConnectReadOnlyAccess	AWS managed	None	Provides read only access
AmazonElasticReadOnlyAccess	AWS managed	None	Provides read only access
AWSMarketplaceFullAccess	AWS managed	None	Provides the ability to sub
ClientVPMServiceRolePolicy	AWS managed	None	Policy to enable AWS Clie
AWSSSODirectoryAdministrator	AWS managed	None	Administrator access for S
AWSIoT1ClickReadOnlyAccess	AWS managed	None	Provides read only access
AutoScalingConsoleReadOnlyAccess	AWS managed	None	Provides read-only access
AmazonOMSRechtst3Rule	AWS managed	None	Provides access to manag
AWSQuickSightListIAM	AWS managed	None	Allow QuickSight to list IA
AWSHealthFullAccess	AWS managed	None	Allows full access to the A

Service is CloudWatch. Allow all actions and resources.

The screenshot shows the 'Create policy' wizard in the AWS IAM console. The 'Visual editor' tab is selected. The policy is named 'CloudWatch (All actions)'. The 'Service' is set to 'CloudWatch'. The 'Actions' are set to 'Manual actions'. The 'Resources' are set to 'All resources'. A note states: 'As a best practice, define permissions for only specific resources in specific accounts. Alternatively, you can grant least privilege using condition keys. Learn more'. The 'Request conditions' section is empty. The 'Add additional permissions' button is visible. The character count is 118 of 6,144.

The screenshot shows the 'Add permissions' wizard in the AWS IAM console. The 'Actions' step is selected, and the 'Manual actions' section is expanded. A yellow tip box provides guidance on defining permissions. The 'Resources' section shows 'All resources' selected. The 'Request conditions' section is optional. The 'Billing' section is expanded, showing 'Service: Billing'. The 'Actions' section is expanded, showing 'Specify the actions allowed in Billing'. The 'Access level' section shows 'Read (9 selected)' and 'Write (4 selected)'. The 'Resources' section shows 'All resources have been selected for you because this service does not allow you to choose specific resources.' The 'Request conditions' section is optional. The 'Add additional permissions' button is visible at the bottom right.

Next

Character count: 6,811 of 6,144

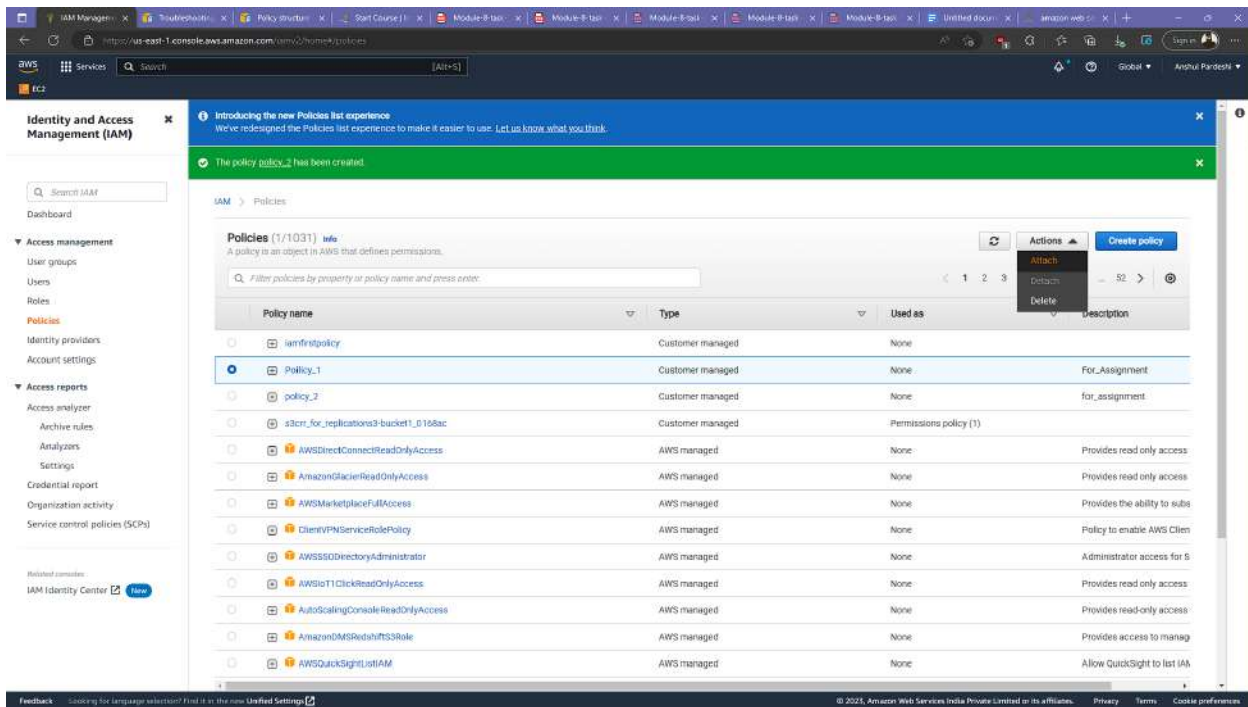
Service	Access level	Resource	Request condition
Billing	Full access	All resources	None
CloudWatch	Full access	All resources	None
EC2	Full List	All resources	None
S3	Full List	All resources	None

This is the policy summarized.

Character count: 6,811 of 6,144

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

Attach policy1.



Identity and Access Management (IAM)

Introducing the new Policies list experience. We've redesigned the Policies list experience to make it easier to use. Let us know what you think.

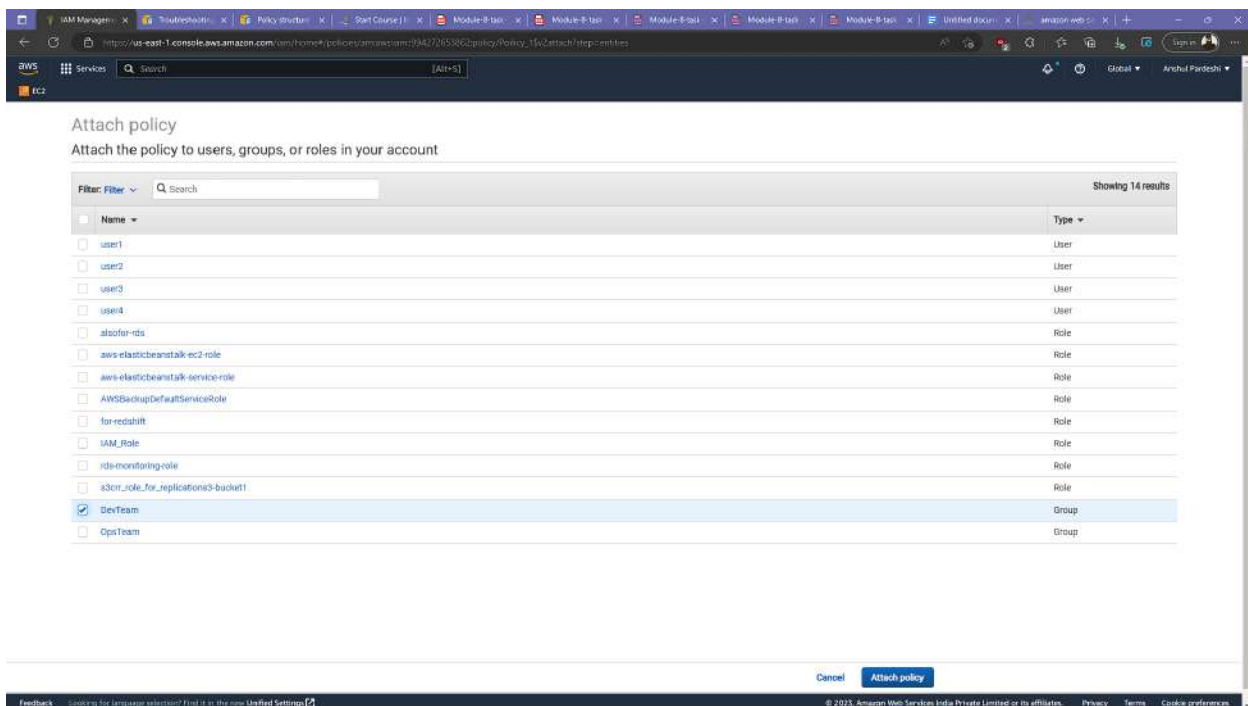
The policy policy_2 has been created.

IAM > Policies

Policies (1/1031) info
A policy is an object in AWS that defines permissions.
Filter policies by property or policy name and press enter.

Policy name	Type	Used as	Description
iamfirstpolicy	Customer managed	None	
Policy_1	Customer managed	None	For_Assignment
policy_2	Customer managed	None	for_assignment
s3out_for_replications3-bucket1-D166ac	Customer managed	Permissions policy (1)	
AWSDirectConnectReadOnlyAccess	AWS managed	None	Provides read only access
AmazonGlacierReadOnlyAccess	AWS managed	None	Provides read only access
AWSMarketplaceFullAccess	AWS managed	None	Provides the ability to subs
ClientVPMServicerolePolicy	AWS managed	None	Policy to enable AWS Clie
AWSSSODirectoryAdministrator	AWS managed	None	Administrator access for S
AWSIoT1ClickReadOnlyAccess	AWS managed	None	Provides read only access
AutoScalingConsoleReadOnlyAccess	AWS managed	None	Provides read-only access
AmazonDMSRedshiftS3Role	AWS managed	None	Provides access to manag
AWSQuickSightListIAM	AWS managed	None	Allow QuickSight to list IA

To DevTeam



Attach policy

Attach the policy to users, groups, or roles in your account

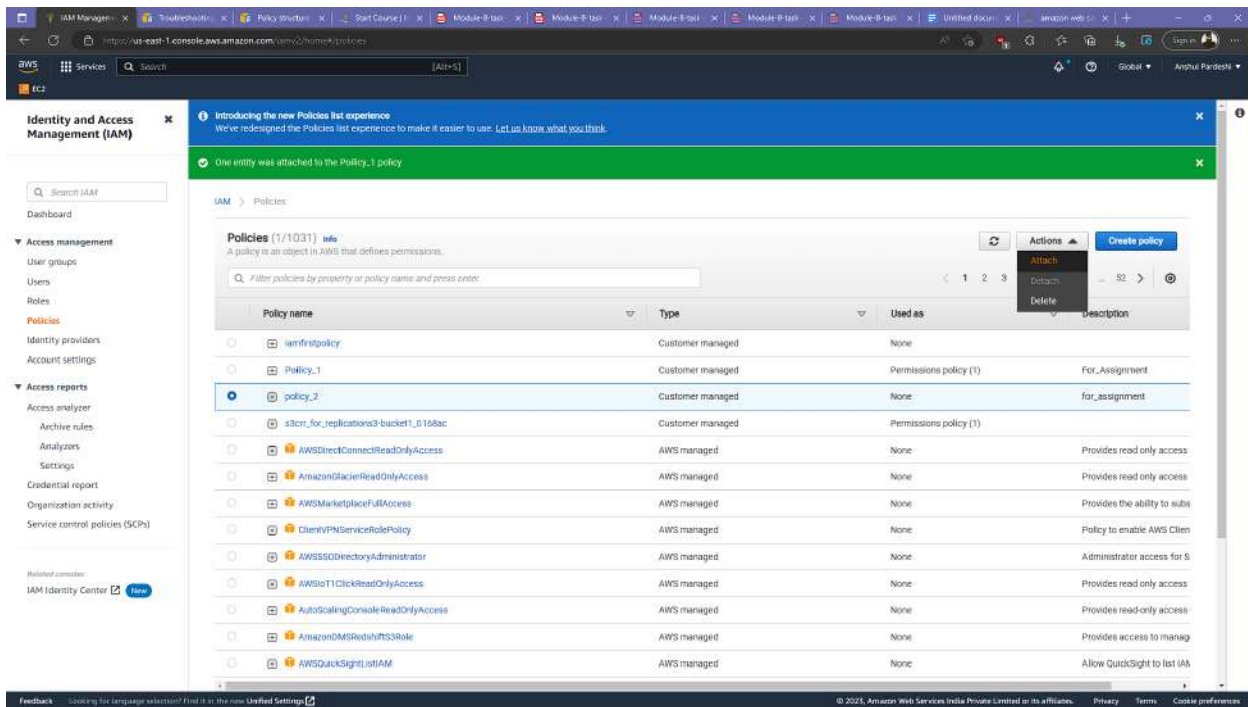
Filter: Filter Search

Showing 14 results

Name	Type
user1	User
user2	User
user3	User
user4	User
alsofer-rds	Role
aws-elasticbeanstalk-ec2-role	Role
aws-elasticbeanstalk-service-role	Role
AWSBackupDefaultServiceRole	Role
for-redshift	Role
IAM_Role	Role
rds-monitoring-role	Role
s3out_for_replications3-bucket1	Role
DevTeam	Group
OpsTeam	Group

Cancel Attach policy

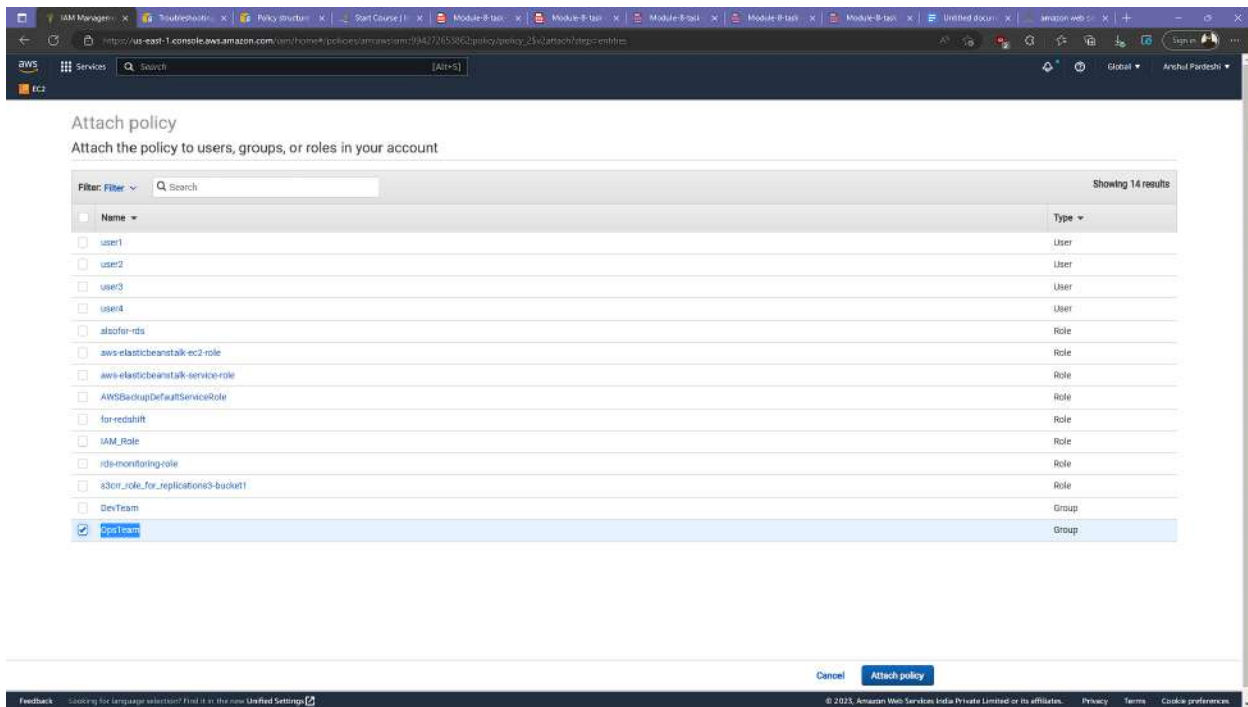
Attach policy2



The screenshot shows the AWS IAM console with the 'Policies' list. A notification at the top states 'One entity was attached to the Policy_1 policy'. The 'policy_2' policy is selected. The 'Attach' button in the Actions menu is highlighted.

Policy name	Type	Used as	Description
iamfirstpolicy	Customer managed	None	
Policy_1	Customer managed	Permissions policy (1)	For_Assignment
policy_2	Customer managed	None	for_assignment
s3out_for_replications3-bucket1_0168ac	Customer managed	Permissions policy (1)	
AWSDirectConnectReadOnlyAccess	AWS managed	None	Provides read only access
AmazonGlacierReadOnlyAccess	AWS managed	None	Provides read only access
AWSMarketplaceFullAccess	AWS managed	None	Provides the ability to subs
ClientVPMServicerolePolicy	AWS managed	None	Policy to enable AWS Clie
AWSSSODirectoryAdministrator	AWS managed	None	Administrator access for S
AWSIoT1ClickReadOnlyAccess	AWS managed	None	Provides read only access
AutoScalingConsoleReadOnlyAccess	AWS managed	None	Provides read-only access
AmazonOMSRedshiftS3Role	AWS managed	None	Provides access to manag
AWSQuickSightListIAM	AWS managed	None	Allow QuickSight to list IA

To OpsTeam.



The screenshot shows the 'Attach policy' dialog in the AWS IAM console. The title is 'Attach policy' and the subtitle is 'Attach the policy to users, groups, or roles in your account'. A list of 14 entities is shown, with 'OpsTeam' selected. The 'Attach policy' button is highlighted.

Name	Type
user1	User
user2	User
user3	User
user4	User
alsofor-rds	Role
aws-elasticbeanstalk-ec2-role	Role
aws-elasticbeanstalk-service-role	Role
AWSBackupDefaultServiceRole	Role
for-redshift	Role
IAM_Role	Role
rds-monitoring-role	Role
s3out_for_replications3-bucket1	Role
DevTeam	Group
OpsTeam	Group