

Module 2: Security Management in AWS

Demo Document 3

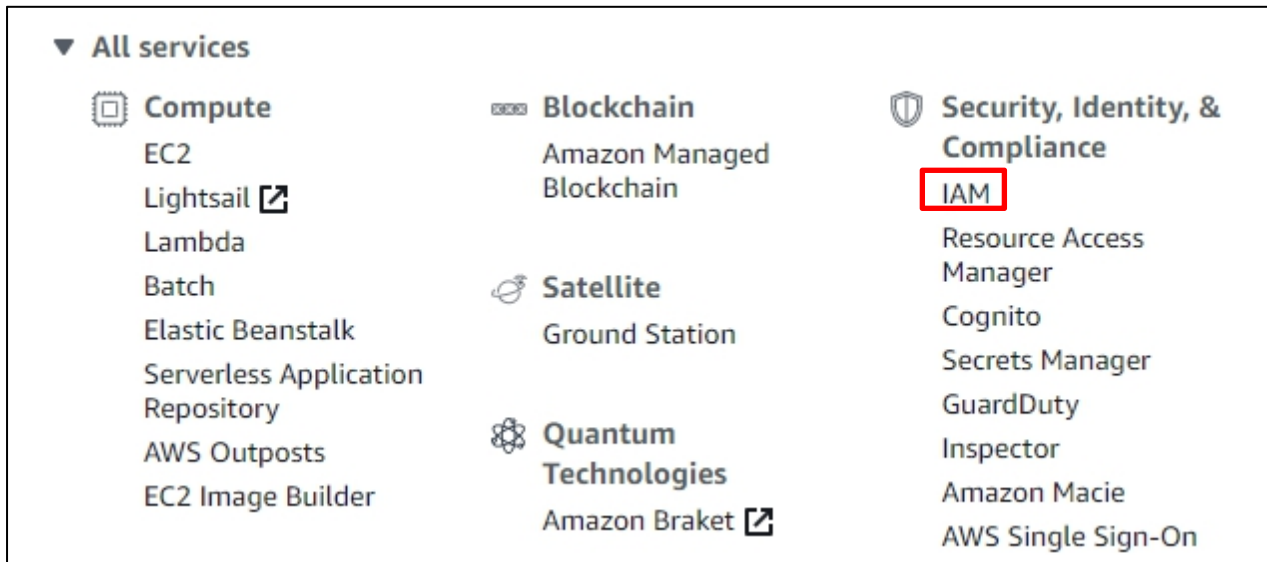
edureka!

edureka!

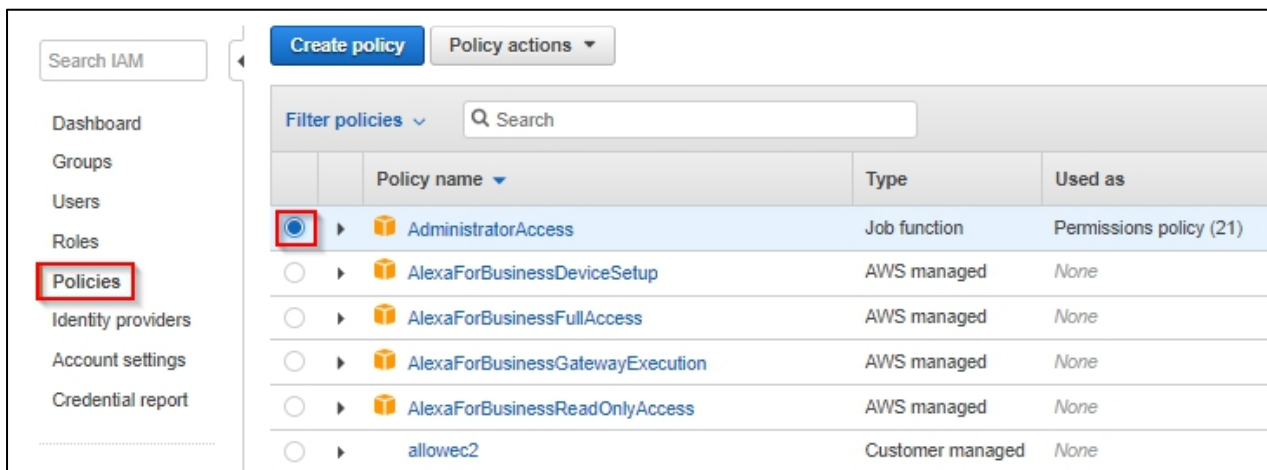
© Brain4ce Education Solutions Pvt. Ltd.

Creating Policies for New User to Have All Admin or Limited Privileges

Step1: Go to the AWS Management Console and select **IAM** under Security, Identity & Compliance.



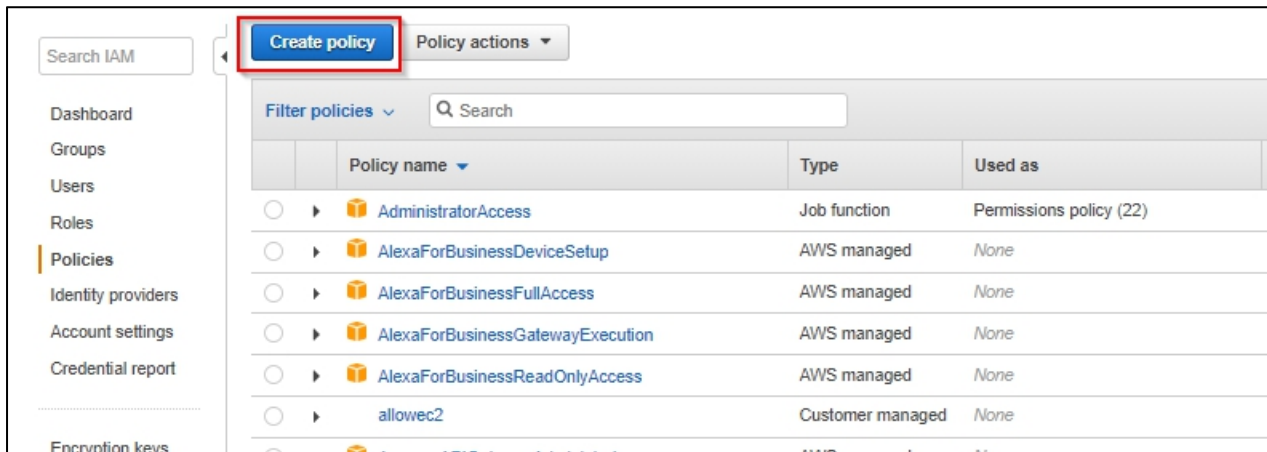
Step2: Creating Policies for New User: Move to **Policies** section under IAM and select **AdministratorAccess**. (By attaching this policy, the user gets the admin access to all the services)



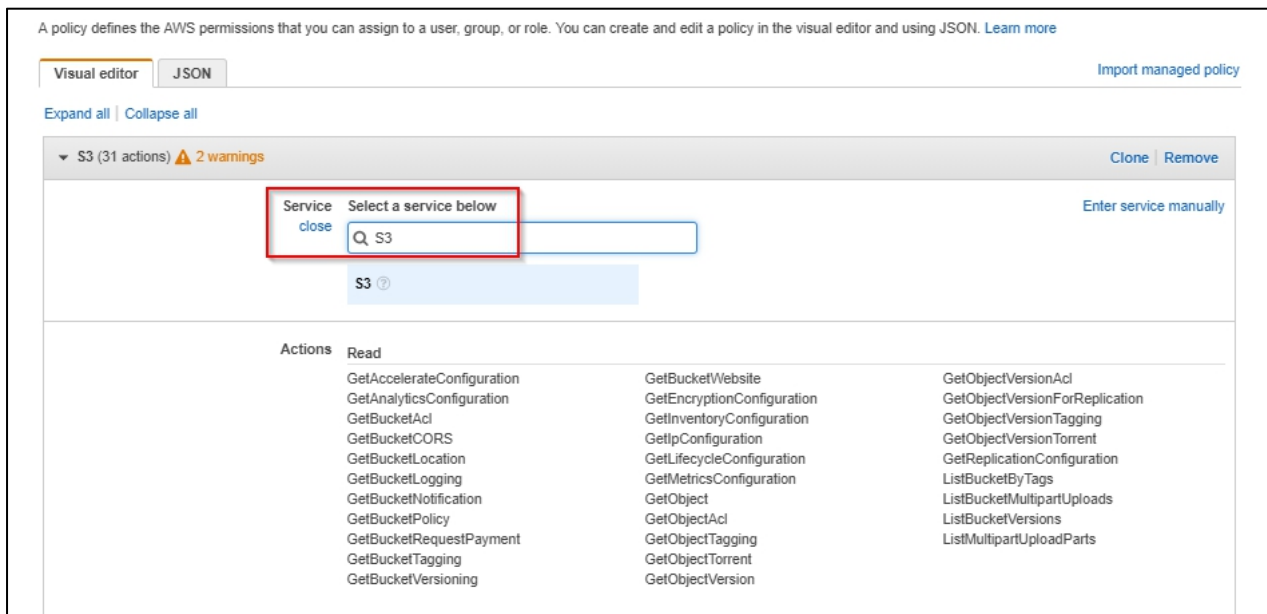
Note: To provide limited access to the user, you can create such a policy and attach it to the user.

For example, let us create a policy that provides the user the permissions of only the **list and read** to all objects in an Amazon S3.

Step-3: Go to **Policies** and click on **Create policy**.



Step-4: Go to **Visual editor** under **Service** and choose **S3** service.



Step-5: Under **Action**, you can choose the action you want to perform. For now, let's select **List** and **Read**.

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor JSON [Import managed policy](#)

[Expand all](#) | [Collapse all](#)

▼ S3 (34 actions) ⚠ 2 warnings [Clone](#) [Remove](#)

Service S3

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

Manual actions [\(add actions\)](#)

☐ All S3 actions (s3:*)

Access level [Expand all](#) | [Collapse all](#)

☒ List (3 selected)

- ☒ HeadBucket ⓘ
- ☒ ListAllMyBuckets ⓘ
- ☒ ListBucket ⓘ

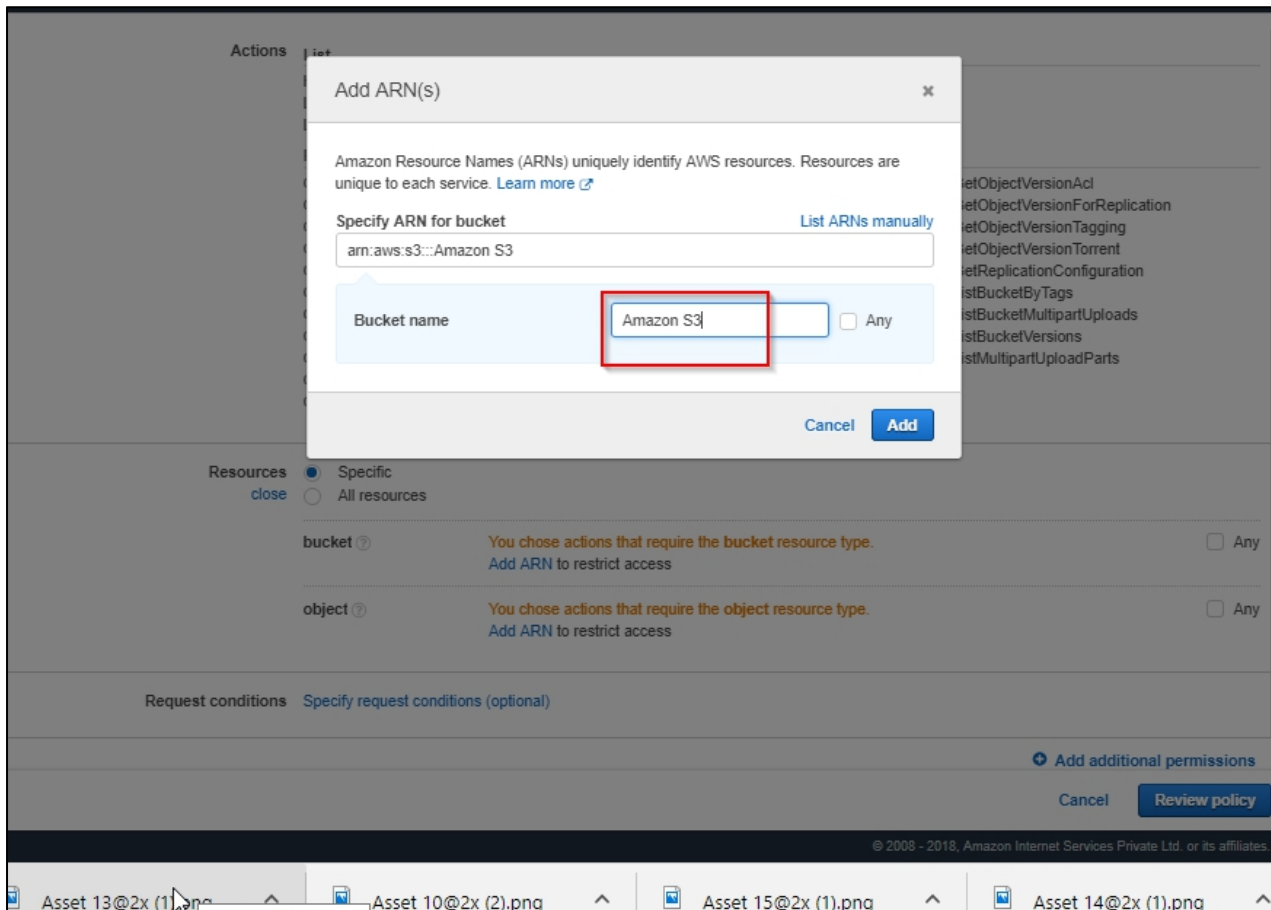
▶ ☒ Read (31 selected)

▶ ☐ Write

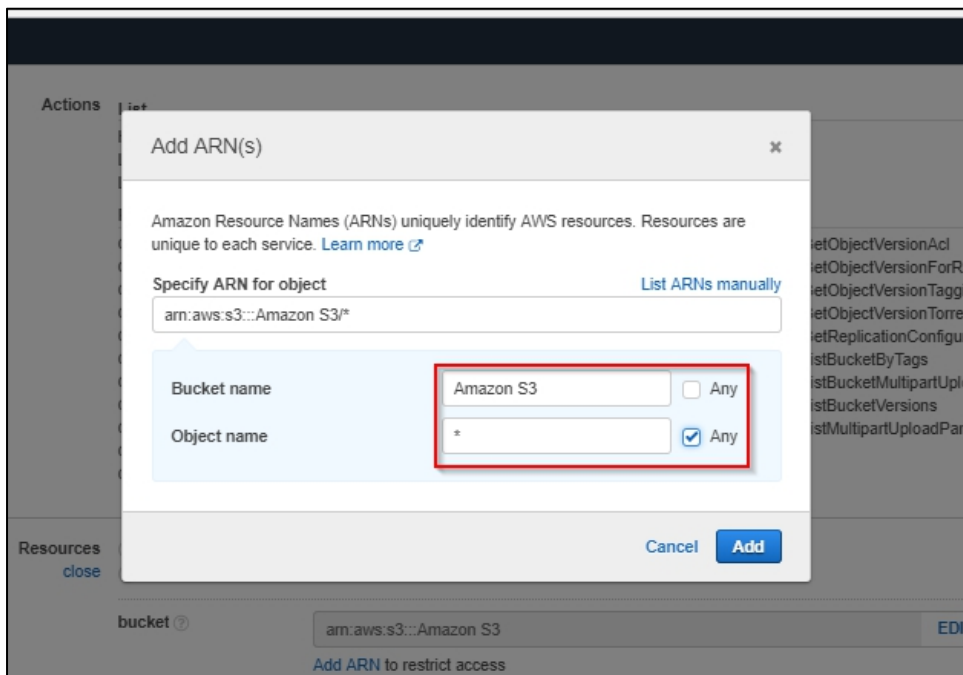
Step-6: You may find specific errors in between. To get rid of them, move to resources at the bottom; just beside the bucket, click on **Add ARN**, and specify ARN.

▼ Resources [close](#) ☒ Specific ☐ All resources

accesspoint ⓘ	Specify accesspoint resource ARN for the GetAccessPointPolicy and 1 more action. ⓘ Add ARN to restrict access	<input type="checkbox"/> Any
bucket ⓘ	Specify bucket resource ARN for the GetBucketLocation and 22 more actions. ⓘ Add ARN to restrict access	<input type="checkbox"/> Any
job ⓘ	Specify job resource ARN for the DescribeJob action. Add ARN to restrict access	<input type="checkbox"/> Any
object ⓘ	Specify object resource ARN for the ListMultipartUploadParts and 11 more actions. ⓘ Add ARN to restrict access	<input type="checkbox"/> Any



Step-7: Specify Object ARN and click on **Review policy**.



Step-8: Specify name and description and click on **Create Policy**.

Review policy

Name* Use alphanumeric and '+', '@', '-' characters. Maximum 128 characters.

Description Maximum 1000 characters. Use alphanumeric and '+', '@', '-' characters.

Summary

Service	Access level	Resource	Request condition
Allow (1 of 144 services) Show remaining 143			
S3	Full: List, Read	Multiple	None

* Required

[Cancel](#) [Previous](#) [Create policy](#)

Step-9: If the policy is created successfully, it will then be added to the policy list.

Search IAM

Dashboard
Groups
Users
Roles
Policies
Identity providers
Account settings
Credential report

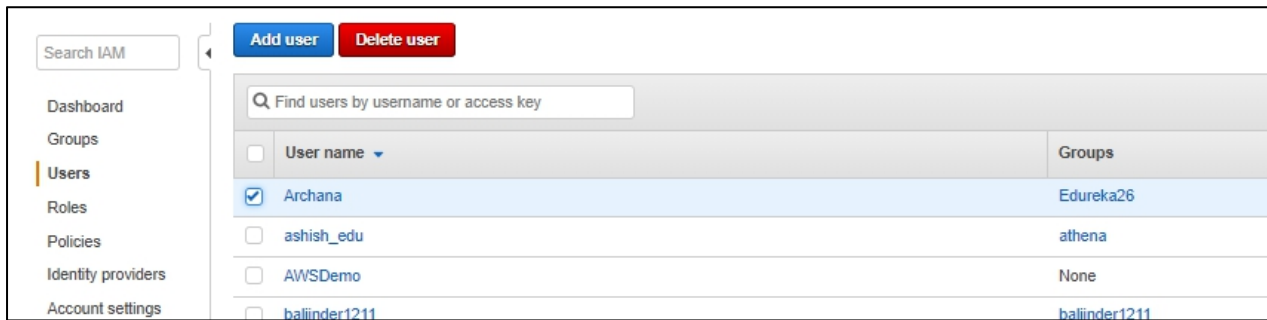
✓ awss3bucketpolicy has been created.

[Create policy](#) [Policy actions](#)

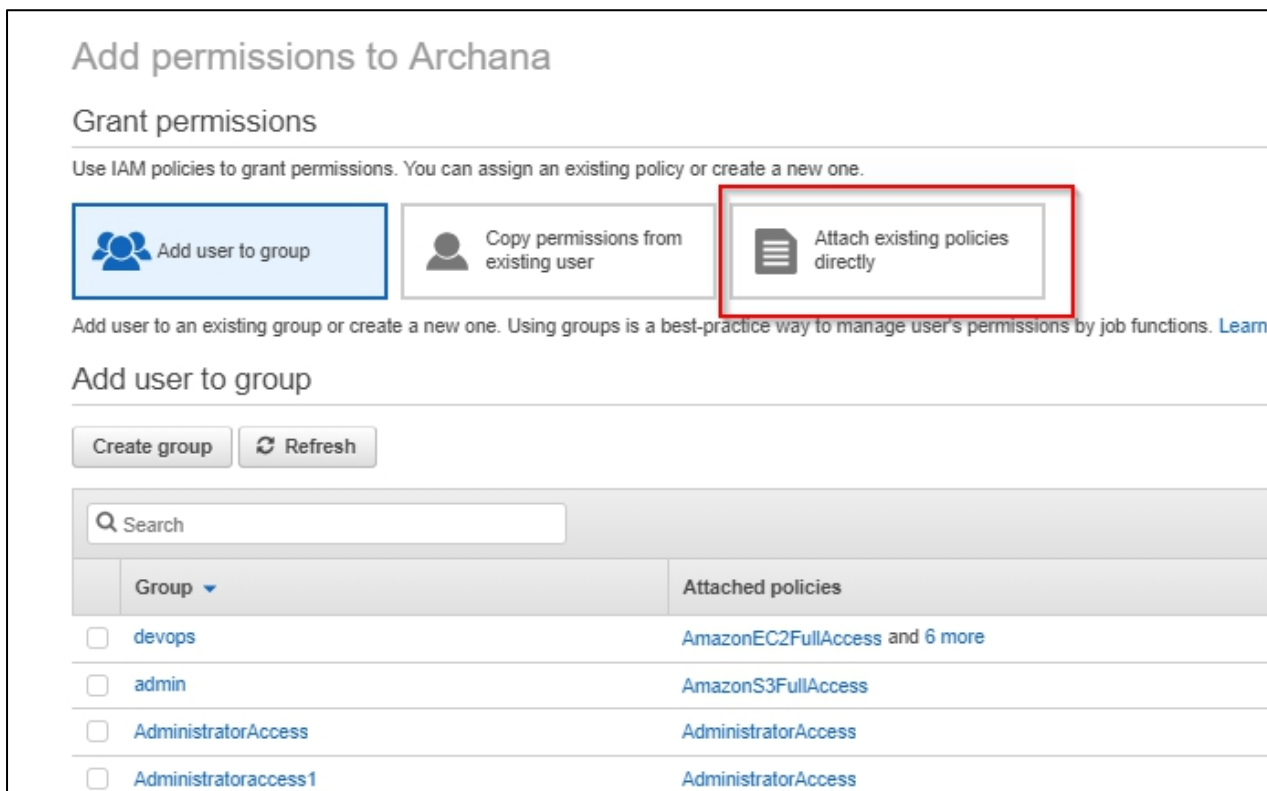
Filter policies

	Policy name	Type	Used as	Description
<input checked="" type="radio"/>	awss3bucketpolicy	Customer managed	None	allows to list and read the s3 objects

Step-10: Go to **users** and attach the **policy** to a user.



Step-11: Click on **Add Permission**, and select the **Policy attach option**.



Step-12: Attach the created policy and click on **Next Review**.

Add permissions to Archana

Grant permissions

Use IAM policies to grant permissions. You can assign an existing policy or create a new one.

Add user to group

Copy permissions from existing user

Attach existing policies directly

Create policy

Filter policies

	Policy name	Type	Used as	Description
<input checked="" type="checkbox"/>	awss3bucketpolicy	Customer managed	None	allows to list and read the s3 objects

Step-13: Click on **Add Permission** to see that the policy is attached to the user. Now, the user can only read and list the **S3 bucket**.

Users > Archana

Summary

User ARN: `arn:aws:iam::245376966395:user/Archana`

Path: `/`

Creation time: 2018-08-24 09:20 UTC+0530

Permissions Groups (1) Security credentials Access Advisor

▼ Permissions policies (1 policy applied)

[Add permissions](#)

Policy name
Attached directly
▶ awss3bucketpolicy

▶ Permissions boundary (not set)

Conclusion:

We have successfully created the **limited privileged policies** for a user.