Module 1: Introduction To DevOps On Cloud

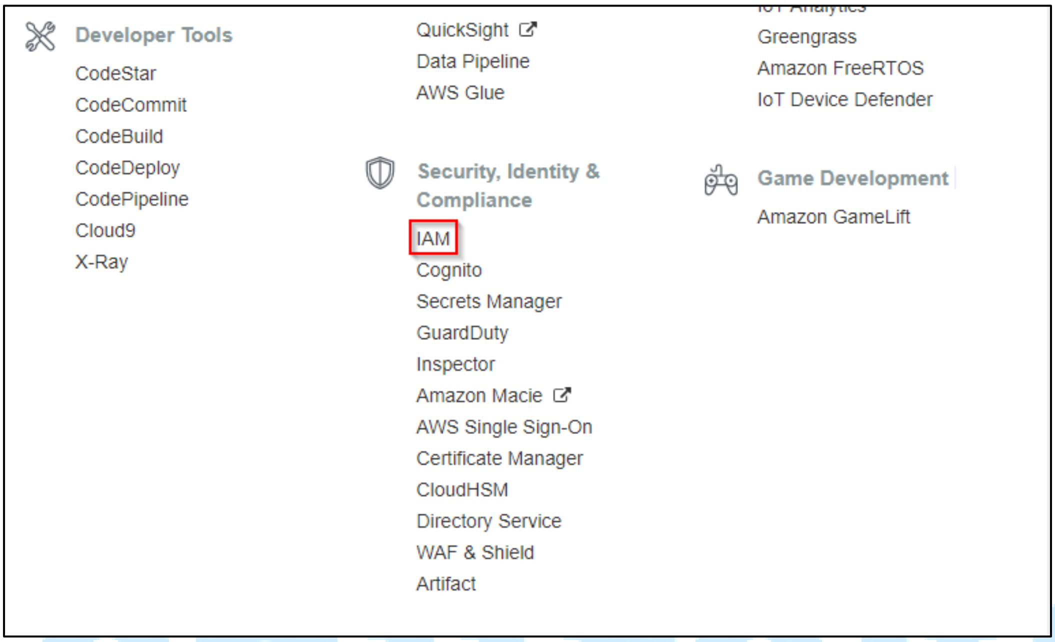
Demo Document 1

edureka!

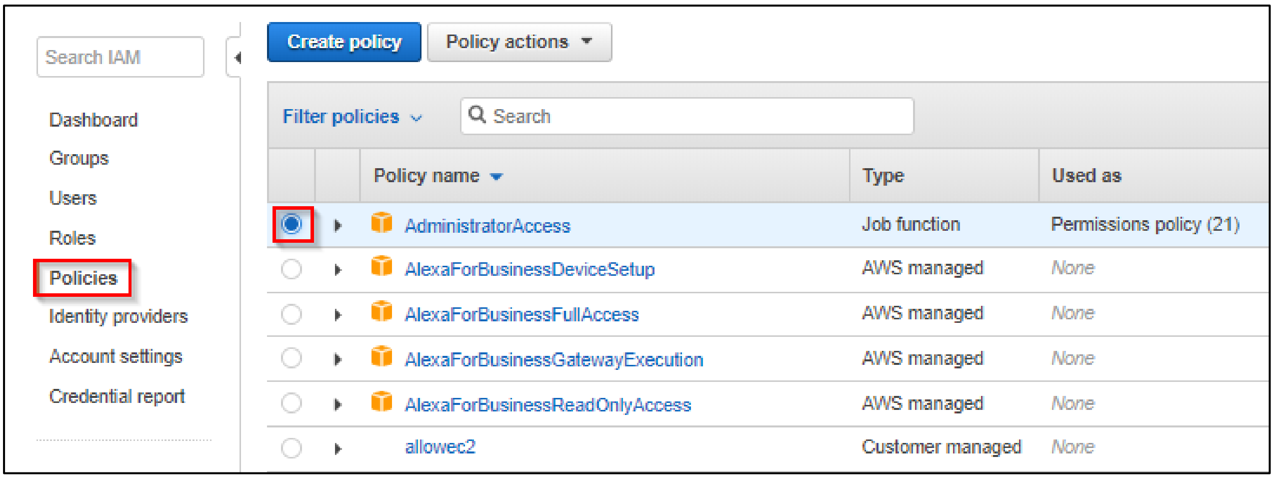
Creating Policies For New User To Have All Admin Or Limited Privileges

DEMO Steps:

Step1: Go to AWS management console and under Security, Identity & Compliance select ***IAM***



Step2: Creating Policies for New User : Move to policies section under IAM and select “AdministratorAccess” (By attaching this policy the user gets all the Admin access to all the services)

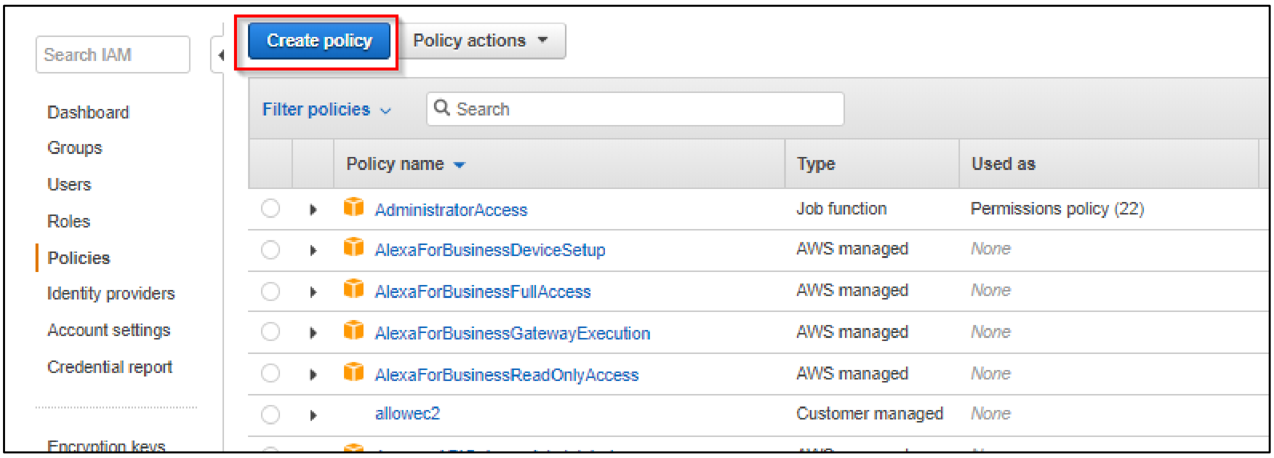


		Policy name	Type	Used as
●	▸	AdministratorAccess	Job function	Permissions policy (21)
○	▸	AlexaForBusinessDeviceSetup	AWS managed	None
○	▸	AlexaForBusinessFullAccess	AWS managed	None
○	▸	AlexaForBusinessGatewayExecution	AWS managed	None
○	▸	AlexaForBusinessReadOnlyAccess	AWS managed	None
○	▸	allowec2	Customer managed	None

Instead of providing Admin access to user if you want to provide limited privileges then you can create the such policy and attach it to the user.

Eg: Lets create a policy which provides the user the permissions of only list and read to all objects in Amazon S3

Step-3: Go to policy and click on "Create Policy"



Search IAM

Dashboard
Groups
Users
Roles
Policies
Identity providers
Account settings
Credential report

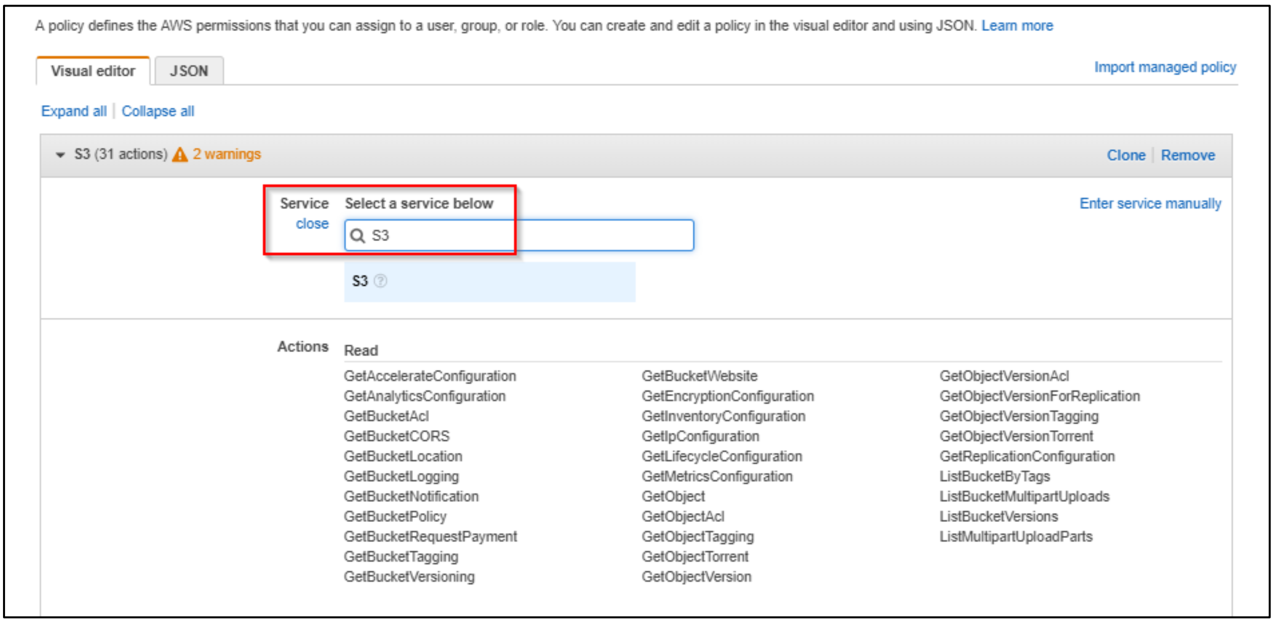
Encryption keys

Create policy | Policy actions ▾

Filter policies ⌄ | Search

		Policy name ▾	Type	Used as
○	▸	AdministratorAccess	Job function	Permissions policy (22)
○	▸	AlexaForBusinessDeviceSetup	AWS managed	None
○	▸	AlexaForBusinessFullAccess	AWS managed	None
○	▸	AlexaForBusinessGatewayExecution	AWS managed	None
○	▸	AlexaForBusinessReadOnlyAccess	AWS managed	None
○	▸	allowec2	Customer managed	None

Step-4: In visual editor under service choose ***S3*** service



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 (31 actions) ⚠ 2 warnings | Clone | Remove

Service: Select a service below (close) | Enter service manually

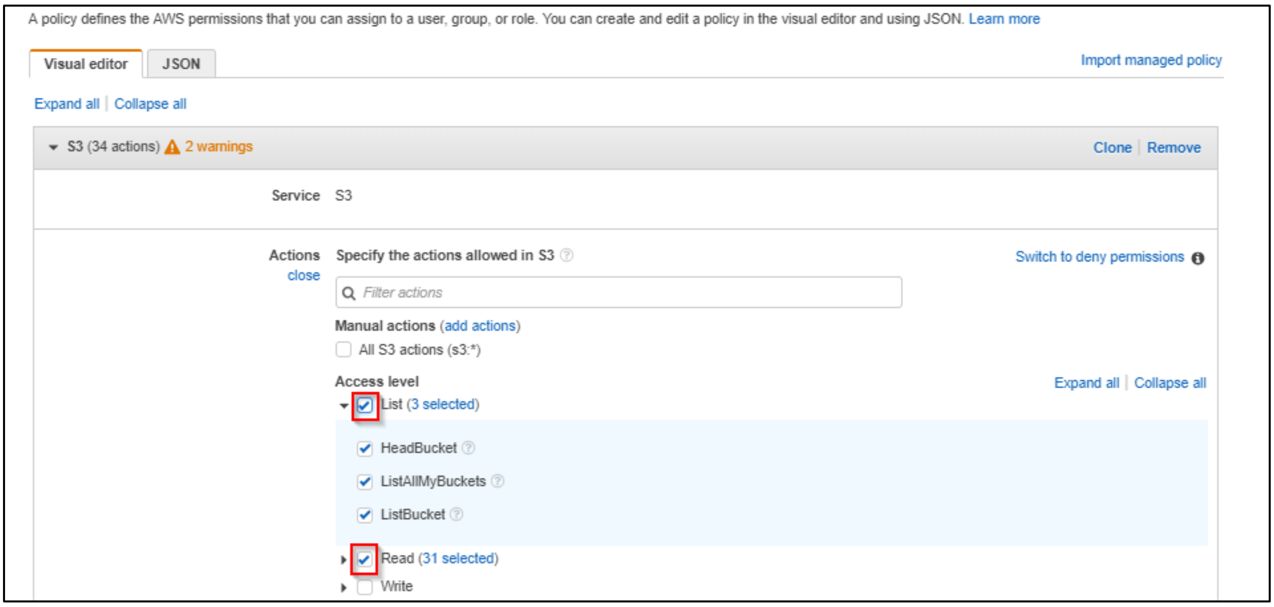
S3

S3

Actions: Read

GetAccelerateConfiguration
GetAnalyticsConfiguration
GetBucketAcl
GetBucketCORS
GetBucketLocation
GetBucketLogging
GetBucketNotification
GetBucketPolicy
GetBucketRequestPayment
GetBucketTagging
GetBucketVersioning
GetBucketWebsite
GetEncryptionConfiguration
GetInventoryConfiguration
GetIpConfiguration
GetLifecycleConfiguration
GetMetricsConfiguration
GetObject
GetObjectAcl
GetObjectTagging
GetObjectTorrent
GetObjectVersion
GetObjectVersionAcl
GetObjectVersionForReplication
GetObjectVersionTagging
GetObjectVersionTorrent
GetReplicationConfiguration
ListBucketByTags
ListBucketMultipartUploads
ListBucketVersions
ListMultipartUploadParts

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 Specify the actions allowed in S3

close
Switch to deny permissions
Filter actions

Manual actions (add actions)

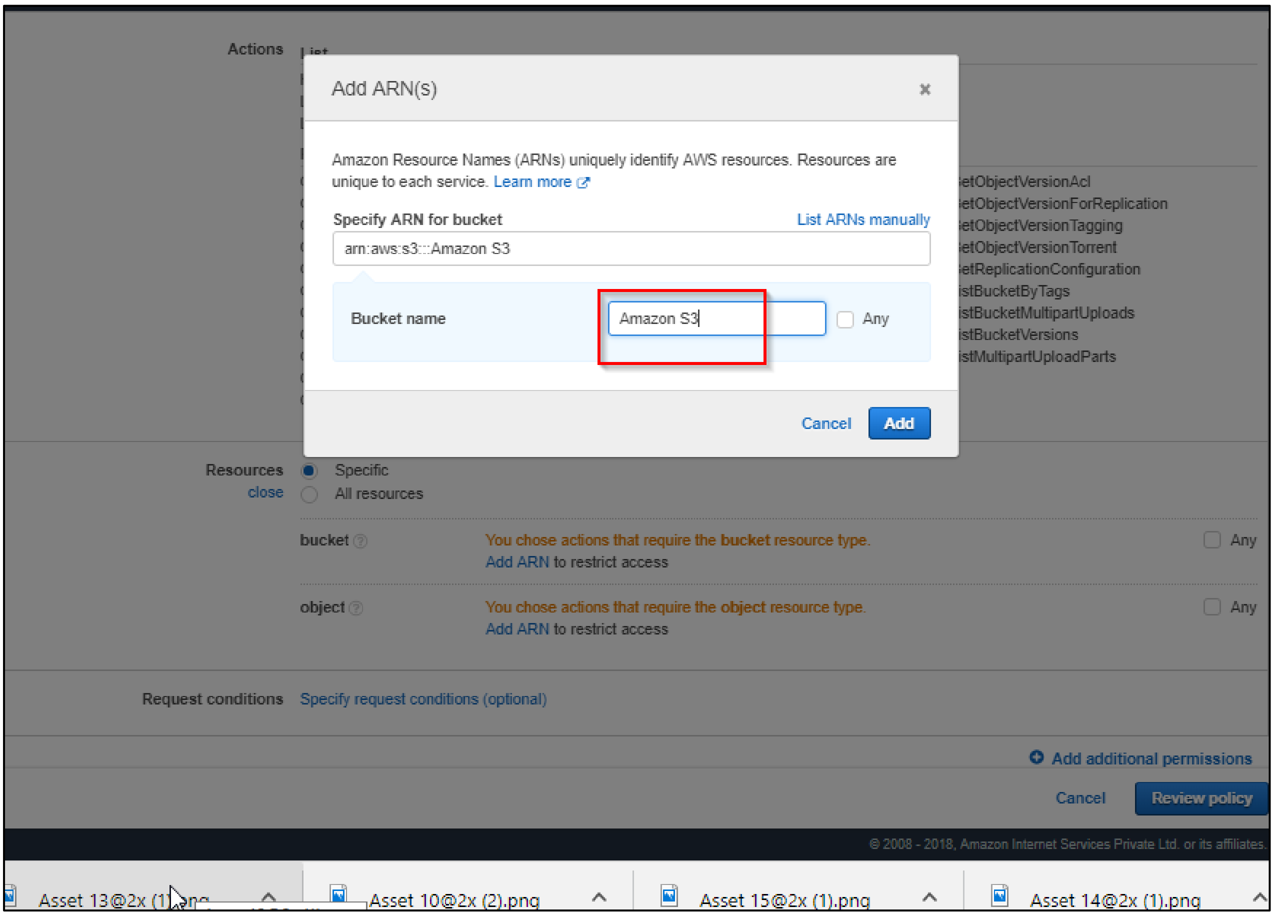
☐ All S3 actions (s3:*)

Access level

Expand all | Collapse all

- ☑ List (3 selected)
  - ☑ HeadBucket
  - ☑ ListAllMyBuckets
  - ☑ ListBucket
- ☑ Read (31 selected)
- ☐ Write

Step-6: You may find certain errors, to get off them go to resources at bottom, beside bucket click on add ARN and specify ARN



Add ARN(s)

Amazon Resource Names (ARNs) uniquely identify AWS resources. Resources are unique to each service. Learn more

Specify ARN for bucket

arn:aws:s3:::Amazon S3

Bucket name: Amazon S3 ☐ Any

Resources ● Specific ○ All resources

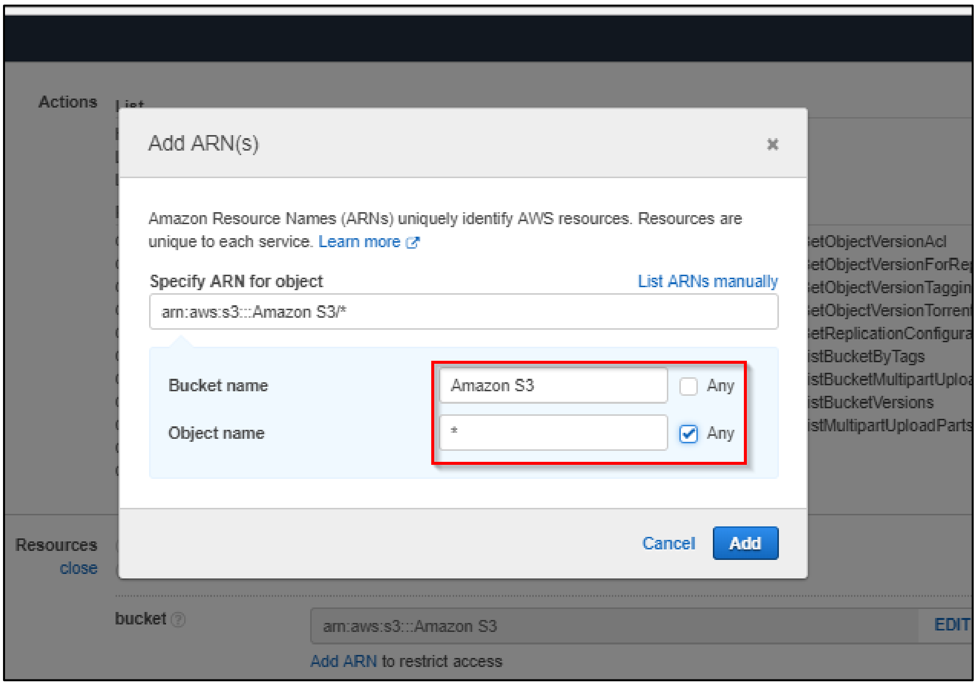
bucket: You chose actions that require the bucket resource type. Add ARN to restrict access ☐ Any

object: You chose actions that require the object resource type. Add ARN to restrict access ☐ Any

Request conditions: Specify request conditions (optional)

Add additional permissions
Cancel
Review policy
© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates.
Asset 13@2x (1).png
Asset 10@2x (2).png
Asset 15@2x (1).png
Asset 14@2x (1).png

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



Add ARN(s)

Amazon Resource Names (ARNs) uniquely identify AWS resources. Resources are unique to each service. Learn more

Specify ARN for object

arn:aws:s3:::Amazon S3/*

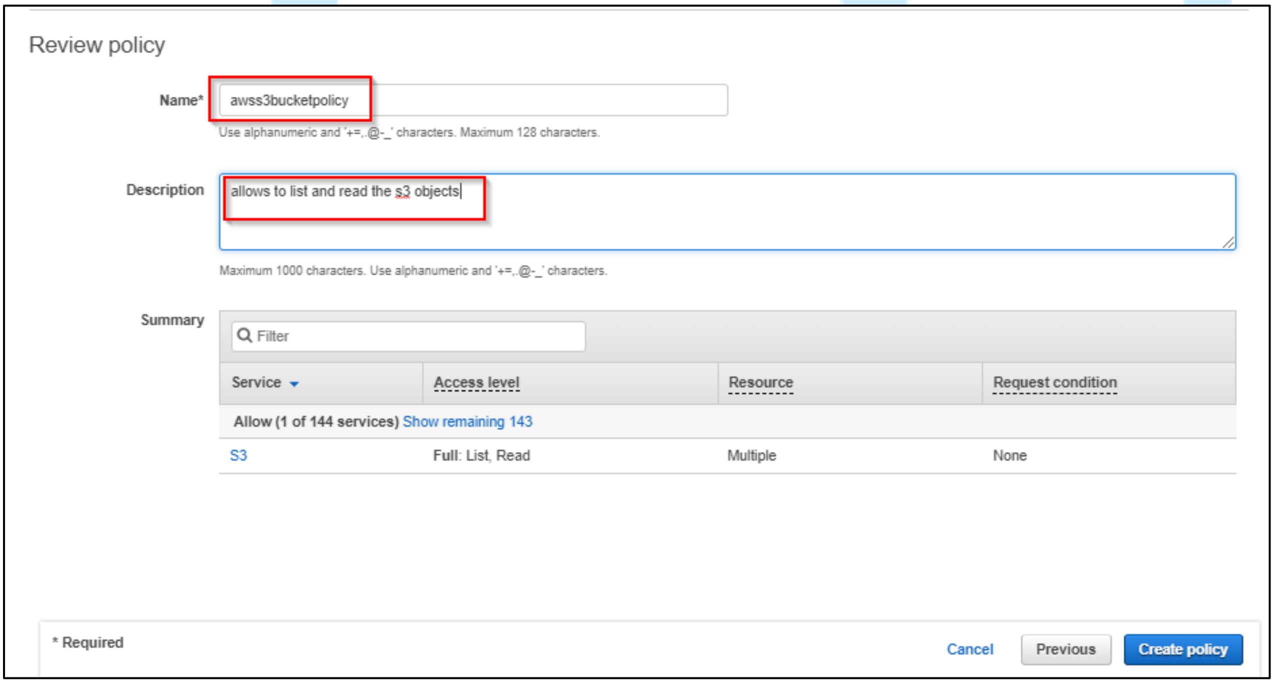
Bucket name: Amazon S3 □ Any

Object name: * ☑ Any

bucket: arn:aws:s3:::Amazon S3

Add ARN to restrict access

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



Review policy

Name*: awss3bucketpolicy

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

Description: allows to list and read the s3 objects

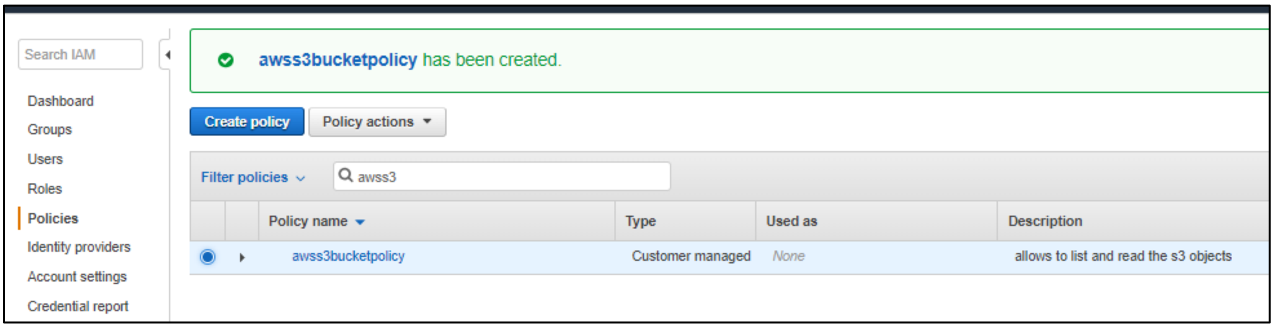
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Summary

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

* Required

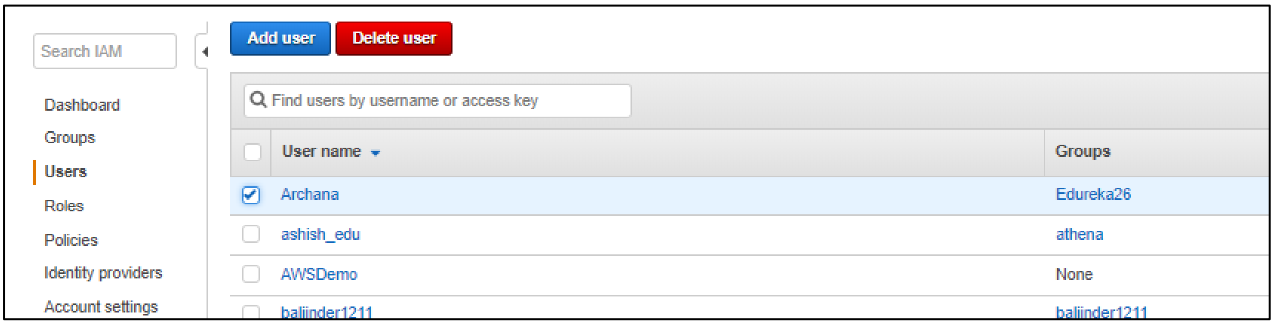
Step-9: If the policy is created successfully then it will be added in policy list



awss3bucketpolicy has been created.

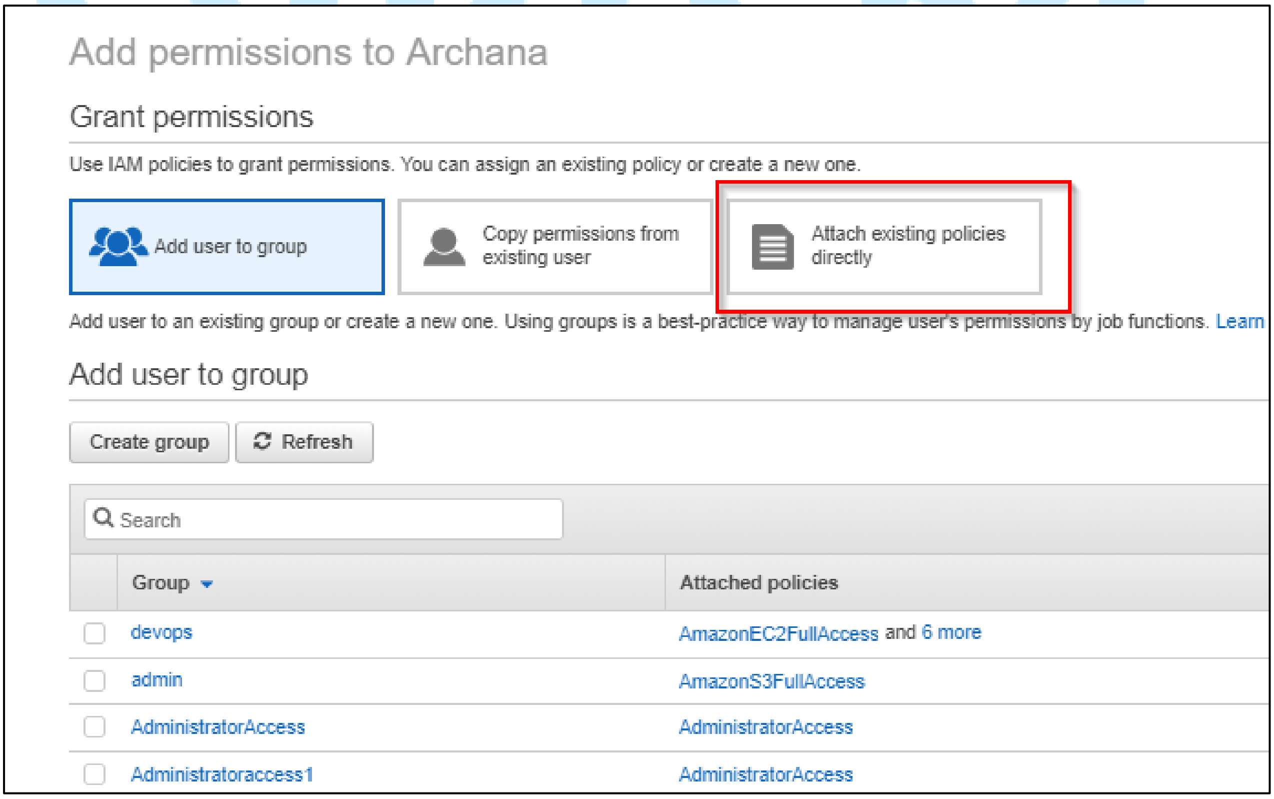
		Policy name	Type	Used as	Description
●	▸	awss3bucketpolicy	Customer managed	None	allows to list and read the s3 objects

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



□	User name	Groups
☑	Archana	Edureka26
□	ashish_edu	athena
□	AWSDemo	None
□	baljinder1211	baljinder1211

Step-11: Click on "Add Permission" and select the ***policy attach option***


Add user to group
Copy permissions from existing user
Attach existing policies directly
Create group
Refresh
Search

Add permissions to Archana

Grant permissions

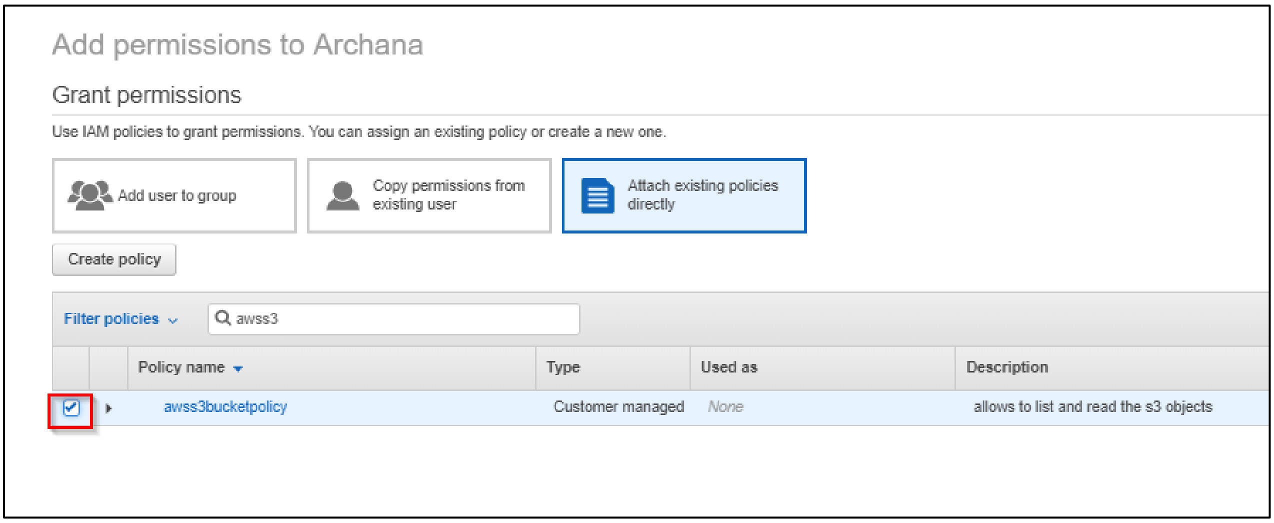
Use IAM policies to grant permissions. You can assign an existing policy or create a new one.

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn

Add user to group

	Group	Attached policies
□	devops	AmazonEC2FullAccess and 6 more
□	admin	AmazonS3FullAccess
□	AdministratorAccess	AdministratorAccess
□	Administratoraccess1	AdministratorAccess

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



Add permissions to Archana

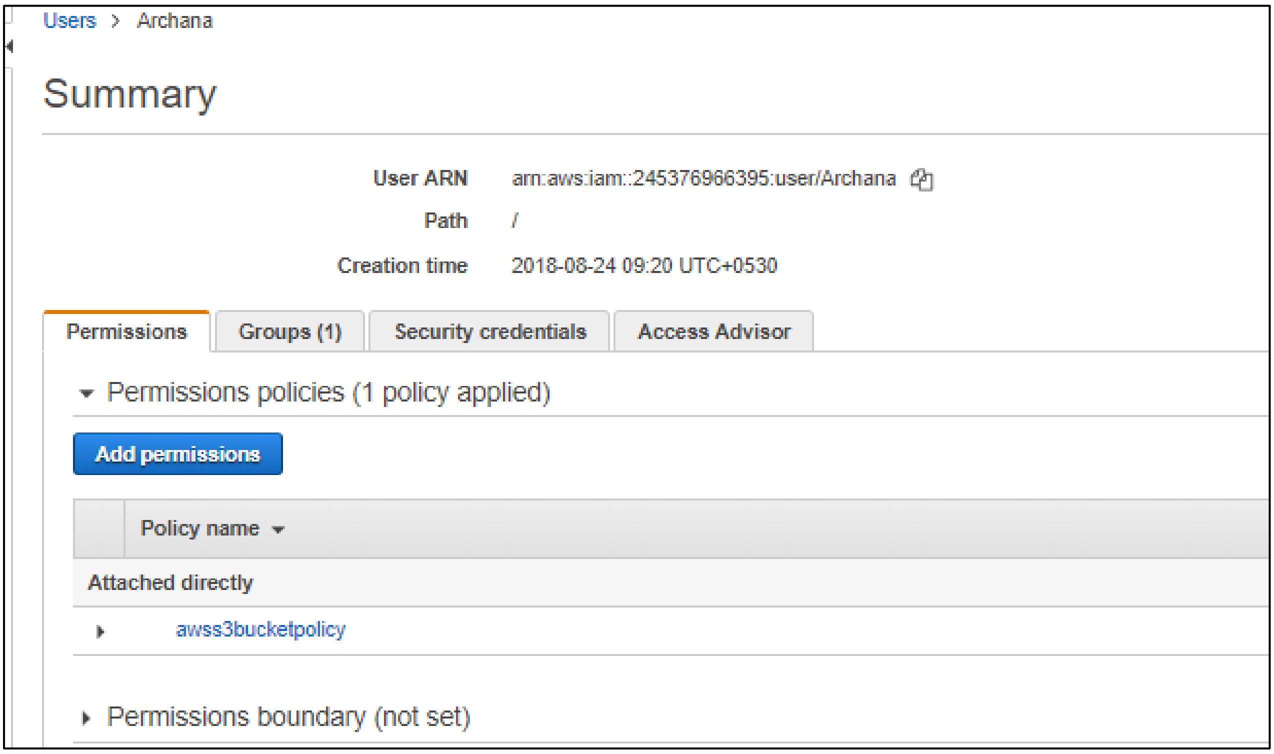
Grant permissions

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
awss3

	Policy name	Type	Used as	Description
☑	awss3bucketpolicy	Customer managed	None	allows to list and read the s3 objects

Step-13: Click on “Add Permission” and policy is attached to user so now 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

Policy name
Attached directly
awss3bucketpolicy

Conclusion:

We have successfully created the ***limited privileged policies*** to attach a user