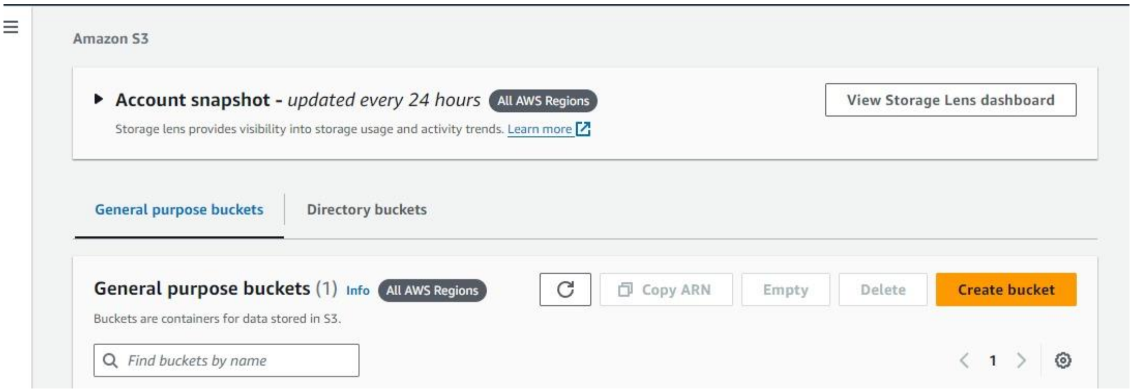
AWS SOLUTIONS ARCHITECT
ASSIGNMENT-1
HARINI L
22BCE5233

Create an IAM policy, user and assign a policy to the group of users and access S3 bucket

- CREATING IAM POLICY



Amazon S3

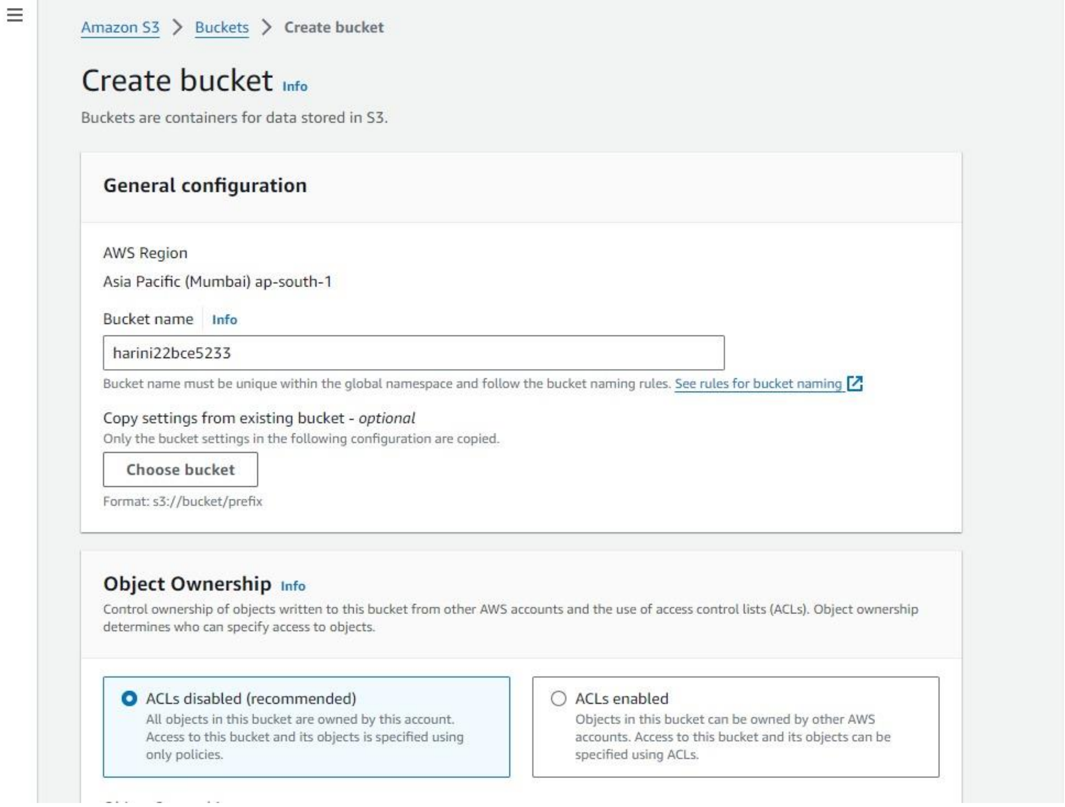
▶ **Account snapshot -** *updated every 24 hours* All AWS Regions

Storage lens provides visibility into storage usage and activity trends. Learn more

General purpose buckets (1) Info All AWS Regions

Buckets are containers for data stored in S3.

CREATING S3 BUCKET



Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region

Asia Pacific (Mumbai) ap-south-1

Bucket name Info

harini22bce5233

Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

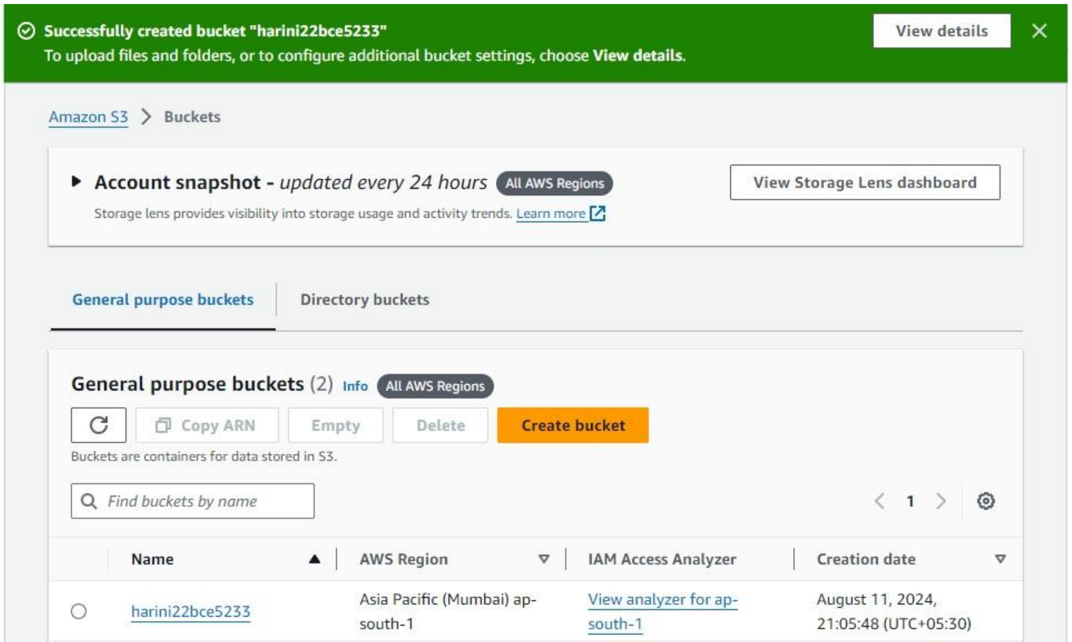
Format: s3://bucket/prefix

Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

● ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

○ ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.



Successfully created bucket "harini22bce5233"

To upload files and folders, or to configure additional bucket settings, choose **View details**.

Amazon S3 > Buckets

Account snapshot - *updated every 24 hours* All AWS Regions

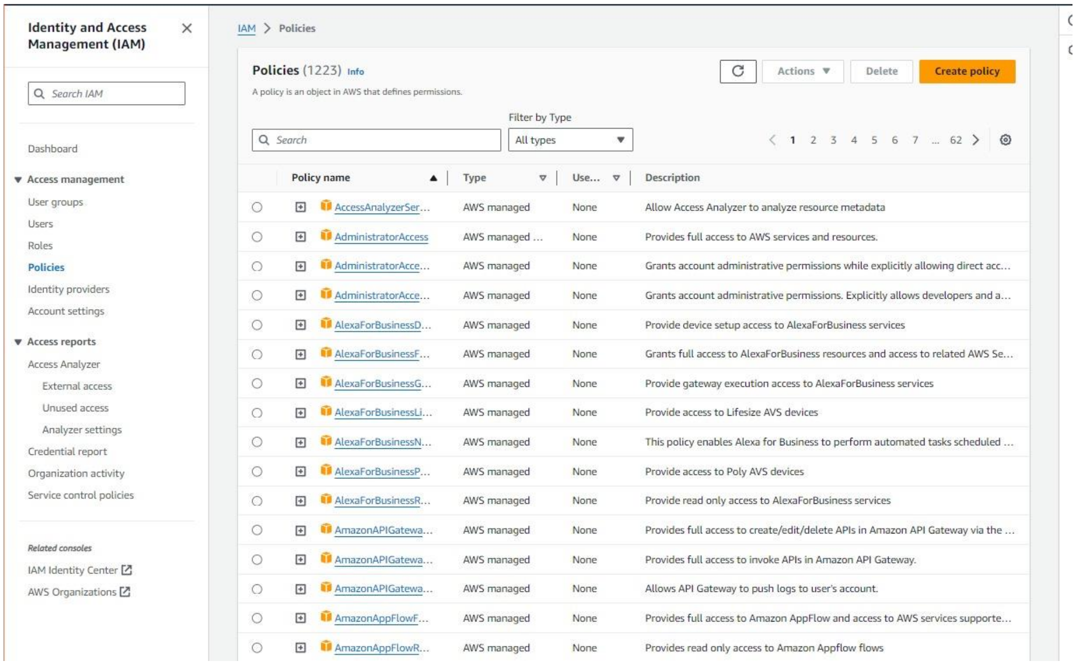
Storage lens provides visibility into storage usage and activity trends. Learn more

General purpose buckets (2) Info All AWS Regions

Buckets are containers for data stored in S3.

	Name ▲	AWS Region ▽	IAM Access Analyzer	Creation date ▽
○	harini22bce5233	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	August 11, 2024, 21:05:48 (UTC+05:30)

CREATING USER GROUPS AND ASSIGNING POLICY

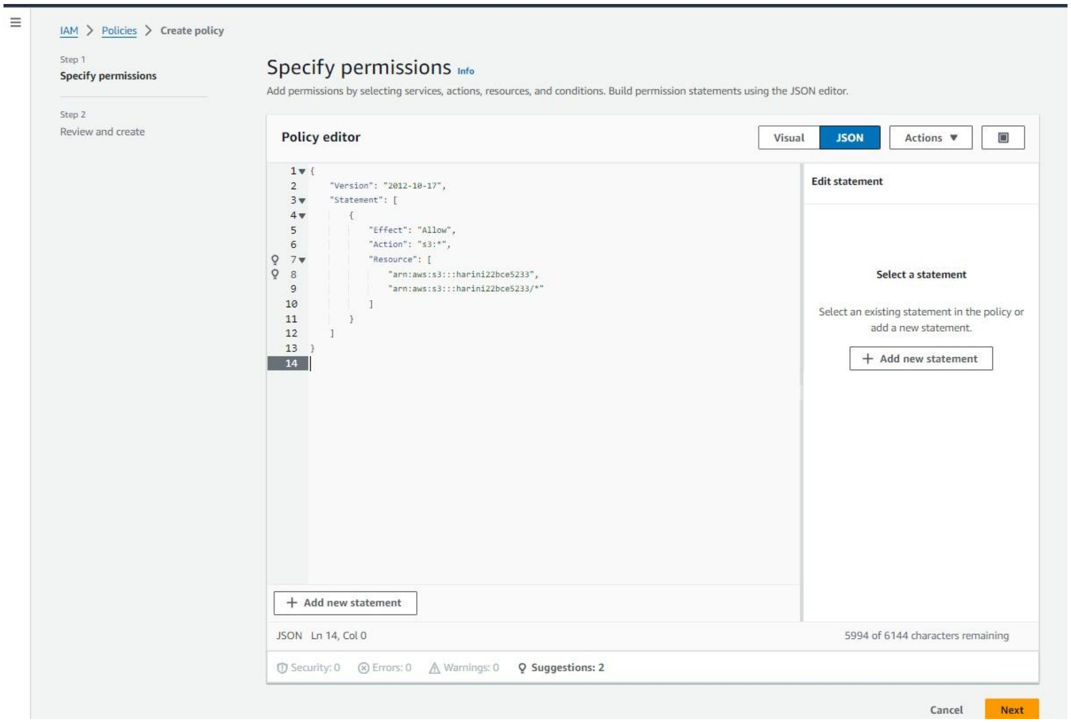


IAM > Policies

Policies (1223) Info

A policy is an object in AWS that defines permissions.

		Policy name ▲	Type ▽	Use... ▽	Description
○	⊞	AccessAnalyzerSer...	AWS managed	None	Allow Access Analyzer to analyze resource metadata
○	⊞	AdministratorAccess	AWS managed ...	None	Provides full access to AWS services and resources.
○	⊞	AdministratorAcce...	AWS managed	None	Grants account administrative permissions while explicitly allowing direct acc...
○	⊞	AdministratorAcce...	AWS managed	None	Grants account administrative permissions. Explicitly allows developers and a...
○	⊞	AlexaForBusinessD...	AWS managed	None	Provide device setup access to AlexaForBusiness services
○	⊞	AlexaForBusinessF...	AWS managed	None	Grants full access to AlexaForBusiness resources and access to related AWS Se...
○	⊞	AlexaForBusinessG...	AWS managed	None	Provide gateway execution access to AlexaForBusiness services
○	⊞	AlexaForBusinessLi...	AWS managed	None	Provide access to Lifesize AVS devices
○	⊞	AlexaForBusinessN...	AWS managed	None	This policy enables Alexa for Business to perform automated tasks scheduled ...
○	⊞	AlexaForBusinessP...	AWS managed	None	Provide access to Poly AVS devices
○	⊞	AlexaForBusinessR...	AWS managed	None	Provide read only access to AlexaForBusiness services
○	⊞	AmazonAPIGatewa...	AWS managed	None	Provides full access to create/edit/delete APIs in Amazon API Gateway via the ...
○	⊞	AmazonAPIGatewa...	AWS managed	None	Provides full access to invoke APIs in Amazon API Gateway.
○	⊞	AmazonAPIGatewa...	AWS managed	None	Allows API Gateway to push logs to user's account.
○	⊞	AmazonAppFlowF...	AWS managed	None	Provides full access to Amazon AppFlow and access to AWS services supporte...
○	⊞	AmazonAppFlowR...	AWS managed	None	Provides read only access to Amazon Appflow flows



IAM > Policies > Create policy

Step 1
Specify permissions

Step 2
Review and create

Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::harini22bce5233",
                "arn:aws:s3:::harini22bce5233/*"
            ]
        }
    ]
}
```

Edit statement

Select a statement

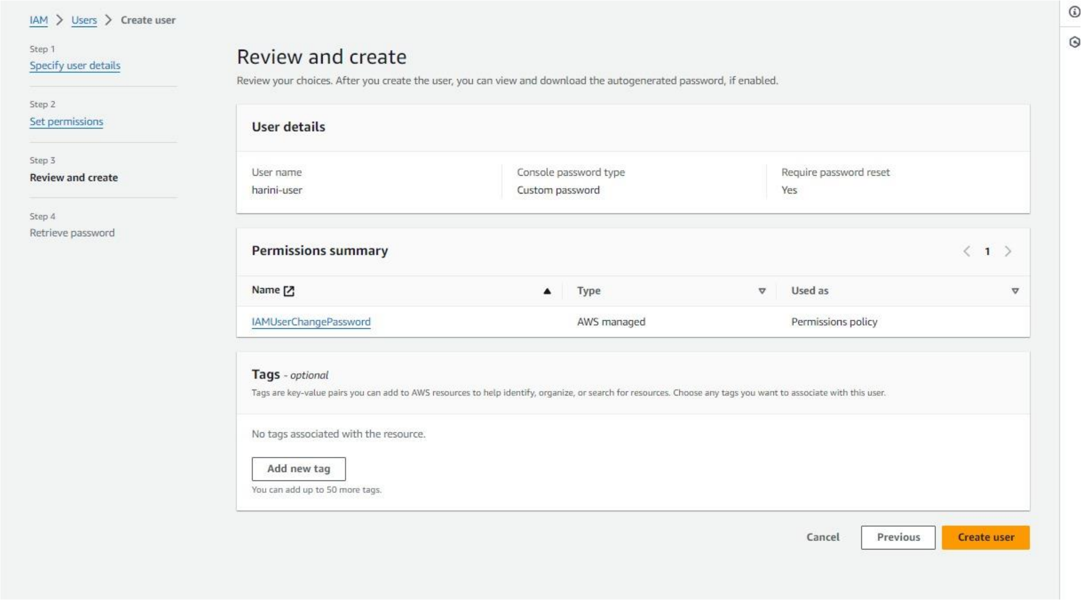
Select an existing statement in the policy or add a new statement.

JSON Ln 14, Col 0

5994 of 6144 characters remaining

Security: 0 Errors: 0 Warnings: 0 **Suggestions: 2**

CREATING USER



IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name	Console password type	Require password reset
harini-user	Custom password	Yes

Permissions summary

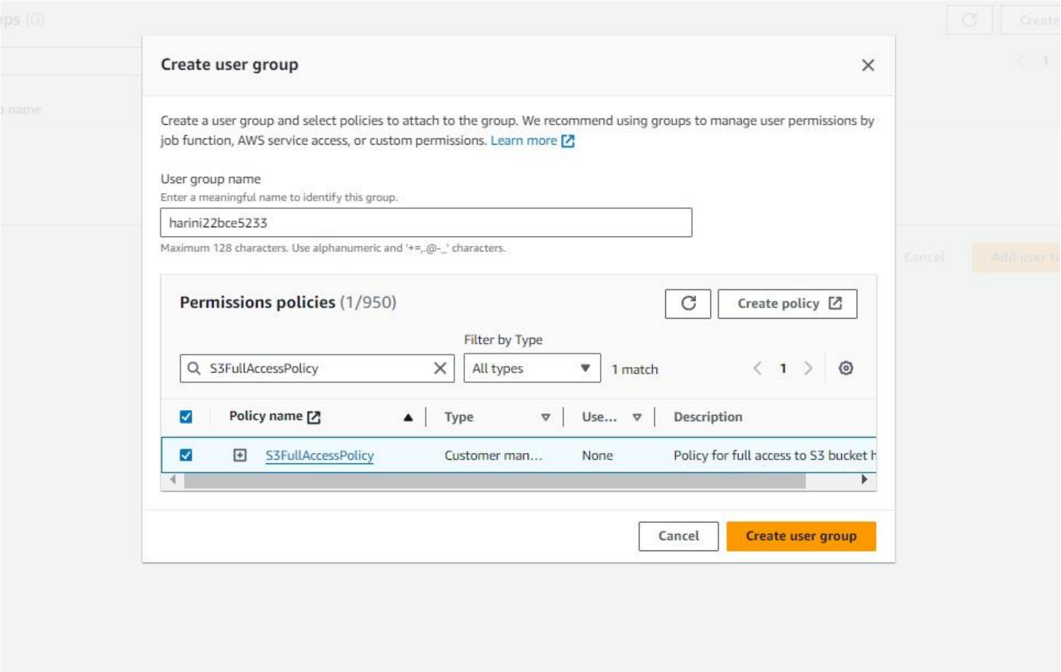
Name	Type	Used as
IAMUserChangePassword	AWS managed	Permissions policy

Tags - *optional*

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

You can add up to 50 more tags.



Create user group

Create a user group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. Learn more

User group name

Enter a meaningful name to identify this group.

harini22bce5233

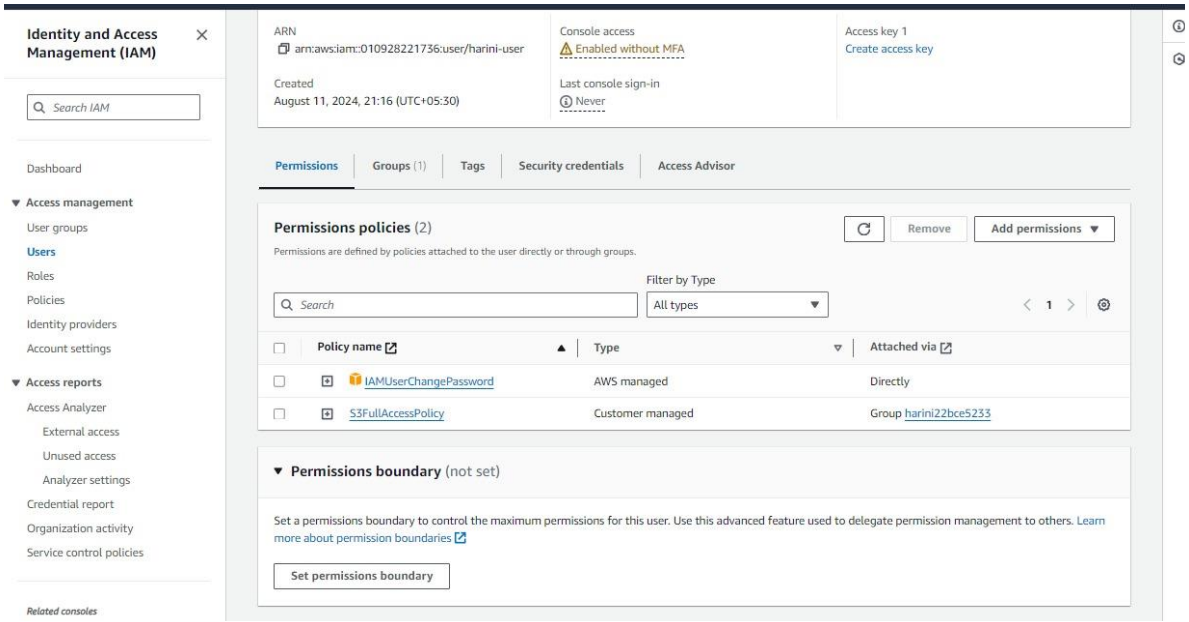
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Permissions policies (1/950)

Filter by Type: All types

S3FullAccessPolicy — 1 match

☑	Policy name	Type	Use...	Description
☑	S3FullAccessPolicy	Customer man...	None	Policy for full access to S3 bucket h



ARN
arn:aws:iam::010928221736:user/harini-user

Created
August 11, 2024, 21:16 (UTC+05:30)

Console access
⚠ Enabled without MFA

Last console sign-in
Never

Access key 1
Create access key

Permissions policies (2)

Permissions are defined by policies attached to the user directly or through groups.

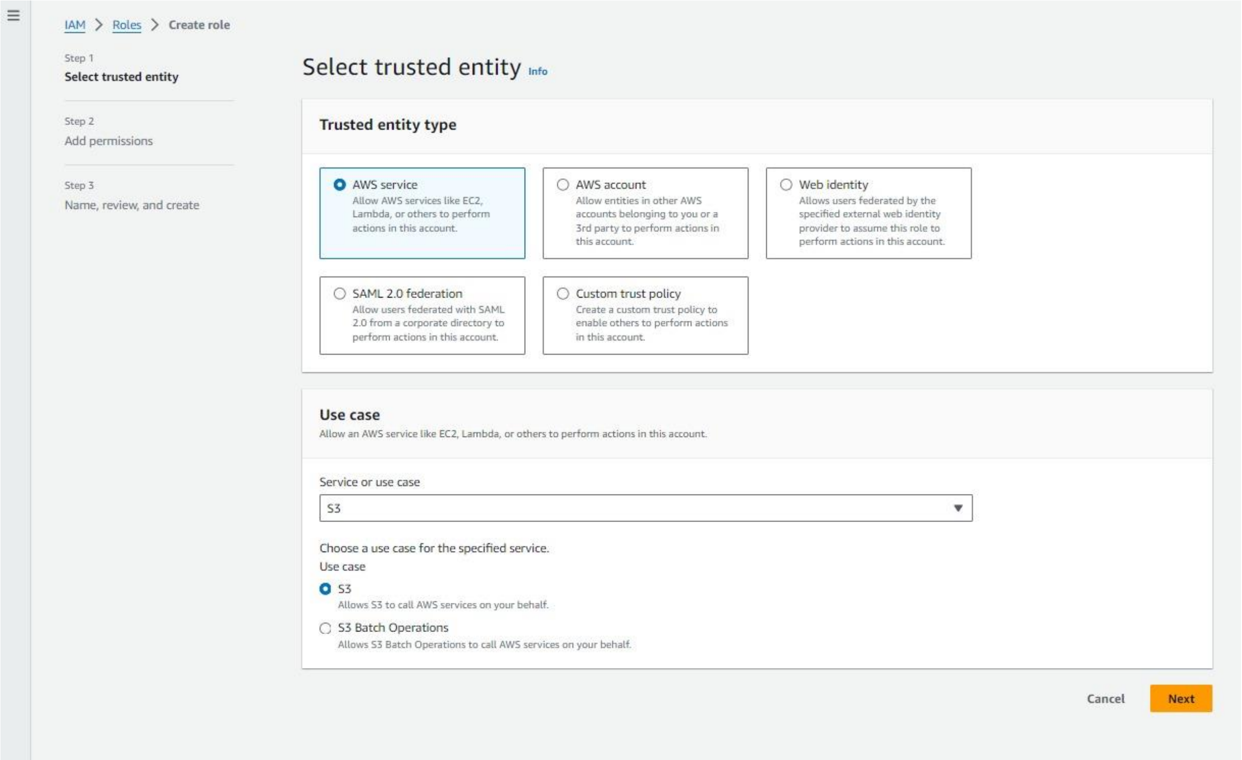
Filter by Type: All types

□	Policy name	Type	Attached via
□	IAMUserChangePassword	AWS managed	Directly
□	S3FullAccessPolicy	Customer managed	Group harini22bce5233

Permissions boundary (not set)

Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. Learn more about permission boundaries

Selecting trusted entity



IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity Info

Trusted entity type

● AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case
S3 ▼

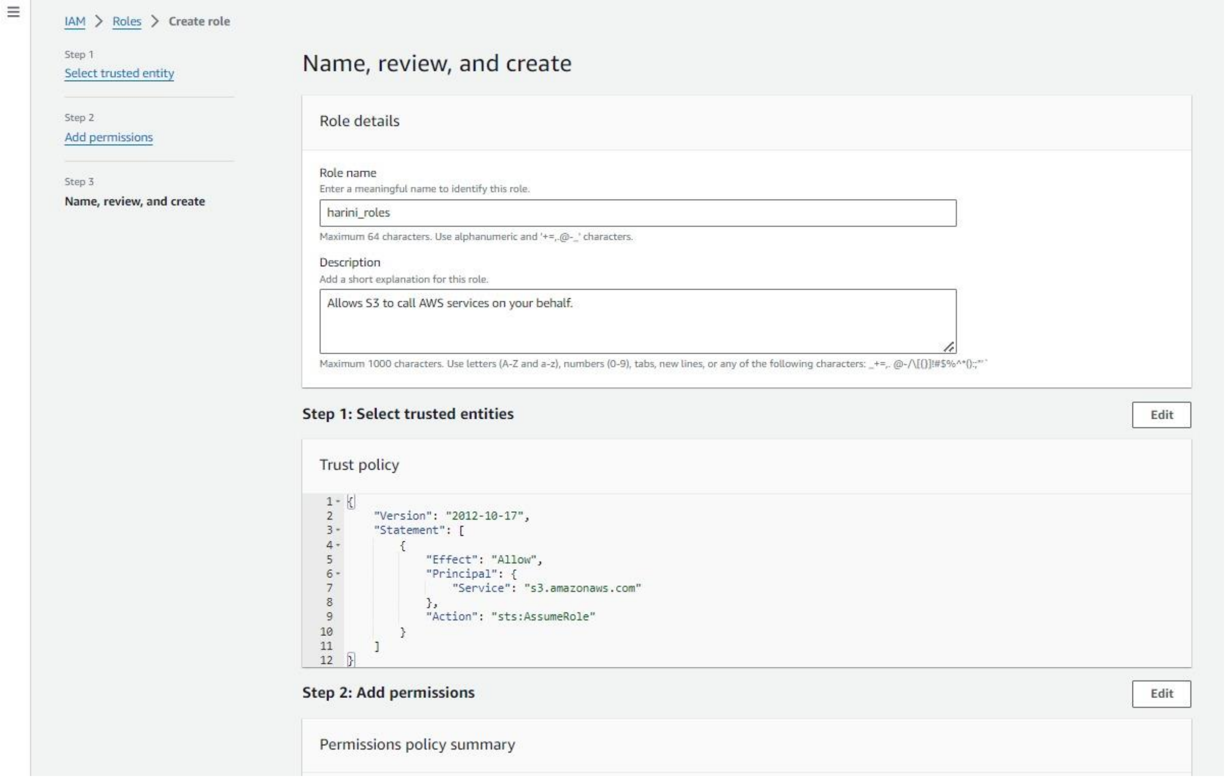
Choose a use case for the specified service.
Use case

● S3
Allows S3 to call AWS services on your behalf.

○ S3 Batch Operations
Allows S3 Batch Operations to call AWS services on your behalf.

Cancel Next

Create roles and attach the policy to the role



IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.
harini_roles
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Description
Add a short explanation for this role.
Allows S3 to call AWS services on your behalf.
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=,. @-/\[{}]!#$%^*():;"'`

Step 1: Select trusted entities Edit

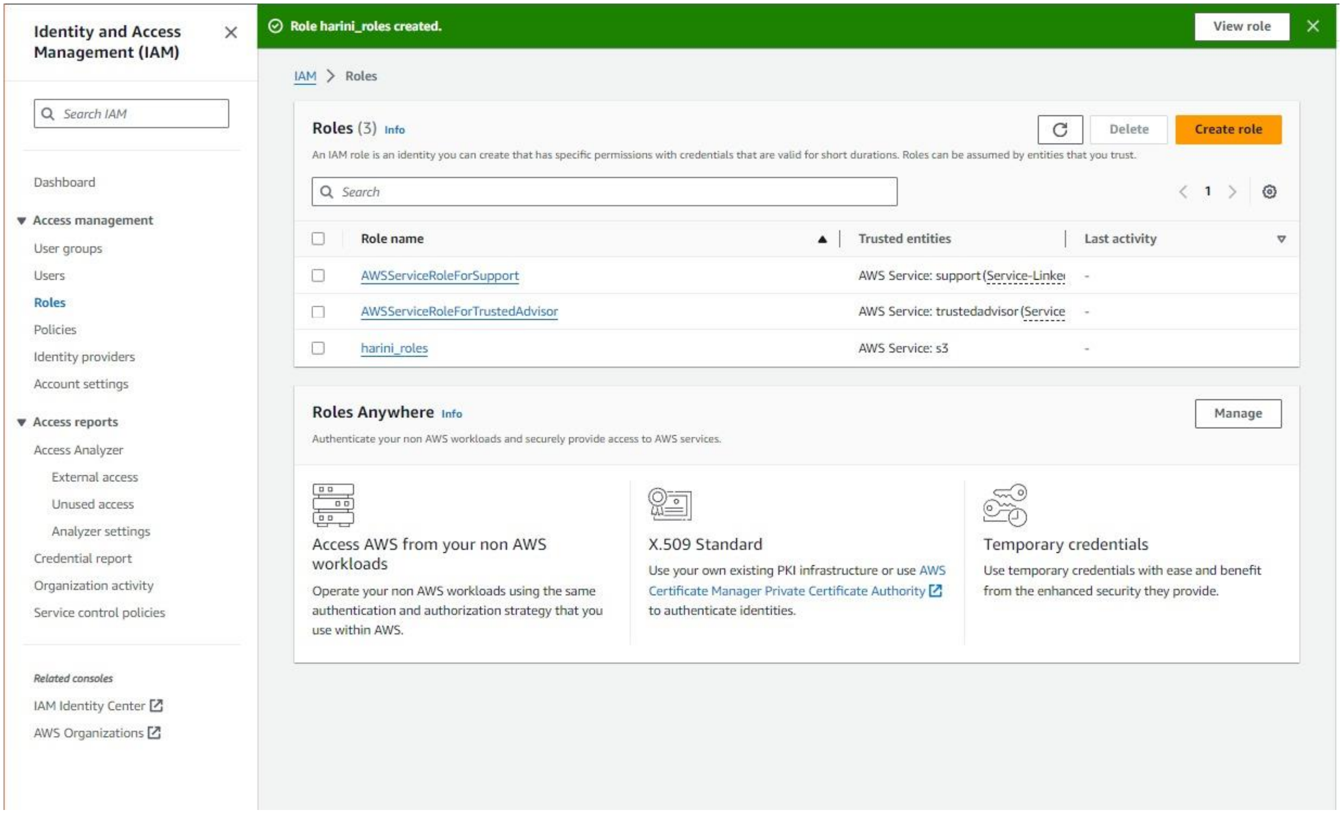
Trust policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Step 2: Add permissions Edit

Permissions policy summary

Now the roles have been created successfully



Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

Access Analyzer

External access

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies

Related consoles

IAM Identity Center

AWS Organizations

Role harini_roles created.

View role

IAM > Roles

Roles (3) Info

Delete

Create role

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Search

□	Role name	Trusted entities	Last activity
□	AWSServiceRoleForSupport	AWS Service: support (Service-Linke	-
□	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service	-
□	harini_roles	AWS Service: s3	-

Roles Anywhere Info

Manage

Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads

Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.

X.509 Standard

Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority to authenticate identities.

Temporary credentials

Use temporary credentials with ease and benefit from the enhanced security they provide.