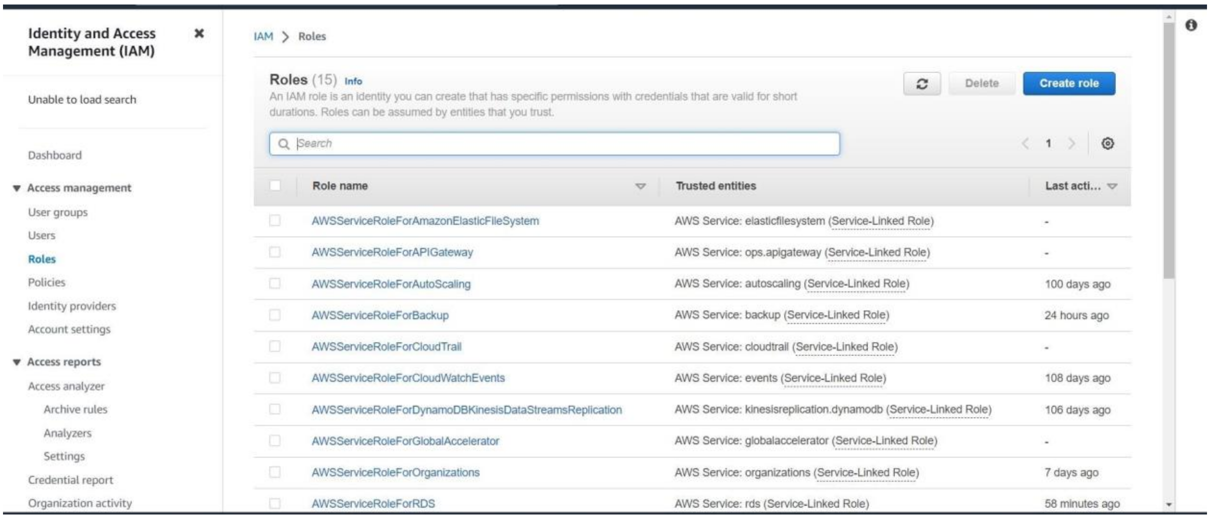
Phase-5 Practice Project: Assisted Practice -

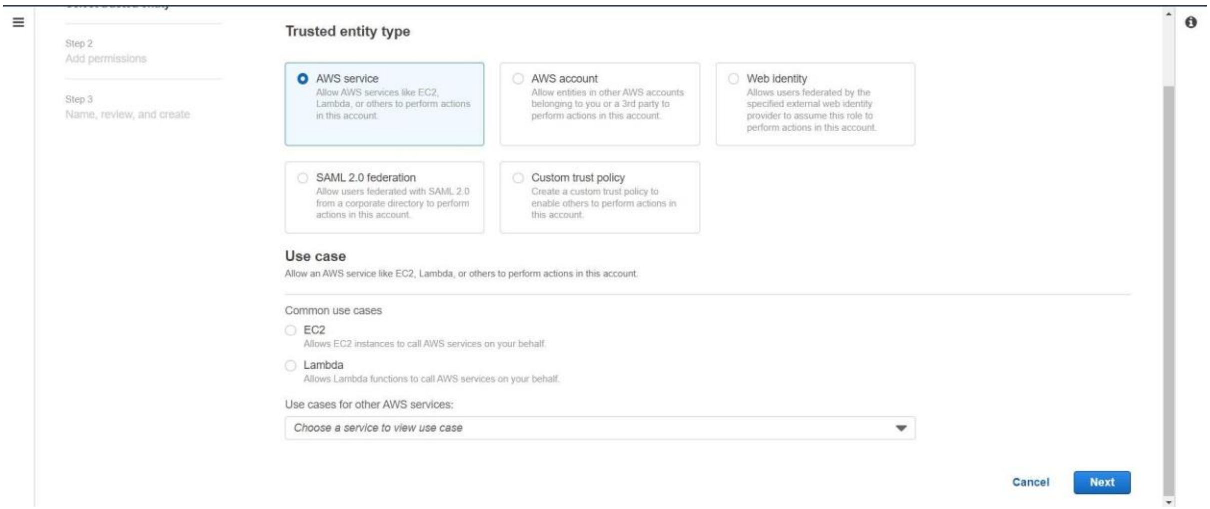
15. Create an IAM Role.



Roles (15) Info

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.

□	Role name	Trusted entities	Last acti...
□	AWSServiceRoleForAmazonElasticFileSystem	AWS Service: elasticfilesystem (Service-Linked Role)	-
□	AWSServiceRoleForAPIGateway	AWS Service: ops.apigateway (Service-Linked Role)	-
□	AWSServiceRoleForAutoScaling	AWS Service: autoscaling (Service-Linked Role)	100 days ago
□	AWSServiceRoleForBackup	AWS Service: backup (Service-Linked Role)	24 hours ago
□	AWSServiceRoleForCloudTrail	AWS Service: cloudtrail (Service-Linked Role)	-
□	AWSServiceRoleForCloudWatchEvents	AWS Service: events (Service-Linked Role)	108 days ago
□	AWSServiceRoleForDynamoDBKinesisDataStreamsReplication	AWS Service: kinesisreplication.dynamodb (Service-Linked Role)	106 days ago
□	AWSServiceRoleForGlobalAccelerator	AWS Service: globalaccelerator (Service-Linked Role)	-
□	AWSServiceRoleForOrganizations	AWS Service: organizations (Service-Linked Role)	7 days ago
□	AWSServiceRoleForRDS	AWS Service: rds (Service-Linked Role)	58 minutes ago



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.

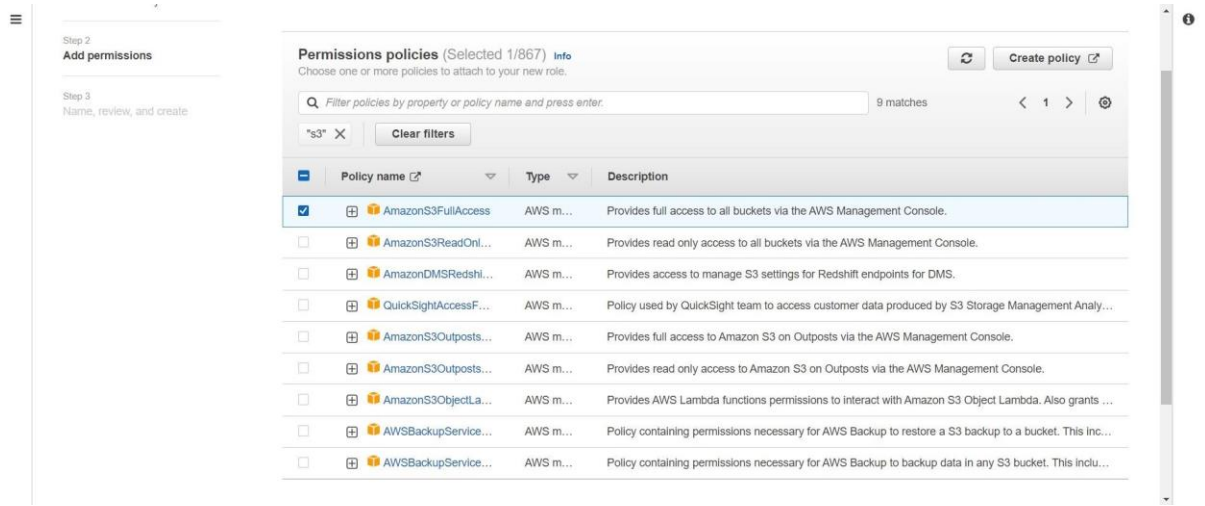
Common use cases

○ EC2
Allows EC2 instances to call AWS services on your behalf.

○ Lambda
Allows Lambda functions to call AWS services on your behalf.

Use cases for other AWS services:

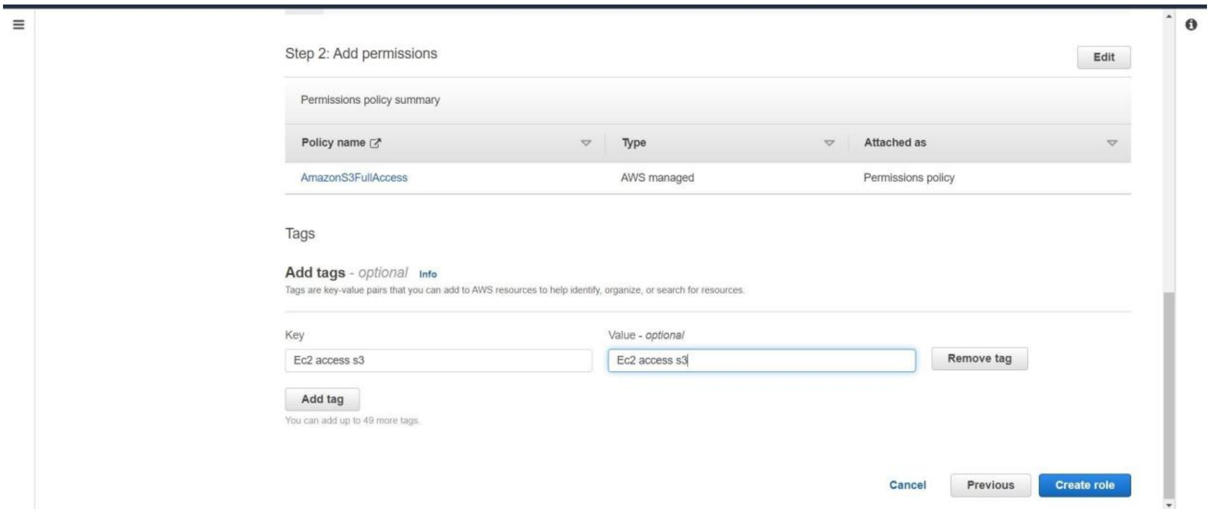
Choose a service to view use case



Permissions policies (Selected 1/867) Info

Choose one or more policies to attach to your new role.

☐	Policy name	Type	Description
☑	AmazonS3FullAccess	AWS m...	Provides full access to all buckets via the AWS Management Console.
□	AmazonS3ReadOnl...	AWS m...	Provides read only access to all buckets via the AWS Management Console.
□	AmazonDMSRedshi...	AWS m...	Provides access to manage S3 settings for Redshift endpoints for DMS.
□	QuickSightAccessF...	AWS m...	Policy used by QuickSight team to access customer data produced by S3 Storage Management Analy...
□	AmazonS3Outposts...	AWS m...	Provides full access to Amazon S3 on Outposts via the AWS Management Console.
□	AmazonS3Outposts...	AWS m...	Provides read only access to Amazon S3 on Outposts via the AWS Management Console.
□	AmazonS3ObjectLa...	AWS m...	Provides AWS Lambda functions permissions to interact with Amazon S3 Object Lambda. Also grants ...
□	AWSBackupService...	AWS m...	Policy containing permissions necessary for AWS Backup to restore a S3 backup to a bucket. This inc...
□	AWSBackupService...	AWS m...	Policy containing permissions necessary for AWS Backup to backup data in any S3 bucket. This inclu...



Step 2: Add permissions

Edit

Permissions policy summary

Policy name	Type	Attached as
AmazonS3FullAccess	AWS managed	Permissions policy

Tags

Add tags - *optional* Info

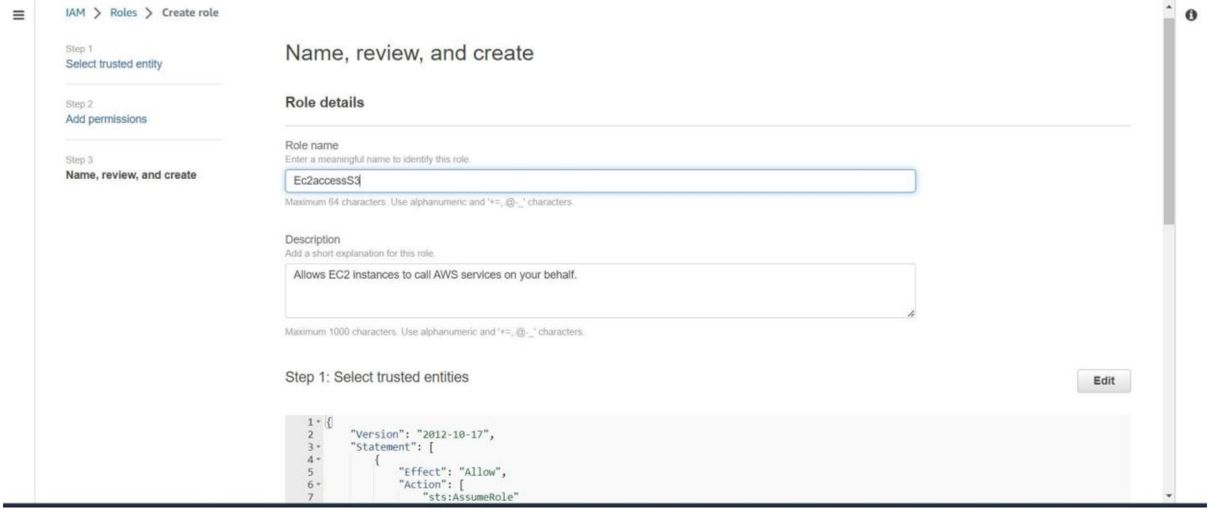
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

Key	Value - *optional*	
Ec2 access s3	Ec2 access s3	Remove tag

Add tag

You can add up to 49 more tags.

Cancel Previous Create role



Name, review, and create

Role details

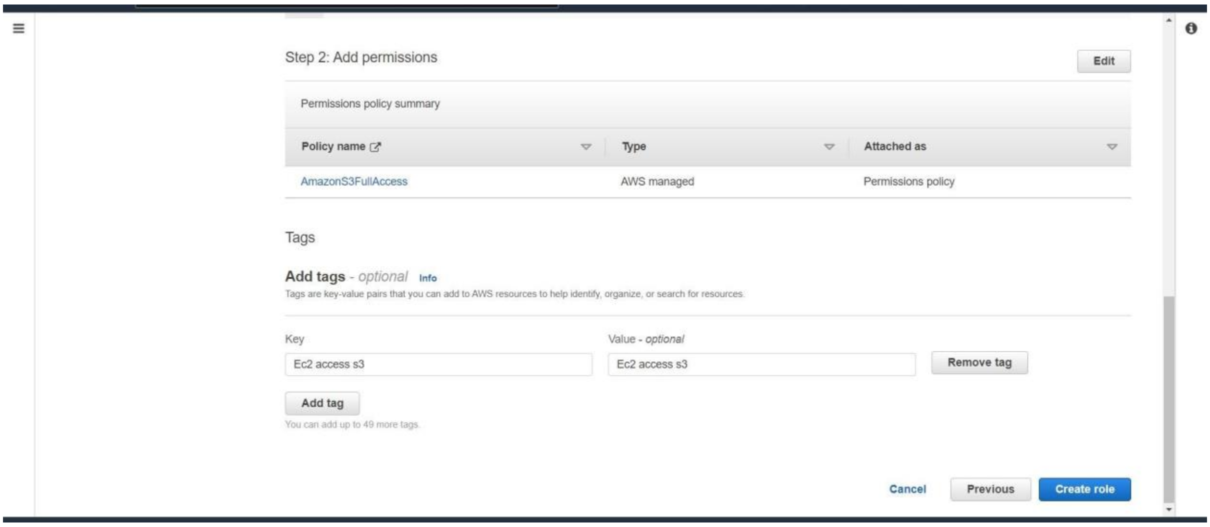
Role name
Enter a meaningful name to identify this role.
Ec2accessS3
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Step 1: Select trusted entities

Edit

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
```



Step 2: Add permissions

Edit

Permissions policy summary

Policy name	Type	Attached as
AmazonS3FullAccess	AWS managed	Permissions policy

Tags

Add tags - *optional* Info

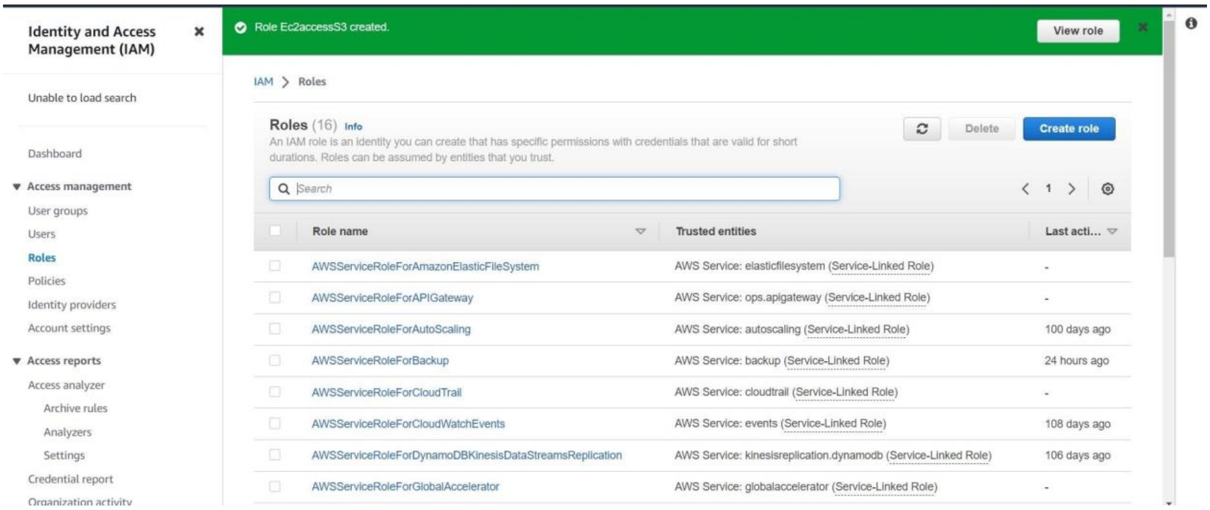
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

Key	Value - *optional*	
Ec2 access s3	Ec2 access s3	Remove tag

Add tag

You can add up to 49 more tags.

Cancel Previous Create role

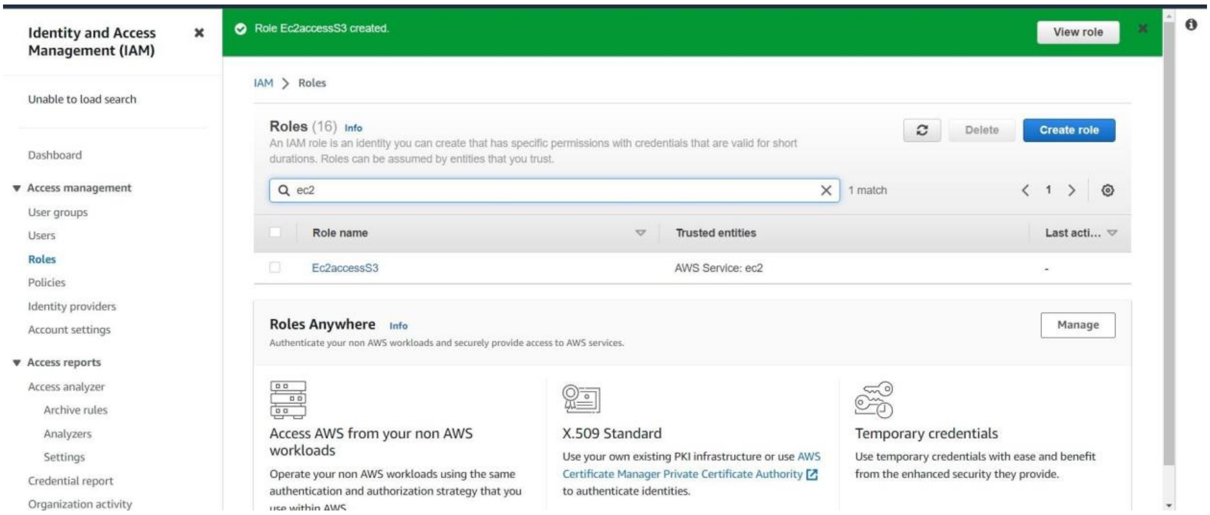


Role Ec2accessS3 created.

Roles (16) Info

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.

Role name	Trusted entities	Last acti...
AWSServiceRoleForAmazonElasticFileSystem	AWS Service: elasticfilesystem (Service-Linked Role)	-
AWSServiceRoleForAPIGateway	AWS Service: ops.apigateway (Service-Linked Role)	-
AWSServiceRoleForAutoScaling	AWS Service: autoscaling (Service-Linked Role)	100 days ago
AWSServiceRoleForBackup	AWS Service: backup (Service-Linked Role)	24 hours ago
AWSServiceRoleForCloudTrail	AWS Service: cloudtrail (Service-Linked Role)	-
AWSServiceRoleForCloudWatchEvents	AWS Service: events (Service-Linked Role)	108 days ago
AWSServiceRoleForDynamoDBKinesisDataStreamsReplication	AWS Service: kinesisreplication.dynamodb (Service-Linked Role)	106 days ago
AWSServiceRoleForGlobalAccelerator	AWS Service: globalaccelerator (Service-Linked Role)	-



Role Ec2accessS3 created.

Roles (16) Info

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.

ec2 1 match

Role name	Trusted entities	Last acti...
Ec2accessS3	AWS Service: ec2	-

Roles Anywhere Info

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.