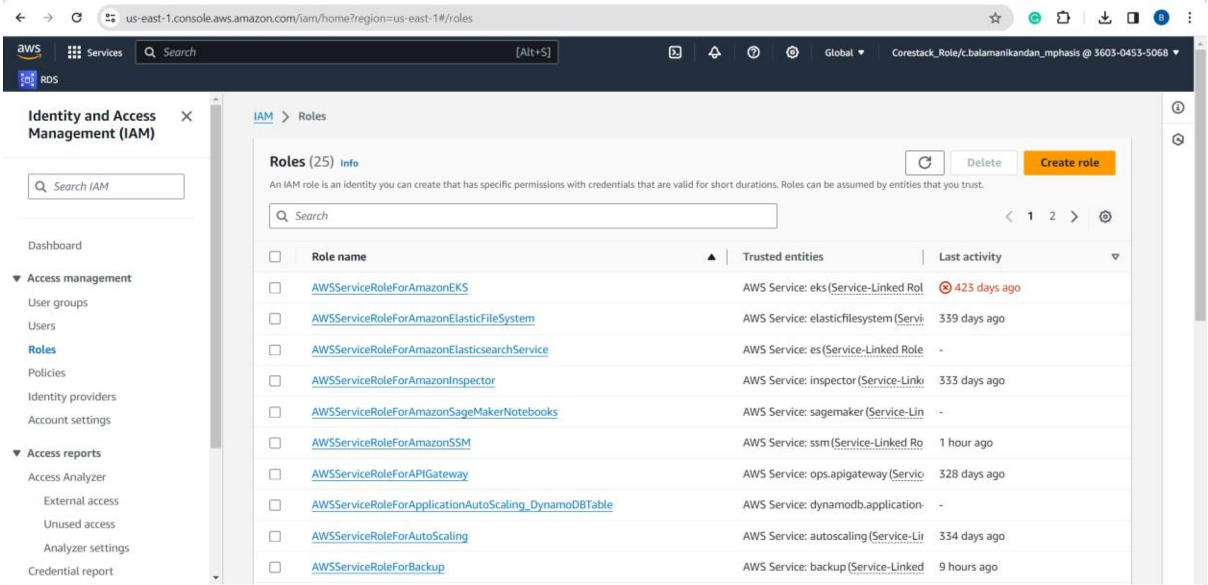
Assisted Practice Project15: Create an IAM Role C Balamanikandan

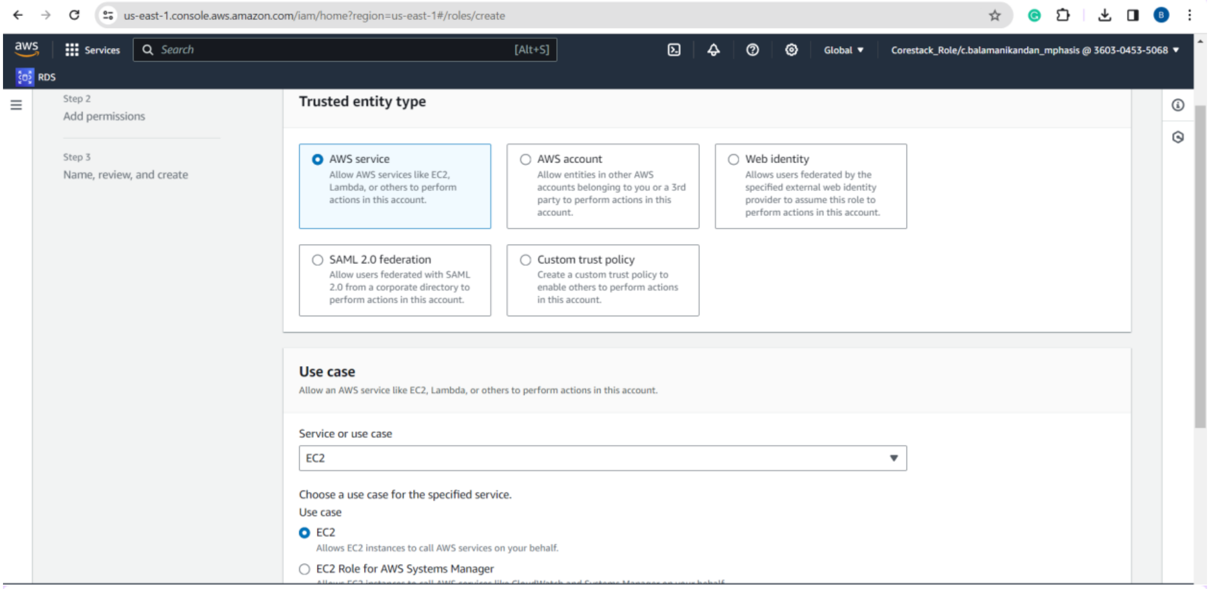


us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles

Roles (25) 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 activity
□	AWSServiceRoleForAmazonEKS	AWS Service: eks (Service-Linked Rol	⊗ 423 days ago
□	AWSServiceRoleForAmazonElasticFileSystem	AWS Service: elasticfilesystem (Servi	339 days ago
□	AWSServiceRoleForAmazonElasticsearchService	AWS Service: es (Service-Linked Role	-
□	AWSServiceRoleForAmazonInspector	AWS Service: inspector (Service-Link	333 days ago
□	AWSServiceRoleForAmazonSageMakerNotebooks	AWS Service: sagemaker (Service-Lin	-
□	AWSServiceRoleForAmazonSSM	AWS Service: ssm (Service-Linked Ro	1 hour ago
□	AWSServiceRoleForAPIGateway	AWS Service: ops.apigateway (Servic	328 days ago
□	AWSServiceRoleForApplicationAutoScaling_DynamoDBTable	AWS Service: dynamodb.application-	-
□	AWSServiceRoleForAutoScaling	AWS Service: autoscaling (Service-Lir	334 days ago
□	AWSServiceRoleForBackup	AWS Service: backup (Service-Linked	9 hours ago



us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/create

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

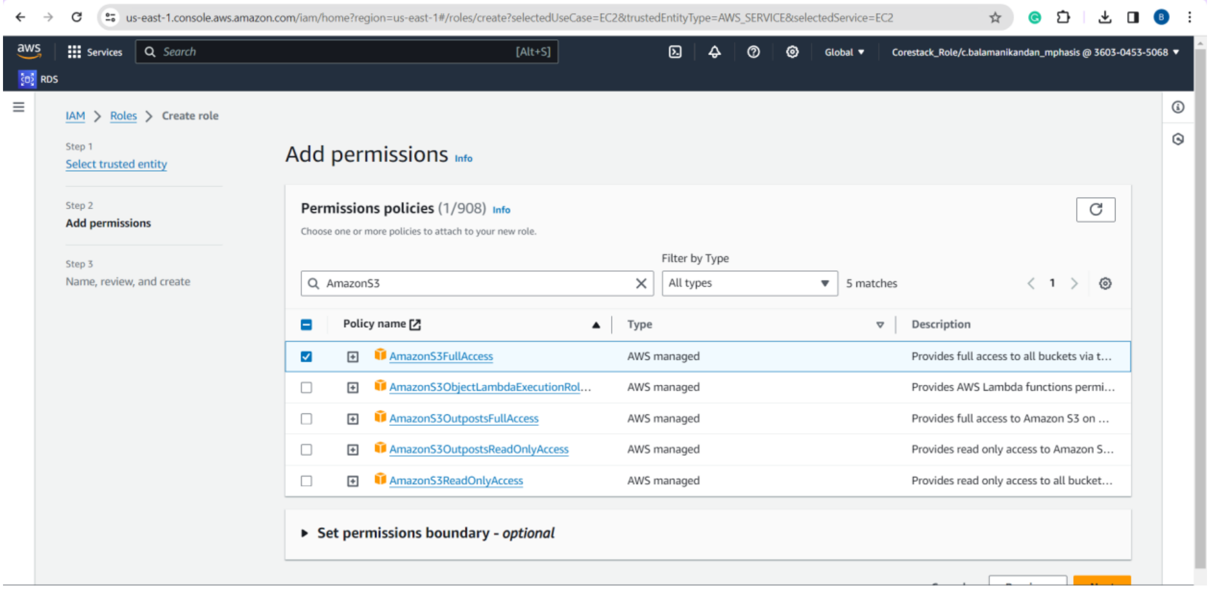
EC2 ▾

Choose a use case for the specified service.

Use case

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

○ EC2 Role for AWS Systems Manager



us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/create?selectedUseCase=EC2&trustedEntityType=AWS_SERVICE&selectedService=EC2

Add permissions Info

Permissions policies (1/908) Info

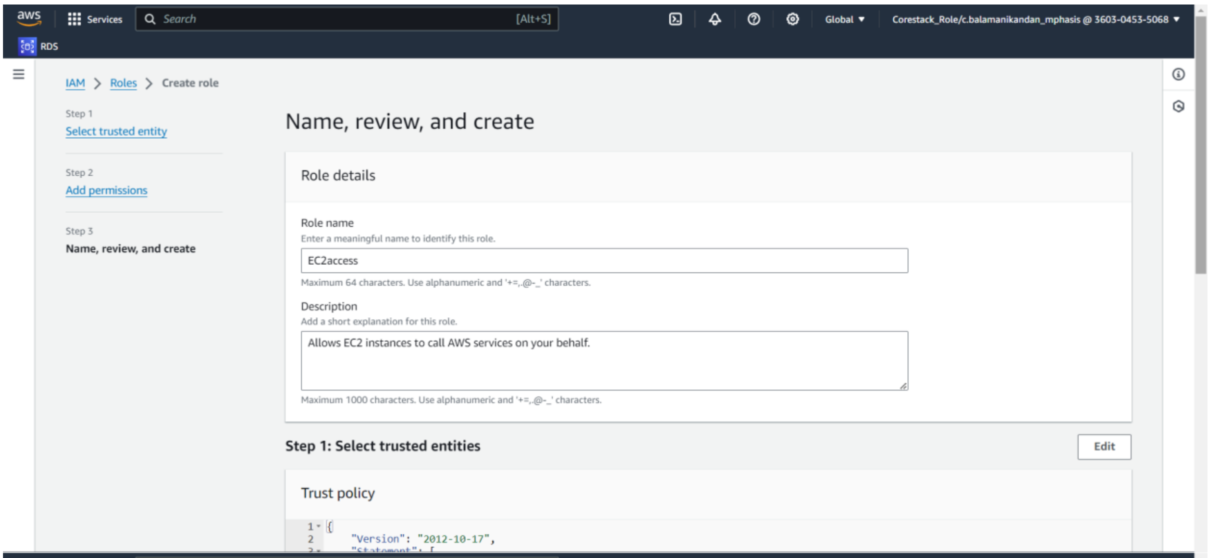
Choose one or more policies to attach to your new role.

Filter by Type

AmazonS3 | All types ▾ | 5 matches

▬	Policy name ▲	Type	Description
☑	AmazonS3FullAccess	AWS managed	Provides full access to all buckets via t...
□	AmazonS3ObjectLambdaExecutionRol...	AWS managed	Provides AWS Lambda functions permi...
□	AmazonS3OutpostsFullAccess	AWS managed	Provides full access to Amazon S3 on ...
□	AmazonS3OutpostsReadOnlyAccess	AWS managed	Provides read only access to Amazon S...
□	AmazonS3ReadOnlyAccess	AWS managed	Provides read only access to all bucket...

▸ Set permissions boundary - *optional*



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

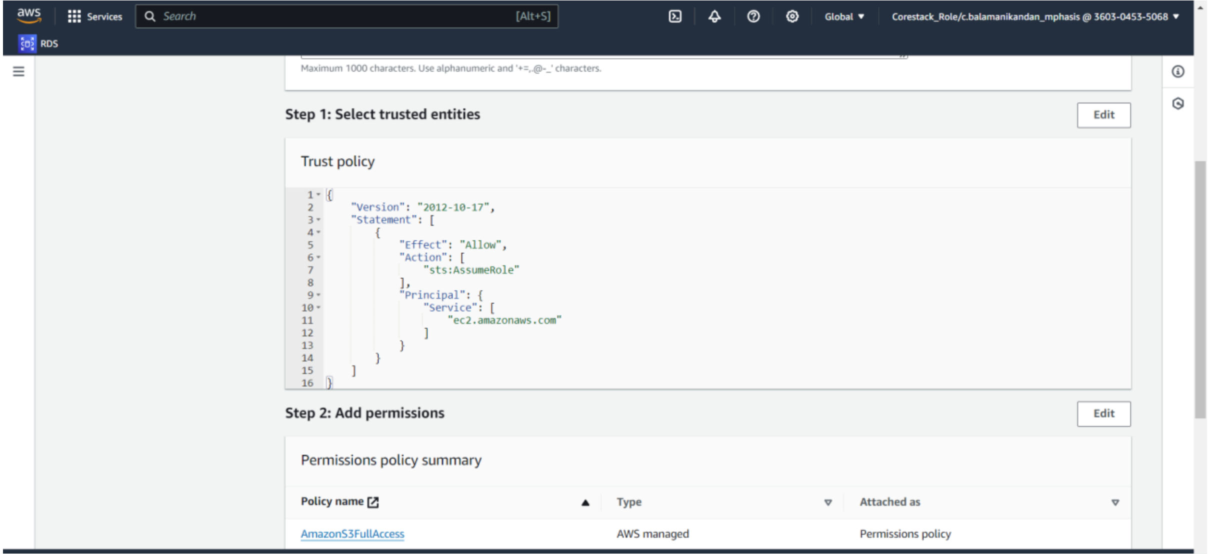
Role name
Enter a meaningful name to identify this role.
EC2access
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

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

Trust policy

```
{
    "Version": "2012-10-17",
```


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

Step 1: Select trusted entities

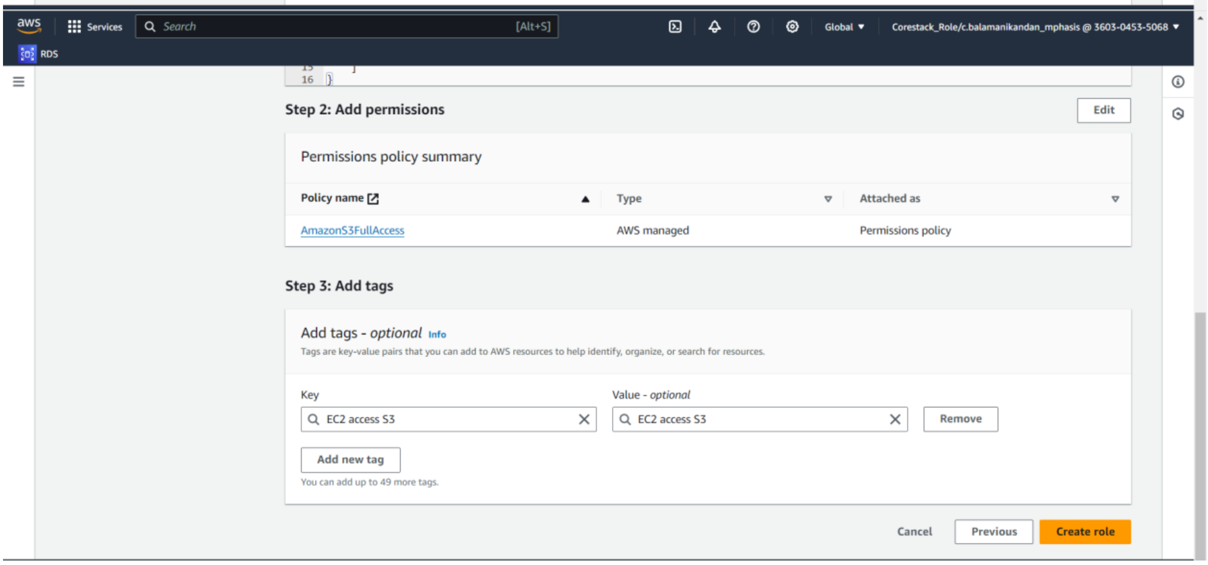
Trust policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Principal": {
                "Service": [
                    "ec2.amazonaws.com"
                ]
            }
        }
    ]
}
```

Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
AmazonS3FullAccess	AWS managed	Permissions policy


Step 2: Add permissions

Permissions policy summary

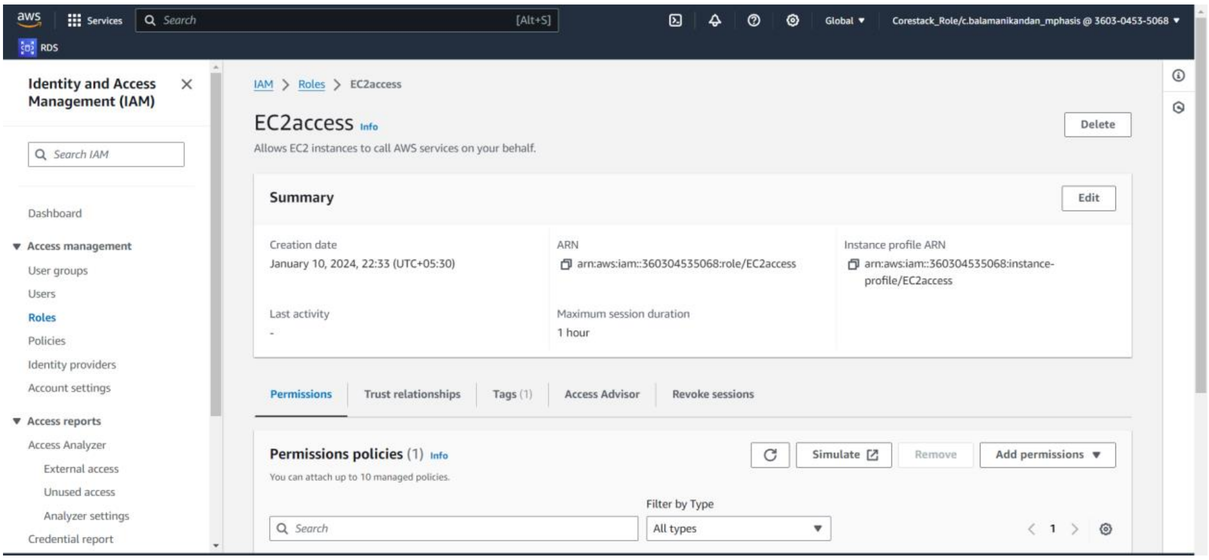
Policy name	Type	Attached as
AmazonS3FullAccess	AWS managed	Permissions policy

Step 3: Add 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

You can add up to 49 more tags.



EC2access

Allows EC2 instances to call AWS services on your behalf.

Summary

Creation date: January 10, 2024, 22:33 (UTC+05:30)

ARN: arn:aws:iam::360304535068:role/EC2access

Instance profile ARN: arn:aws:iam::360304535068:instance-profile/EC2access

Last activity: -

Maximum session duration: 1 hour

Permissions policies (1)

You can attach up to 10 managed policies.

Filter by Type: All types