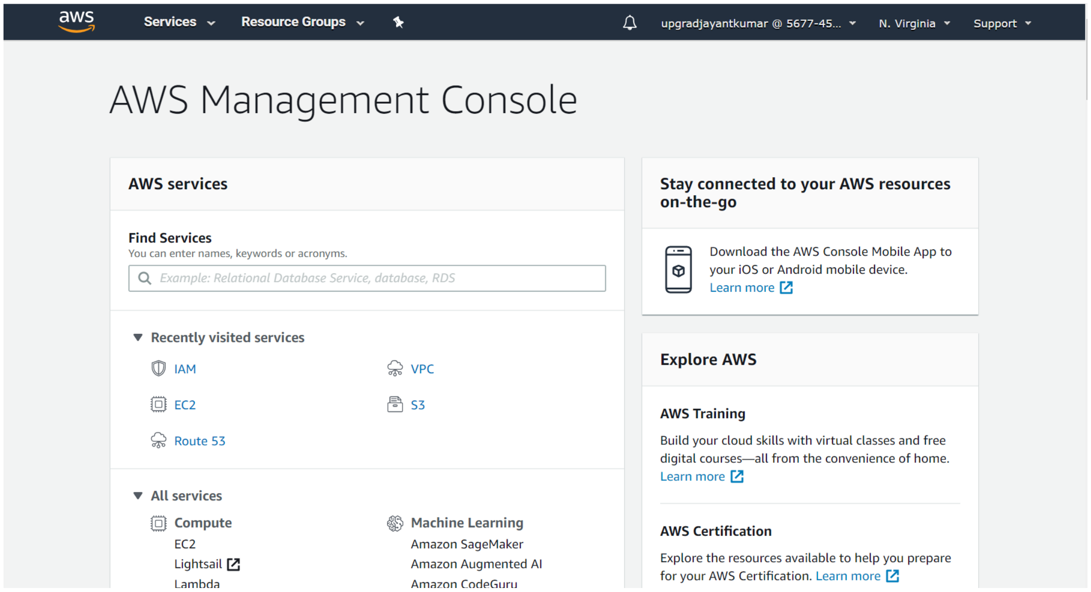
Steps to Create a Role for S3 Full Access for a Redshift Cluster

Once the S3 bucket is created, you need to create an IAM role. It will give permission to the S3 bucket to perform the **READ** and **WRITE** operations by Redshift cluster. Please follow the steps given below to create an IAM role.

Step 1: From the AWS Management Console**,** Go to **'IAM'** service



AWS Management Console

AWS services

Find Services
You can enter names, keywords or acronyms.
Example: Relational Database Service, database, RDS

Stay connected to your AWS resources on-the-go

Download the AWS Console Mobile App to your iOS or Android mobile device. Learn more

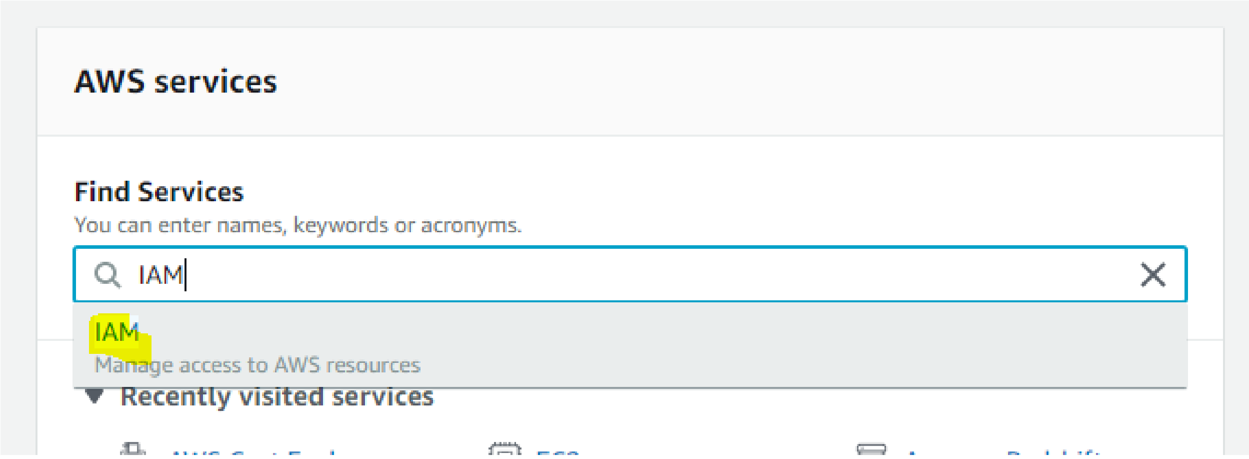
Explore AWS

AWS Training

Build your cloud skills with virtual classes and free digital courses—all from the convenience of home. Learn more

AWS Certification

Explore the resources available to help you prepare for your AWS Certification. Learn more



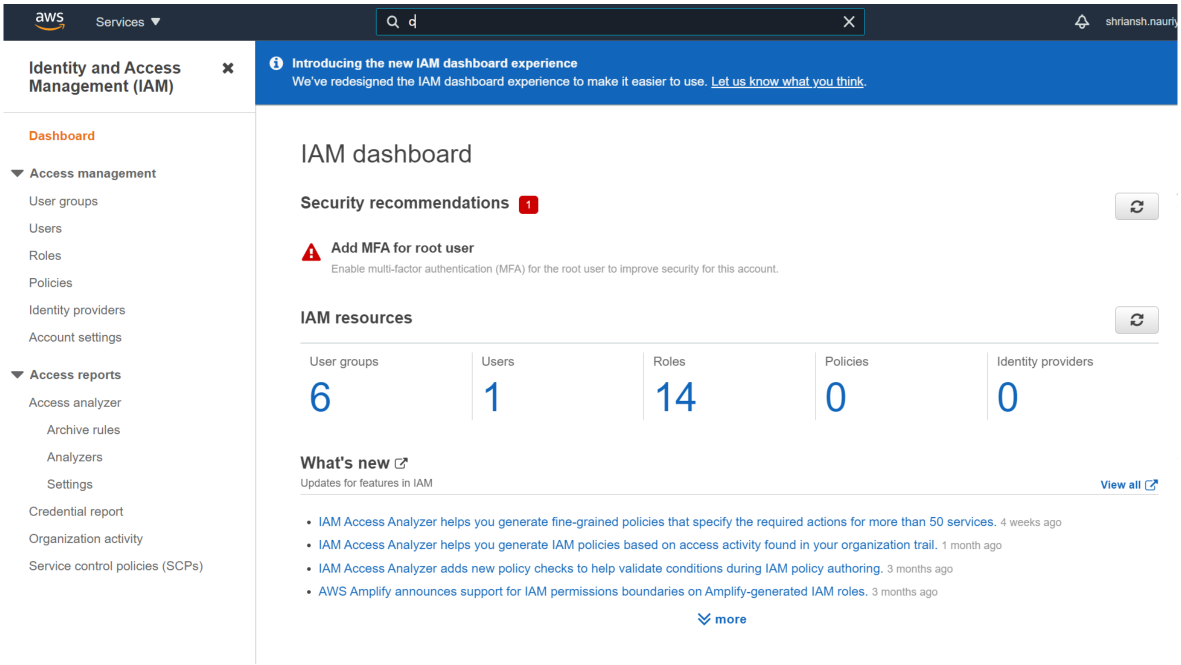
AWS services

Find Services
You can enter names, keywords or acronyms.

IAM

IAM
Manage access to AWS resources

Step 2: Click on **‘Roles’** > click on ‘**Create Role**’



Identity and Access Management (IAM) ✖

Introducing the new IAM dashboard experience
We've redesigned the IAM dashboard experience to make it easier to use. Let us know what you think.

Dashboard

▼ Access management
- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

▼ Access reports
- Access analyzer
  - Archive rules
  - Analyzers
  - Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

IAM dashboard

Security recommendations 1

Add MFA for root user
Enable multi-factor authentication (MFA) for the root user to improve security for this account.

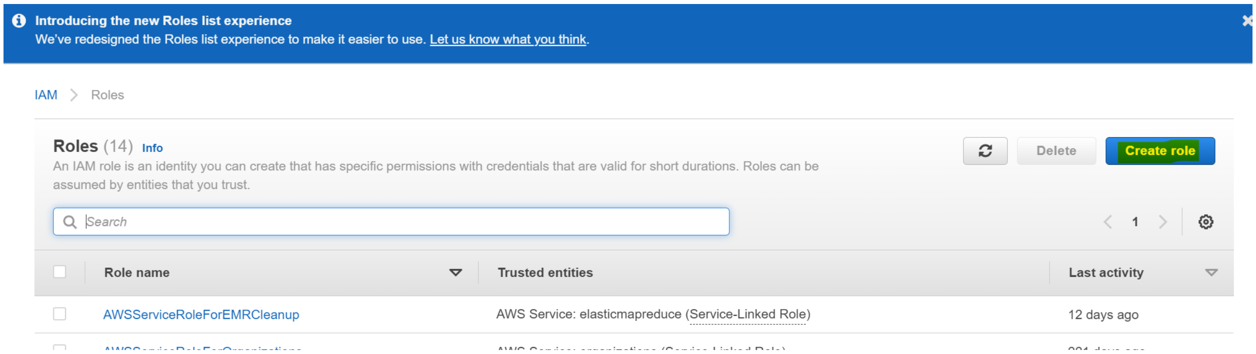
IAM resources

User groups	Users	Roles	Policies	Identity providers
6	1	14	0	0

What's new
Updates for features in IAM
View all

- IAM Access Analyzer helps you generate fine-grained policies that specify the required actions for more than 50 services. 4 weeks ago
- IAM Access Analyzer helps you generate IAM policies based on access activity found in your organization trail. 1 month ago
- IAM Access Analyzer adds new policy checks to help validate conditions during IAM policy authoring. 3 months ago
- AWS Amplify announces support for IAM permissions boundaries on Amplify-generated IAM roles. 3 months ago

more



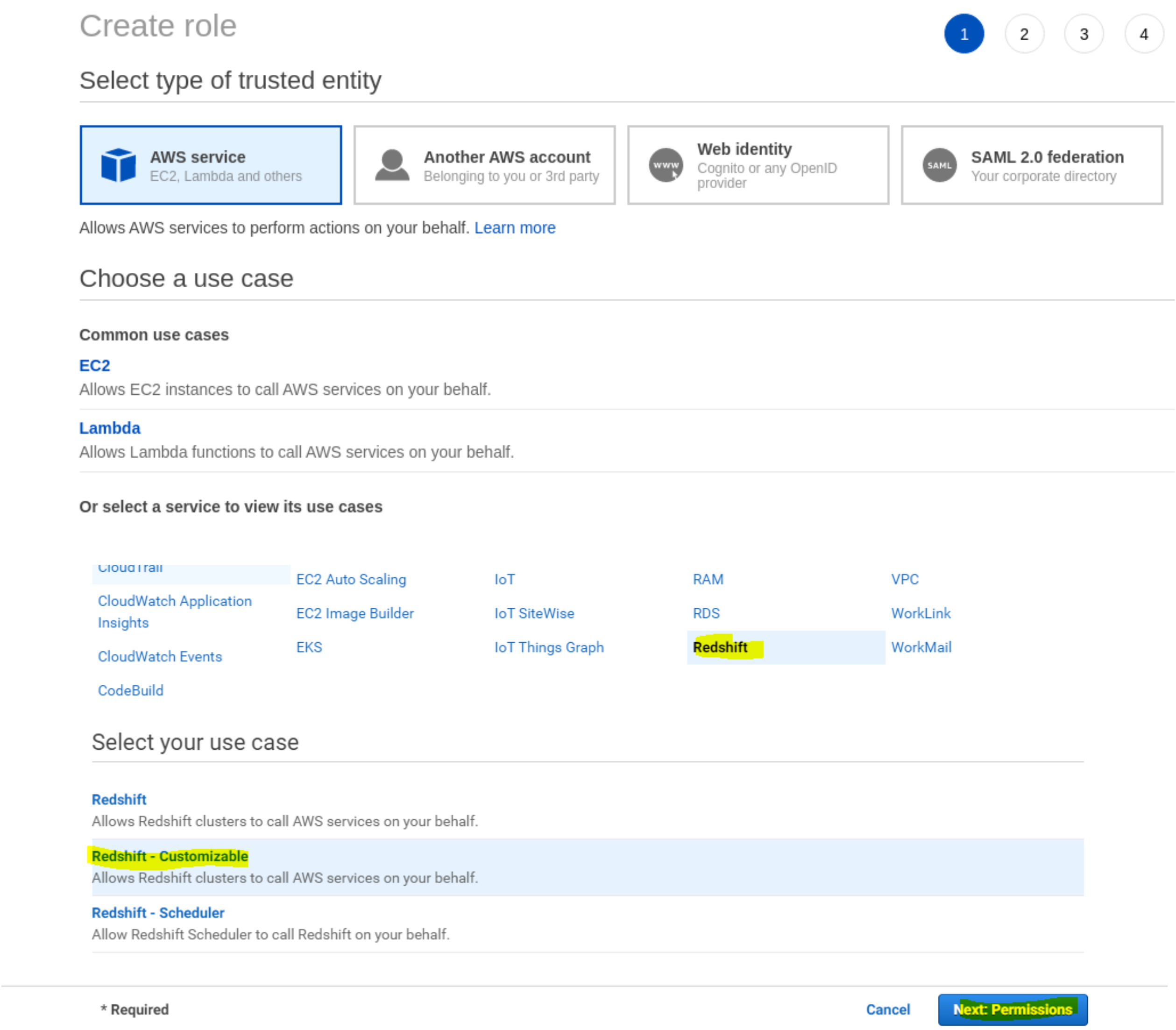
Introducing the new Roles list experience
We've redesigned the Roles list experience to make it easier to use. Let us know what you think.

IAM > Roles

Roles (14) 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
□	AWSServiceRoleForEMRCleanup	AWS Service: elasticmapreduce (Service-Linked Role)	12 days ago

Step 3: Select **Redshift** from the option '**or select a service to view its use case**', and then select **Redshift- Customizable** from **'Select your use case'**, click on **Next: Permissions**.



Create role

Select type of trusted entity

Allows AWS services to perform actions on your behalf. Learn more

Choose a use case

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.

Or select a service to view its use cases

CloudTrail
CloudWatch Application Insights
CloudWatch Events
CodeBuild
EC2 Auto Scaling
EC2 Image Builder
EKS
IoT
IoT SiteWise
IoT Things Graph
RAM
RDS
Redshift
VPC
WorkLink
WorkMail

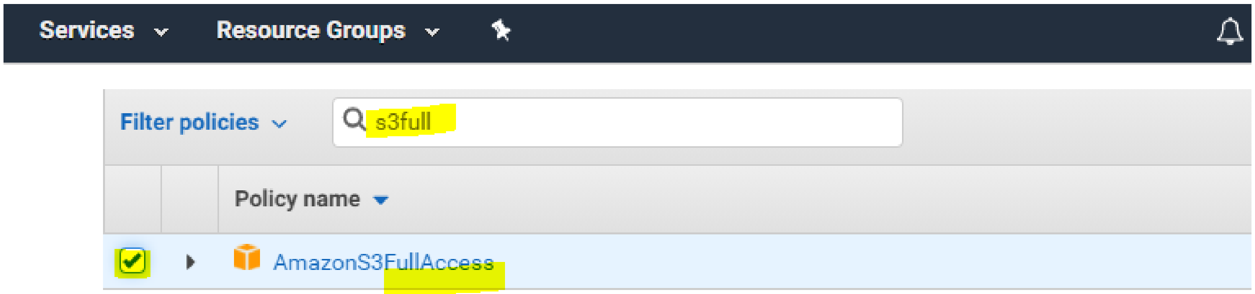
Select your use case

Redshift
Allows Redshift clusters to call AWS services on your behalf.

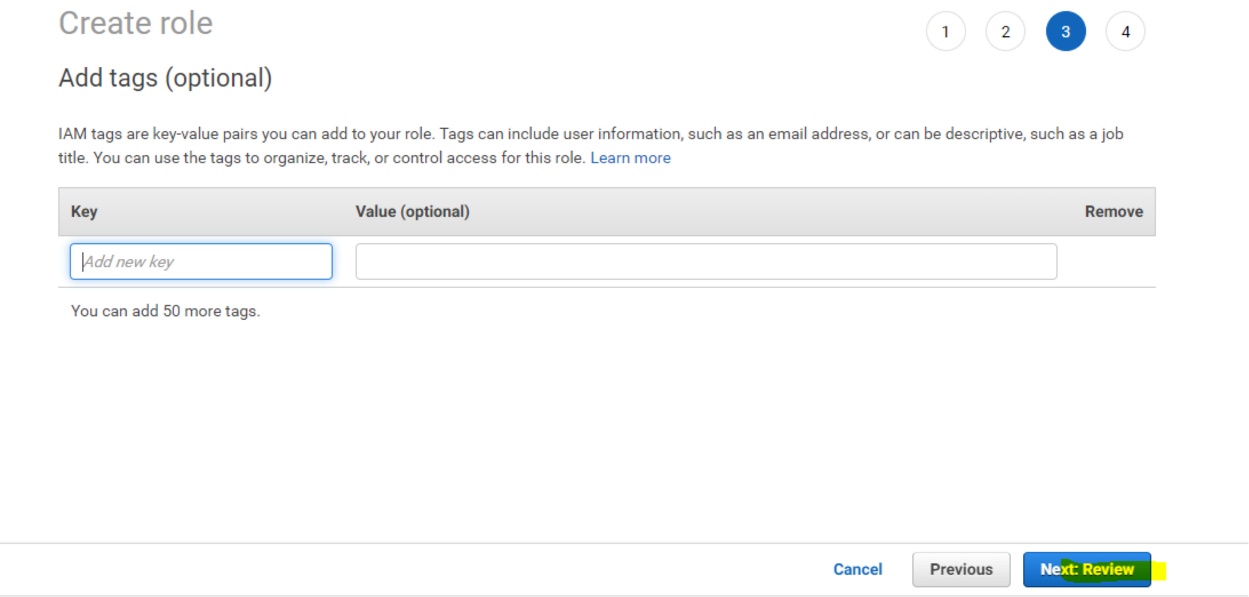
Redshift - Customizable
Allows Redshift clusters to call AWS services on your behalf.

Redshift - Scheduler
Allow Redshift Scheduler to call Redshift on your behalf.

Step 4: In the search field, type '**s3full**' and then click the checkbox for '**AmazonS3FullAccess**' policy. After this, click on **'Next'** again



Step 5: Click on '**Next: Review**'


Create role

Add tags (optional)

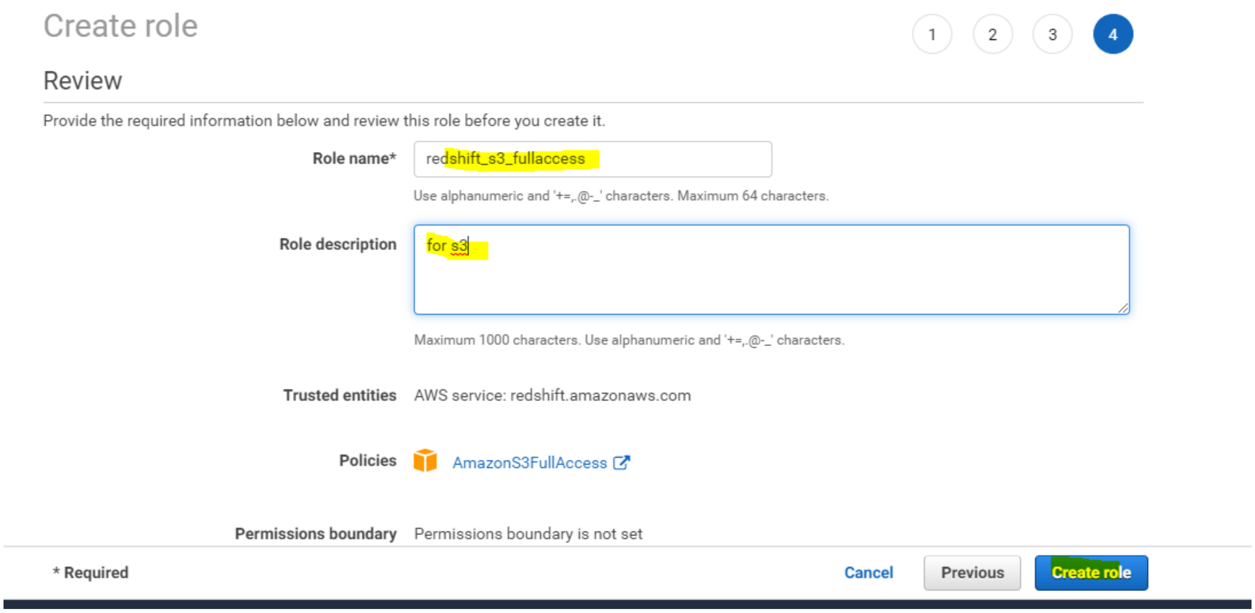
IAM tags are key-value pairs you can add to your role. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this role. Learn more

Key	Value (optional)	Remove
Add new key		

You can add 50 more tags.

Step 6: Provide a name to your role, this will be used later to reference this role while creating the Redshift cluster.

Assign a **'Role name**' and write a '**Role description**' > click on '**Create role**'



Create role

Review

Provide the required information below and review this role before you create it.

Role name* redshift_s3_fullaccess

Use alphanumeric and '+=,.@-_' characters. Maximum 64 characters.

Role description for s3

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

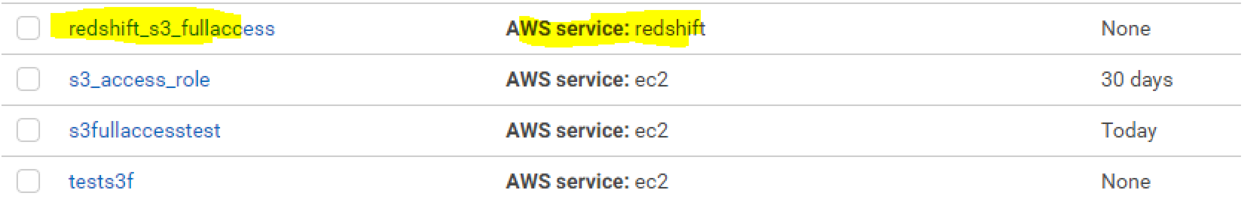
Trusted entities AWS service: redshift.amazonaws.com

Policies AmazonS3FullAccess

Permissions boundary Permissions boundary is not set

* Required

Step 7: You should be able to see your role in the list.



☐	redshift_s3_fullaccess	**AWS service:** redshift	None
☐	s3_access_role	**AWS service:** ec2	30 days
☐	s3fullaccesstest	**AWS service:** ec2	Today
☐	tests3f	**AWS service:** ec2	None