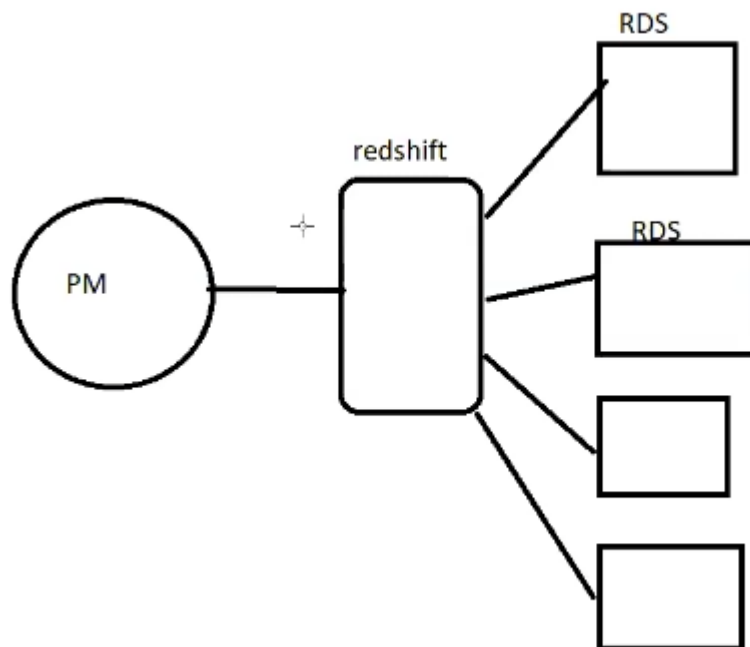


REDSHIFT AND CLOUDTRAIL

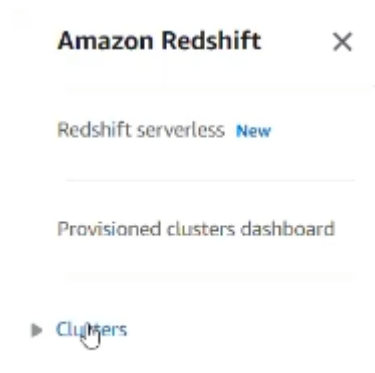
REDSHIFT -- DATA WAREHOUSE

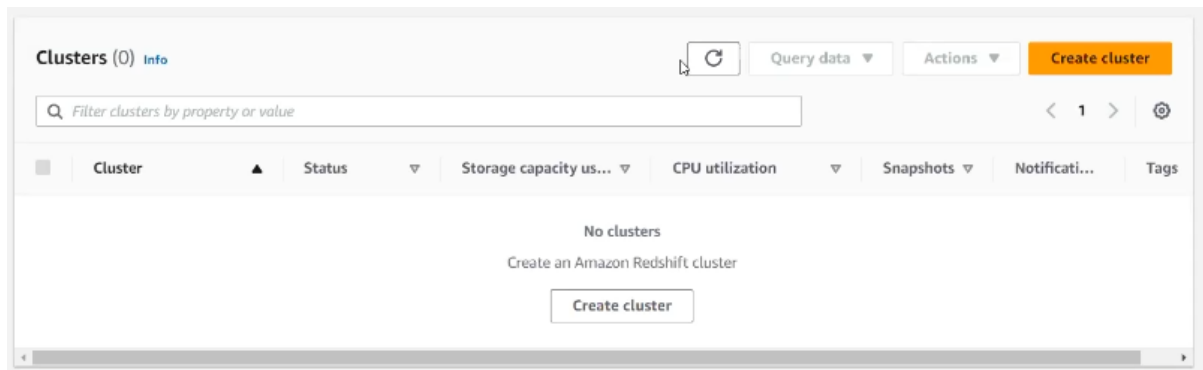
Collection of RDS servers = REDSHIFT



Change unstructured data to structured data = semi structured database

Analytics – amazon redshift





Pair of instances is cluster

Cluster configuration

Cluster identifier
This is the unique key that identifies a cluster.

redshift-cluster-1

The identifier must be from 1-63 characters. Valid characters are a-z (lowercase only) and - (hyphen).

Choose the size of the cluster

☒ I'll choose

☐ Help me choose

Node type [Info](#)
Choose a node type that meets your CPU, RAM, storage capacity, and drive type requirements.

ra3.4xlarge

Number of nodes
Enter the number of nodes that you need.

2

Range (2-32)

Dc2large

No of nodes 2

dc2.large | 2 nodes

<p>\$453.60/month</p> <p>Estimated on-demand compute price</p> <p>Save more than 60% of your costs by purchasing reserved nodes. Learn more</p>	<p>320 GB</p> <p>Total compressed storage</p> <p>The total storage capacity for the cluster if you deploy the number of nodes that you chose.</p>
--	--

Database configuration

Database configurations

Admin user name
Enter a login ID for the admin user of your DB instance.

The name must be 1-128 alphanumeric characters, and it can't be a [reserved word](#).

☐ **Auto generate password**
Amazon Redshift can generate a password for you, or you can specify your own password.

Admin user password
Must be 8-64 characters long. Must contain at least one uppercase letter, one lowercase letter and one number. Can be any printable ASCII character except "/", "*", or "@".

☐ **Show password**

Associated IAM roles (0) [Info](#)

Create, associate, or remove an IAM role. You can associate up to 50 IAM roles. You can also choose an IAM role and set it as the default for this cluster.

Set default ▾Manage IAM roles ▾

< 1 >

<input type="checkbox"/>	IAM roles	Status	Role type
No resources No associated IAM roles			
<button>Associate IAM role</button>			

Select IAM

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:

-
- ☒ **Redshift - Customizable**
Allows Redshift clusters to call AWS services on your behalf.
- ☐ **Redshift**
Allows Redshift clusters to call AWS services on your behalf.
- ☐ **Redshift - Scheduler**
Allow Redshift Scheduler to call Redshift on your behalf.

Cancel

Next

Select redshift

Redshift customizable

Redshift s3 full access permission

"s3" X Clear filters			
	Policy name	Type	Description
<input type="checkbox"/>	s3buck	Custom...	
<input type="checkbox"/>	s3bucketonly06	Custom...	
<input type="checkbox"/>	S3bucketonlysaru	Custom...	
<input type="checkbox"/>	s3only09	Custom...	
<input type="checkbox"/>	sunils3bucket	Custom...	
<input type="checkbox"/>	tamils3	Custom...	
<input type="checkbox"/>	varshinis3policy	Custom...	
<input checked="" type="checkbox"/>	AmazonS3FullAccess	AWS m...	

Creating role reds3.

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.

reds3

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

Associated IAM roles (0) Info

Create, associate, or remove an IAM role. You can associate up to 50 IAM roles. You can also choose an IAM role and set it as the default for this cluster.

Set default

Manage IAM roles

Q Search for associated IAM role by name, status, or role type

< 1 >

IAM roles

Status

Role type

No resources

No associated IAM roles

Associate IAM role

Associate IAM roles

IAM roles

Choose from existing IAM roles. You can associate up to 50 IAM roles with this cluster.

Q

Search for IAM role to associate

< 1 >

☐

IAM roles

☐

[AWSServiceRoleForRedshift](#)

☐

[s3red](#)

Cancel

Associate IAM roles

Reds3

Additional configurations

☒ Use defaults

These configurations are optional, and default settings have been defined to help you get started with your cluster. Turn off "Use defaults" to modify these settings now.

Network

Using default VPC (vpc-04d11bda6dc1e3aa5) and default subnet.

Backup

Automated snapshots are created about every eight hours or following every 5 GB per node of data changes, whichever comes first.

Maintenance

Using current maintenance track.

Security

Using default (sg-027c8491c2f19a582) cluster security group.

Configuration

Using default.redshift-1.0 parameter group with no database encryption.

Cancel

Create cluster

Clusters (1) Info

Q

Filter clusters by property or value

Q

Query data

Actions

Create cluster

< 1 >

<input type="checkbox"/>	Cluster	Status	Storage capacity us...	CPU utilization	Snapshots	Notificati...	Tags
<input type="checkbox"/>	redshift10am dc2.large 2 nodes 320 GB	Creating					

S3 create bucket redshiftbucket10am

Amazon S3 > Buckets > Create bucket

Create bucket [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name

Bucket name must be globally unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region

Asia Pacific (Mumbai) ap-south-1

Copy settings from existing bucket - *optional*
Only the bucket settings in the following configuration are copied.


[Choose bucket](#)

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.

 We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.

Object Ownership

☒ Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

☐ Object writer
The object writer remains the object owner.

 If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. [Learn more](#)

- ☐ **Block all public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
- ☐ **Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
 - ☐ **Block public access to buckets and objects granted through any access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
 - ☐ **Block public access to buckets and objects granted through new public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
 - ☐ **Block public and cross-account access to buckets and objects through any public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.



Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

- ☐ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Bucket versioning enable

Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption key type [Info](#)

- ☒ Amazon S3 managed keys (SSE-S3)
☐ AWS Key Management Service key (SSE-KMS)

Bucket Key

When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS.

[Learn more](#) [?](#)

- ☒ Disable
☐ Enable

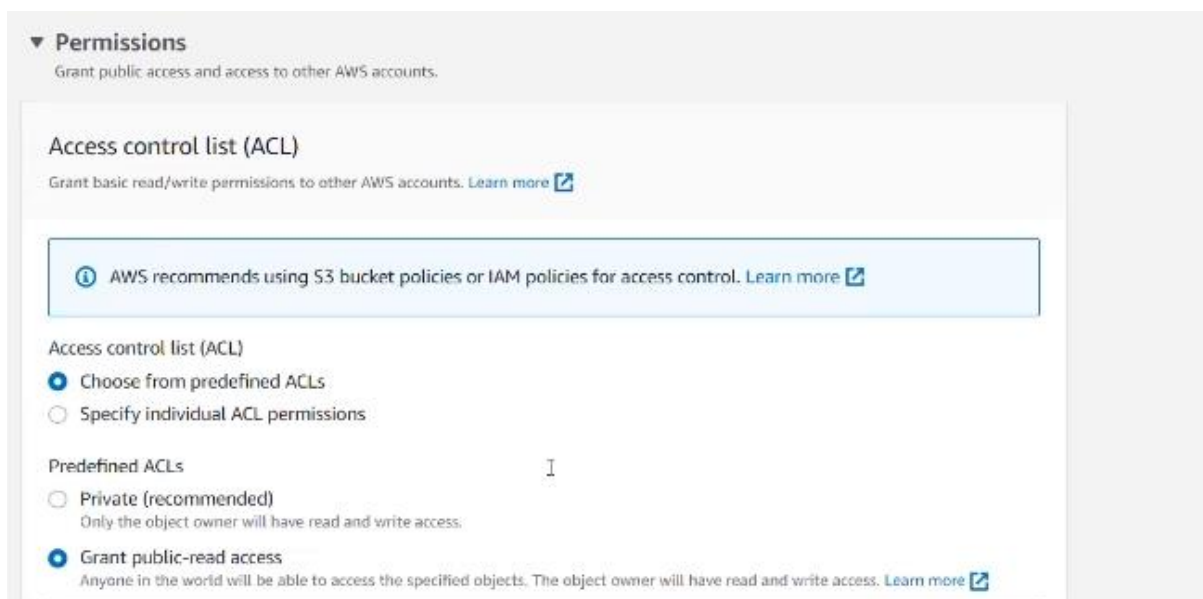
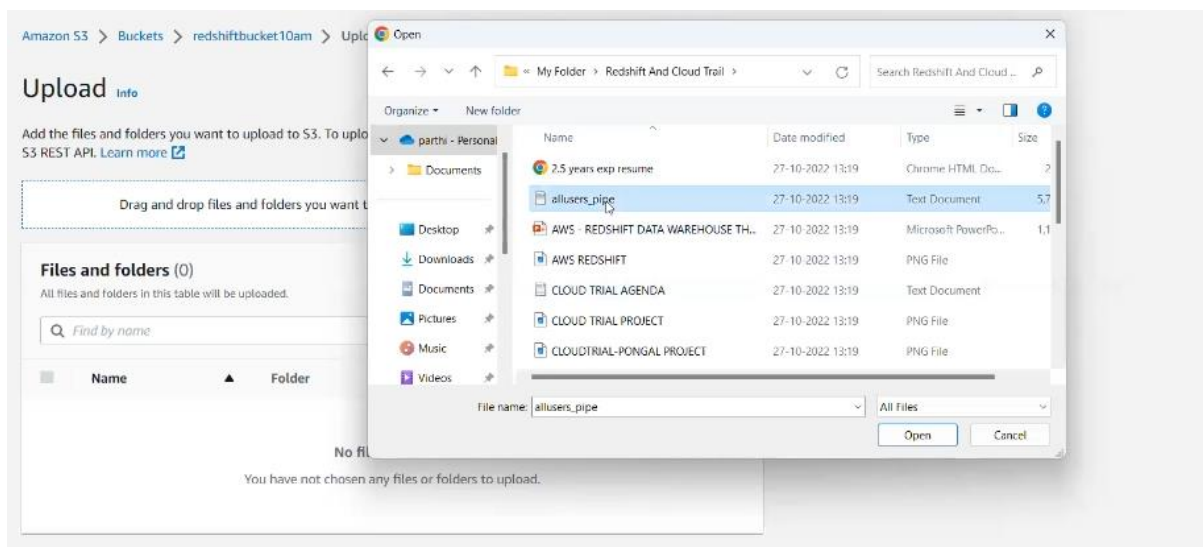
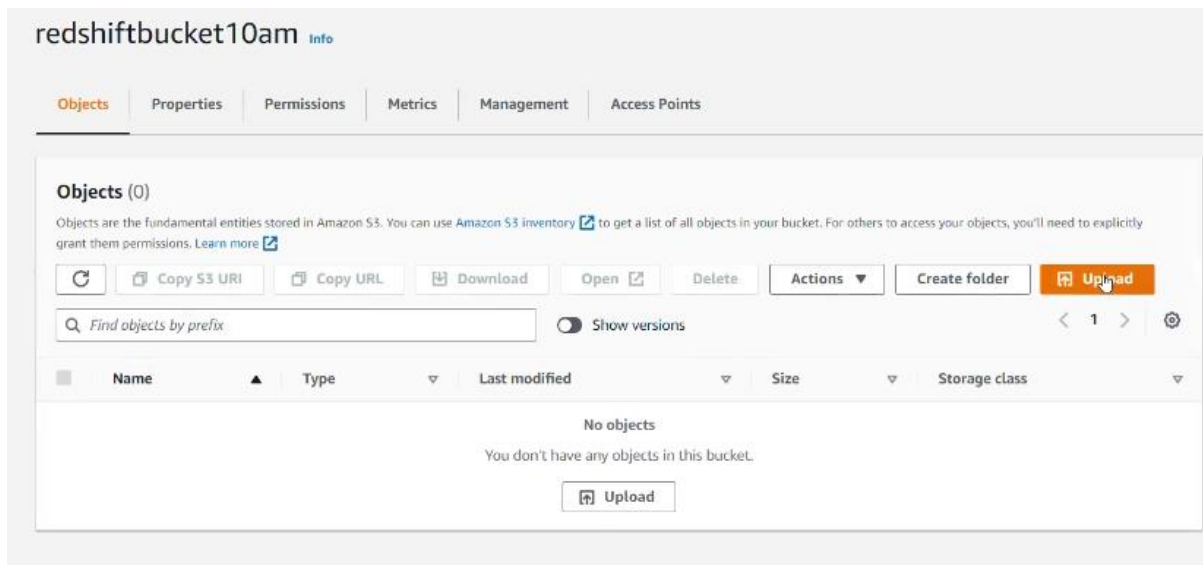
► Advanced settings

[?](#) After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel

Create bucket

Upload object in the bucket



Amazon S3 > Buckets > redshiftbucket10am

redshiftbucket10am [Info](#)

Objects | Properties | Permissions | Metrics | Management | Access Points

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

[Refresh](#) [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

[Show versions](#)

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	allusers_pipe.txt	txt	May 3, 2023, 10:59:54 (UTC+05:30)	5.6 MB	Standard

Cluster created

Amazon Redshift > Clusters > redshift10am

redshift10am

[Actions](#) [Edit](#) [Add partner integration](#) [Query data](#)

General information [Refresh](#)

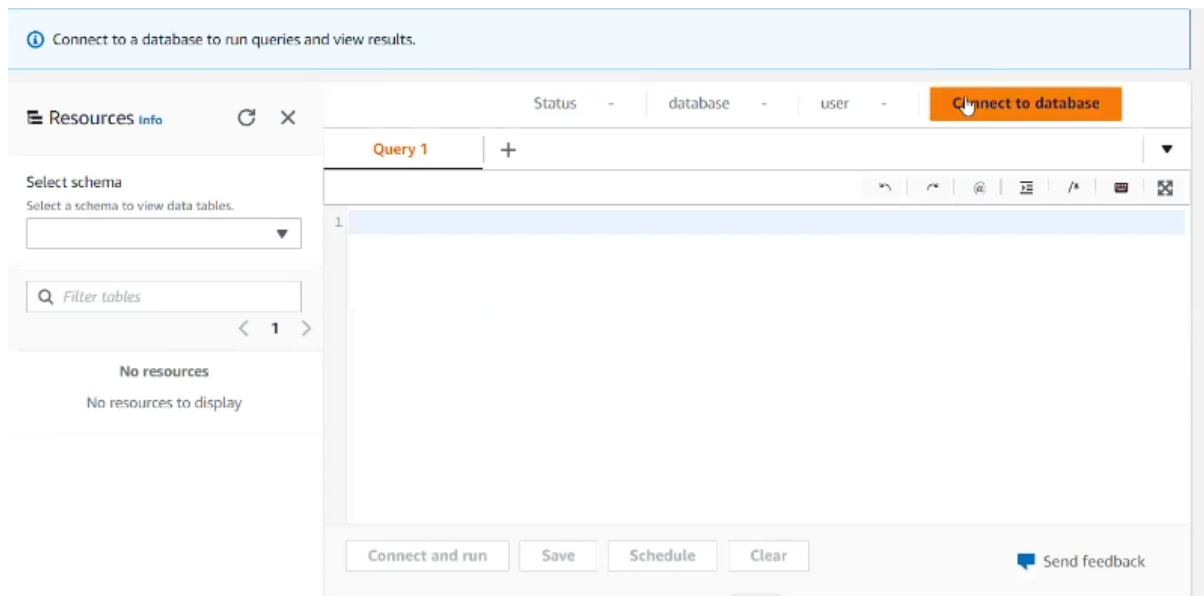
Cluster identifier redshift10am	Status Available Date created May 03, 2023, 10:59 (UTC+05:30) Storage used - Multi-AZ No	Node type dc2.large Number of nodes 2	Endpoint redshift10am.coil2gvzilun.ap-south-1.r... JDBC URL jdbc:redshift://redshift10am.coil2gvzil... ODBC URL Driver={Amazon Redshift (x64)}; Server...
------------------------------------	--	--	--

Cluster performance | Query monitoring | Schedules | Maintenance | **Properties**

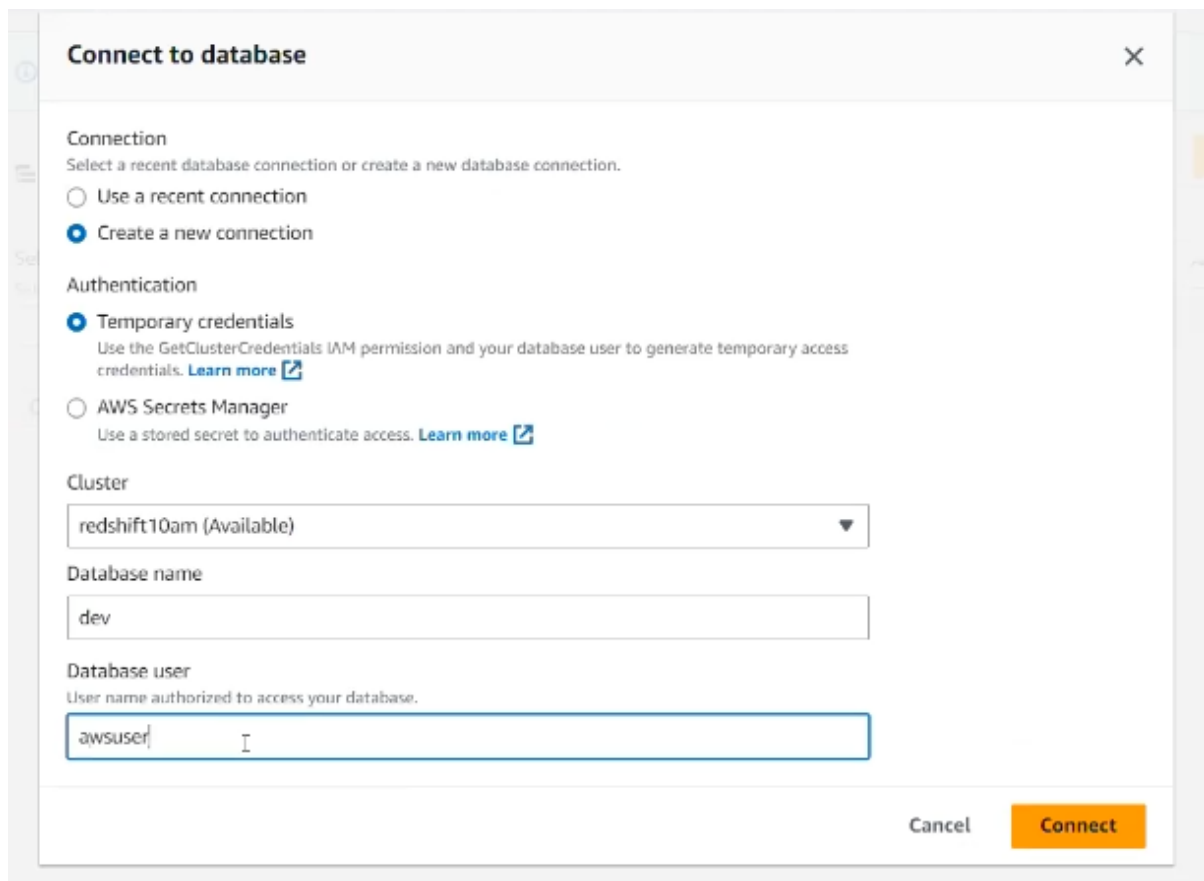
Database configurations [Edit admin credentials](#) [Rotate encryption keys](#) [Edit](#)

Database name dev	Parameter group Defines database parameter and query queues for all the databases. default.redshift-1.0	Encryption Disabled AWS KMS key ID -	Audit logging Disabled
Port 5439	SSH ingestion setting (cluster public key) ssh-rsa AAAAB3NzaC1yc2EAAAADA...		

Query editor



Connect to database



```
create table users(
  userid integer not null distkey sortkey,
  username char(8),
  firstname varchar(30),
  lastname varchar(30),
  city varchar(30),
  state char(2),
  email varchar(100),
  phone char(14),
  likesports boolean,
  liketheatre boolean,
  likeconcerts boolean,
  likejazz boolean,
  likeclassical boolean,
  likeopera boolean,
  likerock boolean,
  likevegas boolean,
  likebroadway boolean,
  likemusicals boolean);
```

Copy and paste this in query editor

User table created

Go to IAM COPY ARN

[IAM](#) > [Roles](#) > reds3

reds3

Delete

Allows Redshift clusters to call AWS services on your behalf.

Summary

Edit

Creation date

May 03, 2023, 10:57 (UTC+05:30) ⓘ

ARN

arn:aws:iam::174912287653:role/reds3

Last activity

None

Maximum session duration

1 hour

```
copy users from 's3://redshiftbucket10am/allusers_pipe.txt'
credentials 'aws_iam_role=arn:aws:iam::174912287653:role/reds3'
delimiter '|' region 'ap-south-1';
```

SELECT *

FROM USERS

Rows returned (49990)

Export ▼

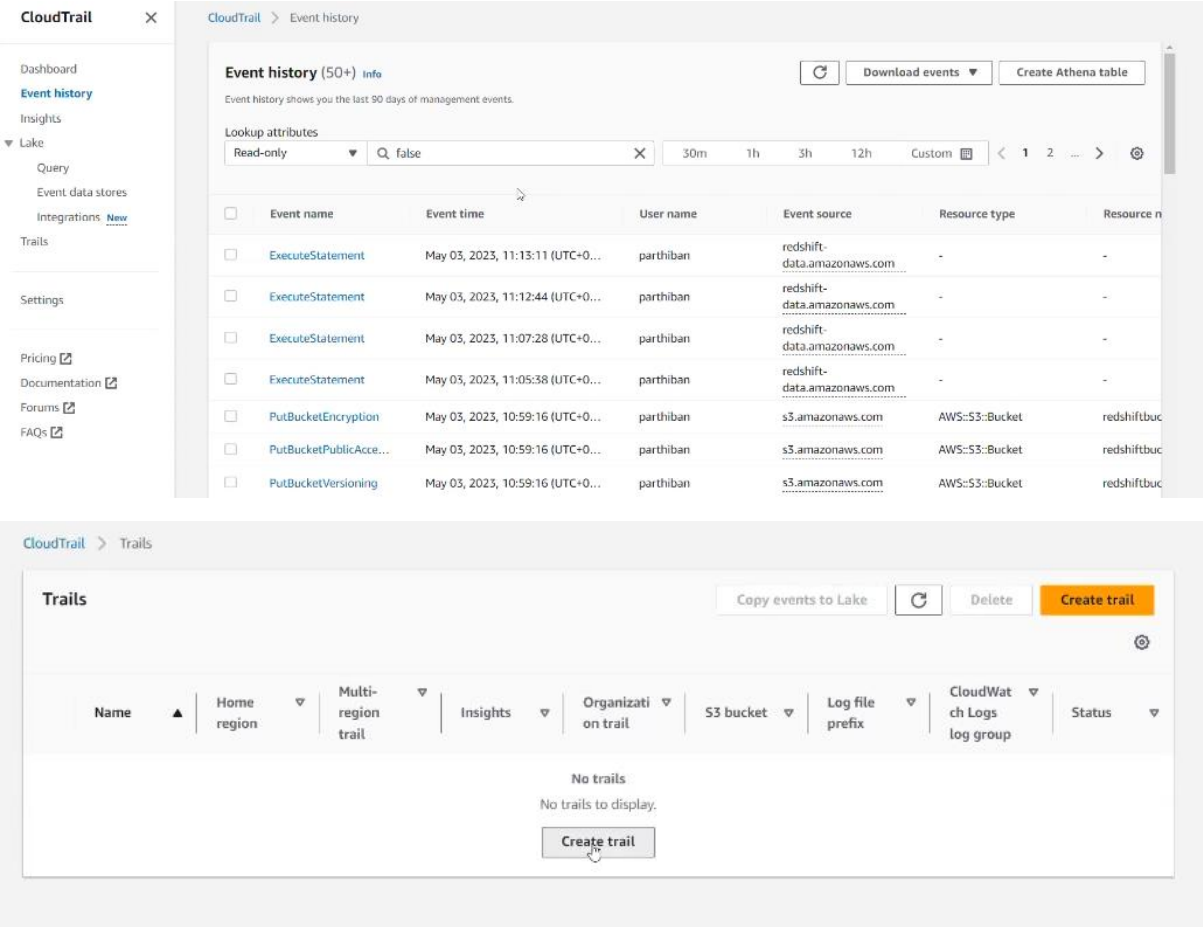
Q Search rows

< 1 2 3 4 5 6 7 ... 4999 > ⚙

userid ▼	username ▼	firstname ▼	lastname ▼	city ▼	state ▼	email ▼
3	IFT66TXU	Lars	Ratliff	High Point	ME	amet.faucibus.ut@condimentumegetvolutpat.ca
8	AZG78YIP	Colton	Roy	Guayama	AK	ullamcorper.nisl@Cras.edu
12	FVK28WAS	Bruce	Beck	Kona	OH	ac@velit.ca
13	QTF33MCG	Henry	Cochran	Bossier City	QC	Aliquam.vulputate.ullamcorper@amalesuada.org
17	WWZ18EOX	Cody	Moss	Mobile	ON	dolor.nonummy@ipsumdolorsit.ca
21	JEO48YJJ	Ralph	Bird	Charlotte	NM	justo.nec.ante@quismassa.edu
26	XBG73AGE	Wing	Jennings	Roswell	WI	non@enimsitamet.edu
30	HMF84NKS	Guy	Cochran	Effingham	NU	Nullam.enim@Maecenas.com

CLOUDTRAIL

CloudTrail is a monitoring tool it's a service that captures user actions



Trail name

Enter a display name for your trail.

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

☐ Enable for all accounts in my organization

To review accounts in your organization, open AWS Organizations. [See all accounts](#)

Storage location [Info](#)

☒ Create new S3 bucket
Create a bucket to store logs for the trail.

☐ Use existing S3 bucket
Choose an existing bucket to store logs for this trail.

Trail log bucket and folder

Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.

Logs will be stored in aws-cloudtrail-logs-174912287653-3af2328c/AWSLogs/174912287653

Log file SSE-KMS encryption [Info](#)

☒ Enabled

☒ New

☐ Existing

AWS KMS alias

KMS key and S3 bucket must be in the same region.

Step 1

Choose trail attributes

Step 2

Choose log events

Step 3

Review and create

Choose log events

Events [Info](#)

Record API activity for individual resources, or for all current and future resources in AWS account. [Additional charges apply](#)

Event type

Choose the type of events that you want to log.

☒ Management events

Capture management operations performed on your AWS resources.

☐ Data events

Log the resource operations performed on or within a resource.

☐ Insights events

Identify unusual activity, errors, or user behavior in your account.

Management events [Info](#)

Management events show information about management operations performed on resources in your AWS account.

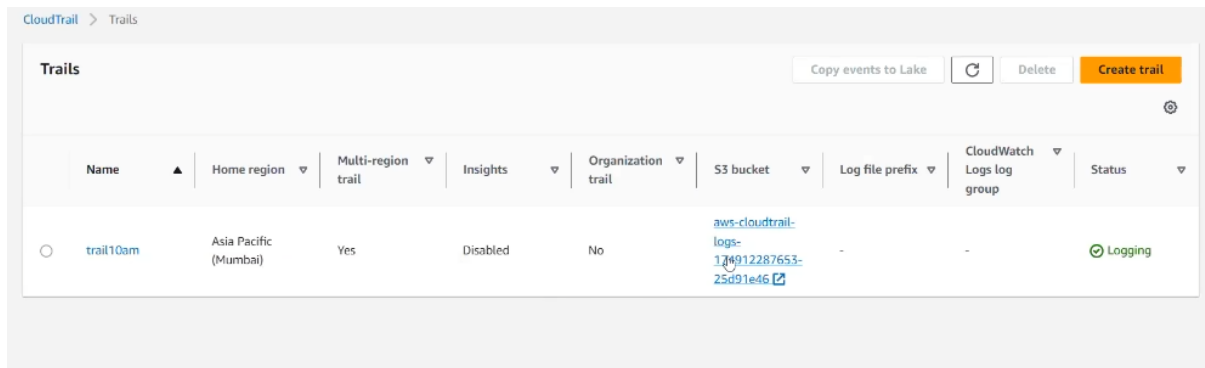
No additional charges apply to log management events on this trail because this is your first copy of management events.

API activity

Choose the activities you want to log.

☒ Read

☒ Write



S3 bucket created

