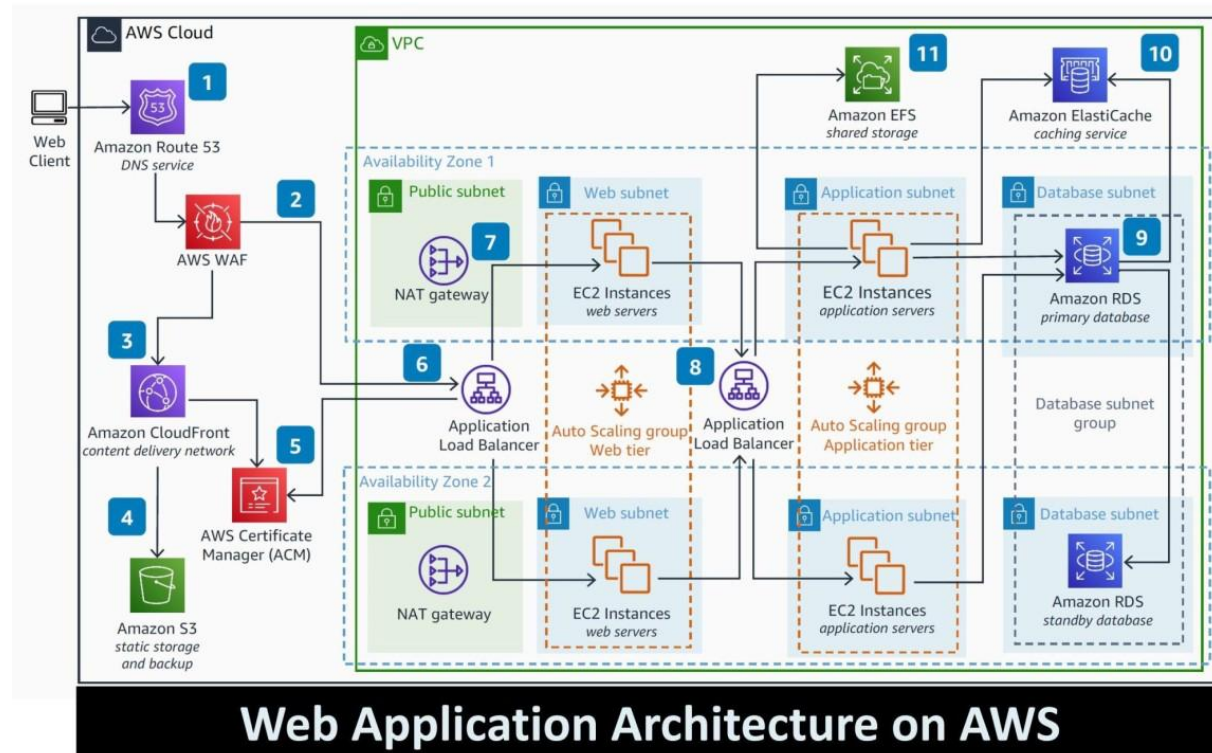


# COMPLETE 3 TIER ARCHITECTURE

## MODEL DIAGRAM



CREATE 1 VPC

2 PUB , 2 PRIVATE , ANOTHER 2 PRIVATE SUBNET

CREATE AUTO SCALING GROUP FOR PUB SUBNET AND CHECK THE LOAD BALANCER DNS IT WILL WORK

CREATE 2ND AUTO SCALING GROUP FOR PRIVATE SUBNET WITH INTERNAL LOAD BALANCER CHECK THIS DNS WITH THE ROUTE 53

NOW ADD THIS ROUTE 53 4 AWS DNS TO THE HOSTINGER WEBSITE WHERE YOU ALREADY GOT THE DOMAIN NAME

Record for theparthibanm.online was successfully created. Route 53 propagates your changes to all of the Route 53 authoritative DNS servers within 60 seconds. Use "View status" button to check propagation status.

View status

Record details

Edit record

Record name  
theparthibanm.online

Record type  
NS

Value  
ns-187.awsdns-23.com.  
ns-1796.awsdns-32.co.uk.  
ns-560.awsdns-06.net.  
ns-1094.awsdns-08.org.

Alias  
No

Hosted zone details

Edit hosted zone

Records (3) | DNSSEC signing | Hosted zone tags (0)

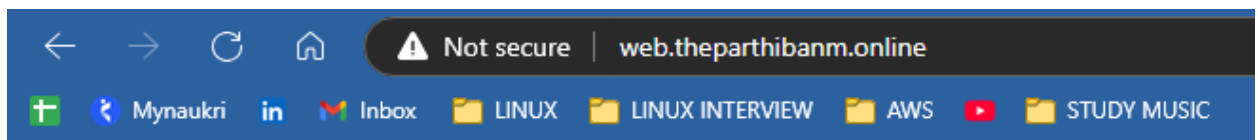
Records (1/3) Info

The following table lists the existing records in theparthibanm.online. You can't delete the SOA record or the NS record named theparthibanm.online.

Filter records by property or value

Type Routing p... Alias

Record name	Type	Routing	Diff	Alias	Value/Route traffic to	TTL	Health	Evalu
theparthibanm.online	NS	Simple	-	No	ns-187.awsdns-23.com. ns-1796.awsdns-32.co.uk. ns-560.awsdns-06.net. ns-1094.awsdns-08.org.	172800	-	-
theparthibanm.online	SOA	Simple	-	No	ns-187.awsdns-23.com. a...	900	-	-
web.theparthibanm....	A	Simple	-	Yes	duatstack.myasg1-1-200...	-	-	Yes



this is cloud watch test

create nat gateway for private subnets

create a db instance in the private subnet 5

Databases (1)

Group resources

Modify

Actions

Restore from S3

Create database

Filter by databases

DB identifier	Status	Role	Engine	Region	Size	Recommendations	CPU
database-1	Available	Instance	MySQL C...	ap-south...	db.t4g.m...	-	-

### Summary

DB identifier database-1	Status Available	Role Instance	Engine MySQL Community
CPU 2.88%	Class db.t4g.micro	Current activity 0 Connections	Region & AZ ap-south-1a

[Connectivity & security](#)
[Monitoring](#)
[Logs & events](#)
[Configuration](#)
[Zero-ETL integrations](#)
[Maintenance & backu](#)

### Connectivity & security

#### Endpoint & port

Endpoint copied

database-1.cn46s2kq0hwd.ap-sout  
h-1.rds.amazonaws.com

Port  
3306

#### Networking

Availability Zone  
ap-south-1a

VPC  
myownvpc (vpc-0dbeb12abc45cee4a)

Subnet group  
default-vpc-0dbeb12abc45cee4a

#### Security

VPC security groups  
[httpd \(sg-03d71f0562556b5f4\)](#)  
Active  
[default \(sg-0ae78585eeffe2205\)](#)  
Active

Publicly accessible  
No

enable the mysql port in the security group

## Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

### Inbound rules [Info](#)

Security group rule ID	Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Source <a href="#">Info</a>
sgr-09e44705ad43b080b	HTTP	TCP	80	Custom <input type="text" value="0.0.0.0/0"/>
sgr-09cdf9daed0a1f9af	SSH	TCP	22	Custom <input type="text" value="0.0.0.0/0"/>
-	MYSQL/Aurora	TCP	3306	Anywh... <input type="text" value="0.0.0.0/0"/>

Add rule

take the public instance connect and take console of private instance and acces the db instance

```

Last login: Thu Oct 24 12:50:36 2024 from 192.168.2.6
[ec2-user@ip-192-168-3-7 ~]$ sudo -i
[root@ip-192-168-3-7 ~]# yum whatprovides mysql
Amazon Linux 2023 repository
Amazon Linux 2023 Kernel Livepatch repository
mariadb105-3:10.5.16-1.amzn2023.0.7.x86_64 : A very fast and robust SQL database server
Repo      : amazonlinux
Matched from:
Filename  : /usr/bin/mysql

mariadb105-3:10.5.18-1.amzn2023.0.1.x86_64 : A very fast and robust SQL database server
Repo      : amazonlinux
Matched from:
Filename  : /usr/bin/mysql

mariadb105-3:10.5.20-1.amzn2023.0.1.x86_64 : A very fast and robust SQL database server
Repo      : amazonlinux
Matched from:
Filename  : /usr/bin/mysql

mariadb105-3:10.5.23-1.amzn2023.0.1.x86_64 : A very fast and robust SQL database server
Repo      : amazonlinux
Matched from:
Filename  : /usr/bin/mysql

mariadb105-3:10.5.25-1.amzn2023.0.1.x86_64 : A very fast and robust SQL database server
Repo      : amazonlinux
Matched from:
Filename  : /usr/bin/mysql

[root@ip-192-168-3-7 ~]# yum install mariadb105-3:10.5.16-1.amzn2023.0.7.x86_64

```

```

Complete!
[root@ip-192-168-3-7 ~]# show databases;
-bash: show: command not found
[root@ip-192-168-3-7 ~]# mysql -u admin -h database-1.cn46s2kq0hwd.ap-south-1.rds.amazonaws.com -pparthi123
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 44
Server version: 8.0.39 Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

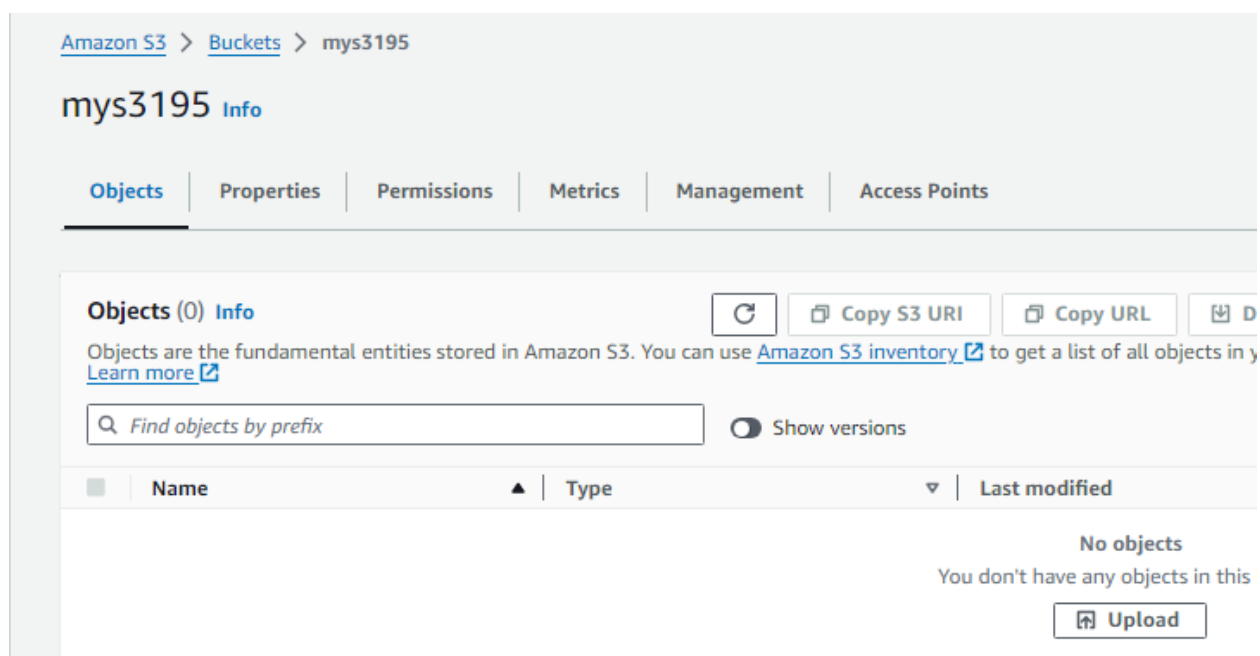
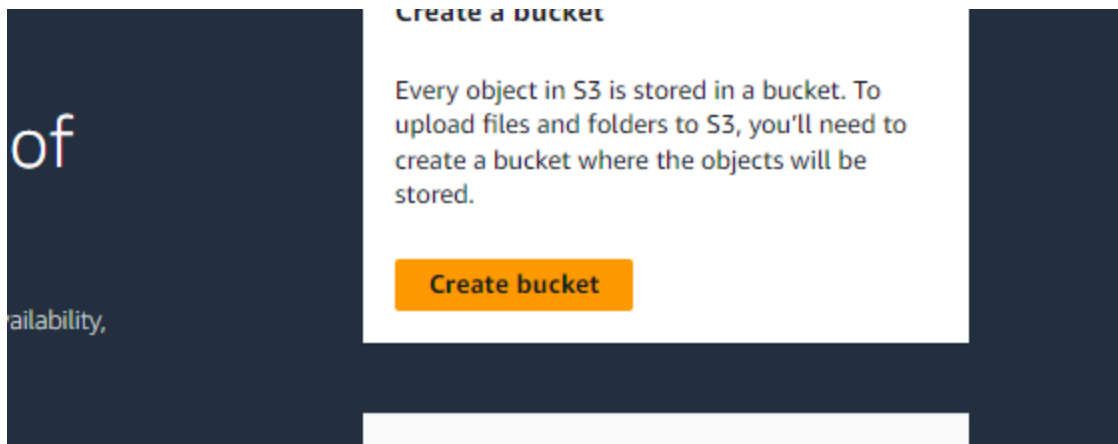
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| sys |
+-----+
4 rows in set (0.015 sec)

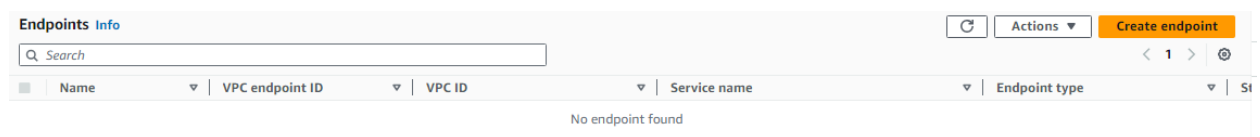
MySQL [(none)]> |

```

create s3 bucket



create endpoint for vpc



## Endpoint settings

### Name tag - optional

Creates a tag with a key of 'Name' and a value that you specify.

myvpcentpoint1

### Service category

Select the service category

☒ AWS services  
Services provided by Amazon

☐ PrivateLink Ready partner services  
Services with an AWS Service Ready de

☐ EC2 Instance Connect Endpoint  
An elastic network interface that allow you to connect to resources in a private subnet

☐ Other endpoint services  
Find services shared with you by service

## Services (1/2)

Search

Service Name = com.amazonaws.ap-south-1.s3 X

Clear filters

	Service Name	Owner	Type
<input type="radio"/>	com.amazonaws.ap-south-1.s3	amazon	Gateway
<input checked="" type="radio"/>	com.amazonaws.ap-south-1.s3	amazon	Interface

Services

EC2

EFS

IAM

VPC

RDS

Route 53

CloudWatch

S3

VPC

Select the VPC in which to create the endpoint

VPC

The VPC in which to create your endpoint.

vpc-0ddeb12abc45cee4a (myownvpc)

Additional settings

Subnets ( 2/3 ) Info

Availability Zone	Subnet ID	Designate IP addresses	IPv4 address	IPv6 address
<input checked="" type="checkbox"/> ap-south-1a (aps1-az1)	subnet-06d098c2d3694568b	<input type="checkbox"/>		
<input checked="" type="checkbox"/> ap-south-1b (aps1-az3)	subnet-00b50cd48fb4a6ab	<input type="checkbox"/>		
<input type="checkbox"/> ap-south-1c (aps1-az2)	No subnet available			

IP address type

☒ IPv4

☐ IPv6

☐ Dualstack

Security groups (2) Info

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Security groups (2/2) Info

Q Search

<input checked="" type="checkbox"/>	Group ID	Group name	VPC ID	Description
<input checked="" type="checkbox"/>	<a href="#">sg-03d71f0562556b5f4</a>	httpd	<a href="#">vpc-0dbeb12abc45cee4a</a>	http
<input checked="" type="checkbox"/>	<a href="#">sg-0ae78585eeffe2205</a>	default	<a href="#">vpc-0dbeb12abc45cee4a</a>	default VPC security group

sg-03d71f0562556b5f4 X

sg-0ae78585eeffe2205 X

Policy Info

VPC endpoint policy controls access to the service.

☒ Full access

Allow access by any user or service within the VPC using credentials from any Amazon Web Services accounts to any resources in this Amazon Web Services service Amazon Web Services service-specific policies (e.g. Amazon S3 bucket policies, any S3 ACL policies) — must grant the necessary permissions for access to succeed.

☐ Custom

Use the [policy creation tool](#) to generate a policy, then paste the generated policy below.

1	
---	--

Endpoints (1/1) Info

Q Search

<input checked="" type="checkbox"/>	Name	VPC endpoint ID	VPC ID	
<input checked="" type="checkbox"/>	myvpceendpoint1	<a href="#">vpce-00797636c20884054</a>	<a href="#">vpc-0dbeb12abc45cee4a</a>   myown...	c

upload file to s3 bucket

[Amazon S3](#) > [Buckets](#) > [mys3195](#) > Upload

## Upload [Info](#)

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

**Files and folders** (1 Total, 4.8 KB)

[Remove](#)

[Add files](#)

[Add folder](#)

All files and folders in this table will be uploaded.

< 1 >

<input type="checkbox"/>	Name	Folder
<input type="checkbox"/>	index.html	-

## Destination [Info](#)

Destination

[s3://mys3195](#)

### ► Destination details


Bucket settings that impact new objects stored in the specified destination.

## udShell [Feedback](#)

Grant public access and access to other AWS accounts.

## Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. [Learn more](#)

 AWS recommends using S3 bucket policies or IAM policies for access control. [Learn more](#)

Access control list (ACL)

- ☒ Choose from predefined ACLs
- ☐ Specify individual ACL permissions

Predefined ACLs

- ☐ Private (recommended)  
Only the object owner will have read and write access.

- ☒ Grant public-read access  
Anyone in the world will be able to access the specified objects. The object owner will have read and write access. [Learn more](#)



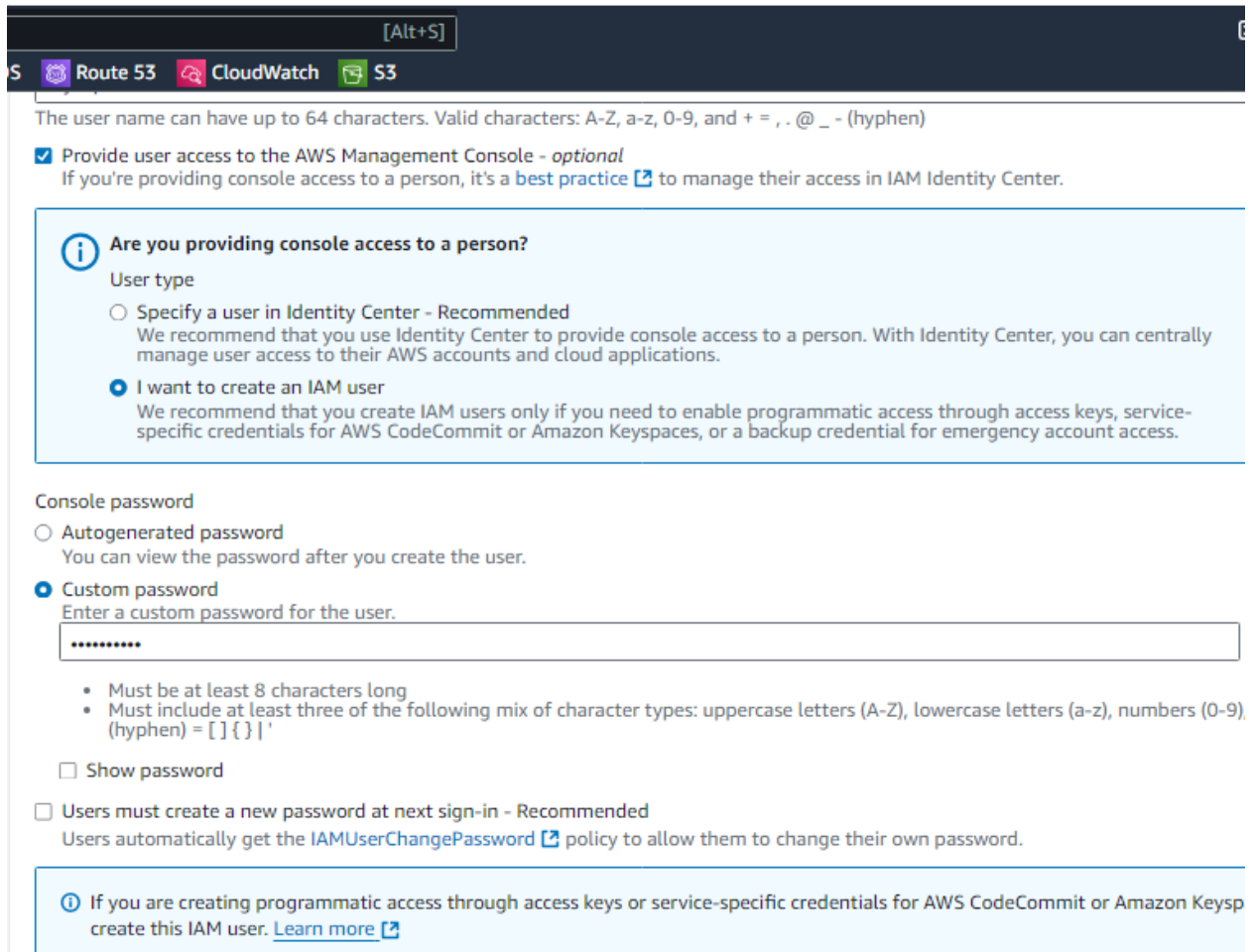
### Granting public-read access is not recommended

Anyone in the world will be able to access the specified objects. [Learn more](#)

☒ I understand the risk of granting public-read access to the specified objects.



create one IAM user



[Alt+S]

S Route 53 CloudWatch S3

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ \_ - (hyphen)

☒ Provide user access to the AWS Management Console - *optional*  
If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

**i Are you providing console access to a person?**

User type

- ☐ Specify a user in Identity Center - Recommended  
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.
- ☒ I want to create an IAM user  
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

- ☐ Autogenerated password  
You can view the password after you create the user.
- ☒ Custom password  
Enter a custom password for the user.

\*\*\*\*\*

  - Must be at least 8 characters long
  - Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), (hyphen) = [ ] { } ' '

☐ Show password

☐ Users must create a new password at next sign-in - Recommended  
Users automatically get the `IAMUserChangePassword` policy to allow them to change their own password.

**i** If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, create this IAM user. [Learn more](#)

attach s3 policy for that user

## Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

### Permissions options

☐ Add user to group

Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

☐ Copy permissions

Copy all group memberships, attached managed policies, and inline policies from an existing user.

☒ Attach policies directly

Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

### Permissions policies (1/1242)

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



Create policy

Q s3

Filter by Type

All types

12 matches

< 1 > ⚙

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	AmazonDMSRedshiftS3Role	AWS managed	0
<input checked="" type="checkbox"/>	AmazonS3FullAccess	AWS managed	0
<input type="checkbox"/>	AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	0

## create access key for the user

Create access key

### Retrieve access keys [Info](#)

#### Access key

If you lose or forget your secret access key, create a new access key and make the old key inactive.

Access key

AKIAW5BDRF6WD4BNZLUI

Secret access key copied

nmPcwGU2f/2tqYXKBLrdsFL3qa/+QxjEArMZ3GlR [Hide](#)

#### Access key best practices

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the [best practices for managing AWS access keys](#).

Download .csv file

Done

## connect your public instance and check the output



export to amazon s3

RDS > Snapshots > fvbv > Export to Amazon S3

## Export to Amazon S3 [Info](#)

Use RDS DB snapshot export to Amazon S3 to extract data from snapshots and store it in a compressed, queryable format in an S3 bucket in your AWS account.

### Settings

#### Export identifier

Enter a name to identify the export. The name must be unique across all DB snapshot exports owned by your AWS account in the current AWS Region.

export-identifier

The export identifier is case-insensitive, but is stored as all lowercase (as in "myexport"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

### Exported data

#### Exported data format

Amount of data to be exported

#### ☐ Partial

Part of the database is exported. You can define which part by using identifiers.

### S3 destination



#### S3 bucket

mys3195

#### S3 prefix - optional [Info](#)

To group objects in a bucket, S3 uses a prefix before object names. The forward slash (/) in the prefix represents a folder. For example, use the prefix exports/2019 for a 2019 folder in an exports folder. RDS will append the prefix with a "/".

### IAM role



#### IAM role

Choose or create an IAM role to grant write access to your S3 bucket.

Choose an option

### Encryption

