

School: CLOUDBOOSTA	Course: Cloud Computing & DevOps
Name: AKOSA SAMUEL ONYEJEKWE	Module: Serverless Computing & Database
	Class 6: Assignment 2 of 6_ Database_1
Student No: CBALC0168	Issue Date: April 1, 2026

Tasks:

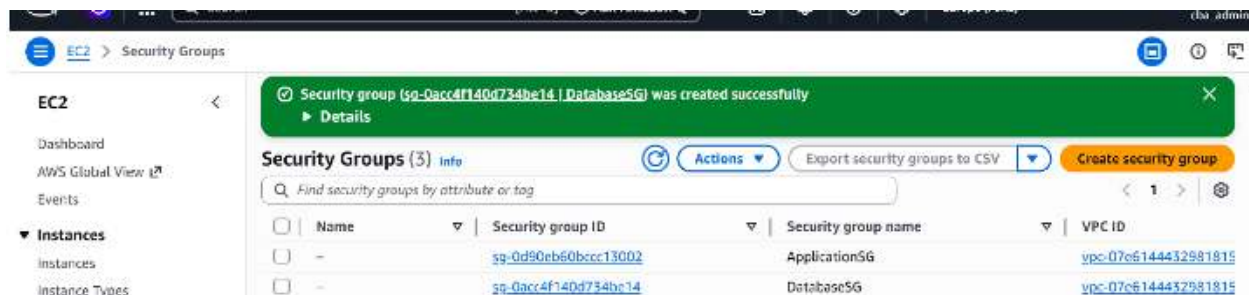
1. Create Application Security Group
2. Configure Database Security Group
3. Launch Amazon EC2 instance
4. Create Amazon RDS database
5. Inspect and verify database

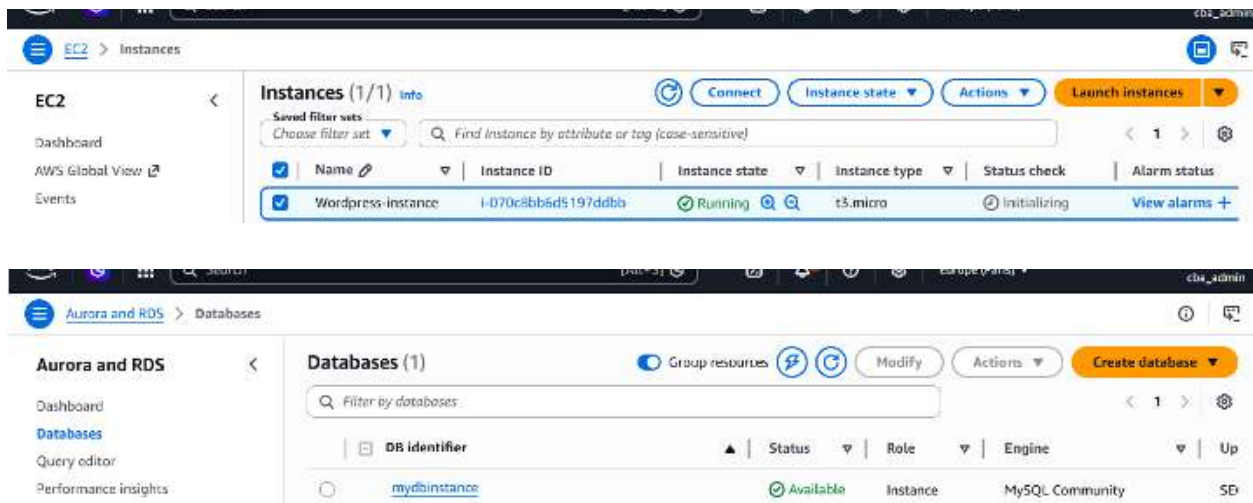
Goal:

To deploy a WordPress-based architecture by provisioning an EC2 instance and creating a managed database using Amazon RDS.

Result:

- Application Security Group successfully created
- Database Security Group configured with MySQL access
- EC2 instance launched successfully
- Amazon RDS database created using MySQL engine
- Database status changed to **Available**
- Database endpoint generated for connectivity





Evidence from screenshots:

- Security groups created (page 9)
- EC2 instance running (page 13)
- Database creation in progress (page 19)
- Database available (page 20)
- Database endpoint visible (page 21)

Action:

Step 1: Logged into AWS Account

- Logged in as IAM user with administrative access

Evidence:

- Login step defined (page 10)

Step 2: Created Application Security Group

- Security Group Name: **ApplicationSG**
- Description: Allow incoming traffic from the internet
- Configured inbound rules:
 - HTTP
 - HTTPS
 - SSH
- Source: Anywhere (IPv4)

Evidence:

- Configuration steps (page 11-13)

- Security group creation interface (page 6)

Step 3: Configured Database Security Group

- Security Group Name: **DatabaseSG**
- Description: Allow EC2 to access database
- Inbound rule:
 - MySQL/Aurora (Port 3306)
- Source: ApplicationSG

Evidence:

- Configuration details (page 14-16)
- MySQL rule shown (page 8)

Step 4: Launched EC2 Instance

- Instance Name: **WordPress-instance**
- AMI: Amazon Linux 2023
- Instance Type: t3.micro
- VPC: Default
- Subnet: eu-west-2a
- Security Group: ApplicationSG

Evidence:

- EC2 configuration (page 17-21)
- Successful launch message (page 12)
- Instance running (page 13)

Step 5: Created Amazon RDS Database

- Engine: MySQL
- Version: MySQL 8.0.42
- Template: Free Tier
- DB Identifier: [REDACTED]
- Username: [REDACTED]
- Password: [REDACTED]
- Instance Type: db.t4g.micro
- Storage: 20GB (gp2)

Evidence:

- Database configuration steps (page 22-25)
- RDS setup interface (page 14-15)

Step 6: Configured Connectivity

- Connected RDS to EC2 instance
- Public access: Disabled
- Security group: DatabaseSG
- Authentication: Password authentication

Evidence:

- Connectivity setup (page 26-28)
- Security group linkage (page 16)

Step 7: Final Configuration and Deployment

- Initial database name: mydbinstance
- Disabled:
 - Automatic backups
 - Maintenance
 - Delete protection
- Created database

Evidence:

- Final configuration (page 29-30)

Step 8: Verified Database

- Waited until status changed to **Available**
- Accessed database details
- Retrieved endpoint

Evidence:

- Database available (page 20)
- Endpoint shown under connectivity (page 21)
- Verification step (page 31-32)

Screenshots follow.

Summary

- Security groups were configured for application and database layers
- EC2 instance was successfully provisioned
- Amazon RDS MySQL database was created and configured
- Database connected securely to EC2 instance
- Database reached **Available** state and endpoint was generated

✓ Lab objective achieved:

“Configured Security Groups, provisioned EC2, created and verified an RDS database”

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [Info](#)

Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
HTTP	TCP	80	An... 0.0.0.0/0		Delete
HTTPS	TCP	443	An... 0.0.0.0/0		Delete
SSH	TCP	22	An... 0.0.0.0/0		Delete
Add rule					

Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Outbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Destination Info	Description - optional Info	
All traffic	All	All	Cu... 0.0.0.0/0		Delete
Add rule					

Rules with destination of 0.0.0.0/0 or ::/0 allow your instances to send traffic to any IPv4 or IPv6 address. We recommend setting security group rules to be more restrictive and to only allow traffic to specific known IP addresses.

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

You can add up to 50 more tags

[Cancel](#)[Create security group](#)

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [Info](#)

Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info
MYSQL/Aurora	TCP	3306	Cus...	sg-0d90eb60bccc sg-0d90eb60bccc13002
Delete				
Add rule				

Outbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Destination Info	Description - optional Info
All traffic	All	All	Cus...	0.0.0.0/0
Delete				
Add rule				

 Rules with destination of 0.0.0.0/0 or ::/0 allow your instances to send traffic to any IPv4 or IPv6 address. We recommend setting security group rules to be more restrictive and to only allow traffic to specific known IP addresses. 

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

You can add up to 50 more tags

- EC2
- Dashboard
- AWS Global View
- Events
- Instances
- Instances
- Instance Types
- Launch Templates
- Spot Requests
- Savings Plans
- Reserved Instances
- Dedicated Hosts
- Capacity Reservations
- Capacity Manager
- Images
- AMIs
- AMI Catalog
- Elastic Block Store
- Volumes
- Snapshots
- Lifecycle Manager
- Network & Security
- Security Groups
- Elastic IPs
- Placement Groups
- Key Pairs
- Network Interfaces
- Load Balancing
- Load Balancers
- Target Groups
- Trust Stores
- Auto Scaling
- Auto Scaling Groups
- Settings

Security group (sg-0acc4f140d734be14 | DatabaseSG) was created successfully

Details

Security Groups (3)

Find security groups by attribute or tag

	Name	Security group ID	Security group name	VPC ID
	-	sg-0d90eb60bcc13002	ApplicationSG	vpc-07e6144432981815
	-	sg-0acc4f140d734be14	DatabaseSG	vpc-07e6144432981815

Select a security group

VPC - required [Info](#)

vpc-07e61444329818154 (default)

172.31.0.0/16

Subnet [Info](#)

subnet-01e394d88afafecbfa

VPC: vpc-07e61444329818154 Owner: 009850210027
Availability Zone: eu-west-3a (euw3-az1) Zone type: Availability Zone
IP addresses available: 4091 CIDR: 172.31.0.0/20

[Create new subnet](#)

Auto-assign public IP [Info](#)

Enable

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☐ Create security group

☒ Select existing security group

Common security groups [Info](#)

Select security groups

[Compare security group rules](#)

ApplicationSG sg-0d90eb60bcc13002

VPC: vpc-07e61444329818154

Security groups that you add or remove here will be added to or removed from all your network interfaces.

[▶ Advanced network configuration](#)

▼ Configure storage [Info](#)

[Advanced](#)

1x GiB

Root volume, 3000 IOPS, Not encrypted

[Add new volume](#)

Click refresh to view backup information

The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems

[Edit](#)

[▶ Advanced details](#) [Info](#)

 **Success**
Successfully initiated launch of instance (i-070c8bb6d5197ddb)

► Launch log

Next Steps

 What would you like to do next with this instance, for example "create alarm" or "create backup"

< 1 2 3 4 5 6 >

Create billing usage alerts

To manage costs and avoid surprise bills, set up email notifications for billing usage thresholds.

Create billing alerts 

Connect to your instance

Once your instance is running, log into it from your local computer.

Connect to instance 

[Learn more](#) 

Connect an RDS database

Configure the connection between an EC2 instance and a database to allow traffic flow between them.

Connect an RDS database 

[Create a new RDS database](#) 

[Learn more](#) 

Create EBS snapshot policy

Create a policy that automates the creation, retention, and deletion of EBS snapshots

Create EBS snapshot policy 

Manage detailed monitoring

Enable or disable detailed monitoring for the instance. If you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period.

Manage detailed monitoring 

Create Load Balancer

Create a application, network gateway or classic Elastic Load Balancer

Create Load Balancer 

Create AWS budget

AWS Budgets allows you to create budgets, forecast spend, and take action on your costs and usage from a single location.

Create AWS budget 

Manage CloudWatch alarms

Create or update Amazon CloudWatch alarms for the instance.

Manage CloudWatch alarms 

[View all instances](#)

- EC2 > Instances
- EC2
- Dashboard
- AWS Global View
- Events
- Instances
- Instances
- Instance Types
- Launch Templates
- Spot Requests
- Savings Plans
- Reserved Instances
- Dedicated Hosts
- Capacity Reservations
- Capacity Manager
- Images
- AMIs
- AMI Catalog
- Elastic Block Store
- Volumes
- Snapshots
- Lifecycle Manager
- Network & Security
- Security Groups
- Elastic IPs
- Placement Groups
- Key Pairs
- Network Interfaces
- Load Balancing
- Load Balancers
- Target Groups
- Trust Stores
- Auto Scaling
- Auto Scaling Groups
- Settings

Instances (1/1) Info

Connect Instance state Actions Launch instances

Save filter sets Choose filter set Find Instance by attribute or tag (case-sensitive)

☒	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
☒	Wordpress-instance	i-070c8bb6d5197ddb	Running	t3.micro	Initializing	View alarms

i-070c8bb6d5197ddb (Wordpress-instance)

Details Status and alarms Monitoring Security Networking Storage Tags

Instance summary

Instance ID	Public IPv4 address	Private IPv4 addresses
i-070c8bb6d5197ddb	51.44.10.70	172.31.8.60

Create database [Info](#)

Engine options

Engine type [Info](#)

☐ Aurora (MySQL Compatible)


☐ Aurora (PostgreSQL Compatible)


☒ MySQL


☐ PostgreSQL


☐ MariaDB


☐ Oracle


☐ Microsoft SQL Server


☐ IBM Db2


Choose a database creation method

☒ **Full configuration**
You set all of the configuration options, including ones for availability, security, backups, and maintenance.

☐ **Easy create**
Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Templates

Choose a sample template to meet your use case.

☐ **Production**
Use defaults for high availability and fast, consistent performance.

☐ **Dev/Test**
This instance is intended for development use outside of a production environment.

☒ **Sandbox**
To develop new applications, test existing applications, or gain hands-on experience with Amazon RDS.

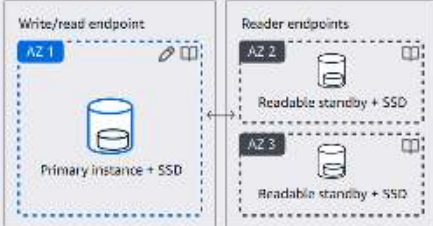
Availability and durability

Deployment options [Info](#)

Choose the deployment option that provides the availability and durability needed for your use case. AWS is committed to a certain level of uptime depending on the deployment option you choose. Learn more in the [Amazon RDS service level agreement \(SLA\)](#).

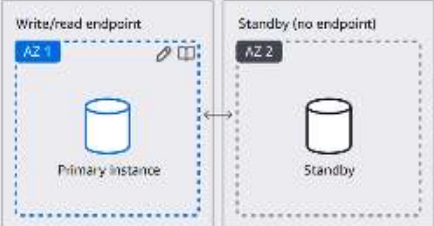
☐ **Multi-AZ DB cluster deployment (3 instances)**
Creates a primary DB instance with two readable standbys in separate Availability Zones. This setup provides:

- 99.95% uptime
- Redundancy across Availability Zones
- Increased read capacity
- Reduced write latency



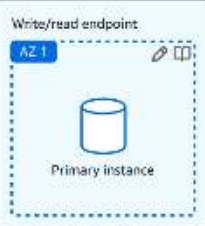
☐ **Multi-AZ DB instance deployment (2 instances)**
Creates a primary DB instance with a non-readable standby instance in a separate Availability Zone. This setup provides:

- 99.95% uptime
- Redundancy across Availability Zones



☒ **Single-AZ DB instance deployment (1 instance)**
Creates a single DB instance without standby instances. This setup provides:

- 99.5% uptime
- No data redundancy



Settings

Edition

☒ MySQL Community

Engine version [Info](#)

View the engine versions that support the following database features.

▼ Hide filters

- ☒ **Show only versions that support the Multi-AZ DB cluster** [Info](#)
Create a Multi-AZ DB cluster with one primary DB instance and two readable standby DB instances. Multi-AZ DB clusters provide up to 2x faster transaction commit latency and automatic failover in typically under 35 seconds.
- ☐ **Show only versions that support the Amazon RDS Optimized Writes** [Info](#)

Engine version

MySQL 8.4.7

☐ Enable RDS Extended Support [Info](#)

Amazon RDS Extended Support is a [paid offering](#). By selecting this option, you consent to being charged for this offering if you are running your database major version past the RDS end of standard support date for that version. Check the end of standard support date for your major version in the [RDS for MySQL documentation](#).

DB instance identifier [Info](#)

Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

mydbinstance

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in 'mydbinstance'). Constraints: 1 to 63 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

Credentials Settings

Master username [Info](#)

Type a login ID for the master user of your DB instance.

mydbinstance

1 to 16 alphanumeric characters. The first character must be a letter.

Credentials management

You can use AWS Secrets Manager or manage your master user credentials.

☐ Managed in AWS Secrets Manager - most secure

RDS generates a password for you and manages it throughout its lifecycle using AWS Secrets Manager.

☒ Self managed

Create your own password or have RDS create a password that you manage.

☐ Auto generate password

Amazon RDS can generate a password for you, or you can specify your own password.

Master password [Info](#)

Password strength [Average](#)

Minimum constraints: At least 8 printable ASCII characters. Can't contain any of the following symbols: / ' ' @

Confirm master password [Info](#)

▼ Additional credentials settings

Database authentication options [Info](#)

☒ Password authentication

Authenticates using database passwords.

☐ Password and IAM database authentication

Authenticates using the database password and user credentials through AWS IAM users and roles.

☐ Password and Kerberos authentication

Choose a directory in which you want to allow authorized users to authenticate with this DB instance using Kerberos Authentication.

Instance configuration

The DB instance configuration options below are limited to those supported by the engine that you selected above.

DB instance class [Info](#)

▼ Hide filters

☒ Show instance classes that support Amazon RDS Optimized Writes [Info](#)

Amazon RDS Optimized Writes improves write throughput by up to 2x at no additional cost.

☐ Include previous generation classes

☐ Standard classes (includes m classes)

☐ Memory optimized classes (includes r and x classes)

☒ Burstable classes (includes t classes)

Instance type

db.t4g.micro

2 vCPUs 1 GiB RAM EBS Bandwidth: Up to 2,085 Mbps Network: Up to 5 Gbps

Storage

Storage type [Info](#)

Provisioned IOPS SSD (io2) storage volumes are now available.

General Purpose SSD (gp2)

Baseline performance determined by volume size

Allocated storage [Info](#)

20

GiB

Allocated storage value must be 20 GiB to 6,144 GiB.

▼ Additional storage configuration

Storage autoscaling [Info](#)

Provides dynamic scaling support for your database's storage based on your application's needs.

☒ Enable storage autoscaling

Enabling this feature will allow the storage to increase after the specified threshold is exceeded.

Maximum storage threshold [Info](#)

Charges will apply when your database autoscales to the specified threshold

1000

GiB

Allocated storage value must be 22 GiB to 6,144 GiB.

Connectivity [Info](#)



Compute resource

Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

☐ Don't connect to an EC2 compute resource

Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.

☒ Connect to an EC2 compute resource

Set up a connection to an EC2 compute resource for this database.

EC2 instance [Info](#)

Choose the EC2 instance to add as the compute resource for this database. A VPC security group is added to this EC2 instance. A VPC security group is also added to the database with an inbound rule that allows the EC2 instance to access the database.

i-070c8bb6d5197ddbb

Wordpress-instance



Some VPC settings can't be changed when a compute resource is added

Adding an EC2 compute resource automatically selects the VPC, DB subnet group, and public access settings for this database. To allow the EC2 instance to access the database, a VPC security group `rds-ec2-X` is added to the database and another called `ec2-rds-X` to the EC2 instance. You can remove the new security group for the database only by removing the compute resource.

Virtual private cloud (VPC) [Info](#)

Choose the VPC. The VPC defines the virtual networking environment for this DB instance.

Default VPC (vpc-07e61444329818154)

3 Subnets, 1 Availability Zones



After a database is created, you can't change its VPC. Only VPCs with a corresponding DB subnet group are listed.

After a database is created, you can't change its VPC.

DB subnet group [Info](#)

Choose the DB subnet group. The DB subnet group defines which subnets and IP ranges the DB instance can use in the VPC that you selected.

☐ Choose existing

Choose existing DB subnet group

☒ Automatic setup

RDS creates a new subnet group for you or reuses an existing subnet group

DB subnet group name

rds-ec2-db-subnet-group-1

New DB subnet group created.

Public access [Info](#)

☐ Yes

RDS assigns a public IP address to the database. Amazon EC2 instances and other resources outside of the VPC can connect to your database. Resources inside the VPC can also connect to the database. Choose one or more VPC security groups that specify which resources can connect to the database.

☒ No

RDS doesn't assign a public IP address to the database. Only Amazon EC2 instances and other resources inside the VPC can connect to your database. Choose one or more VPC security groups that specify which resources can connect to the database.

VPC security group (firewall) [Info](#)

Choose one or more VPC security groups to allow access to your database. Make sure that the security group rules allow the appropriate incoming traffic.

☒ Choose existing

Choose existing VPC security groups

☐ Create new

Create new VPC security group

Additional VPC security group

Choose one or more options.

DatabaseSG

Amazon RDS will add a new VPC security group `rds-ec2-1` to allow connectivity with your compute resource.

Availability zone [Info](#)

eu-west-3a

RDS Proxy

RDS Proxy is a fully managed, highly available database proxy that improves application scalability, resiliency, and security.

☐ **Create an RDS Proxy** [Info](#)

RDS automatically creates an IAM role and a Secrets Manager secret for the proxy. RDS Proxy has additional costs. For more information, see [Amazon RDS Proxy pricing](#).

Certificate authority - optional [Info](#)

Using a server certificate provides an extra layer of security by validating that the connection is being made to an Amazon database. It does so by checking the server certificate that is automatically installed on all databases that you provision.

rds-ca-rsa2048-g1 (default)

Expiry: May 26, 2061

If you don't select a certificate authority, RDS chooses one for you.

▼ Additional configuration**Database port** [Info](#)

TCP/IP port that the database will use for application connections.

3306

Tags - optional

A tag consists of a case-sensitive key-value pair.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

Monitoring [Info](#)

Choose monitoring tools for this database. Database Insights provides a combined view of Performance Insights and Enhanced Monitoring for your fleet of databases. **Database Insights** pricing is separate from RDS monthly estimates. See [Amazon CloudWatch pricing](#).

☐ Database Insights - Advanced

- Retains 15 months of performance history
- Fleet-level monitoring
- Integration with CloudWatch Application Signals

☒ Database Insights - Standard**▼ Additional monitoring settings**

Enhanced Monitoring, CloudWatch Logs and DevOps Guru

Enhanced Monitoring☐ **Enable Enhanced monitoring**

Enabling Enhanced Monitoring metrics are useful when you want to see how different processes or threads use the CPU.

Log exports

Select the log types to publish to Amazon CloudWatch Logs

- ☐ Audit log
- ☐ Error log
- ☐ General log
- ☐ iam-db-auth-error log
- ☐ Slow query log

IAM role

The following service-linked role is used for publishing logs to CloudWatch Logs.

RDS service-linked role

▼ Additional configuration

Database options, encryption turned on, backup turned off, backtrack turned off, maintenance, CloudWatch Logs, delete protection turned on.

Database options**Initial database name** [Info](#)

mydbinstance

If you do not specify a database name, Amazon RDS does not create a database.

DB parameter group [Info](#)

default.mysql8.4

Option group [Info](#)

default:mysql-8-4

Backup

- ☐ **Enable automated backup**
Creates a point-in-time snapshot of your database.

Backup tags [Info](#)

Copies tags from the source database to the automated backup and snapshots respectively.

- ☐ **Copy tags to automated backup**
This is a one-time setting. Future tag modifications need manual updates.

- ☒ **Enable encryption**
Choose to encrypt the given instance. Master key IDs and aliases appear in the list after they have been created using the AWS Key Management Service console. [Info](#)

AWS KMS key [Info](#)

(default) aws/rds

Account

009850210027

KMS key ID

alias/aws/rds

Maintenance

Auto minor version upgrade [Info](#)

- ☐ **Enable auto minor version upgrade**
Enabling auto minor version upgrade will automatically upgrade your database minor version. For limitations and more details, see [Automatically upgrading the minor engine version documentation](#).

Maintenance window [Info](#)

Select the period you want pending modifications or maintenance applied to the database by Amazon RDS.

- ☐ Choose a window
- ☒ No preference

- ☒ **Enable deletion protection**
Protects the database from being deleted accidentally. While this option is enabled, you can't delete the database.

 You are responsible for ensuring that you have all of the necessary rights for any third-party products or services that you use with AWS services.

[Cancel](#)

[Create database](#)

Aurora and RDS

- Dashboard
- Databases**
- Query editor
- Performance insights
- Snapshots
- Exports in Amazon S3
- Automated backups
- Reserved instances
- Proxies

- Subnet groups
- Parameter groups
- Option groups
- Custom engine versions
- Zero-ETL integrations

- Events
- Event subscriptions

- Recommendations 0
- Certificate update

Creating database mydbinstance

Your database might take a few minutes to launch. You can use settings from mydbinstance to simplify configuration of suggested database add-ons while we finish creating your DB for you.

View connection details

Databases (1) Group resources Modify Actions Create database

DB identifier	Status	Role	Engine	Up
mydbinstance	Creating	Instance	MySQL Community	SEt

Aurora and RDS

Dashboard

Databases

Query editor

Performance insights

Snapshots

Exports in Amazon S3

Automated backups

Reserved instances

Proxies

Subnet groups

Parameter groups

Option groups

Custom engine versions

Zero-ETL integrations

Events

Event subscriptions

Recommendations 0

Certificate update

Databases (1)

Group resources

Modify

Actions

Create database

Filter by databases

DB identifier	Status	Role	Engine	Up
mydbinstance	Available	Instance	MySQL Community	SEC

Aurora and RDS

Dashboard

Databases

Query editor

Performance insights

Snapshots

Exports in Amazon S3

Automated backups

Reserved instances

Proxies

Subnet groups

mydbinstance

Modify

Actions

Summary

DB identifier
mydbinstance

CPU
26.90%

Recommendations

Status
Available

Class
db.t4g.micro

Role
Instance

Current activity
0 Connections

Engine
MySQL Community

Region & AZ
eu-west-3a

Connectivity & security

Monitoring

Logs & events

Configuration

Zero-ETL integrations

Ma

Connect using

Code snippets

CloudShell

Endpoints

Database name
mydbinstance

Master username
mydbinstance

Internet access gateway
Disabled

Port
3306

Endpoint type
Instance endpoint

Additional configurations

Connectivity & security

Endpoint & port

Networking

Security

Endpoint
mydbinstance.czoioksq48s6.eu-west-3.rds.amazonaws.com

Port
3306

Availability Zone
eu-west-3a

VPC
vpc-07e61444329818154

Subnet group
rds-ec2-db-subnet-group-1

Subnets
subnet-0271b6c6d37b87224
subnet-01ae63c8cf25ba91f
subnet-0cc28f4ec837fcebdc

Network type
IPv4

VPC security groups
rds-ec2-1 (sg-0667f6b0178bd24d8)
DatabaseSG (sg-0acc4f140d734be14)

Publicly accessible
No

Certificate authority
rds-ca-rsa2048-g1

Certificate authority date
May 26, 2061, 02:18 (UTC+03:00)

DB instance certificate expiration date
March 28, 2027, 17:58 (UTC+03:00)

Connected compute resources (1)

Connections to compute resources that were created automatically by RDS are shown here. Connections to compute resources that were created manually aren't shown.

Filter by compute resources

Resource identifier

Resource type

Availability Zone

VPC security group

Compute resource security group

i-070c8bb6d5197ddbb

EC2 instance

eu-west-3a

rds-ec2-1

ec2-rds-1

Security group rules (3)

Filter by Security group rules

Security group	Type	Rule
DatabaseSG (sg-0acc4f140d734be14)	EC2 Security Group - Inbound	sg-0d90eb60bccc13002
DatabaseSG (sg-0acc4f140d734be14)	CIDR/IP - Outbound	0.0.0.0/0
rds-ec2-1 (sg-0667f6b0178bd24d8)	EC2 Security Group - Inbound	sg-0dbba1e64f5e701e0

Replication (1)

Filter by Replication

DB identifier	Role	Region & AZ	Replication source	Replication state	Lag
mydbinstance	Instance	eu-west-3a	-	-	-