Lab 2 - Build a Database Server

Objective: To create relational database server in aws.

Task 1: Create a Security Group for the RDS DB Instance

In this task, you will create a security group to allow your web server to access your RDS DB instance. The security group will be used when you launch the database instance.

5. In the left navigation pane, choose Create snapshot.
6. Choose Create security group and then configure:
    - Security group name**:** DB Security Group
    - Description**:** Permit Access from Security Group
    - VPC**:** Lab VPC

    You will now add a rule to the security group to permit inbound database requests.

7. In the Inbound rules pane, choose Add rule

    The security group currently has no rules. You will add a rule to permit access from the Web Security Group.

8. Configure the following settings:
    - Type**:** MySQL/Aurora (3306)
    - CIDR, IP, Security Group or Prefix List**:** Type sgand then select Web Security Group.

    This configures the Database security group to permit inbound traffic on port 3306 from any EC2 instance that is associated with the Web Security Group.

9. Choose Create security group

    You will use this security group when launching the Amazon RDS database.

Task 2: Create a DB Subnet Group

In this task, you will create a DB subnet group that is used to tell RDS which subnets can be used for the database. Each DB subnet group requires subnets in at least two Availability Zones.

1. On the Services menu, choose RDS.
2. In the left navigation pane, choose Subnet groups.
    a. If the navigation pane is not visible, choose the menu icon in the top-left corner.
3. Choose Create DB Subnet Group then configure:
    a. Name**:** DB Subnet Group
    b. Description**:** DB Subnet Group
    c. VPC**:** Lab VPC
4. Scroll down to the Add Subnets section.
5. Expand the list of values under Availability Zones and select the first two zones: us-east-1a and us-east-1b.
6. Expand the list of values under Subnets and select the subnets associated with the CIDR ranges 10**.**0.1.0/24 and 10.0.3.0/24.
    a. These subnets should now be shown in the Subnets selected table.
7. Choose Create
    a. You will use this DB subnet group when creating the database in the next task.

Task 3: Create an Amazon RDS DB Instance

In this task, you will configure and launch a Multi-AZ Amazon RDS for MySQL database instance.

Amazon RDS Multi-AZ deployments provide enhanced availability and durability for Database (DB) instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB instance, Amazon RDS automatically creates a primary DB instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ).

1. In the left navigation pane, choose Databases.
2. Choose Create database

    a. If you see Switch to the new database creation flow at the top of the screen, please choose it.
3. Select MySQL.
4. Under Settings, configure:
    a. DB instance identifier**:** lab db
    b. Master username**:** main
    c. Master password**:** lab password
    d. Confirm password**:** lab password
5. Under DB instance class, configure:
    a. Select Burstable classes (includes t classes).
    b. Select db.t3.micro
6. Under Storage, configure:
    a. Storage type**:** General Purpose (SSD)
    b. Allocated storage**:** *20*
7. Under Connectivity, configure:
    a. Virtual Private Cloud (VPC): Lab VPC
8. Under Existing VPC security groups, from the dropdown list:
    a. Choose DB Security Group.
    b. Deselect default.
9. Expand Additional configuration, then configure:
    a. Initial database name**:**lab
    b. Uncheck Enable automatic backups.
    c. Uncheck Enable encryption
    d. Uncheck Enable Enhanced monitoring.
    e. This will turn off backups, which is not normally recommended, but will make the database deploy faster for this lab.
10. Choose Create database
    a. Your database will now be launched.
    b. If you receive an error that mentions "not authorized to perform: iam:CreateRole", make sure you unchecked Enable Enhanced monitoring in the previous step.
11. Choose lab-db (choose the link itself).

12. Wait until Info changes to Modifying or Available.
13. Scroll down to the Connectivity & security section and copy the Endpoint field.
    a. It will look similar to: lab-db.cggq8lhnxvnv.us-west-2.rds.amazonaws.com
14. Paste the Endpoint value into a text editor. You will use it later in the lab.

Task 4: Interact with Your Database

In this task, you will open a web application running on your web server and configure it to use the database.

1. To copy the WebServer IP address, choose on the Details drop down menu above these instructions, and then choose Show.
2. Open a new web browser tab, paste the WebServer IP address and press Enter.
    a. The web application will be displayed, showing information about the EC2 instance.
3. Choose the RDS link at the top of the page.
    a. You will now configure the application to connect to your database.
4. Configure the following settings:
    a. Endpoint**:** Paste the Endpoint you copied to a text editor earlier
    b. Database**:**lab
    c. Username**:** main
    d. Password**:** lab password
    e. Choose Submit
    f. A message will appear explaining that the application is running a command to copy information to the database. After a few seconds the application will display an Address Book.
    g. The Address Book application is using the RDS database to store information.
5. Test the web application by adding, editing and removing contacts.
    a. The data is being persisted to the database and is automatically replicating to the second Availability Zone.

Conclusion: Database has been created and secured with Security Groups