Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while managing time-consuming database administration tasks, which allows you to focus on your applications and business. Amazon RDS provides you with six familiar database engines to choose from: Amazon Aurora, Oracle, Microsoft SQL Server, PostgreSQL, MySQL, and MariaDB.

Objectives

After completing this lab, you can:

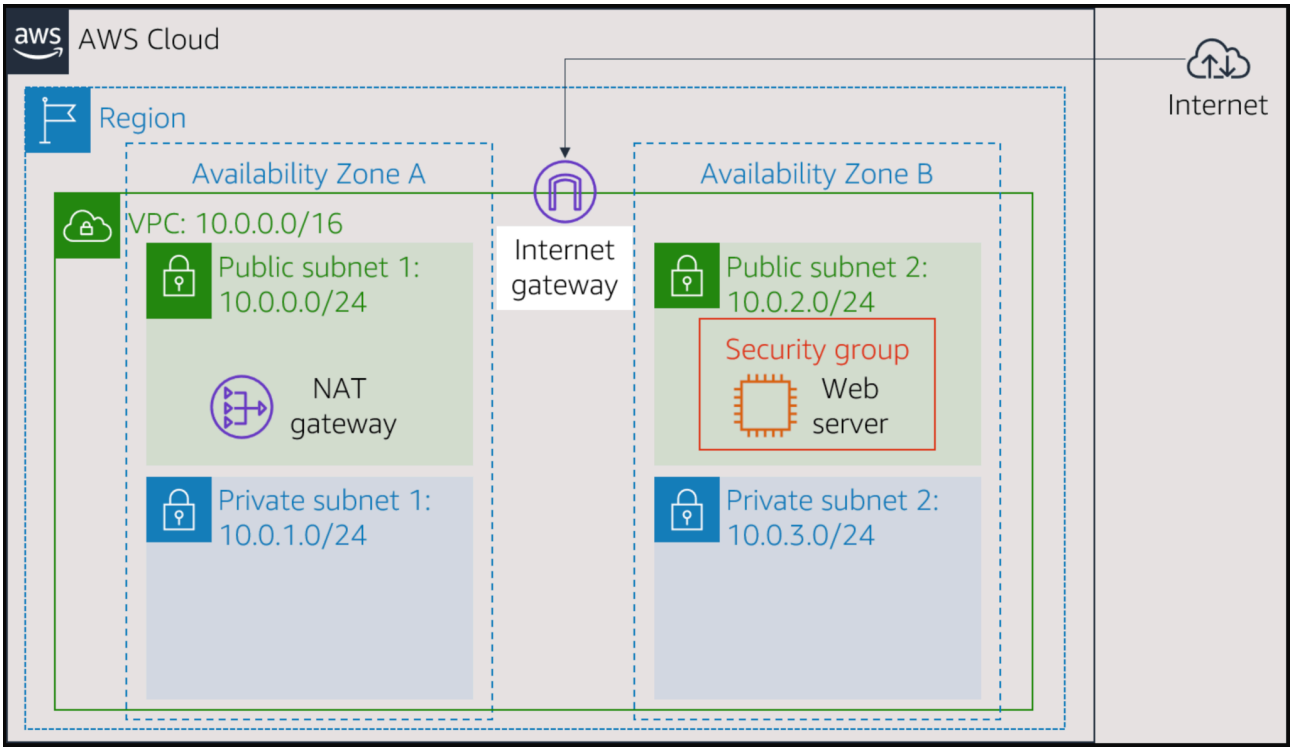
- Launch an Amazon RDS DB instance with high availability.
- Configure the DB instance to permit connections from your web server.
- Open a web application and interact with your database.

Duration

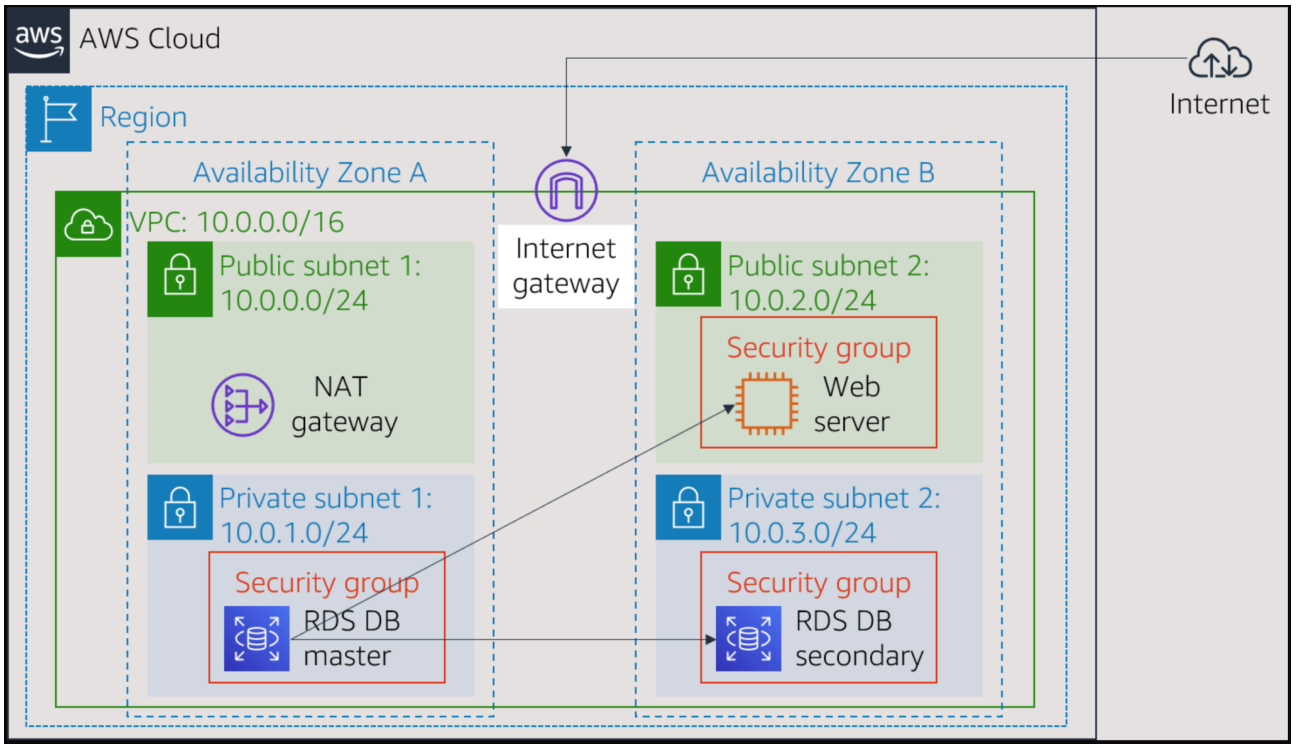
This lab takes approximately **30 minutes**.

Scenario

You start with the following infrastructure:



At the end of the lab, this is the infrastructure:



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.

1. In the **AWS Management Console**, on the Services menu, choose **VPC**.
2. In the left navigation pane, choose **Security Groups**.
3. Choose to Create a security group and then configure:
   - **Security group name:** `DB Security Group`
   - **Description:** `Permit access from Web Security Group`
   - **VPC:** *Lab VPC*
4. You will now add a rule to the security group to permit inbound database requests.
5. 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*.
6. Configure the following settings:
   - **Type:** *MySQL/Aurora (3306)*
   - **CIDR, IP, Security Group, or Prefix List:** Type `sg` and then select *Web Security Group*.
7. 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*.

8. Choose to Create a 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.

9. On the Services menu, choose **RDS**.
10. In the left navigation pane, choose **Subnet groups**.
    If the navigation pane is not visible, choose the menu icon in the top-left corner.
11. Choose Create DB Subnet Group then configure:
    - **Name:** `DB-Subnet-Group`
    - **Description:** `DB Subnet Group`
    - **VPC:** *Lab VPC*
12. Scroll down to the **Add Subnets** section.
13. Expand the list of values under **Availability Zones** and select the first two zones: **us-east-1a** and **us-east-1b**.
14. 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**.
    These subnets should now be shown in the **Subnets selected** table.
15. Choose Create
    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).

16. In the left navigation pane, choose **Databases**.
17. Choose Create database
    If you see **Switch to the new database creation flow** at the top of the screen, please choose it.
18. Select **MySQL**.
19. Under **Settings**, configure:
    - **DB instance identifier:** `lab-db`
    - **Master username:** `main`
    - **Master password:** `lab-password`
    - **Confirm password:** `lab-password`
20. Under **DB instance class**, configure:
    - Select **Burstable classes (includes t classes)**.
    - Select *db.t3.micro*
21. Under **Storage**, configure:
    - **Storage type:** *General Purpose (SSD)*
    - **Allocated storage:** *20*
22. Under **Connectivity**, configure:
    - **Virtual Private Cloud (VPC):** *Lab VPC*
23. Under **Existing VPC security groups**, from the dropdown list:
    - Choose *DB Security Group*.
    - Deselect *default*.
24. Expand **Additional configuration**, then configure:
    - **Initial database name:** `lab`
    - Uncheck **Enable automatic backups**.
    - Uncheck **Enable encryption**
    - Uncheck **Enable Enhanced monitoring**.
25. This will turn off backups, which is not normally recommended but will make the database deploy faster for this lab.
26. Choose Create database
    Your database will now be launched.
    If you receive an error that mentions "not authorized to perform: iam:CreateRole", make sure you unchecked *Enable Enhanced monitoring* in the previous step.
27. Choose **lab-db** (choose the link itself).
    You will now need to wait **approximately 4 minutes** for the database to be available. The deployment process is deploying a database in two different Availability zones.
    While you are waiting, you might want to review the Amazon RDS FAQs or grab a cup of coffee.
28. Wait until **Info** changes to **Modifying** or **Available**.
29. Scroll down to the **Connectivity & security** section and copy the **Endpoint** field.
    It will look similar to: *lab-db.cggq8lhnxvnv.us-west-2.rds.amazonaws.com*
30. 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.

31. To copy the **WebServer** IP address, choose the Details drop-down menu above these instructions, and then choose Show.
32. Open a new web browser tab, paste the *WebServer* IP address and press Enter.
    The web application will be displayed, showing information about the EC2 instance.
33. Choose the **RDS** link at the top of the page.
    You will now configure the application to connect to your database.
34. Configure the following settings:
    - **Endpoint:** Paste the Endpoint you copied to a text editor earlier
    - **Database:** `lab`
    - **Username:** `main`
    - **Password:** `lab-password`
    - Choose **Submit**
35. 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**.
    The Address Book application is using the RDS database to store information.
36. Test the web application by adding, editing, and removing contacts.
    The data is persisted in the database and is automatically replicated to the second Availability Zone.

Lab Complete

Congratulations! You have completed the lab.