WHIZLABS 0 K

Home / AWS / Guided Lab / How to Encrypt an Unencrypted RDS DB Instance

How to Encrypt an Unencrypted RDS DB Instance

Level: **Intermediate**

Amazon RDS Amazon Web Services

Required Points	10
Lab Duration	01:20:00
Average Start time	Less than a minute

Start Lab →

Need help?

How to use Hands on Lab

Troubleshooting Lab

FAQs

Submit Feedback | Share

Lab Overview

Database Engineer

Database

Lab Details

1. This lab walks you through the steps to create an unencrypted instance with the Encrypt option.

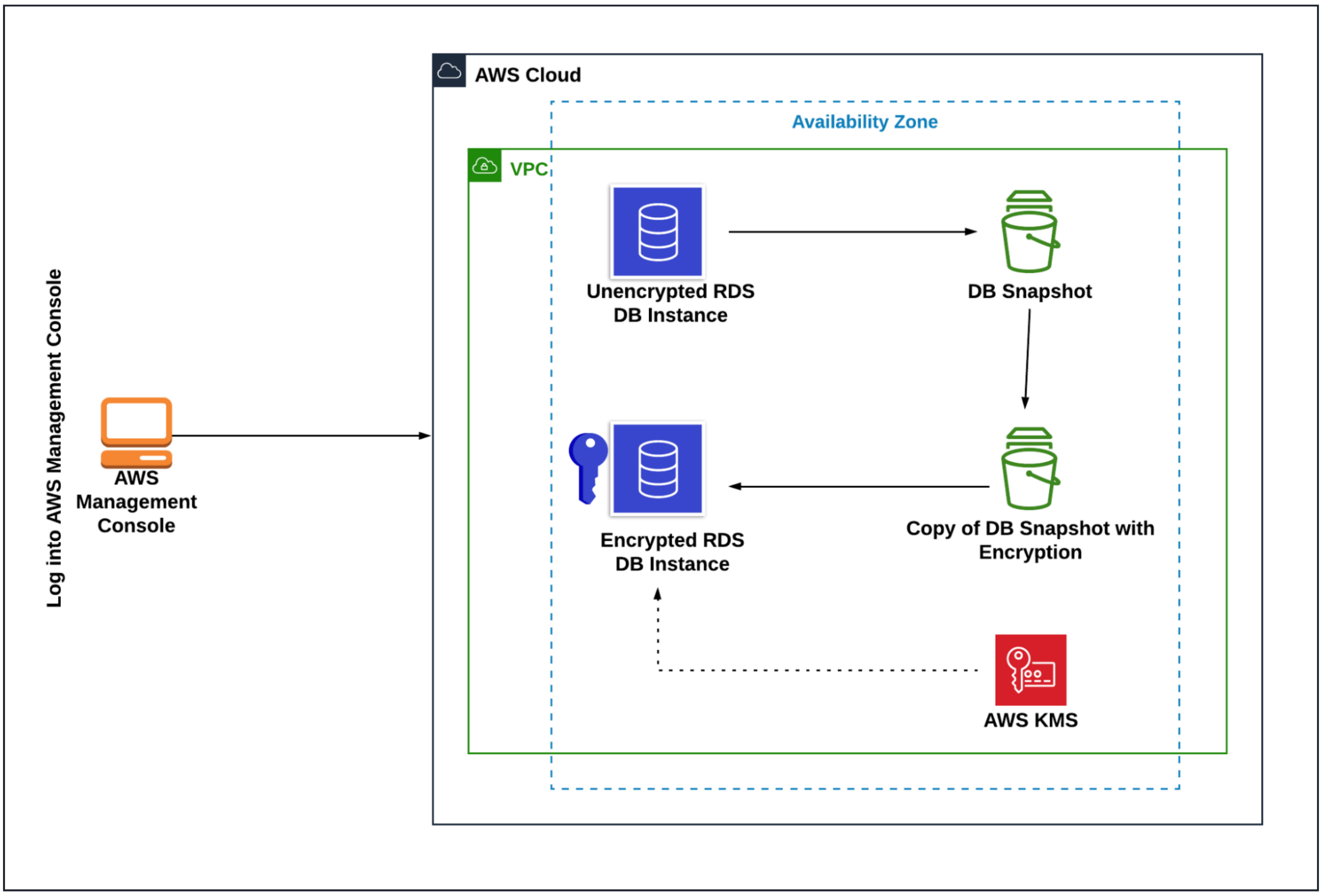
Privacy - Terms

2. You will practice this lab by not enabling the encryption of DB Instance while creating.
3. Duration: **1 hour 20 minutes**
4. AWS Region: **US East (N. Virginia) us-east-1**

Introduction

1. Amazon RDS can encrypt your Amazon RDS DB Instances.
2. When the encrypt option is enabled for the AWS RDS Resources, we are able to encrypt **DB Instances**, **Automated Backups**, **Read replicas**, **Snapshots** and **Logs**.
3. Amazon RDS encrypted DB instances use the AES-256 encryption algorithm to encrypt your data on the server that hosts your Amazon RDS DB instances.
4. The Encrypt option can be enabled only when you are launching the DB instance, it cannot be enabled after launch. However, copies of unencrypted snapshots can be encrypted.

Architecture Diagram


Log into AWS Management Console
AWS Management Console
AWS Cloud
Availability Zone
VPC
Unencrypted RDS DB Instance
DB Snapshot
Copy of DB Snapshot with Encryption
Encrypted RDS DB Instance
AWS KMS

Task Details

1. Sign in to AWS Management Console.
2. Create an Amazon RDS DB Instance (without enabling encrypt option).
3. Take a snapshot from an existing DB Instance.
4. Make a copy of the snapshot and encrypt it.
5. Restore DB Instance from the encrypted snapshot.
6. Change the name of the original DB Instance.
7. Change the name of the Restored DB Instance to the original DB Instance name.
8. Delete the original RDS Instance and snapshot.
9. Validation of the lab.
10. Deleting AWS Resources

Case Study

1. Suppose we have created an RDS DB Instance without enabling the encryption. As days passed by the project became bigger and began to store more sensitive data.
2. As you are quite aware of security issues, you wanted to check on the AWS console that your database was well encrypted.
3. Your database was totally **Unencrypted**. And when you check to encrypt the database, you have **no option** to encrypt the database.

Launching Lab Environment

1. To launch the lab environment, Click on the **Start Lab** button.
2. Please wait until the cloud environment is provisioned. It will take less than a minute to provision.
3. Once the Lab is started, you will be provided with **IAM user name**, **Password**, **Access Key**, and **Secret Access Key**.

Note : You can only start one lab at any given time