**RDS advantages:**

1. **Automatic Backups**

**Manual Backups (snapshots)**

1. **Multi – AZ**
2. **Read Replicas**

**Database Module**

--------------------------

1) RDS - SQL

----------------

SQL (Structured Query language)

RDS (Relational Database Service)

Two types of backups

----------------------------

1) Manual (DB Snapshots)

2) Automated

We take the backup, in the form of snapshot.

If database is lost, we restore snapshot as database.

We will have downtime, in this case.

===========

Everyday AWS will take the full backup of database automatically.

Backup is maintained for the last 35 days (Retention Period)

Default retention period is 7 Days.

AWS will take incremental backup in every 1 min.

Incremental backup is called transactional logs.

If we intentionally delete the database, backup will also be deleted.

Manual backups are user initiated.

Even if you delete the database intentionally, we will have manual backups.

How can we eliminate the downtime

-------------------------------------------------

By using multi availability zone.

**Read Replicas**

---------------------

To protect from load.

++++++++++++++++++++++++++++++++++++

Practical

------------

Services ----- Database --- RDS

**Create database**

We get all the options.

Select check box - Only enable options eligible for RDS Free tier usage (Few options will be greyed out)

Select Mysql --- Next --- DB Instance class (db.t2.micro)

Under Settings

DB instance identifier - mydbinstance (It’s like Instance name)

master username - mydbinstance (db username)

master password - mydbinstance, confirm password

Next --- Public accessibility - No

Create new security group (Observation: new security group will be created automatically)

database name - mydbinstance (database name)

Create database -- All DB instance details

++++++++++++++++++++++++++

Let’s understand Snapshots

----------------------

In dashboard -- snapshot,

We can see one Automatic Backup is created.

The moment, a database is created, Automatic Backup is created automatically.

Every day, one Automatic Backup is created automatically.

How to take manual snapshots?

----------------------------------------

Dashboard --- databases -- select your database --- Actions -- take snapshot (do not click)

How to restore the snapshot to the database

---------------------------------------------------

select the snapshot -- actions -- Restore snapshot (do not click)

To copy snapshot to another region

-----------------------------------------

Actions -- copy snapshot -- select the destination region (Theory)

**Multi AZ**

-----------------

Select your database -- modify -- Multi AZ Deployment - yes --

continue -- Modify DB Instance (Theory)

How to create Read Replicas

--------------------------------------

Select your database -- Actions -- create read replica (Theory)

How to delete the database

-----------------------------------------

You cannot delete directly.

Step 1: Select your database -- Modify -- Scroll down uncheck Delete protection -- continue -- Modify DB Instance

Step 2: Select your database -- Actions -- delete - uncheck create final snapshot

Select - I Acknowledge

Type - delete me

Delete

It takes 3-4 min to get delete from the dashboard.

snapshot will also be deleted automatically.

+++++++

++++++++++++++++++

**Cloud Trail**

------------------

It’s an auditing service.

In IAM, we have learnt how to create users, groups, assign users to groups etc.

Let’s Say, someone has deleted S3 bucket?

How to know, which users has done this?

At what time, it has happened?

We can track this information using cloud trail.

All the activities can be tracked by user using cloud trail.

Services -- CloudTrail

Select event history

Observation: We can see the records of the events which we have performed.

Select a particular event, we can get more detail information.

We can apply filters

Filter: Resource type Bucket

We can see the events related to the Se Bucket

We can apply filter based on time period.

We can download the list of events.

Note: Root user can see the Event history.

IAM users will not have access to see the event history.

++++++++++++++++