Amazon RDS

- Amazon Relational Database Service (Amazon RDS)
- Amazon RDS is a managed database service.
- Using RDS has more advantages over deploying DB on EC2
- RDS is a managed service:
    - Automated provisioning, OS patching
    - Continuous backups and restore to specific timestamp (Point in Time Restore)!
    - Monitoring dashboards
    - Read replicas for improved read performance
    - Multi AZ setup for DR (Disaster Recovery)
    - Maintenance windows for upgrades
    - Scaling capability (vertical and horizontal)
    - Storage backed by EBS (gp2 or io1)
- BUT you can't SSH into your instances

Amazon RDS DB Instance

- *DB instance* is an isolated database environment

Blue/Green Deployments

- A blue/green deployment copies a production database in a separate, synchronized staging environment.
- can make changes to the database in the staging without affecting the production DB.
- When you are ready, you can promote the staging DB to be the new production DB

- Cross-Region automated backups: using backup replication, replicate snapshots and transaction logs to a destination Region.
- **Cross-Region read replicas**: Create Server read replica in a different Region from the source DB instance
- **Database Activity Streams**: monitor and set alarms for auditing activity in Oracle db and SQL Server db.
- **Dual Stack Mode:** resources can communicate with a DB instance over (IPv4), (IPv6), or both.
- You can export RDS DB snapshot data to an Amazon S3 bucket.
- After the data is exported, you can analyze the exported data directly through tools like Amazon Athena or Amazon Redshift Spectrum.
- Using an authentication token from IAM database authentication you can authenticate without a password to connect to a DB instance.
- **Multi-AZ DB cluster:**
    - provides a high availability deployment mode
    - Cluster has a writer DB instance and two reader DB instances in three separate Availability Zones in the same Region.
- **Performance Insights dashboard:** visualize the database load on your Amazon RDS DB instance.
- **RDS Custom:** Using RDS Custom, you can access and customize DB environment and operating system.
- **RDS Proxy:** makes applications more scalable by pooling and sharing established database connections.

Database authentication options:

- Password authentication: create users and specify passwords with SQL statements
- (IAM) database authentication: don't need password, use an authentication token.
- Kerberos authentication: use external authentication of database users using Kerberos and Microsoft Active Directory.

Accessing a DB instance in a VPC

1. A DB instance in a VPC accessed by an Amazon EC2 instance in the same VPC
2. A DB instance in a VPC accessed by an EC2 instance in a different VPC - use VPC peering to access the DB instance.
3. A DB instance in a VPC accessed by a client application through the internet - configure a VPC with a single public subnet, configure an internet gateway to enable communication over the internet. access must be granted using the inbound rules of the DB instance's security group,
4. A DB instance in a VPC accessed by a private network
   - An AWS Site-to-Site VPN connection
   - An AWS Direct Connect connection
   - An AWS Client VPN connection

DB parameter groups

- Database parameters specify how the database is configured. e.g. amount or resources, memory
- If DB param group is not defined, DB instance uses default DB param group.
- You cannot modify default parameter group. Create new parameter group for custom config.
- DB instance must be rebooted to use custom param group.
- DB instance parameters are either static or dynamic.
- Static param if changed, manual reboot required to take effect.
- Dynamic params, takes effect immediately without requiring reboot.

Creating an Amazon ElastiCache cache using Amazon RDS DB instance settings

- ElastiCache is a fully managed, in-memory caching service.
- provides microsecond read and write latencies that support flexible, real-time use cases.
- ElastiCache can help you accelerate application and database performance.
- AWS takes care of OS maintenance / patching, optimizations, setup, configuration, monitoring, failure recovery and backups
- Using ElastiCache involves heavy application code changes
- Helps reduce load off of databases for read intensive workloads
- ElastiCache is to get managed Redis or Memcached

Managing an Amazon RDS DB instance

Connecting to an instance :

- Can automatically connect a DB instance using EC2 or lambda functions.
- Often, your DB instance is in a private subnet and your EC2 instance is in a public subnet within a VPC.
- RDS automatically manages VPC security group for your EC2 instance and for your RDS db.
- can use the Amazon RDS console to automatically connect a Lambda function to your DB instance.
- Your Lambda function and DB instance are in the same VPC.
- Should have right permissions to connect.

- use RDS Proxy to include a proxy in your connection. Lambda functions make frequent short database connections that benefit from the connection pooling that RDS Proxy offers.
- use any IAM authentication that you've already set up for your Lambda function, instead of managing database credentials in your Lambda application code.

Stopping an instance :

- Can stop temporarily for cost optimization.
- Stopping and starting a DB instance is faster than creating a DB snapshot, deleting your DB instance, and then restoring the snapshot.
- When in a stopped state, DB instance retains:
    - Instance ID
    - Domain Name Server (DNS) endpoint
    - Parameter group
    - Security group
    - Option group
    - Amazon S3 transaction logs (necessary for a point-in-time restore)
- storage volumes remain attached to the DB instance, and their data is kept.
- deletes any data stored in the RAM
- doesn’t retain public IP address. Different IP on restart.
- should always connect to a DB instance using the DNS endpoint, not the IP address.
- stopped, you are charged for provisioned storage, backup storage, including manual snapshots and automated backups
- If you don't manually start your DB instance after it is stopped for seven consecutive days, RDS automatically starts your DB instance for you.
- You can't stop a DB instance that has a read replica, or that is a read replica.
- can't modify anything in stopped DB instance.

Modifying an instance :

- can either apply immediately or defer until the next maintenance window.
- Some require manually reboot DB instance for the change to take effect. e.g. parameter group changes
- use the --apply-immediately parameter or option to apply changes immediately

Renaming an instance

- the endpoint for the DB instance changes, because the URL includes the name
- old DNS name that was used by the DB instance is immediately deleted,new DNS name becomes effective in 10 minutes.
- All read replicas associated with a DB instance remain associated
- Snapshots, Metrics and events associated are retained/ maintained

Rebooting an instance

- Use Cases:
    - Associating a new DB parameter group
    - Applying a change to a static parameter in an existing DB parameter group
    - Testing Multi-AZ failover
    - Troubleshooting
- Can reboot source instance and its read replicas independently.

- After reboot completes replications resumes automatically.

DB Read replicas

- A *read replica* is a read-only copy of a DB instance.
- Reduce read load on primary instance
- To create read replicas, Amazon RDS uses the built-in replication features of the DB engine.
- if updates made to the primary DB instance, Amazon RDS copies them asynchronously to the read replica.
- Use Cases:
    - Scaling beyond compute or I/O capacity for read-heavy database workloads.
    - Serving read traffic while the source DB instance is unavailable
    - Business reporting or data warehousing scenarios
    - Implementing disaster recovery.
- How read replicas work:
    - Amazon RDS takes a snapshot of source instance and creates a read-only instance from snapshot.
    - Read replicas are updated asynchronously whenever any update in source instance.
    - source DB instance experiences a brief I/O suspension (about 1 min) while the DB snapshot occurs.
    - This suspension can be avoided in Multi-AZ deployment.
    - must enable automatic backups on the source DB instance before creating read replica
- Standby replica can be created in another AZ for high availability in Multi-Az deployment
- Replication with the standby replica is synchronous.
- Unlike a read replica, a standby replica can't serve read traffic.
- In Cross-region deployment, read replica resides in different region than source DB
- By default, read replica storage type is same as source DB instance
- We can have different storage type for read replica.
- If want to increase storage type of read replica, increase at least by 10% more, else get an error.
- Circular replication is not supported. i.e. read replica cannot replicate back to source .
- promoting a read replica:
    - can promote a read replica into a standalone DB instance.
    - RDS reboots the DB instance, after promoting read replica

  Use Cases:
    - Can use read replica promotion as a data recovery scheme if the primary DB instance fails.
    - if your source DB instance is not on preferred storage configuration, can create a read replica, upgrade the storage, then promote the read replica to a standalone instance.
- ARN for an Amazon RDS

  arn:aws:rds:*<region>*:*<account number>*:*<resourcetype>*:*<name>*

RDS Storage Autoscaling

- With autoscaling enabled, RDS scales automatically When it detects you are running out of free db storage.
- Avoid manually scaling your database storage
- You have to set Maximum Storage Threshold (maximum limit for DB storage) at least 10% more than the current allocated storage.
- Automatically modify storage if:
    - Free storage is less than 10% of allocated storage

    - Low-storage lasts at least 5 minutes
    - 6 hours have passed since last modification
- Useful for applications with unpredictable workloads
- Supports all RDS database engines

Deleting DB instance

- can delete a DB instance using the AWS Management Console, the AWS CLI, or the RDS API.
- By default, deletion protection is turned on
- make sure that deletion protection is turned off before deleting an instance.
- you can take a final snapshot, you can use it to restore your deleted DB instance
- final snapshot must be taken when DB is in available state.
- You must do the following:
    - Provide the name of the DB instance
    - Enable or disable the option to take a final DB snapshot of the instance
    - Enable or disable the option to retain automated backups

Multi-AZ deployment

- Multi-AZ deployments can have one standby or two standby DB instances.
- Multi-AZ DB instance deployment – one standby instance
- Multi-AZ DB Cluster deployment – two standby instances
- A Multi-AZ DB instance deployment:
    - high availability and failover support for DB instances
    - RDS automatically provisions and maintains a synchronous standby replica in a different AZ
    - primary DB instance is synchronously replicated across AZs to a standby replica
    - provides data redundancy and minimize latency spikes during system backups
    - can create a Multi-AZ DB instance deployment by simply specifying Multi-AZ when creating a DB instance.
    - There is only one row for the DB instance.
    - The value of Role is Instance or Primary.
    - The value of Multi-AZ is Yes.
    -
- A Multi-AZ DB cluster deployment has the following characteristics:
    - high availability, increased capacity for read workloads, and lower write latency
    - A Multi-AZ DB cluster has a writer DB instance and two reader DB instances in three separate Availability Zones in the same AWS Region.
    - There is a cluster-level row with three DB instance rows under it.
    - For the cluster-level row, the value of Role is Multi-AZ DB cluster.
    - For each instance-level row, the value of Role is Writer instance or Reader instance.
    - For each instance-level row, the value of Multi-AZ is 3 Zones.
    - Multi-AZ DB cluster deployments use semi synchronous replication, needs acknowledgement from read replica to commit changes.
    - Use RDS Proxy (can pool and share database connections) to improve their ability to scale.
- To modify Single-AZ deployment to a Multi-AZ DB instance deployment

1. Takes a snapshot of the primary DB instance's Amazon Elastic Block Store (EBS) volumes.

2. Creates new volumes for the standby replica from the snapshot. These volumes initialize in the background, and maximum volume performance is achieved after the data is fully initialized.
3. Turns on synchronous block-level replication between the volumes of the primary and standby replicas.

- Using a snapshot to create the standby instance avoids downtime but can impact performance.
- To avoid the performance impact, create read replica and enable backups on read replica
- Convert the read replica to Multi-AZ, and run queries that load the data into the read replica's volumes (on both AZs).
- Then promote the read replica to be the primary DB instance.
- Amazon RDS handles failovers automatically.
- Automatically changes the DNS record of the DB instance to point to the standby DB instance.
- need to re-establish any existing connections to your DB instance, JVM settings
- The primary DB instance switches over automatically to the standby replica if :
    - OS underlying the RDS database instance is being patched in an offline operation.
    - Primary host of RDS multi-AZ is unhealthy or unreachable due to loss of connectivity or busy
    - Storage volume of primary instance is experienced failure
    - User requested a failover
- Set up DB event subscriptions to notify you by email or SMS that a failover has been initiated

- If there is a planned or unplanned outage of your writer DB instance in a Multi-AZ DB cluster, Amazon RDS automatically fails over to a reader DB instance in different Availability Zone.
- Failover times are typically under 35 seconds, depends on the database activity.
- A Multi-AZ DB cluster has three DB instances instead of a single DB instance.
- you don't need to specify exactly which DB instance in the DB cluster to connect to or or write your own logic for rerouting connections when some DB instances aren't available.
- writer endpoint- connects to the writer DB instance, supports both read and write operations.
- reader endpoint- connects to either of the two reader DB instances, support only read operation
- instance endpoint- connects to a specific DB instance (reader or writer)

RDS Backups

- RDS creates and saves automated backups of DB instance or Multi-AZ DB
- Automated backups occur daily during the preferred backup window, continues after the window ends until it finishes.
- If not specified, default backup window is of 30-minute
- Total backup storage space equals the sum of the storage for all backups in that Region.
- can set the backup retention period. Default is 1 day if DB instance is created using RDS API or CLI, or is 7 days if created using console.
- can set the backup retention period of a DB instance to between 0 and 35 days.
- When you delete a DB instance, you can choose to retain automated backups.
- Retained automated backups contain system snapshots and transaction logs from a DB instance.
- Retained automated backups and manual snapshots incur billing charges until they're deleted.