Tutorials Dojo RDS Quiz

* Review
  + IAM DB Authentication with MySQL and PostgreSQL
  + Secure all in flight data -
    - Download RDS Root CA certificate. Import the certificate to the servers and configure the application to use SSL to encrypt the connection to RDS.
      * Microsoft SQL Server ONLY
      * When you create an SQL Server DB Instance, RDS creates an SSL certificate for it. The SSL certificate includes the DB instance endpoint as the Common Name (CN) for the SSL certificate to guard against spoofing attacks.
    - Force all connections to the DB instance to use SSL by setting the rds.force\_ssl parameter to true + reboot.
      * By default, the parameter is set to false.
      * Parameter is static = reboot required
  + Use SSL to connect to RDS DB instance.
    - Force SSL for all connections – happens transparently to the client, and the client doesn’t have to do any work to use SSL.
    - Encrypt specific connections – this sets up an SSL connection from a specific client computer, and you must do work on the client to encrypt connection.
  + Protect confidential data of customers – ensure that the RDS DB can only be accessed using the profile credentials specific to your EC2 instances via an authentication token.
    - Enable IAM DB Authentication
  + Transparent Data Encryption (TDE)
    - Primarily used to encrypt stored data on DB instances running Microsoft SQL Server
  + IAM DB Authentication is only supported in MySQL and PostgreSQL DB engines.
    - You don’t need to use a PW when you connect to a DB instance, you use an authentication token.
  + When failing over (Multi-AZ), RDS flips the canonical name record (CNAME) for the DB instance to point at the standby, which is in turn promoted to become the new primary.
    - IP Addresses are per subnet and subnets cannot span multiple AZs