RDS Connectivity

1 — Introduction
These settings control how applications or tools connect to your database after it's created

2 — Compute resource

1 — Don't Connect to an EC2 Compute Resource
1. The database is not directly integrated with any specific EC2 instance.
2. However, you can still connect to it from an EC2 instance or other resources, but you need to manually set up the security group
3. This involves configuring the security group to allow traffic from the specific EC2 instance or a range of IP addresses that need access to the database.
4. Examples
   1. Publicly accessible databases where the application server can be hosted anywhere
   2. Databases accessed by services like AWS Lambda or other non-EC2 resources

2 — Connect to an EC2 Compute Resource
1. This means the database is associated or integrated directly with a specific EC2 instance or instances
2. The database access is configured to work closely with an EC2 compute resource, usually within the same VPC or security group, enhancing connectivity and security
3. Examples
   1. An application hosted on an EC2 instance accessing the database directly within the same VPC or using the same security group settings
   2. Tight integration for performance or security reasons, like a private database accessible only by a specific EC2 instance

3 — DB subnet group
1. A DB subnet group defines which subnets in a virtual private cloud (VPC) are designated for your database.
2. A DB subnet group has subnets in at least two Availability Zones in its AWS Region.
3. For security, the subnets in a DB subnet group are typically private.
4. When setting up a DB Subnet Group for Amazon RDS, you have two options
   1. Choose Existing — Offers more control and customization
   2. Automatic Setup — Quick, convenient, and AWS handles the configuration

4 — Public access
1. Select Yes if you want EC2 instances and other resources outside of the VPC hosting the database to connect to it
2. If you select No, Amazon RDS doesn't assign a public IP address to the database. In this case, no resources outside of the VPC can connect to it without extra configuration.

5 — VPC security group
1. The security group associated with a database controls the inbound and outbound traffic for the database.
2. If you set up a connection to an EC2 instance, RDS creates a security group for the database.
   1. The security has an inbound rule with the EC2 instance's security group as the source.
   2. The security group added by RDS ensures that the the EC2 instance can access the database.

6 — Certificate authority - optional
1. If you install the certificate from the CA onto your application server, communication between your application and the database will be encrypted. This keeps your data secure as it travels.
2. If you don't install the certificate, the communication will not be encrypted, which may expose your data to security risks.
3. How to Get and Install the Certificate — You can get the certificate directly from the AWS website https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html