Connecting to your PostgreSQL database in Amazon Lightsail using SSL

Last updated: January 2, 2020

Amazon Lightsail creates an SSL certificate, and installs it on your PostgreSQL (Postgres) managed database when it's provisioned. The certificate is signed by a certificate authority (CA), and it includes the database endpoint as the Common Name (CN) for the SSL certificate to guard against spoofing attacks.

An SSL certificate created by Lightsail is the trusted root entity and should work in most cases but might fail if your application does not accept certificate chains. If your application does not accept certificate chains, you might need to use an intermediate certificate to connect to your AWS Region.

For more information about the CA certificates for your managed database, supported AWS Regions, and how you can download intermediate certificates for your applications, see Downloading an SSL certificate for your managed database in Amazon Lightsail.

Prerequisites

- Install PostgreSQL server on the computer you will use to connect to your database. For more information, see PostgreSQL Downloads in the Postgres website
- Download the appropriate certificate for your database. For information, see Downloading an SSL certificate for your managed database in Amazon Lightsail.

Connect to your Postgres database using SSL

Complete the following steps to connect to your Postgres database using SSL.

1. Open a Terminal or Command Prompt window.

2. Enter the following command to connect to a PostgreSQL database.

   ```
   psql -h DatabaseEndpoint -p 5432 "dbname=DatabaseName user=UserName
   sslrootcert=/path/to/certificate/rds-combined-ca-bundle.pem sslmode=verify-
   full"
   ```

   In the command, replace:

   - *DatabaseEndpoint* with the endpoint of your database.
   - *DatabaseName* with the name of the database you want to connect to.
   - *UserName* with the user name of your database.
   - */path/to/certificate/rds-combined-ca-bundle.pem* with the local path where you downloaded and saved the certificate for your database.

   Example:

```
psql -h ls-8e81e07f8b821917b11e1c6a0e26cb73c203.czowadgeezqi.us-west-
2.rds.amazonaws.com -p 5432 "dbname=dbmaster user=dbmasteruser
sslrootcert=/home/ec2-user/rds-combined-ca-bundle.pem sslmode=verify-full"
```

3. Type the password for the database user you specified in the previous command when prompted, and press **Enter**.

   You should see a result similar to the following example. Your connection is encrypted if you see a value of “SSL connection."