Connecting to your MySQL database in Amazon Lightsail using SSL

Last updated: January 2, 2020

Amazon Lightsail creates an SSL certificate, and installs it on your MySQL 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.

Supported connections

MySQL uses yaSSL for secure connections in the following versions:

- MySQL version 5.7.19 and earlier 5.7 versions
- MySQL version 5.6.37 and earlier 5.6 versions
- MySQL version 5.5.57 and earlier 5.5 versions

MySQL uses OpenSSL for secure connections in the following versions:

- MySQL version 8.0
- MySQL version 5.7.21 and later 5.7 versions
- MySQL version 5.6.39 and later 5.6 versions
- MySQL version 5.5.59 and later 5.5 versions

MySQL managed databases support Transport Layer Security (TLS) versions 1.0, 1.1, and 1.2. The following list shows the TLS support for MySQL versions:

- MySQL 8.0—TLS1.0, TLS 1.1, and TLS 1.2
- MySQL 5.7—TLS1.0, and TLS 1.1. TLS 1.2 is supported only for MySQL 5.7.21 and later.
- MySQL 5.6—TLS1.0
- MySQL 5.5—TLS1.0

Prerequisites

- Install MySQL server on the computer you will use to connect to your database. For more information, see MySQL Community Server download in the MySQL 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 MySQL database using SSL

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

1. Open a Terminal or Command Prompt window.

2. Enter one of the following commands depending on the version of your MySQL database:

   ○ Enter the following command to connect to a database that is MySQL 5.7 or later.

   ```
   mysql -h DatabaseEndpoint --ssl-ca=/path/to/certificate/rds-combined-
   ca-bundle.pem --ssl-mode=VERIFY_IDENTITY -u UserName -p
   ```

   In the command, replace:

   - *DatabaseEndpoint* with the endpoint 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.
   - *UserName* with the user name of your database.

   Example:

   ```
   mysql -h ls-1c51a7c70a4fb55e542829a4e4e0d735ba42.czowadgeezqi.us-west-
   2.rds.amazonaws.com --ssl-ca=/home/ec2-user/rds-combined-ca-bundle.pem
   --ssl-mode=VERIFY_IDENTITY -u dbmasteruser -p
   ```

   ○ Enter the following command to connect to a database that is MySQL 6.7 or earlier.

   ```
   mysql -h DatabaseEndpoint --ssl-ca=/path/to/certificate/rds-combined-
   ca-bundle.pem --ssl-verify-server-cert -u UserName -p
   ```

   In the command, replace:

   - *DatabaseEndpoint* with the endpoint 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.
   - *UserName* with the user name of your database.

   Example:

   ```
   mysql -h ls-1c51a7c70a4fb55e542829a4e4e0d735ba42.czowadgeezqi.us-west-
   2.rds.amazonaws.com --ssl-ca=/home/ec2-user/rds-combined-ca-bundle.pem
   --ssl-verify-server-cert -u dbmasteruser -p
   ```

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:

```
[ec2-user@ip-172-26-5-44 ~]$ mysql -h ls-1c51a.█████ ████████329a4e4e0d735ba42.czowadgeezqi.us-west-2.rds.amazonaws
.com --ssl-ca=/home/ec2-user/rds-ca-2015-root.pem --ssl-verify-server-cert -u dbmasteruser -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2727
Server version: 8.0.16 Source distribution

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> █
```

4. Type **status**, and press **Enter** to view the status of your connection.

Your connection is encrypted if you see a value of "Cipher in use is" next to SSL.

```
mysql> status
--------------
mysql  Ver 14.14 Distrib 5.5.62, for Linux (x86_64) using readline 5.1

Connection id:          2727
Current database:
Current user:           dbmasteruser@172.26.5.44
SSL:                    Cipher in use is DHE-RSA-AES256-SHA
Current pager:          stdout
Using outfile:          ''
Using delimiter:        ;
Server version:         8.0.16 Source distribution
Protocol version:       10
Connection:             ls-1c51a7beedc70a4fb55e542829a4e4e0d735ba42.czowadgeezqi.us-west-2.rds.amazonaws.com via TCP/I
P
Server characterset:    utf8mb4
Db     characterset:    utf8mb4
Client characterset:    utf8
Conn.  characterset:    utf8
TCP port:               3306
Uptime:                 9 days 16 hours 24 min 33 sec

Threads: 3  Questions: 557480  Slow queries: 0  Opens: 242  Flush tables: 3  Open tables: 146  Queries per second avg:
 0.666
--------------
```