Configuring SSL/TLS

MySQL | PostgreSQL (https://cloud.google.com/sql/docs/postgres/configure-ssl-instance) | SQL Server (https://cloud.google.com/sql/docs/sqlserver/configure-ssl-instance)

This page describes how to configure an instance to use SSL/TLS, and how to manage your server and client certificates.

For more information about using SSL/TLS with MySQL, see Using Encrypted Connections (https://dev.mysql.com/doc/refman/5.7/en/encrypted-connections.html) in the MySQL Reference Manual.

Introduction

Cloud SQL supports connecting to an instance using the Transport Layer Security (SSL/TLS) protocol. If you are connecting to an instance using its public IP address, you should use SSL/TLS, so that the data you send to and receive from Cloud SQL is secure.

If you are connecting using private IP, configuring SSL/TLS is optional; private services access (https://cloud.google.com/vpc/docs/private-access-options#service-networking) traffic stays within Google's network at all times.

Cloud SQL uses a self-signed, per-instance server certificate and a certificate (public/private key pair) on the client (for example, an external application accessing the Cloud SQL instance). These certificates work together to enable the server (instance) and client (application) to encrypt their communication. You must have both a valid server certificate and a valid client certificate (key pair) to support encrypted communication.

Note: SSL/TLS is needed to provide security when you connect to Cloud SQL using IP addresses. If you are connecting to your instance only by using the Cloud SQL Proxy (https://cloud.google.com/sql/docs/mysql/sql-proxy) or the Java Socket Library (https://cloud.google.com/sql/docs/mysql/connect-external-app#java), you do not need to configure your

instance to use SSL/TLS. Connections from App Engine applications are encrypted by default whether you configure SSL/TLS for the instance or not.

Enforcing SSL/TLS

Setting up your Cloud SQL instance to accept SSL/TLS connections enables SSL/TLS connections for the instance, but unsecure connections are still accepted. If you do not enforce SSL/TLS for all connections, any issue with your SSL/TLS configuration can cause all connections to default silently to unencrypted. For this reason, if you are accessing your instance using IP, it is strongly recommended that you enforce SSL for all connections.

Connections to your instance through the Cloud SQL Proxy are encrypted whether you configure or enforce SSL/TLS or not. SSL/TLS configuration affects only connections made using IP addresses.

To enforce SSL/TLS for all connections to your instance:

CONSOLE GCLOUD CURL

1. Go to the Cloud SQL Instances page in the Google Cloud Console.
   GO TO THE CLOUD SQL INSTANCES PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/SQL/INSTANC
2. Click the instance name to open its **Instance details** page.
3. Select the **CONNECTIONS** tab.
4. Scroll down to the **SSL connections** section.
5. Click **Allow only SSL connections**.

Managing your server certificates

Cloud SQL creates a server certificate automatically when you create your instance. As long as the server certificate is valid, you do not need to actively manage your server certificate. However, the certificate has an expiration date; after that date, it is no longer valid, and clients are not able to establish a secure connection to your instance using that certificate.

How server certificate rotation works

Cloud SQL provides a way to rotate your server certificate, so that a new certificate can be seamlessly swapped in before the old certificate expires.

About three months before the server certificate expires for a Cloud SQL instance, the project owners will receive an email from Cloud SQL, telling them that the certificate rotation process has been started for that instance. The email provides the name of the instance, and informs the project owners that a new server certificate has been added to the project. The existing server certificate, as well as any client certificates, continue to function normally. In effect, the instance has two server certificates during this time.

The project administrator, or someone with the proper permissions, downloads a new server certificate PEM file, which contains the certificate information for both the current and the new server certificates. Someone must then update all clients that access the Cloud SQL instance using SSL/TLS to use the new PEM file.

After all clients have been updated, the project administrator tells Cloud SQL to rotate to the new server certificate. This means that the old server certificate is no longer recognized, and only the new server certificate can be used.

At this point, the rotation is complete, and no further action is required. The client certificates are unaffected by server certificate rotation.

Rotating your server certificates

If you've received a notice about your certificates expiring, or you have initiated a rotation, then you must take the following steps to complete the rotation:

1. Download the new server certificate information.
2. Update your clients to use the new server certificate information.
3. Complete the rotation, which moves the currently active certificate into the "previous" slot and updates the newly added certificate to be the active certificate.

CONSOLE GCLOUD CURL

Download the new server certificate information:

1. Go to the Cloud SQL Instances page in the Google Cloud Console.

   GO TO THE CLOUD SQL INSTANCES PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/SQL/INSTANC

2. Click the instance name to open its **Instance details** page.
3. Select the **CONNECTIONS** tab.
4. Scroll down to the **Configure SSL server certificates** section.
5. Click **Create new certificate**.
6. Scroll down to **Download SSL server certificates** section.
7. Click **Download**.

   The server certificate information, encoded as a PEM file, is displayed and can be downloaded to your local environment.

8. Update all of your clients to use the new information.

After you have updated your clients, complete the rotation:

1. Return to the **Configure SSL server certificates** section.
2. Click **Rotate certificate**.
3. Confirm that your clients are connecting properly.

   If any clients are not connecting using the newly rotated certificate, you can click **Rollback certificate** to roll back (#rollback) to the previous configuration.

Rolling back a certificate rotation operation

After you complete a certificate rotation, your clients must all use the new certificate to connect to your Cloud SQL instance. If the clients were not updated properly to use the new certificate information, they will not be able to connect using SSL/TLS to your instance. If this happens, you can roll back to the previous certificate configuration.

A rollback operation moves the currently active certificate into the "upcoming" slot (replacing any current "upcoming" certificate). The "previous" certificate becomes the currently active certificate, returning your certificate configuration to the state it was in before you completed the rotation.

Note: Certificate rollback is available only until the old certificate expires.

To roll back to the previous certificate configuration:

CONSOLE GCLOUD CURL

1. Go to the Cloud SQL Instances page in the Google Cloud Console.
   GO TO THE CLOUD SQL INSTANCES PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/SQL/INSTANC
2. Click the instance name to open its **Instance details** page.
3. Select the **CONNECTIONS** tab.
4. Scroll down to the **Configure SSL server certificates** section.
5. Click **Rotate certificate**. It takes a few seconds for the action to complete.
6. Click **Rollback certificate**.

Initiating a rotation

You do not need to wait for the email from Cloud SQL to start a rotation. You can start one at any time. When you start a rotation, a new certificate is created and placed into the "upcoming" slot. If a certificate was already in the "upcoming" slot, it is deleted; there can be only one upcoming certificate.

To initiate a rotation:

CONSOLE GCLOUD CURL

1. Go to the Cloud SQL Instances page in the Google Cloud Console.
   GO TO THE CLOUD SQL INSTANCES PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/SQL/INSTANC
2. Click the instance name to open its **Instance details** page.
3. Select the **CONNECTIONS** tab.
4. Scroll down to the **Configure SSL server certificates** section.
5. Click **Create new certificate**.
6. Complete the rotation as described in Rotating your server certificates (#rotate).

Getting information about your server certificate

You can get information about your server certificate, such as when it expires or what level of encryption it provides.

CONSOLE GCLOUD CURL

1. Go to the Cloud SQL Instances page in the Google Cloud Console.

   GO TO THE CLOUD SQL INSTANCES PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/SQL/INSTANC

2. Click the instance name to open its **Instance details** page.
3. Select the **CONNECTIONS** tab.
4. Scroll down to the **Configure SSL server certificates** section.

   You can see the expiration date of your server certificate in the table.

   To see the certificate type, use the `gcloud` command-line tool.

Resetting your SSL/TLS configuration

You can completely reset your SSL/TLS configuration.

Caution: Performing this action removes the ability to connect to your instance using SSL/TLS until you recreate your client certificates.

GCLOUD CURL

For First Generation instances, this task requires your Cloud SQL instance to be restarted.

Note: Second Generation is replacing First Generation; support for First Generation instances ends January 30, 2020. To upgrade a First Generation instance to Second Generation, see Upgrading a First Generation Instance to Second Generation (https://cloud.google.com/sql/docs/mysql/upgrade-2nd-gen).

1. Refresh the certificate:

```
gcloud sql instances reset-ssl-config [INSTANCE_NAME]
```

2. For First Generation instances, restart the instance to complete the refresh.

```
gcloud sql instances restart [INSTANCE_NAME]
```

3. Create new client certificates (#new-client).

Managing your client certificates

Creating a new client certificate

You can create up to 10 client certificates for each instance. If you lose the private key for a certificate, you must create a new one; the private key cannot be recovered.

CONSOLE (2ND GEN) MORE

1. Go to the Cloud SQL Instances page in the Google Cloud Console.

   GO TO THE CLOUD SQL INSTANCES PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/SQL/INSTANC
2. Click the instance name to open its **Instance details** page.
3. Select the **CONNECTIONS** tab.
4. Scroll down to the **Configure SSL client certificates** section.
5. Click **Create new certificate**.
6. In the **Create a client certificate** dialog box, give the certificate a name unique for this.
7. Click **Create**.
8. In the first section of the **New SSL certificate created** dialog box, click **Download client-key.pem** to download the private key to a file named `client-key.pem`.

Important: Store this private key securely. If you lose it, you must create a new client certificate.

9. In the second section, click **Download client-cert.pem** to download the client certificate to a file named `client-cert.pem`.
10. In the third section, click **Download server-ca.pem** to download the server certificate to a file named `server-ca.pem`.
11. Click **Close**.

At this point, you have:

- A server certificate saved as `server-ca.pem`.
- A client public key certificate saved as `client-cert.pem`.
- A client private key saved as `client-key.pem`.

Depending on which tool you use to connect, these three items are specified in different ways. For example, when connecting using MySQL client, these three files are the values for the `--ssl-ca`, `--ssl-cert`, and `--ssl-key` command options, respectively. For an example connection using MySQL client and SSL/TLS, see Connecting with MySQL Client (https://cloud.google.com/sql/docs/mysql/connect-admin-ip#connect).

Retrieving a client certificate

You can retrieve the public key portion of a client certificate. You cannot retrieve the private key, however. If you have lost your private key, you must create a new certificate.

CONSOLE GCLOUD CURL

1. Go to the Cloud SQL Instances page in the Google Cloud Console.
   GO TO THE CLOUD SQL INSTANCES PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/SQL/INSTANC
2. Click the instance name to open its **Instance details** page.
3. Select the **CONNECTIONS** tab.
4. Scroll down to the **Configure SSL client certificates** section.
5. Click a certificate name. The **SSL Client Certificate** dialog box opens and shows the client certificate (`client-cert.pem`).

Deleting a client certificate

CONSOLE (2ND GEN) MORE

1. Go to the Cloud SQL Instances page in the Google Cloud Console.
   GO TO THE CLOUD SQL INSTANCES PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/SQL/INSTANC
2. Click the instance name to open its **Instance details** page.
3. Select the **CONNECTIONS** tab.
4. Scroll down to the **Configure SSL client certificates** section.
5. Find the certificate you want to delete and click 🗑.
6. In the **Delete client certificate** dialog box, click **OK**.

What's next

- Connect to your instance (https://cloud.google.com/sql/docs/mysql/connect-admin-ip#connect-ssl) with the mysql client using SSL/TLS.
- Learn more about how MySQL uses SSL/TLS (https://dev.mysql.com/doc/refman/5.7/en/encrypted-connections.html).

Last updated December 5, 2019.