Configuring SSL/TLS

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

Beta

This feature is in a pre-release state and might change or have limited support. For more information, see the product launch stages (https://cloud.google.com/products/#product-launch-stages).

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

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.

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/sqlserver/sql-proxy), 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. 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.

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

1. Refresh the certificate:

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

What's next

- Connect to your instance (https://cloud.google.com/sql/docs/sqlserver/connect-admin-ip#connect-ssl) with the sqlcmd client using SSL/TLS.

Last updated December 3, 2019.