TLS settings in PostgreSQL

Last updated by | Lisa Liu | Nov 6, 2020 at 10:36 AM PST

https://docs.microsoft.com/en-us/azure/postgresql/concepts-ssl-connection-security ⬈

https://docs.microsoft.com/en-us/azure/postgresql/howto-tls-configurations ⬈

Configuring TLS settings in Azure Database for PostgreSQL Single - server using Azure portal

06/02/2020

This article describes how you can configure an Azure Database for PostgreSQL to enforce minimum TLS version allowed for connections and deny all connections with lower TLS version than configured minimum TLS version thereby enhancing the network security.

You can enforce TLS version for connecting to their Azure Database for PostgreSQL. Customers now have a choice to set the minimum TLS version for their database server. For example, setting the minimum TLS setting version to TLS 1.0 means your server will allow connections from clients using TLS 1.0, 1.1, and 1.2+. Instead, setting minimum tls version to 1.2+ means you only allow connections from clients using TLS 1.2 and all connections with TLS 1.0 and TLS 1.1 will be rejected.

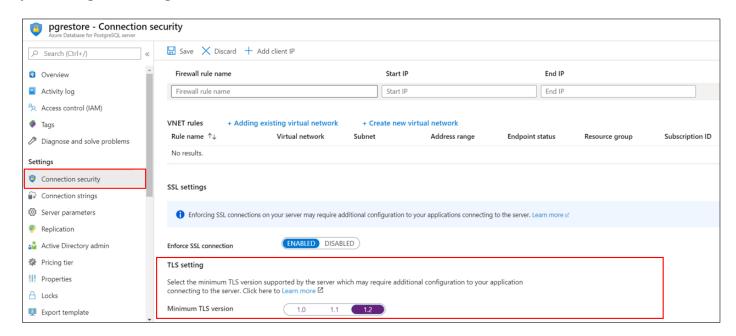## Prerequisites

To complete this how-to guide, you need:

- An Azure Database for PostgreSQL

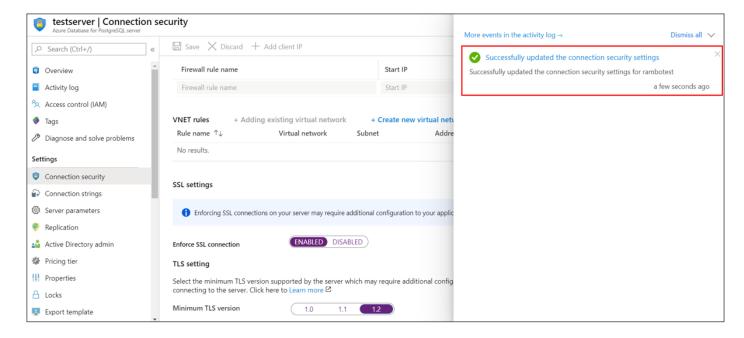## Set TLS configurations for Azure Database for PostgreSQL - Single server

Follow these steps to set PostgreSQL minimum TLS version:

1. In the Azure portal, select your existing Azure Database for PostgreSQL.

2. On the Azure Database for PostgreSQL - Single server page, under **Settings**, click **Connection security** to open the connection security configuration page.

3. In **Minimum TLS version**, select **1.2** to deny connections with TLS version less than TLS 1.2 for your PostgreSQL Single server.

4. Click **Save** to save the changes.

5. A notification will confirm that connection security setting was successfully enabled.

How good have you found this content?