Cloud SQL (https://cloud.google.com/sql/)
Documentation (https://cloud.google.com/sql/docs/)
SQL Server (https://cloud.google.com/sql/docs/sqlserver/) Guides

Configuring private IP connectivity

MySQL (https://cloud.google.com/sql/docs/mysql/configure-private-ip) | PostgreSQL
(https://cloud.google.com/sql/docs/postgres/configure-private-ip) | **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 a SQL Server instance to use private IP. For information
about how private IP works, as well as environment and management requirements, see Private
IP (https://cloud.google.com/sql/docs/sqlserver/private-ip).

Before you begin

Before configuring a Cloud SQL instance to use private IP, you must consider the following:

- You must choose a VPC network (https://cloud.google.com/vpc/docs/vpc) to use. The Google
  Cloud resources you will use to connect to your Cloud SQL instance (either Compute
  Engine instances [VMs] or Google Kubernetes Engine instances) must use this VPC
  network in order to be able to connect. These resources must also be in the same region
  as your Cloud SQL instance.

⭐   **Note:** Your Cloud SQL instances are not created in your VPC network. They are created in the *service
   producer* network (a VPC network internal to Google) that is then connected (peered) to your VPC
   network.

- Before using private IP Cloud SQL instances in a given VPC network for the first time, you
  need to configure *private services access* in the VPC network. This allows resources in the
  VPC network to connect to Cloud SQL instances. As part of this configuration, a range of
  IP addresses must be allocated for use by the Cloud SQL instances. If you wish, you may

select a specific IP range to use. Otherwise, Cloud SQL will automatically allocate an unused range for you. In either case, the instructions below will help you allocate a range of IP addresses. For more information and for additional considerations, see Configuring Private Services Access (https://cloud.google.com/vpc/docs/configure-private-services-access).

The IP range 172.17.0.0/16 is reserved for the Docker bridge network. Any Cloud SQL instances created with an IP in that range will be unreachable. Connections from any IP within that range to Cloud SQL instances using private IP will fail.

- You must enable the Service Networking API
  (https://console.cloud.google.com/apis/library/servicenetworking.googleapis.com) for your project.

  The Service Networking API is used to establish private services access.

Configuring an instance to use private IP at creation time

You can configure a Cloud SQL instance to use private IP when you create the instance.

Note: After you configure an instance to use private IP, you cannot disable private IP connectivity for that instance.

To configure a new instance to use private IP:

CONSOLE   GCLOUD

1. In the Creation wizard, under **Configuration Options**, expand the **Connectivity** section.

2. Select the **Private IP** checkbox.

   The drop-down list shows the available networks in your project. If your project is the service project of a Shared VPC (https://cloud.google.com/vpc/docs/shared-vpc), VPC networks from the host project are also shown.

   ★   **Note:** If you are unable to select the **Private IP** checkbox, you might be missing some permissions on your account (compute.globalAddresses.create and servicenetworking.services.addPeering). As a workaround, use gcloud or the VPC Admin API instead of the console.

3. Select the network where the resources you want to connect from are located.

4. If you previously configured private services access for Cloud SQL in this VPC network, you are done. Select instance settings and create the instance.

5. If this network does not have a range of IP addresses allocated to it for private services access, do one of the following:

   - Click **Allocate and connect** to let Cloud SQL allocate the range for you and create the private connection. You are done; select instance settings and create the instance.

   - Refer to the instructions for configuring private services access for Cloud SQL (#configure-access) below. When finished, proceed with choosing instance settings and creating the instance.

6. If one or more allocated IP ranges exist for your network, and you haven't yet selected the range you want to use to connect to the Cloud SQL service, select the range and click **Connect**. Proceed with choosing instance settings and creating the instance.

Configuring an existing instance to use private IP

You can configure an existing Cloud SQL instance to use private IP.

Note: After you configure an instance to use private IP, you cannot disable private IP connectivity for that instance.

Configuring an existing Cloud SQL instance to use private IP causes the instance to restart, resulting in downtime.

To configure an existing instance to use private IP:

CONSOLE   GCLOUD

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 **Overview** page.

3. Select the **Connections** tab.

4. Select the **Private IP** checkbox.

   The drop-down list shows the available networks in your project. If your project is the service project of a Shared VPC (https://cloud.google.com/vpc/docs/shared-vpc), VPC networks from the host project are also shown.

★ **Note:** If you are unable to select the **Private IP** checkbox, you might be missing some permissions on your account (compute.globalAddresses.create and servicenetworking.services.addPeering). As a workaround, use gcloud or the VPC Admin API instead of the console.

5. Select the network where the resources you want to connect from are located.

6. If you previously configured private services access for Cloud SQL in this VPC network, you are done; click **Save** to update the instance.

7. If this network does not have a range of IP addresses allocated to it for private services access, do one of the following:

   a. Click **Allocate and connect** to let Cloud SQL allocate the range for you and create the private connection. You are done; click **Save** to update the instance.

   b. Refer to the instructions for <u>configuring private services access for Cloud SQL</u> (#configure-access) below. Then click **Save** to update this instance.

8. If one or more allocated IP ranges exist for your network, and you haven't yet selected the range you want to use to connect to the Cloud SQL service, select the range and click **Connect**. Then click **Save** to update the instance.

Configuring private services access for Cloud SQL

This section provides instructions for configuring private services access in your VPC network without creating a Cloud SQL instance. In many cases, Cloud SQL can do this automatically when you launch an instance. However, these manual instructions may be useful if:

- You wish to control the size of the IP address range that is allocated. For example, if you anticipate creating a large number of Cloud SQL instances, you might choose in advance to allocate an IP range that can hold them all.

- You wish to set up private services access from the command line (using `gcloud`).

- You are using <u>Shared VPC</u> (https://cloud.google.com/vpc/docs/shared-vpc) and your organization administrator has delegated network administrative responsibilities to a Network Admin in the host project. The Network Admin can perform the steps below *in the host project* to configure private services access. Subsequently, users who have been delegated privileges in the service project(s) can freely launch Cloud SQL instances by following the instructions in the sections above. Those users need only be granted Network User privileges in the host project.

You only need to perform these steps once per VPC network. For more information and for additional considerations, see Configuring Private Services Access (https://cloud.google.com/vpc/docs/configure-private-services-access).

There are two parts to this process:

- Allocating an IP address range.

- Creating a private connection from your VPC network to the service producer network (where Cloud SQL instances will reside).

Allocating an IP address range

CONSOLE   GCLOUD

1.
   GO TO THE VPC NETWORKS PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/NETWORKING/NETW

   in the Google Cloud Console.

2. Select the VPC network that you wish to use.

3. Select the **Private service connection** tab.

4. In the **Private service connection** tab, select the **Allocated IP ranges for services** tab.

5. Click **Allocated IP range**.

6. For the **Name** of the allocated range, specify `google-managed-services-VPC_NETWORK_NAME`, where `VPC_NETWORK_NAME` is the name of the VPC network you are connecting (for example, `google-managed-services-default`). You may leave the **Description** blank.

7. Specify an **IP range** for the allocation:

   - To specify an IP address range, select **Custom** and then enter a CIDR block, such as `192.168.0.0/16`.

   - To specify a prefix length and let Google select an available range, select **Automatic** and then enter a prefix length, such as `16`.

8. Click **Allocate** to create the allocated range.

Creating a private connection

CONSOLE   GCLOUD

1.

   GO TO THE VPC NETWORKS PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/NETWORKING/NETW

   in the Google Cloud Console.

2. Select the VPC network that you wish to use.

3. Select the **Private service connection** tab.

4. In the **Private service connection** tab, select the **Private connections to services** tab.

5. Click **Create connection** to create a private connection between your network and a service producer.

6. For the **Assigned allocation**, select one or more existing allocated ranges that are not being used by other service producers.

7. Click **Connect** to create the connection.

Using Cloud VPN with Cloud SQL

To enable VPN access, configure your VPC to export custom routes from your associated network to the Cloud SQL host network (https://cloud.google.com/vpc/docs/vpc-peering) over the peering connection. You need to perform this procedure for each database engine that you use (MySQL, PostgreSQL, and SQL Server). Before performing this procedure, create your VPN.

CONSOLE   **GCLOUD**

1. Create a new instance with private IP (#new-private-instance) or configure an existing instance with private IP (#existing-private-instance).

2. Verify that the network peering exists between your VPN and the Cloud SQL network.

   a. Go to the **VPC network details** page for your Cloud SQL network.

   b. Look under **Name** for cloudsql-sqlserver-googleapis-com.

3. Verify that **export** is enabled for the network peering.

   a. Look under **Exchange custom routes**. If it says **Export custom routes**, go to step 4.

   b. Click the name of the peering to view the **Peering connection details** page.

   c. Click **EDIT**.

   d. Check **Export custom routes**.

   e. Click **Save**.

4. Add a route in your on-premise network:

a. **IP range**: Add the reserved IP range. You can find this on the **VPC network details** page under **Destination IP range**.

b. **Next hop**: Add the VPN gateway. You can find the VPN tunnel on the **VPC network details** page under **Next hop**.

What's next

- Learn more about private IP (https://cloud.google.com/sql/docs/sqlserver/private-ip).

- Learn more about private services access (https://cloud.google.com/vpc/docs/private-access-options#service-networking).

- See how to use VPC Service Controls (https://cloud.google.com/sql/docs/sqlserver/admin-api/configure-service-controls) to add a service perimeter.