MySQL (/sql/docs/mysql/configure-private-ip) | **PostgreSQL** | SQL Server (/sql/docs/sqlserver/configure-private-ip)

This page describes how to configure a PostgreSQL instance to use private IP. For information about how private IP works, as well as environment and management requirements, see Private IP (/sql/docs/postgres/private-ip).

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

- You must choose a VPC network (/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 (/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.

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

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:

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

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:

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 Shared VPC (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 (/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).

To enable VPN access, configure your VPC to export custom routes from your associated network to the Cloud SQL host network (/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.

- Learn more about private IP (/sql/docs/postgres/private-ip).
- Learn more about private services access (/vpc/docs/private-access-options#service-networking).
- See how to use VPC Service Controls (/sql/docs/postgres/admin-api/configure-service-controls) to add a service perimeter.