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

Private IP

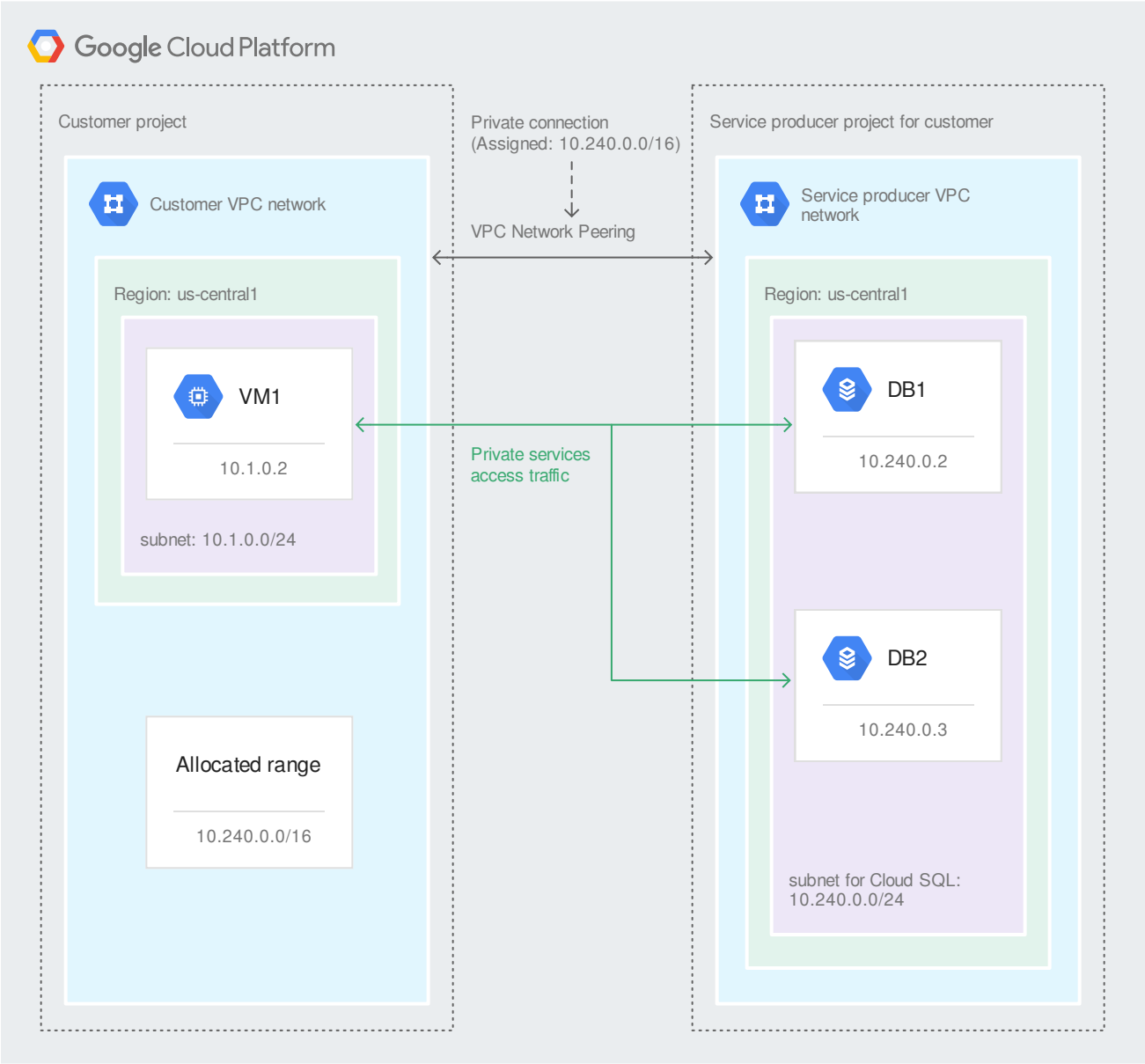
MySQL (https://cloud.google.com/sql/docs/mysql/private-ip) | PostgreSQL (https://cloud.google.com/sql/docs/postgres/private-ip) | **SQL Server**

This page provides information about using private IP to connect to your Cloud SQL instances. For step-by- step instructions for configuring an instance to use private IP, see Configuring Private IP Connectivity (https://cloud.google.com/sql/docs/sqlserver/configure-private-ip).

Overview

When you configure a Cloud SQL instance to use private IP, you use *private services access* (https://cloud.google.com/vpc/docs/private-access-options#service-networking). Private services access is implemented as a VPC peering connection (https://cloud.google.com/vpc/docs/vpc-peering) between your VPC network (https://cloud.google.com/vpc/docs/vpc) and the Google services VPC network where your Cloud SQL instance resides. IP traffic using private services access is never exposed to the public Internet.

The following diagram shows a Cloud SQL instance configured for private IP, and a Compute Engine instance on the peered customer VPC network using private services access to connect to the Cloud SQL instance.



You can use private services access to connect to Cloud SQL instances from Compute Engine or Google Kubernetes Engine instances.

Note: Cloud SQL instances reside on their own internal VPC network; you cannot put Cloud SQL instances on a VPC network that you create.

Benefits

Using private IP to connect to Cloud SQL gives you several advantages over using public IP addresses:

- Lower network latency

  Private IP provides lower latency than public IP.

- Improved network security

  Private services access traffic is never exposed to the public Internet.

Environment requirements

To use private IP, your network and application environment must meet the following requirements. In addition, setting up private IP for the first time requires some additional IAM permissions.

Network requirements

- Connectivity to Cloud SQL instances on private IP addresses depends on private services access (https://cloud.google.com/vpc/docs/private-access-options#service-networking), which uses VPC Network Peering (https://cloud.google.com/vpc/docs/vpc-peering) to connect your VPC network (https://cloud.google.com/vpc/docs/vpc) to a VPC network managed by Google. Cloud SQL instances use subnets in that Google-managed VPC network.
  - You can only access a Cloud SQL instance on its private IP addresses from a *single* VPC network (https://cloud.google.com/vpc/docs/vpc). Each private services access connection requires a single VPC Network peering connection to one VPC network.
  - You *cannot* access a Cloud SQL instance on its private IP addresses from *another* VPC network connected using VPC Network Peering to the VPC network with the private services connection for that Cloud SQL instance.
  - You can access a Cloud SQL instance on its private IP addresses from *another* network using a Cloud VPN tunnel, instance based VPN, or Cloud Interconnect. This applies to both on-premises networks and other VPC networks. To use VPN, you need to export the custom routes from Compute Engine to Cloud SQL. Learn more (https://cloud.google.com/sql/docs/sqlserver/configure-private-ip#vpn).
  - You cannot connect to the private IP of a Cloud SQL instance from a legacy network (https://cloud.google.com/vpc/docs/legacy). Legacy networks do not support VPC

Network Peering or private services access.

- To access a Cloud SQL instance on its private IP addresses, you must use a Google Cloud resource in the same region.
- You must define an allocated IP address range (https://cloud.google.com/vpc/docs/configure-private-services-access#allocating-range) for the Cloud SQL instances in your VPC network. This range is a CIDR block of IP addresses that are available for the private services access connection (and the resulting VPC Network Peering) to use. You *cannot* use these IP addresses in *your* VPC network. An allocated IP address range ensures that subnet IP ranges and destinations for custom routes in your VPC network do not overlap with ones that the private services access connection uses. You can create an allocated IP range manually if you want to control the CIDR block, or you can have Google Cloud create one for you.
- You can create Cloud SQL instances with private IP addresses in a Shared VPC network (https://cloud.google.com/vpc/docs/shared-vpc); however, Google Cloud does not allow you to assign a private IP address for an *existing* Cloud SQL instance to an address in a Shared VPC network.

Application environment requirements

- If you are connecting from GKE, you must be running GKE 1.8 or higher on a VPC-native (https://cloud.google.com/kubernetes-engine/docs/how-to/alias-ips) cluster.
- If you are connecting from App Engine, you must use flexible environment. You cannot use private IP to connect from standard environment.

API and IAM requirements

- You must have enabled the Service Networking API (https://console.cloud.google.com/apis/library/servicenetworking.googleapis.com) for your project. If you are using shared VPC, you also need to enable this API for the host project.

  Enabling APIs requires the servicemanagement.services.bind IAM permission.
- Establishing private services access requires the `Network Administrator` IAM role.

  After private services access is established for your network, you do not need the `Network Administrator` role to configure an instance to use private IP.

Security

Private services access traffic is encrypted and authenticated. For details, see Google Cloud's virtual network encryption and authentication (https://cloud.google.com/security/encryption-in-transit/#virtual-network). If your security requirements mandate SSL/TLS certification that you manage, you can add SSL/TLS to your instance, using the instructions provided in Configuring SSL/TLS (https://cloud.google.com/sql/docs/sqlserver/configure-ssl-instance).

Overview of setting up private services access for your network

When you configure private IP connectivity for the first time on a specific VPC network, you need to perform a one-time procedure to set up private services access for that network. The Cloud SQL instance creation process in the Google Cloud Console (https://console.cloud.google.com/sql) guides you through the following steps:

1. Select the VPC network where the resources you want to connect from are located.
2. If private services access has not yet been established for your VPC network and the Cloud SQL service, you must enable it. This requires an allocated IP address range from your network.
    a. If you have previously allocated an IP range to use, select it and proceed.
    b. If you want Cloud SQL to automatically allocate a range for you, select that option and proceed.
    c. If you want to manually select the IP range to allocate for the private connection, follow the instructions for configuring private services access (https://cloud.google.com/sql/docs/sqlserver/configure-private-ip#configure-access), then return to the Cloud SQL instance creation flow and select the newly created IP range.

Important: When you create a private connection between your VPC network and the Cloud SQL service, it becomes available for use by any Google service that supports private services access. If you later delete the private connection, you remove private connectivity to your Cloud SQL instances and *any other service that is using that connection*. Removing the private connection does not delete or deprovision any resources.

After you have established private services access, you can create a Cloud SQL instance configured to use private IP or configure private IP for an existing Cloud SQL instance by using

the `gcloud` command-line tool or the Cloud SQL Admin API, in addition to the Google Cloud Console. For more information, see Configuring Private IP Connectivity (https://cloud.google.com/sql/docs/sqlserver/configure-private-ip).

Administration considerations

When you manage Cloud SQL instances using private IP, you should be aware of the following facts:

- After you configure a Cloud SQL instance to use private IP, you cannot remove private IP capability from that instance.
- You can configure an instance to use private IP at instance creation time or later.
- Configuring an existing instance to use private IP, or changing the network it is connected to, causes the instance to be restarted. This causes a few minutes of downtime.
- Cloud SQL instances are created in a producer network (a VPC network internal to Google). They are not created in your VPC network.
- The private IP address of the Cloud SQL instance is static; it does not change.
- Replicas inherit their private IP status from their primary instance. You cannot configure private IP directly on a replica.
- You can use both public IP and private IP to connect to the same Cloud SQL instance. Neither connection method affects the other; you must protect the public IP connection whether the instance is configured to use private IP or not.
- You can use the Cloud SQL Proxy to connect to an instance that is also configured to use private IP. The proxy can connect using either the private IP address or a public IP address. If you use the Cloud SQL Proxy to connect to an instance that has both public and private IP addresses assigned, the proxy uses the public IP address by default. Learn more (https://cloud.google.com/sql/docs/sqlserver/sql-proxy#private-ip).
- A private services access connection relies on a VPC Network Peering. However, you do not create the VPC Network peering explicitly, because the peering is internal to Google Cloud. After you create the private services access connection, you can see its underlying VPC Network Peering on the VPC Network Peering page in the Cloud Console, but you should not delete it unless you want to remove the private connection (https://cloud.google.com/vpc/docs/configure-private-services-access#removing-connection).

★ **Important:** Deleting the underlying VPC Network peering for a private services access connection removes private connectivity for all resources that are using it and all services it is connected to.

- After you have established a private services access connection, and created a Cloud SQL instance with private IP configured for that connection, the corresponding (internal) subnet and range used by the Cloud SQL service cannot be modified or deleted. This is true even if you delete the peering and your IP range. After the internal configuration is established, any Cloud SQL instance created in that same region and configured for private IP uses the original internal configuration.

What's next

- See how to configure private IP (https://cloud.google.com/sql/docs/sqlserver/configure-private-ip).
- Learn more about private services access (https://cloud.google.com/vpc/docs/private-access-options#service-networking).
- See how to configure private services access (https://cloud.google.com/sql/docs/sqlserver/configure-private-ip#configure-access) for Cloud SQL instances.

Last updated December 16, 2019.