Connection organization policies

MySQL | PostgreSQL (https://cloud.google.com/sql/docs/postgres/connection-org-policy) | SQL Server (https://cloud.google.com/sql/docs/sqlserver/connection-org-policy)

This page provides overview information about using a connection organization policy with your Cloud SQL project. To get started creating connection organization policies, see Configuring connection organization policies (https://cloud.google.com/sql/docs/mysql/configure-org-policy).

Overview

Connection organization policies provide centralized control of the public IP settings for Cloud SQL, to reduce the security attack surface of Cloud SQL instances from the Internet. An organization policy administrator can use a connection policy to restrict public IP configurations of Cloud SQL at the project, folder, or organization level.

Understanding organization policies

Organization policies let organization administrators set restrictions on how users can configure instances under that organization. Organization policies use rules, called constraints, that the organization administrator places on a project, folder, or organization. Constraints enforce the policy across all instances. If, for example, you try to add an instance to an entity that has an organization policy, the constraint runs a check to ensure the instance configuration follows the requirements of the constraint. If the check fails, Cloud SQL does not create the instance.

As you add projects to an organization or folder that uses an organization policy, the projects inherit the constraints of that policy.

For more information about organization policies, see Organization Policy Service (https://cloud.google.com/resource-manager/docs/organization-policy/overview), Constraints

(https://cloud.google.com/resource-manager/docs/organization-policy/understanding-constraints), and Hierarchy Evaluation (https://cloud.google.com/resource-manager/docs/organization-policy/understanding-hierarchy).

Connection organization policy constraints

For the connection organization policy, there are two types of constraints that enforce access to Cloud SQL instances.

Constraint	Description	Default
Restrict public IP access on Cloud SQL instances	This boolean constraint restricts configuring public IP on Cloud SQL instances where this constraint is set to **`True`**. This constraint is not retroactive, Cloud SQL instances with existing public IP access will still work even after this constraint is enforced. By default, public IP access is allowed to Cloud SQL instances. **`constraints/sql.restrictPublicIp`**	ALLOW
Restrict Authorized Networks on Cloud SQL instances	This boolean constraint restricts adding Authorized Networks for unproxied database access to Cloud SQL instances where this constraint is set to **`True`**. This constraint is not retroactive, Cloud SQL instances with existing Authorized Networks will still work even after this constraint is enforced. By default, Authorized Networks can be added to Cloud SQL instances. **`constraints/sql.restrictAuthorizedNetworks`**	ALLOW

Connection organization policy enforcement rules

Cloud SQL enforces the connection organization policy during the following tasks:

- Instance creation
- Replica creation
- Instance reconfiguration
- Instance clone

- Instance restore
- Upgrade of existing First Generation MySQL instance to Second Generation.

Like all Cloud SQL organization policy constraints (https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints), policy changes do not apply retroactively to existing instances.

- A new policy has no effect on existing instances.
- An existing instance configuration remains valid, unless a user changes the instance configuration from a compliance to non-compliance state using the Console, `gcloud` command-line tool, or RPC.
- A scheduled maintenance update does not cause a policy enforcement, because maintenance does not change the configuration of instances.

Restrictions

When you set the connection organization policy for each project, you need to determine if any one of the following apply to your project:

- Read replicas public IP conflicts (#read-replica-ip-conflicts)
- Incompatibility using gcloud sql connect (#sql-connect)
- GCP hosted services access (#gcp-host)
- MySQL failover replica public IP conflicts (#failover-replica)
- MySQL First Generation instances (#first-gen)

Read replicas public IP address conflicts

Cloud SQL read replicas connect to the master instance over the non-proxied database connection. You use the master instance **Authorized Networks** setting to either explicitly or implicitly configure the read replica public IP addresses.

If both the master and replica instances are within the same region and enable private IP, there is no conflict with connection organization policy constraints.

Incompatibility using `gcloud sql connect`

The `gcloud sql connect` command uses a public IP address to connect to Cloud SQL instances directly. Therefore, it is incompatible with the `sql.restrictPublicIp` constraint.This is generally a problem for instances that use private IP.

In addition, the `gcloud sql connect` command does not use the proxy, making it incompatible with the `sql.restrictAuthorizedNetworks` constraint.

Instead, use the beta version of the command:

```
gcloud beta auth login
gcloud beta sql connect [INSTANCE_ID]
```

This version uses the Cloud SQL Proxy. See `gcloud beta sql connect` (https://cloud.google.com/sdk/gcloud/reference/beta/sql/connect) for reference information.

The first time you run this command, you are prompted to install the gcloud Cloud SQL Proxy component. For that, you need to have write permission to the gcloud SDK installation directory on your client machine.

GCP hosted services access

If your application requires access to Cloud SQL instances from other GCP hosted services, such as App Engine, the application must use public IP addresses. This means you should not enforce the `sql.restrictPublicIp` constraint on the project. You can, however, enforce `sql.restrictAuthorizedNetworks`, as connections from App Engine go through the secure (proxied) connection (https://cloud.google.com/sql/docs/mysql/connect-app-engine).

MySQL failover replica public IP conflicts

A MySQL failover replica acts the same as a read replica for connection organization policies. If both the primary and replica instances are within the same region and enable private IP, there is no conflict with connection organization policy constraints.

MySQL First Generation instances

If your project has MySQL First Generation instances, you need to migrate them to MySQL Second Generation instances that use a public IP address. You must migrate all First Generation instances before enforcing the `sql.restrictPublicIp` constraint on the project.

Known Issues

Restrict Authorized Networks constraint

For Cloud SQL instances that have a pre-existing Authorized Networks entry, additional Authorized Networks entries are allowed, even when using the Restrict Authorized Networks (**sql.restrictAuthorizedNetworks**) constraint. This also affects instances that have enabled readonly or failover replicas, because they have an Authorized Networks entry for the replica that is not visible to the user.

This known issue will be removed when the constraint only allows the removal, not the addition, of Authorized Networks entries.

What's next

- Configuring organization policies (https://cloud.google.com/sql/docs/mysql/configure-org-policy).
- Learn about how private IP (https://cloud.google.com/sql/docs/mysql/private-ip) works with Cloud SQL.
- Learn how to configure private IP (https://cloud.google.com/sql/docs/mysql/configure-private-ip) for Cloud SQL.
- Learn about the organization policy service (https://cloud.google.com/resource-manager/docs/organization-policy/overview).
- Learn about organization policy constraints (https://cloud.google.com/resource-manager/docs/organization-policy/understanding-constraints).

Last updated December 13, 2019.