



# HYCU for Google Cloud SQL

---

**R-Cloud Module Guide**

## Table of Contents

About the module.....	3
Prerequisites.....	3
Instance service account permissions.....	3
Target cloud service account permissions .....	4
Google Cloud Access Token service account permissions .....	4
Limitations .....	5
Consideration .....	6
Protecting data.....	6
Backing up data .....	6
Restoring data .....	7

# Copyright notice

© 2024 HYCU. All rights reserved.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, distributed, transmitted, stored in a retrieval system, modified or translated to another language in any form by any means, without the prior written consent of HYCU.

# About the module

The R-Cloud (formerly HYCU Protégé) module for Google Cloud SQL allows you to protect the data that is stored in your Google Cloud SQL databases.


The module currently supports the following instance types:

- PostgreSQL
- Microsoft SQL Server
- MySQL

## Prerequisites

To enable protection of your Google Cloud SQL instances with R-Cloud, the following service accounts are required:

- Instance service account. The service account that is associated with a Google Cloud SQL instance.
- Target cloud service account. The service account that manages access to the backup data storage for your instances.
- Google Cloud Access Token service account. The service account that enables all the required Google Cloud SQL operations.

 **Note** Instead of the target cloud service account and the Google Cloud Access Token service account, you can also use the HYCU-managed service account (HMSA). For details, see *HYCU R-Cloud Help*.

The sections below list the permissions that must be granted to the listed service accounts.

## Instance service account permissions

Make sure that your Google Cloud SQL instance service account is assigned the Storage Object Admin role in the project where your buckets are defined or on each of the buckets.

Alternatively, you can grant the following permissions to your custom role:

- storage.objects.create
- storage.objects.get

## Target cloud service account permissions

ⓘ **Important** The content of this section applies for the staging target. For details about staging targets, see *HYCU R-Cloud Help*.

Make sure that your target cloud account is assigned the Storage Admin role. This role grants sufficient control of the Google Cloud bucket and allows you to create and read the objects.

Alternatively, you can grant the following permissions to your custom role:

- storage.buckets.get
- storage.objects.create
- storage.objects.get

## Google Cloud Access Token service account permissions

Make sure that your Google Cloud Access Token service account is assigned the Cloud SQL Admin role. This role grants full control over the data export and import within the projects containing the clusters or on locations where the new clusters will be created.

Alternatively, you can grant the following permissions to your custom role:

- resourcemanager.projects.list
- resourcemanager.projects.get
- cloudsql.instances.list
- cloudsql.instances.get
- cloudsql.instances.create
- cloudsql.instances.delete
- cloudsql.instances.export

- `cloudsql . instances . import`
- `cloudsql . databases . list`
- `cloudsql . databases . get`
- `cloudsql . databases . create`
- `cloudsql . databases . delete`

## Limitations

- The OVHcloud buckets cannot be used as a staging target.
- Backing up the users and roles that are defined on the Google Cloud SQL instances is not supported.
- The R-Cloud module for Google Cloud SQL allows you to back up and restore the MySQL instances. However, after a restore, your MySQL triggers and stored procedures will not be preserved. For details, see [Google Cloud documentation](#).
- The Google Cloud SQL backup or restore cannot be aborted.
- *For PostgreSQL:*
  - The maximum supported database size is 5 TB due to Cloud Storage limit of 5 TB per single-object size.
  - When performing a restore with the overwrite option enabled (in-place restore), the only allowed database connection is the one established by the module. If there is an additional connection established with your database, the restore will fail.
- *For Microsoft SQL Server:*
  - System databases (master, msdb, model, and tempdb) are excluded from the backup.
  - Compatibility Level is not checked during the restore operations.
  - Backups done while an instance is in a single-user or read-only mode may cause errors during the import of the exported data.
- *For MySQL:*
  - System databases (mysql, sys, information\_schema, performance\_schema) are excluded from the backup.
  - The triggers and the stored procedures are excluded from the backup.
  - Renaming the database when restoring is not supported.

## Consideration

If a Google Cloud SQL instance is protected in Google Cloud SQL, you cannot perform the in-place restore for either the main instance or for its replica.

To disable the instance deletion protection, update the Google Cloud SQL instance settings. For instructions, see [Google Cloud SQL documentation](#).

## Protecting data

R-Cloud starts protecting the data stored in your Google Cloud SQL database once you add the module as a source.

For details on how to add the module as a source, see [HYCU R-Cloud Help](#).

**Note** The R-Cloud module for Google Cloud SQL backs up data using a staging target. Select the preferred staging target when adding the module as a source in R-Cloud.

## Backing up data

R-Cloud allows you to define the protected Google Cloud SQL instances. For each protected instance, you can:

- Exclude specific databases.
- Specify the Offload configuration option. With the Offload option enabled, the module uses [serverless export](#).

**Note** Serverless export reduces the strain on your production instance but results in additional charges.

For details on how to configure backups for your Google Cloud SQL instances, see [HYCU R-Cloud Help](#).

## Setting up automatic policy assignment

To set up automatic policy assignment, add labels or the `hycu-policy` tag to your Google Cloud SQL instances in Google Compute Engine.

### Procedure

1. In the Google Cloud console, select the instance for which you want to set up automatic policy assignment.
2. In the Configuration section, click **Edit configuration**.
3. In the Labels section, click **Add a label**.
4. Enter the key and value, and then click **Done**.

For details about setting up automatic policy assignment, see *HYCU R-Cloud Help*. For more information about adding labels to Google Cloud SQL instances, see Google Cloud documentation.

## Restoring data

R-Cloud allows you to restore your protected Google Cloud SQL data at the following levels:

- Instance.
- **Note** The instance restore only restores an instance without its databases.
- Database

For details on how to configure the restore for your Google Cloud SQL instances, see *HYCU R-Cloud Help*.

## Instance restore

The following options are available when performing an instance restore:

- Restore the original instance. This overwrites the original instance (in-place restore).
- Restore the instance to a new instance with a different name.

**Important** When restoring an instance, the databases that were part of the original instance will not be restored. The new instances are created using a new service account that lacks the permission to read from the target bucket. To restore the databases, the service account of the new instance must be first assigned the Storage Object Admin IAM role as described above.

### In-place restore for the primary instance and its replicas

To successfully complete the in-place restore for the Google Cloud SQL primary instance and its replicas, perform the following steps:



1. In Google Cloud, manually delete all the Google Cloud SQL replicas of the primary instance.
2. In R-Cloud, restore the Google Cloud SQL primary instance.
3. In Google Cloud, manually re-create the replicas of the restored primary instance.

## Performing disaster recovery of the entire instance

To restore databases to a restored instance, additional permissions must be granted on the restored instance. To perform disaster recovery of the entire instance, complete the following steps:

1. Restore the instance.
2. Grant the service account of the new instance the permission to read from the staging bucket (see above).
3. Restore the databases into the new instance using the override database option.

**ⓘ Important** The module generates a root password when creating a new instance. Change the password after the restore is complete.

## Database restore

R-Cloud allows you to restore one or more databases to a selected Google Cloud SQL instance.

When selecting an instance to restore the databases, define the suffix to be appended to the original database name in R-Cloud.

### Example

```
<original_database_name>_<databaseNameSuffix>
```

If you select the override option, both the instance selector and the suffix field are hidden. The databases will be restored using the original name and override the existing database.

**ⓘ Important** To prevent an unwanted deletion, adding the suffix to the PostgreSQL system database name is mandatory.

The PostgreSQL system database is restored as a standard database with a different name. As a result, the restored PostgreSQL system database cannot be used for restoring the users and the roles on a Google Cloud SQL instance.

The users and the roles must be created manually by completing the following steps:

1. Restore the instance. For details, see [Instance restore](#).
2. In Google Cloud console, create the users and the roles on the restored instance.
3. Restore the databases into the restored instance.

# Provide feedback

For any suggestions and comments regarding this product or its documentation, send us an e-mail to:

[info@hycu.com](mailto:info@hycu.com)

We will be glad to hear from you!

