



HYCU for Google Cloud Run

R-Cloud Module Guide

Table of Contents

About the module.....	3
Prerequisites.....	3
Authentication service account permissions.....	3
Required APIs.....	4
Limitations	4
Protecting data.....	5
Backup.....	5
Restore	5

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

With the R-Cloud (formerly HYCU Protégé) module for Google Cloud Run, you can back up your resources securely and efficiently.

Prerequisites

Before you add the module to R-Cloud as a source, the prerequisites described in this section must be fulfilled.

Authentication service account permissions

The authentication service account that you set while adding the SaaS module as a source in R-Cloud must be granted the minimum permissions set within the Google Cloud projects that contain the services or jobs that you plan to protect, or on the locations where the new services or jobs are going to be created.


The following permissions must be included:

- `compute.regions.list`
- `iam.serviceAccounts.actAs`
- `iam.serviceAccounts.get`
- `resourceManager.projects.list`
- `run.jobs.create`
- `run.jobs.delete`
- `run.jobs.get`
- `run.jobs.list`
- `run.operations.get`
- `run.services.create`
- `run.services.delete`
- `run.services.get`
- `run.services.list`

- `vpcaccess.connectors.get`

Instead of granting the individual permissions, you can also assign the following roles to the authentication service account:

- Cloud Run Admin
- Compute Viewer
- Serverless VPC Access Viewer
- Service Account User

 **Note** Assigning roles might grant permissions that exceed the required minimum permissions for the service accounts.

Required APIs

For each Google Cloud project that contains the services and jobs that you plan to protect, the following APIs must be enabled:

- Compute API
- Cloud Run API
- Google Storage API
- IAM API
- Serverless VPC Access API

Limitations

When adding the module to R-Cloud and while protecting the related SaaS application, the following limitations apply:

- The backup and restore job triggers are not backed up because they are a part of Google Cloud Scheduler which is not included in the backup configuration.
- The customer-managed encryption key (CMEK) is not supported.
- You cannot assign a policy that has Snapshot specified as the backup target type to this type of SaaS application.
- When creating a new Cloud Function, Google Cloud automatically creates a supporting Cloud Run service. These automatically created Cloud Run services are not protected in R-Cloud.

Protecting data

R-Cloud starts protecting the configurations of your Google Cloud Run resources after you add the module as a source to R-Cloud and assign a policy to the related project that hosts the services and jobs.

For details on how to add the module as a source, see *HYCU R-Cloud Help*.

Backup

R-Cloud allows you to back up the protected Google Cloud Run configurations at the following levels:

- Service
- Job

For details on how to configure the backup for Google Cloud Run, see *HYCU R-Cloud Help*.

Restore

R-Cloud supports the following restore options:

- In-place restore: If a resource with the same name already exists on the target, it will be removed and replaced by the restored resource.
- The following options are available if the In-place restore option is disabled:
 - Project: The list of active projects.
 - Region: The name of the region to which the instance will be restored.
 - Suffix: The suffix that will be appended to the resource name. The following formatting rules apply:
 - The maximum length is 20 characters.
 - The suffix must only contain lowercase letters, numbers, and hyphens.
 - The suffix must not end with a hyphen.
 - Override existing: If a service or a job with the same name already exists on the target, it will be removed and replaced by the restored service or job.

ⓘ Important When restoring your services or jobs to a different Google Cloud project, you must grant your destination Google Cloud Run Service Agent an

additional role for the project that hosts your resource images. Depending on your Google Cloud registry type, grant one of the following roles:

- For the Artifact Registry: `artifactregistry.reader`
- For the Container Registry: `storage.objectViewer`

For details on how to create and grant roles to the service agents, see Google Cloud documentation.

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

Provide feedback

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

info@hycu.com

We will be glad to hear from you!

