HYCU

HYCU for Google Cloud Bigtable

R-Cloud Module Guide

Table of Contents

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 Bigtable, you can back up your SaaS application data securely and efficiently.

Prerequisites

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

Access token

The module uses access tokens to be permitted to use the Google Services. The access token must be provided by the client in each request. Otherwise, the request fails with the error `HTTP error 400 - Bad Request`.

Authentication service account permissions

The authentication service account must be granted the following permissions within the projects that contain the instances or in the locations where the new instances will be created:

- `bigtable.appProfiles.create`
- `bigtable.appProfiles.delete`
- `bigtable.appProfiles.get`
- `bigtable.appProfiles.list`
- `bigtable.appProfiles.update`
- `bigtable.backups.create`
- `bigtable.backups.delete`
- `bigtable.backups.get`
- `bigtable.backups.getIamPolicy`
- `bigtable.backups.list`

- bigtable.backups.read
- bigtable.backups.restore
- bigtable.backups.setIamPolicy
- bigtable.backups.update
- bigtable.clusters.create
- bigtable.clusters.delete
- bigtable.clusters.get
- bigtable.clusters.list
- bigtable.clusters.update
- bigtable.hotTablets.list
- bigtable.instances.create
- bigtable.instances.createTagBinding
- bigtable.instances.delete
- bigtable.instances.deleteTagBinding
- bigtable.instances.get
- bigtable.instances.getIamPolicy
- bigtable.instances.list
- bigtable.instances.listEffectiveTags
- bigtable.instances.listTagBindings
- bigtable.instances.ping
- bigtable.instances.setIamPolicy
- bigtable.instances.update
- bigtable.keyvisualizer.get
- bigtable.keyvisualizer.list
- bigtable.locations.list
- bigtable.tables.checkConsistency
- bigtable.tables.create
- bigtable.tables.delete
- bigtable.tables.generateConsistencyToken

- `bigtable.tables.get`
- `bigtable.tables.getIamPolicy`
- `bigtable.tables.list`
- `bigtable.tables.mutateRows`
- `bigtable.tables.readRows`
- `bigtable.tables.sampleRowKeys`
- `bigtable.tables.setIamPolicy`
- `bigtable.tables.undelete`
- `bigtable.tables.update`
- `dataflow.jobs.create`
- `dataflow.jobs.get`
- `iam.serviceAccounts.actAs`
- `iam.serviceAccounts.list`
- `logging.logEntries.list`
- `monitoring.timeSeries.list`
- `resourcemanager.projects.get`
- `resourcemanager.projects.list`
- `storage.buckets.create`
- `storage.buckets.delete`
- `storage.buckets.get`
- `storage.objects.create`
- `storage.objects.delete`
- `storage.objects.get`

Note The permission `resourcemanager.projects.list` cannot be added to the custom Google Cloud permissions. The permission `iam.serviceAccounts.list` is not mandatory. However, enabling this permission will enhance the user experience by allowing the users to select the appropriate job service account.

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

- Bigtable Administrator
- Dataflow Developer
- Service Account User
- Logs Viewer
- Storage Admin

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

Target service account permissions

The target service account must be granted the following permissions in the staging target bucket or in the project where the bucket used as the staging target is defined:

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

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

- Storage Admin

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

Job service account permissions

The job service account must be created in the project where the Bigtable instance is going to be backed up or restored. If the job service account is not selected, the default service account of the project will be used for the backup and restore jobs.

The job service account can be selected in the R-Cloud SaaS configuration options for backup or restore.

The job service account must be granted the following permissions in the projects containing the instances or in the locations where the new instances will be created:

- autoscaling.sites.readRecommendations
- autoscaling.sites.writeMetrics
- autoscaling.sites.writeState
- bigtable.tables.mutateRows
- bigtable.tables.readRows
- bigtable.tables.sampleRowKeys
- cloudbuild.builds.create
- cloudbuild.builds.get
- cloudbuild.builds.list
- cloudbuild.builds.update
- cloudbuild.operations.get
- cloudbuild.operations.list
- compute.instanceGroupManagers.update
- compute.instances.delete
- compute.instances.setDiskAutoDelete
- compute.machineTypes.get
- compute.projects.get
- compute.regions.list
- compute.zones.list
- dataflow.jobs.cancel
- dataflow.jobs.create
- dataflow.jobs.get
- dataflow.jobs.list
- dataflow.jobs.snapshot
- dataflow.jobs.updateContents
- dataflow.messages.list
- dataflow.metrics.get
- dataflow.shuffle.read
- dataflow.shuffle.write

- `dataflow.snapshots.delete`
- `dataflow.snapshots.get`
- `dataflow.snapshots.list`
- `dataflow.streamingWorkItems.ImportState`
- `dataflow.streamingWorkItems.commitWork`
- `dataflow.streamingWorkItems.getData`
- `dataflow.streamingWorkItems.getWork`
- `dataflow.streamingWorkItems.getWorkerMetadata`
- `dataflow.workItems.lease`
- `dataflow.workItems.sendMessage`
- `dataflow.workItems.update`
- `logging.logEntries.create`
- `logging.logEntries.route`
- `monitoring.timeSeries.create`
- `recommender.dataflowDiagnosticsInsights.get`
- `recommender.dataflowDiagnosticsInsights.list`
- `recommender.dataflowDiagnosticsInsights.update`
- `remotebuildexecution.blobs.get`
- `resourcemanager.projects.get`
- `resourcemanager.projects.list`
- `storage.buckets.get`
- `storage.objects.create`
- `storage.objects.delete`
- `storage.objects.get`
- `storage.objects.list`
- `storage.objects.update`

The job service account must be granted the following permissions in the bucket used as a staging target or in the project where the bucket used as a staging target is defined:

- `storage.objects.create`

- `storage.objects.get`
- `storage.objects.delete`
- `storage.objects.list`

> **Note** The permission `resourcemanager.projects.list` cannot be added to the custom Google Cloud permissions.

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

- At the project location:
  - Bigtable User
  - Storage Object Admin
  - Dataflow Admin and Dataflow Worker
- In the staging target bucket permission section or in the staging target bucket project: Storage Object Admin

Required APIs

The following APIs must be enabled on the Google Cloud Platform:

- Bigtable Admin API
- Dataflow API
- Logging API
- Monitoring API
- IAM API
- Cloud Resource Manager API

Limitations

When adding the module and while protecting the related SaaS application, the following limitations apply:

- The OVHcloud buckets cannot be used as a staging target.
- Using the customer-managed encryption key (CMEK) with the instance encryption option is not supported.

Protecting data

R-Cloud starts protecting the data stored in your SaaS module after you add the module as a source to R-Cloud and assign a policy to the related SaaS application.

For details on assigning policies to SaaS applications, see *HYCU R-Cloud Help*.

> **Note** The R-Cloud module for Google Cloud Bigtable 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 back up the following Bigtable resource types:

- Instances
- Tables

For details on how to configure the backup for the SaaS application data, see *HYCU R-Cloud Help*.

Setting up automatic policy assignment

To set up automatic policy assignment, add the `hycu-policy` label to your Bigtable instances in the Google Cloud console.

Procedure

1. In the Google Cloud console, select the Bigtable instance for which you want to set up automatic policy assignment.
2. In the info panel, click **Labels**, and then click **Add label**.

3. Enter the key and the value, and then click **Save**.

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

Restoring data

R-Cloud supports the following restore scenarios:

- Restoring an instance: This option restores an instance by overwriting the existing Bigtable instance or performs a restore to a newly created instance. This scenario will only restore an instance without restoring its tables. When restoring an instance, the following options are available:
  - Override instance: This option recovers the instance with all its original properties. If an instance with the same name already exists, the instance will be removed and replaced by the restored instance. If this option is enabled, the following options will be disabled:
  - Instance ID – the instance identifier
  - Project – the list of active projects.
- Restoring a table: This option restores one or more Bigtable tables to a selected Bigtable instance. When restoring a table, the following options are available:
  - Override Table: If a table already exists, the table will be deleted and replaced by the restored table.
  - Project: The list of active projects with their Bigtable instances.
  - Instance: The list of Bigtable instances.
  - Service account email.
  - The list of service accounts created in the selected project that could potentially be used for the import job operations. The list is available if the `iam.serviceAccounts.list` permission is added to the Authentication Service Account.
  - The input text field in which the user enters the email of their service account to be used for the import job operations. The text field will be active if the `iam.serviceAccounts.list` permission is not added to the Authentication Service Account.

For details on how to restore the SaaS application data, 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!

www.hycu.com

HYCU®