USER GUIDE

HYCU Backup and Recovery as a Service for GCP

Service update date: July 22, 2019

Document edition: First

Legal notices

Copyright notice

Trademarks

HYCU logos, names, trademarks and/or service marks and combinations thereof are the property of HYCU or its affiliates. Other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

GCP™, Google Cloud Platform™, Google Cloud Storage™, and Google Compute Engine™ are trademarks of Google LLC.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Disclaimer

The details and descriptions contained in this document are believed to have been accurate and up to date at the time the document was written. The information contained in this document is subject to change without notice.

HYCU provides this material "as is" and makes no warranty of any kind, expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. HYCU shall not be liable for errors and omissions contained herein. In no event shall HYCU be liable for any direct, indirect, consequential, punitive, special or incidental damages, including, without limitation, damages for loss and profits, loss of anticipated savings, business interruption, or loss of information arising out of the use or inability to use this document, or any action taken based on the information contained herein, even if it has been advised of the possibility of such damages, whether based on warranty, contract, or any other legal theory.

The only warranties for HYCU products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty.

Notice

This document is provided in connection with HYCU products. HYCU may have copyright, patents, patent applications, trademark, or other intellectual property rights covering the subject matter of this document.

Except as expressly provided in any written license agreement from HYCU, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property on HYCU products. Use of underlying HYCU product(s) is governed by their respective Software License and Support Terms.

Important: Please read Software License and Support Terms before using the accompanying software product(s).

HYCU
www.hycu.com

Contents

Chapter 1

About HYCU for GCP

HYCU Backup and Recovery as a Service for GCP (HYCU for GCP) is the first purpose-built backup and recovery solution for the Google Cloud Platform service suite. It is delivered in the form of software-as-a-service (SaaS)—a managed service implemented on the basis of the Google Cloud Storage and Google Compute Engine services. HYCU for GCP is agentless, simple to use, and cost-effective. You can subscribe to HYCU for GCP from the Google Cloud Platform Marketplace.

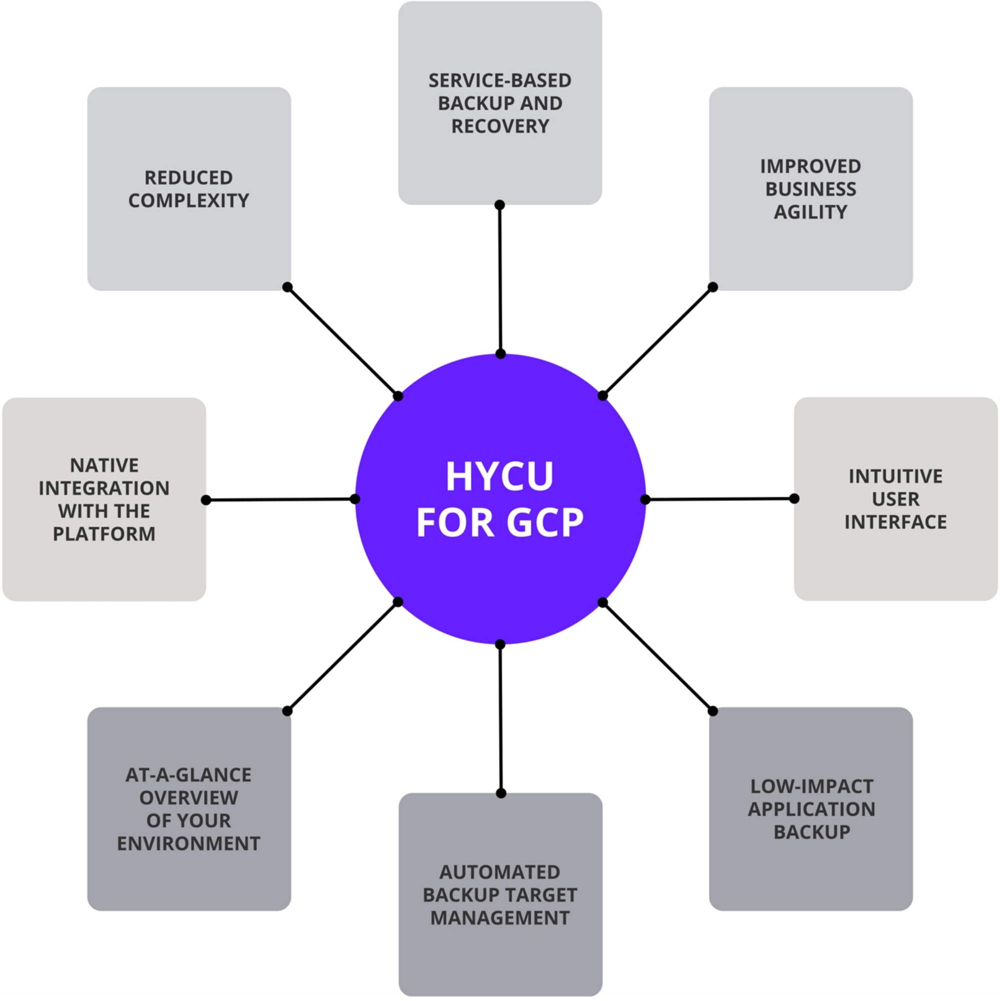

SERVICE-BASED BACKUP AND RECOVERY
REDUCED COMPLEXITY
IMPROVED BUSINESS AGILITY
NATIVE INTEGRATION WITH THE PLATFORM
HYCU FOR GCP
INTUITIVE USER INTERFACE
AT-A-GLANCE OVERVIEW OF YOUR ENVIRONMENT
LOW-IMPACT APPLICATION BACKUP
AUTOMATED BACKUP TARGET MANAGEMENT

Figure 1–1: Solution overview

Key features and benefits

The following features make HYCU for GCP a solution that can transform your business by achieving complete compliance and data protection:

- **Protection against data loss**

  Delivers native data protection for instances (virtual machines) in your projects in the Google Cloud Platform service suite, and ensures easy recoverability.

- **Express setup**

  You can enable data protection for your instances in a few minutes after the service is provisioned for you; no prior actions for solution deployment are required.

- **Predefined and custom policies**

  Simplifies implementation of data protection by providing predefined backup policies, and includes options for policy customization that can address your special data protection needs.

- **Scheduled backups**

  Automatic backup scheduling provides data protection based on your recovery point objectives (RPOs).

- **Choice of sources and targets**

  Selection of backup sources and backup targets is the administrator's choice.

- **Optimization and leveraging of the platform value**

  Native Google Compute Engine snapshots can be used for both backup and recovery. Google Cloud Storage buckets are created and reused automatically, thus avoiding data protection management overhead.

- **Low impact on applications, backup windows**

  Agentless architecture heavily reduces backup load on production instances. In addition, through proper definition of backup windows, you can completely avoid the impact of backup activity on your production environment during peak hours.

- **Application-consistent backup data**

  Support for pre-snapshot commands facilitates application data consistency of your backup images.

- **At-a-glance overview of the data protection status**

  A dashboard in the web user interface helps you identify potential problems and bottlenecks to improve the performance of your data protection environment.

- **Restore of individual files and folders**

  Disk catalogs allow you to narrow the restore scope beyond the level of individual disks.

- **Use of backup images for cloning**

  You are given the possibility of using backup images to clone your instances. Clones can be created in the user-selected project and zone, and can have different network settings.

- **Archives of backup data**

  Data archives, isolated from other backup images, can retain your backup data for a longer time period for future reference. Multiple retention tiers can be used.

- **Integration with Google's billing system, progressive discount**

  Cost of data protection is safely billed by Google through existing billing accounts, without requiring you to enter additional billing information. You get a discount depending on the amount of protected data.

Backup environment overview

The backup environment of HYCU for GCP is built on two groups of components:

- Google Cloud Platform service suite components. These are native parts of the Google Cloud Platform services.
- Components provided by HYCU for GCP itself. They implement data discovery, protection, and analysis.

The following table explains terms that are used in the HYCU for GCP documentation and refer to components of both groups.

Table 1–1: Glossary of terms

Term	Description
HYCU for GCP	A backup and recovery service that is built on top of the Google Cloud Platform service suite and that you can subscribe to.
Web user interface (WUI)	A web-based graphical console that provides access to HYCU for GCP. You can use it to: – Configure and maintain your backup environment. – Schedule or invoke data protection activities and monitor their progress. – Browse log of events.
User account	A Google Account that is used to sign in to the web user interface of HYCU for GCP.
Billing account	An entity in the Google Cloud Platform service suite that defines who pays for a given set of resources. A billing account defines the set of Google Cloud Platform projects that may be visible to a Google Account within

	HYCU for GCP. For more information, see "Extent of data protection" on page 13.
Project	An entity in the Google Cloud Platform resource hierarchy for which data protection can be independently configured and carried out by HYCU for GCP. For information on the resource hierarchy, see the Overview | Cloud Identity and Access Management Documentation | Google Cloud webpage, section *Policy hierarchy*.
Organization account	A Google Account that HYCU for GCP uses for retrieving project information. Initially, the user account that subscribed to the service is used as the organization account, but this can be changed later. For instructions, see "Changing the organization account" on page 66.
VM Instance, instance	A virtual machine (VM) that is hosted in the Google Compute Engine service and for which HYCU for GCP provides data protection. Also referred to as *backup source*.
Backup policy, policy	A set of rules that basically define backup frequency and retention periods for the backup images and copies of backup images. It may also include a rule for archiving backup data.
Instance compliancy	An indicator showing whether the instance is backed up so that the recovery point objective (RPO) in the assigned policy is met.
Instance protection	An indicator showing whether at least one backup image of the instance exists and the instance has a policy assigned.
Policy compliancy	An indicator of joint compliancy of all instances the policy is assigned to.
Backup image	Primary backup data of an instance that can be used to restore the instance. It can be kept in one of the following forms: – Snapshot – Backup data in a bucket
Bucket	A storage container in the Google Cloud Storage service that stores backup data, copies of backup images, or data archives created by HYCU for GCP.
Automatic bucket	A bucket that is created by HYCU for GCP rather than a

	Google Cloud Platform user.
Disk	A persistent disk in the Google Compute Engine service that belongs to some instance. HYCU for GCP is able to restore it separately from other backed up persistent disks.
Disk catalog	A record of an instance disk's inventory that enables restore of individual files or folders. It is a part of the restore point. Creation of disk catalogs is disabled by default. For instructions on how to enable it, see "Configuring instance backup options" on page 39.
Restore point	A state of the backed up data at the time its snapshot was taken. The state can be recreated from a corresponding backup image, copy of backup image, or data archive. If disk cataloging is enabled, each restore point also includes the disk catalog.
Recovery point objective (RPO)	A policy rule that defines the maximum period between the times when two consecutive snapshots of the same instance are taken. Also referred to as *backup frequency*.
Backup window	A user-defined time frame during which new backup tasks are allowed to start.
Backup window specification	A named set of backup windows that can be used in a backup policy.
Default backup policy	A backup policy that you chose to be automatically assigned to subsequently detected instances in the same Google Cloud Platform project.
Project service account	A Google Cloud Platform service account that is chosen within a Google Cloud Platform project to be used for identification of automated requests to HYCU for GCP. Such requests are authenticated similarly to those invoked interactively through the web user interface. Project service account enables specific features of HYCU for GCP. For more information, see "Configuring project service accounts" on page 67
Copy of backup image	A copy of backup image that is stored in a separate bucket and can use different retention setting from the original backup image.
Data archive	A daily, weekly, monthly, or yearly copy of backup image that is retained in a separate bucket for future reference, usually

	for a longer period of time.

Data protection concept

By using HYCU for GCP as your backup and recovery solution, you can be confident that your business data is backed up in a consistent state, reliably stored, and can be restored and accessed in an uncorrupted state.

After you subscribe to the service through the Google Cloud Platform Marketplace, you can enable data protection for a Google Cloud Platform project in four simple steps:

1. Select a Google Cloud Platform project.
2. Select instances.
3. Choose appropriate backup policies or create your own.
4. Assign the backup policies to the instances.

The service then automatically creates appropriate buckets in your Google Cloud Platform project to store backup images into. When you complete the first backup, you can restore the data from the backup image if the data becomes damaged or corrupted.

Extent of data protection

One of the requirements for the service subscription is selection of a billing account. The billing account defines scope of data protection—the set of Google Cloud Platform projects that are visible to HYCU for GCP (referred to as *scoped projects*). The set of scoped projects is the same regardless of who uses the solution through the same subscription. Each project linked to the selected billing account is automatically granted capability of being protected with HYCU for GCP. Due to this special significance, the billing account must be chosen thoughtfully.

> Note You cannot reconfigure HYCU for GCP to use a different billing account as the basis for defining the data protection scope. In the event that you need to change the billing account, contact HYCU Customer Support.

The figure that follows depicts an example set-up where your Google Account has access to five projects in the Google Cloud Platform service suite. By using HYCU for GCP, you are able to protect only two of them (projects D and E). This is because only the two projects are linked to the selected billing account.

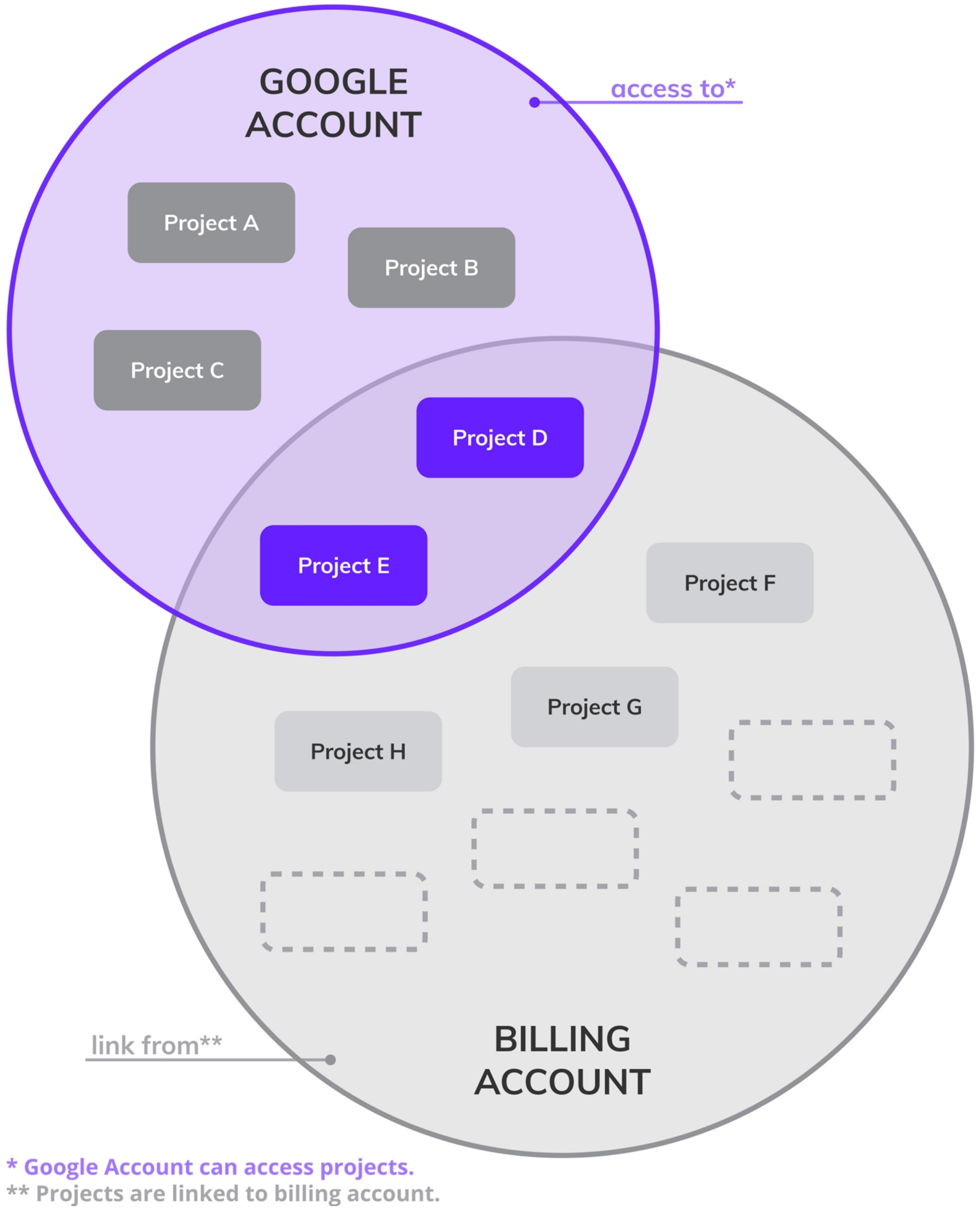


Figure 1–2: Billing account limiting the data protection extent

To expand the set of Google Cloud Platform projects that you can protect, do one of the following:

- In the Google Cloud Platform service suite, link more projects to the selected billing account.
- Subscribe to HYCU for GCP with a different billing account while keeping your existing subscription intact.

Chapter 2

Service pricing

HYCU for GCP is built on top of Google Cloud Platform service suite; it utilizes Google Cloud Platform resources for its service needs. When you enable data protection for a Google Cloud Platform project, HYCU for GCP allocates those resources within the same project. Thus, while using HYCU for GCP, you are charged for both the backup and recovery service and the allocated resources it requires.

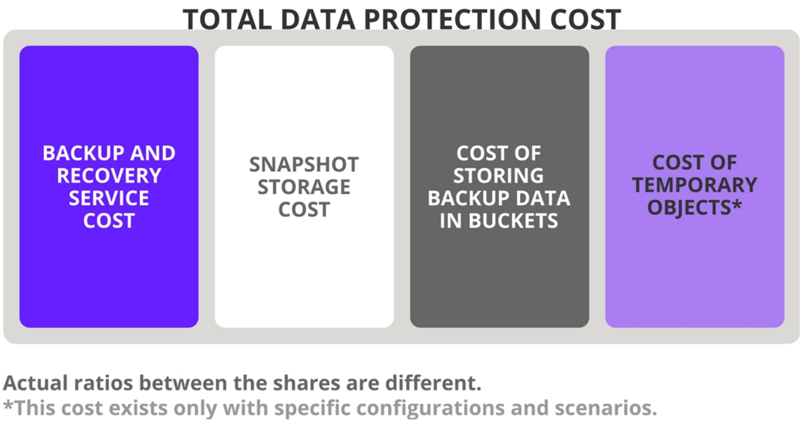

TOTAL DATA PROTECTION COST
BACKUP AND RECOVERY SERVICE COST
SNAPSHOT STORAGE COST
COST OF STORING BACKUP DATA IN BUCKETS
COST OF TEMPORARY OBJECTS*
Actual ratios between the shares are different.
*This cost exists only with specific configurations and scenarios.

Figure 2–1: Shares of total data protection cost

Total cost for protecting your data in Google Cloud Platform service suite consists of the following shares:

- Backup and recovery service cost

  This is a net cost generated by using HYCU for GCP to protect your data. It is the only share of total cost that is charged by HYCU (through Google).

  > Note Backup and recovery service cost is billed by Google in scope of your Google Account.

  This cost depends on frequency of backups, amount of protected data, and time period for which the data is protected. For more information, see "Service pricing" above.

  Each new HYCU for GCP subscription enters a two-week (14-day) trial period during which you are not charged for the backup and recovery service cost.

- Snapshot storage cost

This cost is generated by persistent disk snapshots that occupy storage space in the Google Compute Engine resources. It is charged by Google according to their Google Compute Engine pricing policy. For details, see the Google Compute Engine Pricing webpage.

Factors within HYCU for GCP[1] that influence this cost are:

– The chosen backup target type
– Frequency of backups
– Snapshot sizes
– Backup retention period

If backup images are kept as data in buckets rather than snapshots, this cost is negligible.

- Cost of storing backup images in buckets

  This cost is generated by backup images (including their disk catalogs) that occupy storage space in the Google Cloud Storage buckets. It is charged by Google according to their Google Cloud Storage pricing policy. For details, see the Cloud Storage Pricing webpage.

  Factors within HYCU for GCP[1] that influence this cost are:

  – The chosen backup target type
  – Use of backup data copies
  – Sizes of stored backup images (including their disk catalogs)
  – Backup retention periods
  – Use of data archives and their retention periods

  To minimize this cost, HYCU for GCP compresses backup data before storing them into buckets. If backup images are kept as snapshots and you do not use copies of backup images or data archives, no cost associated with bucket storage is generated.

- Cost of temporary objects used internally by HYCU for GCP

  This cost is generated by temporary objects that are created in your Google Cloud Platform project for the duration of the following processes and tasks:

Process or task	Temporary objects
Instance rediscovery after assigning access credentials	Instance with one disk
Instance rediscovery after enabling disk catalog for backup	Instance with one disk
Backup that includes creation of a disk catalog	Instance with multiple disks
Restore of instances or entire instance disks	Instance with one disk
Restore of individual files or folders	Instance with one disk, additional disks in your target instance

[1] The cost also depends on outside factors.

Backup and recovery pricing

HYCU's pricing principles for HYCU for GCP are similar to those of Google for their Google Cloud Platform service suite. This section explains basic concepts related to the HYCU for GCP pricing, and it also includes a few examples of how the price is calculated.

Pricing unit and billing model

The pricing unit as defined in the HYCU for GCP pricing policy is as follows:

Pricing unit
Gibibyte-month (GiB-M)

> ⚠ Important In the pricing unit definition, data quantity component measures the capacity of protected persistent disks in the protected instances, not the amount of data that is actually backed up.

Based on the pricing unit definition, the price of protecting an instance for a particular time period basically depends on the following factors:

- Number of pricing units that the instance and its protection period comprise

  This factor measures the following product of storage capacity and time period:

  (joint capacity of persistent disks that belong to the instance and are included in backup)
  ×
  (the period during which the instance is being protected)

- Price of one pricing unit

  This factor depends on the pricing tier that the instance is classified into. For details, see "Pricing tiers" on the next page.

The following table lists HYCU for GCP billing model.

Table 2–1: Billing model of HYCU for GCP

Measurement	Minimum	Increment	Notes
Data quantity	10 GiB	1 GiB	Imposed by instance disk size limitations in the Google Compute Engine service.
Time	1 hour	1 hour	Defined by the HYCU for GCP pricing policy.

Pricing tiers

HYCU for GCP pricing policy defines four pricing tiers, depending on how frequently your data is backed up. Each tier defines the amount that you are charged per pricing unit for a particular instance.

In the following table, RPO is the value of the recovery point objective setting (the `Backup every` option) in the effective backup policy.

Table 2–2: HYCU for GCP pricing tiers

Pricing tier	Criterion	Price per unit
platinum	1 hour <= RPO < 4 hours	$0.451
gold	4 hours <= RPO < 12 hours	$0.386
silver	12 hours <= RPO < 24 hours	$0.257
bronze	24 hours <= RPO	$0.128

Discount

If you use HYCU for GCP to protect a significant amount of data, you automatically qualify for a volume use discount. When you use the solution to protect more than 10 TiB of data, HYCU gives you a discount for the entire amount of protected data. The discount increases with quantity and you can get up to a 30% net discount.

In the following table, PDA means amount of protected data (data that belongs to instances that have their protection status set to `Protected`).

Table 2–3: HYCU for GCP price discounts

Discount level	Criterion	Discount rate
Low	10,000 GiB (9,77 TiB) < PDA <= 100,000 GiB	20%
High	100,000 GiB (97,66 TiB) < PDA	30%

Price calculation examples

The following examples illustrate how data protection price is calculated for various use cases with different instance disk sizes, different recovery point objectives (RPOs), and different time periods for the duration of which you require your data to be protected.

> ⚠ Important Google Cloud Platform Console uses incorrect measurement unit for reporting instance disk sizes. For example, a disk whose size is reported as 5 GB (5 gigabytes) has an actual size of 5 GiB (5 gibibytes).

Example

First example.

Suppose you have the following data protection requirement in your Google Cloud Platform project:

Instance count	1
Persistent disk capacity	100 GiB
RPO setting in the effective backup policy	2 hours (= "platinum" tier)
Time period for instance protection	2 months

For this requirement, the data protection price calculation is as follows:

```
100 GiB × $0.451/GiB-M × 2 M = $90
```

Example

Second example.

Suppose you have the following data protection requirement in your Google Cloud Platform project:

Instance count	10
Persistent disk capacity per instance	2 TiB (= 2,048 GiB)
RPO setting in the effective backup policy	4 hours (= "gold" tier)
Time period for instance protection	6 months

For this requirement, the discounted data protection price calculation is as follows:

```
10 × 2,048 GiB = 20,480 GiB
```

```
20,480 GiB × $0.386/GiB-M × 6 M × (1 - 20/100) = $37,945
```

Example

Third example.

Suppose you have the following data protection requirement in your Google Cloud Platform project:

Instance count	24
Persistent disk capacity per instance	5 TiB (= 5,120 GiB)
RPO setting in the effective backup policy	48 hours (= "bronze" tier)
Time period for instance protection	2 weeks (= 14/31 month)

For this requirement, the discounted data protection price calculation is as follows:

```
24 × 5,120 GiB = 122,880 GiB
```

```
122,880 GiB × $0.128/GiB-M × 14/31 M × (1 - 30/100) = $4,972
```

Predefined backup policies and tiers

HYCU for GCP comes with five predefined backup policies, four of which—when assigned—actually protect your data. They classify the instances they are assigned to into pricing tiers. The "exclude" backup policy does not protect data, therefore it does not match any pricing tier.

Table 2–4: Predefined backup policies and their default pricing tiers

Backup policy name	Default pricing tier
platinum	platinum
gold	gold
silver	silver
bronze	bronze
exclude	n/a (not charged)

> ⚠ Important Adjusting the recovery point objective setting (the `Backup every` option) in a backup policy may change pricing tier for the protected instances.

Chapter 3

Establishing a backup environment

The first step for establishing a backup environment is selection of the Google Cloud Platform billing account; this action is already part of the procedure for subscribing to HYCU for GCP. For information how it affects your data protection capabilities, see section "Extent of data protection" on page 13.

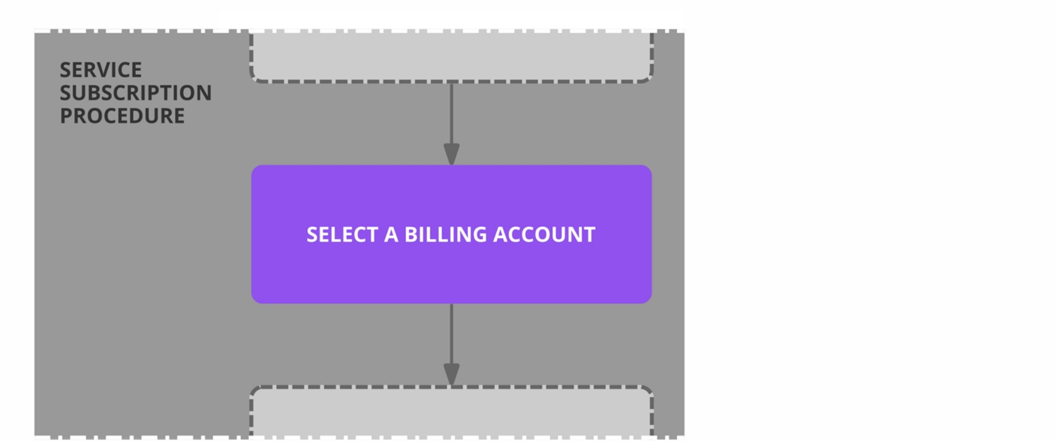


Figure 3–1: Flowchart – preliminary part of establishing a backup environment

After HYCU for GCP is provisioned for you, you must sign in to its web user interface and complete establishing the backup environment in which your data will be effectively protected.

The sequence of actions is as follows:

1. Select the Google Cloud Platform project.
2. *Only if you prefer not to use automatic buckets.* Set up your own buckets.
3. Choose appropriate predefined backup policies or create custom backup policies (if your data protection plan requires them).
4. *Only if you want to exclude individual disks from backup.* Configure instance backup options ("Disks").
5. *Only to enable restore of individual files or folders.* Configure instance backup options ("Create Disk Catalogs").

6. *Optional, applicable only to instances running Microsoft Windows for which restore of individual files or folders is enabled.* Manually assign access credentials to the instances[1].
7. *Only if you plan to use pre-snapshot or post-snapshot commands.* Configure instance backup options ("Pre-Snapshot Command", "Post-Snapshot Command").
8. Assign the policies to instances.

[1] HYCU for GCP automatically creates and assigns credentials to instances running Microsoft Windows. However, if needs of you environment require tight control over user names and passwords and you want to configure credential groups by yourself, you can manually assign the credentials.

The figure that follows depicts the task flow up to the point when backup policies can be assigned.

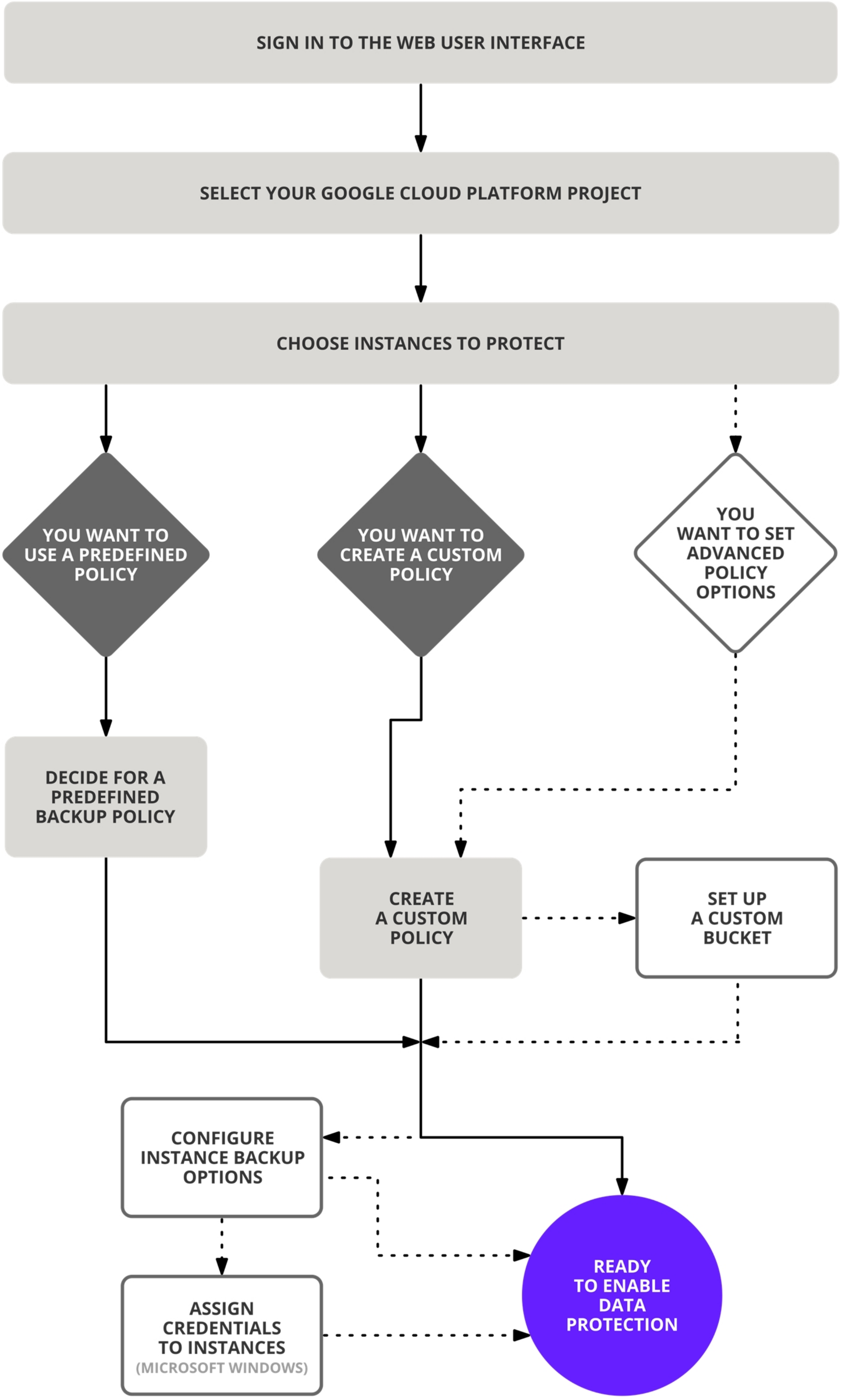

SIGN IN TO THE WEB USER INTERFACE
SELECT YOUR GOOGLE CLOUD PLATFORM PROJECT
CHOOSE INSTANCES TO PROTECT
YOU WANT TO USE A PREDEFINED POLICY
YOU WANT TO CREATE A CUSTOM POLICY
YOU WANT TO SET ADVANCED POLICY OPTIONS
DECIDE FOR A PREDEFINED BACKUP POLICY
CREATE A CUSTOM POLICY
SET UP A CUSTOM BUCKET
CONFIGURE INSTANCE BACKUP OPTIONS
ASSIGN CREDENTIALS TO INSTANCES (MICROSOFT WINDOWS)
READY TO ENABLE DATA PROTECTION

Figure 3–2: Flowchart – main part of establishing a backup environment

See the following sections for the corresponding instructions:

- "Signing in" below
- "Selecting Google Cloud Platform projects" on the next page
- "Defining your backup policy strategy" on the next page
- "Setting up buckets" on page 36
- "Configuring instance backup options" on page 39
- "Enabling access to instances" on page 37

After the backup environment is established, data protection can be accomplished in several ways to fulfill your particular business needs. For instructions, see section "Backing up instances" on page 41.

Signing in

You can access the web user interface of HYCU for GCP by using a supported web browser.

> ⚠ Important Before signing in, ensure that the usage requirements are met. For details, see the *HYCU Backup and Recovery as a Service for GCP Release Notes*, section *Service requirements*.

To sign in to the web user interface, follow these steps:

1. Open a web browser and go to the HYCU Backup and Recovery as a Service for GCP webpage.
2. *Only when using Microsoft Edge or Internet Explorer.* Enable pop-ups for the `endpoints.hycu.com` website.
3. On the sign-in webpage, click **Sign in with Google**.
4. Specify or select the email address of your Google Account. If you are not signed in with that account yet, enter the corresponding password, and click **Next**.

   After a successful sign-in, the Dashboard panel of the web user interface appears with a Google Cloud Platform project already selected.
5. If you have signed in for the first time or you did not disabled it before, a startup tutorial offers to assist you in getting familiar with basic data protection configuration. To accept tutoring, in the startup tutorial window, click **Begin**. Else, select the **Don't show this tutorial anymore** option or click **Close** as appropriate.

   > Note You can manually launch the tutorial any time. To do so, in the web user interface, click **?** , and then select **Startup Tutorial**.

You are now ready to establish your backup environment and enable data protection.

> ⚠ Important Your web user interface session expires after 15 minutes of inactivity. At that time, you get automatically signed out and your unsaved changes are lost.

Selecting Google Cloud Platform projects

HYCU for GCP treats your Google Cloud Platform projects as separate entities. It requires data protection to be configured for the projects individually. This gives you the flexibility to configure data protection according to specific needs of each particular project.

Web user interface of HYCU for GCP can only see the Google Cloud Platform projects that:

- Are linked to the billing account that was selected when subscribing to HYCU for GCP.

  For more information, see:
  – *HYCU Backup and Recovery as a Service for GCP Release Notes*, section *Subscription notes*.
  – Section "Extent of data protection" on page 13

- Currently signed in Google Account has the required role granted on.

  For more information, see the *HYCU Backup and Recovery as a Service for GCP Release Notes*, section *Service requirements*.

During the web user interface session, you always perform actions in scope of the currently selected project.

Selecting a different Google Cloud Platform project

To select a different Google Cloud Platform project, follow these steps:

1. In the toolbar, click ⌄.
2. In the Select Google Cloud Platform Project dialog box, in the Name column, locate the desired project. If needed, click «, ‹, ›, or » to browse through parts of the list. You can also search for a project by entering its name or ID in the Search text box and then pressing **Enter**.
3. Click the project entry.
4. Click **Select**. The web user interface switches the context to the selected Google Cloud Platform project.

> Note HYCU for GCP remembers your last selected project from the latest previous web user interface session.

Defining your backup policy strategy

HYCU for GCP enables you to schedule automatic backups to achieve the optimum level of data protection based on your recovery point objective (RPO) and backup retention requirements. Backups can be scheduled to meet the specified RPO, run in the preferred time frame, and copy backup images into data archives.

When defining your backup policy strategy, take into account the specific needs of your environment and consider the following:

- Recovery point objective (RPO)

  Recovery point objective is the maximum tolerable data loss interval. It is a time period during which all incoming changes to the data are tolerated to be lost in case of a disaster.

- Backup windows

  You can avoid the impact of backup activity during peak hours in your production environment by specifying time frames when backups can be started.

- Data retention and use of data archives

  HYCU for GCP can create additional copies of backup images with longer retention periods as well as isolated long-term data archives with multiple retention tiers.

- Preferred backup policy

  You can choose a specific backup policy to protect all instances in your Google Cloud Platform project. Such default backup policy is automatically assigned to unprotected instances.

- Policy assignment from the Google Compute Engine service

  You can use the Google Compute Engine service to automatically assign backup policies by adding custom metadata tags to instances.

Choosing between policy types

Decide which of the following approaches best suits the needs of your environment:

- Applying a predefined backup policy

  You can use any of the predefined backup policies ("platinum", "gold", "silver", "bronze", or "exclude") to simplify the data protection implementation. For details, see "Predefined backup policies" below.

- Creating a custom backup policy

  If none of the predefined backup policies meets your needs, you can create a new backup policy based on your particular needs. For details, see "Custom backup policies" on the next page.

Your decision should also be based on envisioned usage of default backup policies or planned bulk assignment of policies from the Google Compute Engine service.

Predefined backup policies

When establishing a backup environment, you can take advantage of the predefined backup policies that provide a fast and convenient way of enabling data protection, and cover the most common data protection scenarios.

HYCU for GCP comes with the following predefined backup policies:

Name	Description
platinum	Data is backed up every 2 hours, snapshots are kept for 1 day, copies of backup images are retained for 1 week.
gold	Data is backed up every 4 hours, snapshots are kept for 1 day, copies of backup images are retained for 1 week.
silver	Data is backed up every 12 hours, snapshots are kept for 1 day, copies of backup images are retained for 1 week.
bronze	Data is backed up every 24 hours, snapshots are kept for 2 days, copies of backup images are retained for 1 week.
exclude	Instances are not scheduled for backup and they cannot be manually backed up either.

To exclude instances from data protection, assign them the "exclude" backup policy. Such instances are also excluded from compliancy and protection status determination. As a result, they are omitted from the figures depicted in the Instances widget on the dashboard.

> Note Predefined backup policies use automatic buckets for backup image storage. For more information on bucket types in HYCU for GCP, see "Setting up buckets" on page 36.

Consider also the following:

- No backup windows are assigned to predefined backup policies by default. For instructions on how to create and assign backup window specifications, see "Creating backup window specifications" on page 30.
- No data archives are created by predefined backup policies by default. For instructions on how to create data archives, see "Creating data archives" on page 32.

Custom backup policies

If your data protection needs are not covered with any of the predefined backup policies, you can create a new backup policy. In this case, besides setting the desired RPO and retention time, you can also select one or more policy options for optimal policy implementation. These policy options are the following:

Policy option	Description
Backup window	Allows you to choose a backup window specification. Each backup window specification includes one or more time frames during which new backup tasks are allowed to start.
Copy	Allows you to create a copy of the backup image and store it in a bucket.

Policy option	Description
Archiving	Allows you to preserve your data in a data archive for future reference.

Creating custom backup policies

You can create a custom backup policy that will meet all the needs of your data protection environment.

Prerequisites

- *Only if you plan to enable the Backup Window policy option.* At least one backup window specification exists in the selected Google Cloud Platform project. For instructions on how to create backup window specifications, see “Creating backup window specifications” on page 30.
- *Only if you plan to use a bucket of your choice.* The user-created bucket exists in the selected Google Cloud Platform project.
- *Only if you plan to enable the Archiving policy option.* A data archive exists. For instructions on how to create data archives, see “Creating data archives” on page 32.
- *Only if you plan to restore individual files or folders.* If you select Snapshot as a backup target type, make sure to also enable the Copy policy option. Also, make sure that disk cataloging is enabled on the related instance (see “Configuring instance backup options” on page 39).

Consideration

If you want that your data are stored locally as a snapshot and in a bucket, you select the Snapshot backup target type and also enable the Copy policy option.

> Accessing the Policies panel
>
> To access the Policies panel, in the navigation pane, click 🛡 **Policies**. Alternatively, in the Dashboard panel, click the **Policies** widget title.

To create a custom backup policy, follow these steps:

1. In the Policies panel, click + **New**. The New Policy dialog box appears.
2. Enter a name and, optionally, a description of your backup policy.
3. Enable the required policy options by clicking them:
   - **Backup Window**
   - **Copy**
   - **Archiving**
4. In the Backup section, do the following:
   a. In the Backup every field, set the RPO (in months, weeks, days, hours, or minutes).
   b. In the Retention text box, set a retention period (in months, weeks, or days) for the

data.

c. Select one of the following backup target types:

- **Snapshot**: Keeps local snapshots of instance disks in the Google Compute Engine service.

  > ⚠ Important If snapshots created by HYCU for GCP are deleted—either from the Google Cloud Platform Console or the gcloud command line—you will not be able to restore from snapshot. You can still restore your data from buckets if you create a copy or a data archive.
  >
  > For information on how the snapshots are named, see "Objects created by the service" on page 84.

- **Bucket**: Stores data to an automatically selected or user-created bucket in the selected Google Cloud Platform project.

d. *Only if you selected Bucket.* From the Bucket drop-down menu, select a bucket that you want to use for storing backup data.

If you select the **Automatically selected** option, a bucket in the region of the instance is chosen.

e. *Only if you selected Snapshot.* Under Snapshot Location, select **Regional** or **Multi-regional**.

> Example
>
> If your instance resides in the `us-central1-a` zone, with the Multi-regional option selected, a snapshot of the instance is replicated to all `us` regions, whereas with the Regional option selected, a snapshot is stored only in the `us-central1` region.

5. Depending on which policy options you have enabled, do the following:

Enabled option	Procedure
Backup Window	In the Backup Window section, from the Backup window specification drop-down menu, select a backup window for backup jobs. If no backup window is available and you want to create one, see "Creating backup window specifications" on the next page. If you do not select a backup window, the **Always** option is shown, which means that your backups are allowed to run at any time. Note If a backup job could not start during the specified time frames, an event of the Warning severity is created.
Copy	In the Copy section, do the following:

Enabled option	Procedure
	a. Set a retention period (in months, weeks, or days) for the copy of backup image. b. From the Bucket drop-down menu, select a bucket that you want to use for storing backup data. If you want your bucket to be selected automatically, make sure the **Automatically selected** option is selected. In this case, the HYCU automatically selects a bucket from the Google Compute Engine region. If you want to select a user-created bucket, make sure that this bucket is different from the one you selected for the backup.
Archiving	In the Archiving section, from the drop-down menu, select a data archive. If no data archive is available and you want to create one, see “Creating data archives” on page 32

6. Click **Save**.

The custom backup policy is created and added to the list of backup policies. For details on managing backup policies, see “Managing backup policies” on page 55.

Creating backup window specifications

HYCU for GCP enables you to define time frames when new backup tasks are allowed to start. You can use time frame definitions to prevent your backup environment from becoming overloaded. For example, you can schedule your backup tasks to run outside production hours to reduce the load during peak hours.

You can use backup window specifications with both predefined backup policies and custom backup policies.

> ⚠ Important When putting a backup window specification into use, check if the recovery point objective (RPO) of each affected backup policy can be achieved with the specified time frames. If the period defined for a RPO is shorter than any time frame during which backups are *not* allowed to start, the delayed backup tasks will result in a transient uncompliant status of the affected instances and backup policies.

> #### Accessing the Policies panel
>
> To access the Policies panel, in the navigation pane, click 🛡 **Policies**. Alternatively, in the Dashboard panel, click the **Policies** widget title.

To create a backup window specification, follow these steps:

1. In the Policies panel, click 📅 **Backup Window**.
2. In the Backup Window dialog box that appears, click + **New**.
3. In the New dialog box that appears, enter a name for your backup window

specification and, optionally, a description.

4. From the Time Zone drop-down list, select the time zone that the backup window specification will be based on.
5. Select the days of the week and hours during which you allow backups to run. Click and drag to quickly select a time frame that includes your preferred days and hours. Click an hour label (at the top) to select that hourly period on all days of the week. Click a day label (on the left) to select that entire day.

   The selected time frames are displayed as entries in the Time Frames field. To delete a selected time frame, click × next to its entry.
6. Click **Save**.
7. In the Backup Window dialog box, click **Close**.

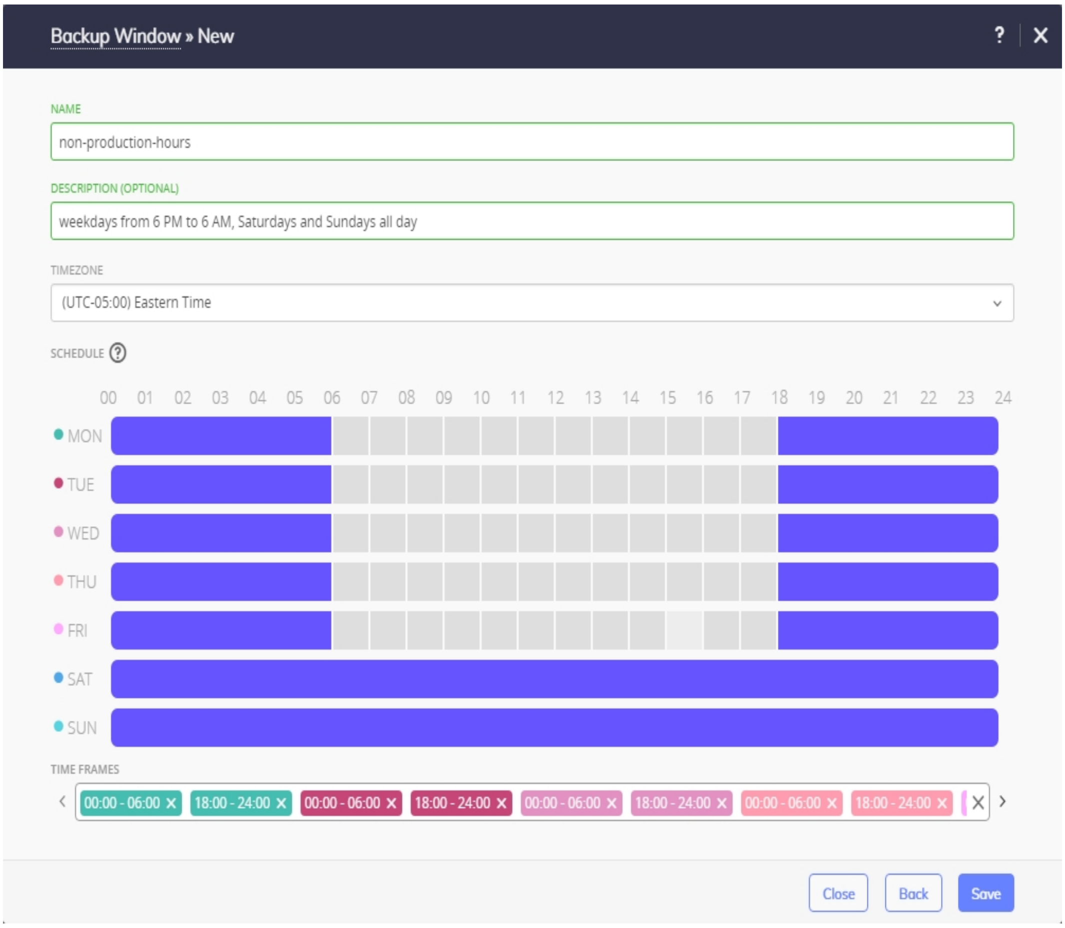
You can later edit any of the existing backup window specifications (click ✎ **Edit** and make the required modifications) or delete the ones that you do not need anymore (click 🗑 **Delete**).

After you create a backup window specification, you can do the following:

- Specify a backup window specification when creating a new backup policy. For details, see “Creating custom backup policies” on page 28.
- Assign a backup window specification to an existing backup policy. To do so, select the backup policy, click ✎ **Edit**, and then make the required modifications.

Example

You have selected the "bronze" backup policy and specified the time frames allowed for the backup tasks to be on weekdays from 6 PM to 6 AM (Eastern Time), and on Saturday and Sunday all day long.



Backup Window » New

NAME

non-production-hours

DESCRIPTION (OPTIONAL)

weekdays from 6 PM to 6 AM, Saturdays and Sundays all day

TIMEZONE

(UTC-05:00) Eastern Time

SCHEDULE

TIME FRAMES

00:00 - 06:00 × 18:00 - 24:00 × 00:00 - 06:00 × 18:00 - 24:00 × 00:00 - 06:00 × 18:00 - 24:00 × 00:00 - 06:00 × 18:00 - 24:00 ×

In this case, the backup tasks can be run every 24 hours at any point of time within the specified time frame.

Creating data archives

HYCU for GCP enables you to create an archive of your data and keep it for a longer period of time. By archiving data, the data is stored for future reference on a daily, weekly, monthly, or yearly basis. Your data is isolated from current activity and safely stored in a secure local or cloud archive location.

Prerequisite

Only if you plan to use a bucket of your choice for the data archive. Make sure that the user-created bucket exists in the currently selected Google Cloud Platform project.

Recommendation

Reserve the archive bucket only for data archives, make sure that no backup data is stored in the archive bucket.

> ### Accessing the Policies panel
>
> To access the Policies panel, in the navigation pane, click **Policies**.

To create a data archive, follow these steps:

1. In the Policies panel, click **Archiving**.
2. In the Archiving dialog box that appears, click + **New**. The New dialog box appears.
3. Enter a name for your data archive and, optionally, a description.
4. Enable the required archiving options by clicking them:

Daily	Allows you to create a daily archive of data.
Weekly	Allows you to create a weekly archive of data.
Monthly	Allows you to create a monthly archive of data.
Yearly	Allows you to create a yearly archive of data.

5. In the Start at field, specify the hour and the minute when the archive job should start.
6. From the Time zone drop-down menu, specify the time zone for archiving.
7. Provide information about when to archive data.

   > Note This information is specific to the archiving option you enabled. For example, for a weekly archiving, you specify a day of the week, whereas for monthly archiving, you specify a day of the month.

8. In the Retention field, set the retention period to be used.

   > Note This information is specific to the archiving option you enabled. For example, for a weekly archiving, you set the retention in weeks, whereas for monthly archiving, you set the retention in months.

9. From the Bucket drop-down menu, select a bucket that you want to use for storing the data archive.

   If you select the **Automatically selected** option, a bucket in the region of the instance is chosen.

10. Form the Storage class drop-down menu, select the storage class you want to use for storing the data archive.

    If you select the **Automatically selected** option, a storage class is automatically selected depending on the specified retention. If you want to select another storage class, see the detailed description of storage classes in the Google Cloud Platform documentation. Make sure that your choice does not negatively affect your storage costs.

11. Click **Save**.

You can later edit any of the existing data archives (click ✎ **Edit** and make the required modifications) or delete the ones that you do not need anymore (click 🗑 **Delete**). Keep in mind that you cannot modify an archive bucket if an archiving job is in progress on that bucket.

After you create a data archive, you can do the following:

- Specify a data archive when creating a new policy. For details, see "Creating custom backup policies" on page 28.
- Assign a data archive to the existing backup policy. To do so, select the backup policy, click ✎ **Edit**, and then make the required modifications.

Setting default backup policies

When you consider one of the predefined or custom backup policies satisfies all your data protection needs, you can set the policy as the default backup policy in the selected Google Cloud Platform project. HYCU for GCP then automatically assigns the policy to all newly detected instances. If you want, you can make HYCU for GCP assign the backup policy also to each already visible instance that still lacks an assigned policy.

> ⚠ Important Automatic assignment of default backup policies is overridden by assignment of policies from the Google Compute Engine service. For more information, see "Assigning backup policies from the Google Compute Engine service" on the next page.

> ### Accessing the Policies panel
>
> To access the Policies panel, in the navigation pane, click 🛡 **Policies**. Alternatively, in the Dashboard panel, click the **Policies** widget title.

To set a default backup policy for the currently selected Google Cloud Platform project, follow these steps:

1. In the Policies panel, select the policy that you want to set as default, and then click 🛡 **Set Default**.
2. In the Set Default Policy dialog box that appears, do one of the following:
   - Click **Yes** to assign the default backup policy to future instances (once detected) as well as all already visible instances that currently lack an assigned policy.
   - Click **No** to assign the default backup policy only to future instances once they are detected.

If you later decide not to use this backup policy as the default one, click 🛡 **Clear Default**.

Assigning backup policies from the Google Compute Engine service

Within a complex backup environment, and when your data protection approach requires use of diverse backup policies, you can utilize Google Cloud Platform service suite to automate policy assignment in HYCU for GCP. When you add proper custom metadata tags to instances in the Google Compute Engine service, HYCU for GCP detects them during the next instance synchronization and automatically assigns corresponding backup policies.

This approach improves the automatic policy assignment as follows:

- It offers you more control over automatic policy assignment than the default policy provides.
- It enables mass assignment of policies.
- You can use it for exclusion of instances from data protection—with the help of the predefined "exclude" policy,

Considerations

- A backup policy that is assigned from the Google Compute Engine service takes precedence over the default backup policy and over the manually assigned backup policy. This means that for each synchronized instance with proper metadata tag, the tag defines which backup policy gets assigned to the instance.

Prerequisites

- In HYCU for GCP, an appropriate service account is assigned to the parent Google Cloud Platform project of the instance that you plan to protect.

To assign backup policies to instances from the Google Compute Engine service, do the following:

1. Choose a Google Cloud Platform project whose instances you want to protect.
2. Within the project, chose an instance and add it the "hycu-policy" custom metadata tag in the Google Compute Engine service. Use the following data:

Key	Value
hycu-policy	*<PolicyName>*

   In the above table, `<PolicyName>` is the name of a backup policy that is configured for the chosen Google Cloud Platform project in HYCU for GCP. If you specify `exclude` for the tag value, the instance will be assigned the "exclude" policy.

   Custom metadata tags can be added from the Google Cloud Platform Console, the gcloud command line, or by using the Google Cloud Platform API. For instructions, see the Storing and Retrieving Instance Metadata | Compute Engine Documentation | Google Cloud webpage.

3. Repeat step 2 for each additional instance to which you want to assign a policy this way.
4. Sign in to the web user interface of HYCU for GCP.
5. Select the same Google Cloud Platform project as you did in step 1. For instructions on selecting projects in HYCU for GCP, see "Selecting a different Google Cloud Platform project" on page 25.
6. In the navigation pane, click **Instances**.
7. Click **Synchronize** or wait until the next instance synchronization cycle.

   In the Instances panel, names in the Policy column indicate a successful assignment of policies to all synchronized instances.

When you modify the value of an existing "hycu-policy" metadata tag, the change is propagated in the same way as when the tag is added.

> ⚠ Important If an instance has a backup policy assigned by means of a metadata tag, a subsequent assignment of a different policy in HYCU for GCP causes the tag to be automatically deleted from the instance.

Setting up buckets

Buckets are Google Cloud Storage resources in which backup images of protected data are stored. For storing its backup images, HYCU for GCP can use two bucket types, depending on how a backup policy is configured:

- User-created buckets

  Buckets of this type are the buckets that already exist in the Google Cloud Storage service. When configuring a backup policy, you can select a bucket of choice from the currently scoped Google Cloud Platform project. Selection is further limited to buckets that are visible to the Google Account with which you are signed in to HYCU for GCP.

  Only buckets of this type require your involvement to be set up.

- Automatic buckets

  Buckets of this type are created automatically during backup. Their names appear in the Buckets panel of the HYCU for GCP WUI. For maximum restore speed, they are created at the same location (the Google Cloud Storage region) as the backed up instances. Automatic buckets are reused for multiple instances where possible.

  > Note You can use automatic buckets also for storing individual files and folders that are restored from instance backup images.

  Automatic buckets are visible to the Google Cloud Platform services in the same way as the buckets you create yourself. When automatic buckets no longer contain backup images, they remain available in your project.

  For information on how the automatic buckets are named, see "Objects created by the service" on page 84.

> Caution Never delete any buckets used by HYCU for GCP from the Google Cloud

> Platform Console or the gcloud command line. Deletion of a bucket that stores backup images results in a data loss.
>
> Additionally, within buckets, ensure that the `hycu/backups/` folders are always preserved.

Storage cost charge

Storage of backup images in buckets is charged by Google according to their Google Cloud Storage pricing policy. For more information, see the Cloud Storage Pricing page on the Google Cloud Platform website.

How to set up user-created buckets

Setting up a user-created bucket means:

- Making the bucket available for backup and restore purposes in HYCU for GCP.
- Defining a soft limit on the bucket's storage space that is allowed to be used for backup images.

> ### Accessing the Buckets panel
>
> To access the Buckets panel, in the navigation pane, click **Buckets**. Alternatively, in the Dashboard panel, click the **Buckets** widget title.

To set up a user-created (custom) bucket, follow these steps:

1. In the Buckets panel, click + **Add**. The Add Bucket dialog box appears.
2. From the Buckets drop-down list, select the desired bucket.
3. Specify the amount of bucket storage space that is allowed to be used by backup images created by HYCU for GCP. To do this, edit the value in the Size text box and select a unit of measurement from the drop-down list as required.

   > Note The specified amount represents a soft limit, therefore actual usage may exceed it. It also adds to the joint bucket capacity that is shown within the Buckets widget in the Dashboard panel.
4. Click **Save**.

The bucket is added to the list of buckets and can be used for configuring backup policies. For details on managing buckets, see "Managing buckets" on page 52.

Enabling access to instances

HYCU for GCP requires access to objects in the instance operating system in order to:

- Create disk catalogs during backup to make restore of individual files or folders possible.
- Perform restore of individual files or folders to the original instance
- Run pre-snapshot or post-snapshot commands.

Access to the instances that are running Microsoft Windows must be specially allowed for HYCU for GCP by:

– Configuring user account within the instances in the Google Compute Engine service.

– Assigning the corresponding credential groups to such instances in HYCU for GCP.

> Note Pairs of user names and the corresponding passwords are referred to as credential groups in the HYCU for GCP web user interface.

HYCU for GCP gives you two options:

- Allow HYCU for GCP to configure new user accounts and automatically assign the credential groups.

  Choose this option to utilize the built-in automation. The configuration and assignment are invoked automatically when disk catalog creation is enabled for an instance that lacks assigned credentials.

  Names of automatically applied credential groups appear in the Credential group column of the Instances panel. They follow the `auto-<InstanceName>` template.

- Manually assign user account credentials.

  Choose this option to use existing user accounts or if needs of you environment require tight control over user names and passwords.

You can always manually unassign the existing credential groups from instances or replace them with new ones anytime.

Prerequisites

- A user account is configured within each instance through the Google Compute Engine service.

  For more information, see the Creating Passwords for Windows Instances | Compute Engine Documentation | Google Cloud webpage.

> Accessing the Instances panel
>
> To access the Instances panel, in the navigation pane, click **Instances**. Alternatively, in the Dashboard panel, click the **Instances** widget title.

To assign a credential group, follow these steps:

1. In the Instances panel, select your instance.
2. Click **Credentials**. The Credential Groups dialog box appears.
3. Click + **New** to create a new credential group.
4. Enter a name for the credential group, and then enter the valid user name and password of a user account that was configured within the instance through the Google Compute Engine service.
5. Click **Save** to save the credential group.
6. Click **Assign**.

7. Repeat steps 1 to 6 for each additional Microsoft Windows instance that you plan to protect.

> Tip If several instances share the same user name and password, you can use multiple selection to assign the same credential group in one step.

To unassign a credential group from an instance, in the Instances panel, select the instance, click **Credentials**, and then click **Unassign**.

You can also edit any of the existing credential groups (in the Credential Groups dialog box, select a credential group, click **Edit** , and then make the required modifications) or delete the ones that you do not need anymore (in the Credential Groups dialog box, select a credential group and then click **Delete**).

Configuring instance backup options

Before you protect the instances, you can adjust instance protection configuration to the needs of your environment as follows:

- Exclude instance disks from backup. By default, all disks of an instance are selected for backup.
- Provide the possibility to restore individual files or folders by enabling disk cataloging. By default, creation of disk catalogs is disabled.

  > Important To be able to restore individual files or folders, make sure that the backup data is stored in a backup or copy bucket. You cannot restore individual files or folders if backup data is stored only as snapshot or in data archives.

- Specify the commands to be run just before and immediately after HYCU for GCP takes a snapshot of the instance. You can use such pre-snapshot and post-snapshot commands to prepare the instance for a backup or to perform any additional tasks afterward.

Configure backup options separately for each instance for which the default options do not meet your data protection needs.

Consideration

If you enable disk catalog creation or specify pre-snapshot or post-snapshot commands, keep in mind that these backup options have further prerequisites which must be fulfilled at the time of the backup. For details, see section “Backing up instances” on page 41.

> ### Accessing the Instances panel
>
> To access the Instances panel, in the navigation pane, click **Instances**. Alternatively, in the Dashboard panel, click the **Instances** widget title.

To configure instance backup options, follow these steps:

1. In the Instances panel, select your instance.
2. Click **Configuration**. The Instance Configuration dialog box appears.

3. In the Disks drop-down list, click each desired disk to mark it as excluded from or included in the backup tasks.

   > Note Boot disk cannot be excluded from backup (cannot be left unprotected when its instance is protected).
   >
   > Instance disk selection for backup affects the total cost for protecting your data.

4. Use the **Create Disk Catalogs** switch to define whether the disk catalogs should be created and restore of individual files or folders be made possible (switch is on) or not (switch is off).

5. *Optional.* In the Pre-Snapshot Command text box, enter the command that HYCU for GCP runs just before it creates a snapshot of the instance. In the Post-Snapshot Command text box, enter the command that HYCU for GCP runs immediately after it creates a snapshot of the instance. You can specify the commands independently of each other.

   The commands are run from the home directory of the user account that HYCU for GCP uses for running the commands. Depending on the operating system on the instance, the following user account is used:

   - GNU/Linux: The user account that runs the backup session. For scheduled backups, this is the user or service account that assigned a policy to the instance.
   - Microsoft Windows: The user account that is assigned to the instance in HYCU for GCP through a credential group.

   > ⚠ Important Snapshot is created even if the pre-snapshot command fails. The post-snapshot command is run even if the pre-snapshot command or snapshot creation fail.
   >
   > When a pre-snapshot or post-snapshot command returns an exit code different from 0 or when it writes to the standard error output stream (stderr), HYCU for GCP sets the status of the restore point to Done with errors.

   > ### Example
   >
   > Examples of pre-snapshot and post-snapshot commands for different instance operating systems.
   >
   > GNU/Linux:
   >
   > ```
   > bash /home/<UserName>/freeze_db.sh
   > bash /home/<UserName>/thaw_db.sh
   > ```
   >
   > Microsoft Windows:
   >
   > ```
   > %USERPROFILE%\quiesce_db.bat
   > %USERPROFILE%\resume_db.bat
   > ```

6. Click **Save**.

Use the same procedure to change configured instance backup options.

Chapter 4

Protecting instances

HYCU for GCP enables you to protect your instance data with fast and reliable backup and restore operations.

For details on how to efficiently protect instance data, see the following sections:

- "Backing up instances" below
- "Restoring entire instances" on page 43
- "Restoring individual files or folders" on page 46

Backing up instances

With HYCU for GCP, you can back up your instances in a fast and efficient way.

Prerequisites

- *Only if you require the possibility to restore individual files or folders.* Ensure the following:
  - Restore of individual files or folders is supported on the operating system that is running on the original instance. See the *HYCU Backup and Recovery as a Service for GCP Compatibility Matrix*, section *Guest operating systems*, subsection *Supported operating system families*.
  - Source disk volume uses one of the supported file systems. See the *HYCU Backup and Recovery as a Service for GCP Compatibility Matrix*, section *Guest operating systems*, subsection *File-level restore availability*.
  - Creation of disk catalogs is enabled for the original instance. For instructions on how to enable creation of disk catalogs, see section "Configuring instance backup options" on page 39.
- *Only if you require the possibility to restore individual files or folders that originally reside on an instance running Microsoft Windows.* Ensure the following:
  - General and Microsoft Windows-specific usage prerequisites related to restore of individual files or folders are fulfilled. See the *HYCU Backup and Recovery as a Service for GCP Release Notes*, section *Service requirements*, subsection *Prerequisites for using the service*.
  - Correct credential group is assigned to the original instance, and the corresponding credentials belong to a user account with sufficient privileges. For instructions on

how to assign access credentials, see section "Enabling access to instances" on page 37.

- *Only if pre-snapshot or post-snapshot commands are specified for the instance backup options.* Ensure the following:
  - General and operating system-specific usage prerequisites related to the use of pre-snapshot and post-snapshot commands are fulfilled. See the *HYCU Backup and Recovery as a Service for GCP Release Notes*, section *Service requirements*, subsection *Prerequisites for using the service*.
  - *Only for Microsoft Windows instances.* A correct access credential group is assigned to the instance, and the corresponding credentials belong to a user account with sufficient privileges. For instructions on how to enable access to instances, see section "Enabling access to instances" on page 37.

Methods of invoking backups

While you can manually invoke a backup of an instance any time, continuous protection is only achieved by assigning it an appropriate backup policy. For instructions on how to back up instances manually, see "Performing manual backups" on page 59.

Backup policies can be assigned to instances:

- Manually—for the instances selected in the web user interface of HYCU for GCP.

  See the procedure that follows.

- Automatically—by configuring a default backup policy in HYCU for GCP for the parent Google Cloud Platform project.

  See "Setting default backup policies" on page 34.

- Automatically—by adding a custom metadata tag to instances in the Google Compute Engine service.

  See "Assigning backup policies from the Google Compute Engine service" on page 35.

Procedure for manual policy assignment

Accessing the Instances panel

To access the Instances panel, in the navigation pane, click **Instances**. Alternatively, in the Dashboard panel, click the **Instances** widget title.

To back up instances, follow these steps:

1. Select a Google Cloud Platform project. For instructions, see "Selecting a different Google Cloud Platform project" on page 25.

2. Select the instances that you want to back up.

   You can update the instance list by clicking **Synchronize**. To narrow down the list of displayed instances, use the filtering options as described in "Filtering and sorting data in panels" on page 61.

3. Click **Policies**. The Policies dialog box opens.

4. From the list of available backup policies, select the desired backup policy.

   Of the predefined backup policies, the "platinum", "gold", "silver", and "bronze" policies actually protect the data, whereas the "exclude" policy serves as a "container" for unprotected instances.

5. Click **Assign** to assign the backup policy to the selected instances.

When an instance is assigned a protecting backup policy for the first time, the backup task starts immediately. Subsequent backups are scheduled according to the values defined in the policy.

> Note The first backup task may be delayed if a backup image of the instance already exists. Delay length depends on the age of the backup image and the recovery point objective setting (value of the `Backup every` option) in the newly assigned backup policy.

You can also perform a manual backup of individual instances at any time. For details, see “Performing manual backups” on page 59.

> Tip Assign the "exclude" policy to instances not needing protection, so that the corresponding statistic in the Dashboard panel remains accurate.

Restoring entire instances

When restoring an entire instance, you can select among the following restore options:

Restore option	Description
Restore instance	Enables you to restore an instance to its original location with original settings. Select this option to replace the original instance (or its individual disks) with the restored instance (or individual restored disks). For instructions, see “How to restore an instance” on the next page ⚠ Important HYCU for GCP does not delete user-created objects (instances, instance disks) from the Google Compute Engine service. A manual delete action is required before you initiate the process for restoring data to its original location.
Clone instance	Enables you to create a clone of the original instance by restoring it (or a subset of its disks) to a new location with custom settings: project, geographic location, configuration of networks where the instance is accessible. Select this option to keep the original instance. For instructions, see “How to clone an instance” on page 45.

For best performance, both the restore and cloning processes make use of backup data in the following order where possible: snapshot, backup image or its copy that are stored in a bucket, data archive.

> Accessing the Instances panel
>
> To access the Instances panel, in the navigation pane, click **Instances**. Alternatively, in the Dashboard panel, click the **Instances** widget title.

How to restore an instance

To restore an instance to its original location with original settings (with optional disk selection), you must first manually delete the objects that you plan to restore.

> Caution Unprotected data (new data that has been stored on the instance after its last successful backup) is lost during the deletion.

Deleting original objects before the restore

The following table lists objects that you must delete in different restore scenarios.

In order to restore...	Delete...
An entire instance (all instance disks)	The instance and all instance disks[1].
A boot disk	The instance and its boot disk[2].
A particular non-boot disk	That particular disk.

[1] In Google Cloud Platform Console, disks may be configured for automatic deletion when the instance they are attached to is deleted.

[2] In Google Cloud Platform Console, boot disks may be configured for automatic deletion when the instance they are attached to is deleted. The action listed in the table preserves all other attached disks that are configured to be kept after instance deletion. You should attach such disks to the restored instance after the task completes.

Restoring instances or instance disks

After the deletion, open the web user interface of HYCU for GCP, and follow these steps:

1. In the Instances panel, click the instance that you want to restore to open the Details section.

   > Note The Details section appears only if you click an instance. Selecting the check box before the name of the instance does not open the Details section.

2. In the Details section that appears at the bottom of the screen, select the desired restore point.
3. Click **Restore Instance**. The Instance Restore Options dialog box opens.
4. Select **Restore**, and then click **Next**.

5. From the Disks drop-down list, select the instance disks that you want to restore.
6. Click **Restore**.

How to clone an instance

To create a clone of the original instance, restore it with a new name to the original or different location. When cloning, you can customize the following settings: selection of the backed up disks, project, region and zone, network configuration.

Cloning instances

Follow these steps:

1. In the Instances panel, click the instance that you want to restore to open the Details section.

   > Note The Details section appears only if you click an instance. Selecting the check box before the name of the instance will not open the Details section.

2. In the Details section that appears at the bottom of the screen, select the desired restore point.
3. Click **Restore Instance**. The Instance Restore Options dialog box opens.
4. Select **Restore as**, and then click **Next**.
5. In the New Instance Name text box, specify a new name for the instance.
6. From the Disks drop-down list, select the instance disks that you want to restore.

   > Note The boot disk is restored even when you do not select it.

7. From the Target Project drop-down list, select the project that you want to clone the instance to. Original project of the instance is preselected.
8. From the Target Region and Target Zone drop-down lists, select the Google Cloud Storage region and zone to clone the instance to. Original region and zone of the instance are preselected.
9. Under Network Interfaces, review a list of networks that the original instance was configured in (list of the network interfaces that instance had at the time of backup). The list shows the following for each network:
   - Subnetwork name (for VPC networks and shared VPC networks) or network name (for legacy networks).
   - *Present in case of a shared VPC network.* Name of the host project of the network.
   - Network type: "Subnet" for VPC networks and shared VPC networks, "Legacy" for legacy networks.

   For each configured network interface, an instance can use also an external IP address besides the mandatory internal IP address. By default, cloning preserves external IP address configuration of the backed up instance.

   To remove network interfaces, do the following:

   a. Click 🗑 in the line of a network interface entry.
   b. Repeat step a for each additional network interface that you want to remove.

   To add or remove external IP address to or from network interfaces, do the following:

   a. Click ✎ in the line of a network interface entry.
   b. Use the External IP switch to define whether the network interface should also use an external IP address (switch is on) or not (switch is off), and then click **Save**.
   c. Repeat steps a to c for each additional network interface that you want to reconfigure.

   To add network interfaces, do the following:

   a. Click **Add Network Interfaces**.
   b. From the Target Networks drop-down list, select a network that you want to add the cloned instance to. Available choices depend on the networks configured in the parent project of the instance and other (shared) networks that your user account has access to.
   c. Use the External IP switch to define whether the network interface should also use an external IP address (switch is on) or not (switch is off).
   d. Click **Add**.
   e. Repeat steps a to d for each additional network interface that you want to configure for the cloned instance.

10. Click **Restore**.

Restoring individual files or folders

You can restore individual files or folders to:

- The original location or a new location on the original instance
- A bucket of choice in the same Google Cloud Platform project

You can use this restore method when one or more individual files or folders have been deleted for some reason and are now missing on the instance.

Prerequisites

- Disk catalogs exist for the backed up disks of the original instance.
- *Only if you selected Snapshot as a backup target type.* A copy of the backup image is stored in a bucket.
- *Only for restore into the original instance.* Target disk volume uses one of the supported file systems. See the *HYCU Backup and Recovery as a Service for GCP Compatibility Matrix*, section *Guest operating systems*, subsection *File-level restore availability*.
- *Only for restore into the original instance running Microsoft Windows.* Ensure the following:

  - General and Microsoft Windows-specific usage prerequisites related to restore of individual files or folders are fulfilled. See the *HYCU Backup and Recovery as a Service for GCP Release Notes*, section *Service requirements*, subsection *Prerequisites for using the service*.
  - Valid access credentials are assigned to the original instance, and they belong to a user account with sufficient privileges. Credential assignment is performed automatically by HYCU for GCP. For instructions on how to manually assign access credentials, see section "Enabling access to instances" on page 37.
- *Only for restore into the original instance running GNU/Linux.* General and GNU/Linux-specific usage prerequisites related to restore of individual files or folders are fulfilled. See the *HYCU Backup and Recovery as a Service for GCP Release Notes*, section *Service requirements*, subsection *Prerequisites for using the service*.
- *Only for restore into a bucket*. In the web user interface of HYCU for GCP, at least one bucket exists in the Buckets list in the project of the original instance. For information on how to add user-created buckets to this list, see section "How to set up user-created buckets" on page 37.

Considerations

- For restore of individual files or folders, HYCU for GCP treats folders as bare containers of file system objects. This means that in a restore task:
  – Folders are never renamed, even when you choose to rename objects by selecting a corresponding option in the web user interface.
  – Folder access control lists (ACLs) are never restored, and the original folder ACLs are maintained on the file system.

> Accessing the Instances panel
>
> To access the Instances panel, in the navigation pane, click **Instances**. Alternatively, in the Dashboard panel, click the **Instances** widget title.

How to restore individual files or folders

To restore individual files or folders, follow these steps:

1. In the Instances panel, click the instance that contains the files or folders that you want to restore—to open the Details section.

   > Note The Details section appears only if you click an instance. Selecting the check box before the name of the instance does not open the Details section.

2. In the Details section that appears at the bottom of the screen, select the desired restore point, and then click **Restore Files**.
3. In the Choose Disks dialog box, from the Disks drop-down list, review the instance disk selection.

   > Tip You can shorten the disk catalog preparation time by deselecting the disks

> that do not apply (disks that do not store the files or folders that you want to restore).

4. In the Choose File and Folders dialog box, from the list of available files and folders, select the ones that you want to restore, and then click **Next**.

   If needed, click «, ‹ , › , or » to browse through parts of the list.. You can also search for a file or a folder by entering its name in the Search text box and then pressing **Enter**.

   The File Restore Options dialog box appears.

5. In the File Restore Options dialog box, select whether you want to restore the files to the original instance or a bucket of choice.

Original instance	To restore the files or folders into the original instance, follow these steps: a. Select **Restore into Instance**, and then click **Next**. b. In the Restore into Instance dialog box, select the location on the instance where you want to restore the files or folders to, and provide the required information. ⊖ Caution Contents of original files on the disk are lost once overwritten during the restore process. Make a selection: • **Original location** Select how HYCU for GCP should handle file or folder names when there are file system objects with the same names at the original location on the instance disk. You can choose among the following options: – **Overwrite original** This selection directs HYCU for GCP to overwrite the object on disk with restored data. – **Rename original** This selection causes the original file to be renamed before the data is restored. – **Rename restored** This selection causes the restored file to get a new name. For information on which name templates are used for renaming original and restored files, see “Objects created by the service” on page 84. • **Alternate location** In the **Path on the Original Disk** dialog box, specify the

	path to an alternate location on the same instance in the following format:
	○ GNU/Linux:
	`/<Path>/<FolderName>`
	○ Microsoft Windows:
	`<DriveLetter>:\<Path>\<FolderName>`
	Restored objects overwrite the objects with the same names that might exist at the alternate location.
	c. Depending on your preference for restore of the file access control lists (ACLs), do one of the following:
	• Select the **Restore ACL** option.
	This will make HYCU for GCP restore original ACLs and apply them of the restored files.
	• Keep the **Restore ACL** option unselected.
	This will make HYCU for GCP apply inherited ACLs on the restored files—according to the file system ACL inheritance rules.

Bucket of choice	To restore files or folders into a bucket, follow these steps: a. Select **Restore into Bucket**, and then click **Next**. b. From the Target bucket drop-down list, select the desired bucket where you want to restore data to. Restored objects are copied into the selected bucket. For information on their exact locations in the bucket, see “Objects created by the service” on page 84.

6. Click **Restore**.

> ⚠ Important If you chose to restore data to the original instance, and the instance is not accessible, the restore operation fails. An instance is not accessible in the following cases:
>
> – Discovery by HYCU for GCP is not successful.
> – The instance is stopped.
> – The instance no longer exists.
>
> An instance running Microsoft Windows may also not be accessible when:
>
> – The instance has no assigned access credentials in HYCU for GCP.
> – The assigned credentials are incorrect.
> – The assigned credentials belong to a user account with insufficient privileges.

Chapter 5

Performing common tasks

To ensure secure and reliable performance of HYCU for GCP, the solution provides various mechanisms to support your daily activities.

In order to...	Follow instructions in....
Achieve any of the following: – Get an at-a-glance overview of the data protection status in your environment. – Identify possible bottlenecks. – Inspect different areas of the environment protected by HYCU for GCP.	Section "Using the dashboard" on the next page.
Achieve any of the following: – View bucket information. – Deactivate or activate a bucket. – Edit or remove a bucket.	Section "Managing buckets" on page 52.
Achieve either of the following: – View backup policy information. – Edit or delete a backup policy.	Section "Managing backup policies" on page 55.
View the backup status of instances.	Section "Viewing instance details " on page 56.
Back up data manually.	Section "Performing manual backups" on page 59.
Mark a restore point as expired.	Section "Manually marking restore points as expired" on page 59.
Achieve either of the following: – Track tasks that are running in your environment. – Get insight into the status of a specific task.	Section "Checking task statuses" on page 60.
View all events that occurred in your backup environment.	Section "Viewing events" on page 60.
Achieve either of the following:	Section "Filtering and sorting data in

In order to...	Follow instructions in....
– Narrow down the list of displayed elements in panels. – Sort the list of displayed elements in panels.	panels” on page 61.

Using the dashboard

Web user interface of HYCU for GCP includes an intuitive dashboard. The dashboard:

- Provides an at-a-glance overview of the data protection status in your environment, substantiated with relevant statistics.
- Enables you to monitor all data protection activities and quickly identify areas that require your attention.
- Allows you to easily access the area of interest by simply clicking the title of the corresponding widget.

> Tip We recommend that you use the dashboard as a starting point for your everyday tasks.

Accessing the Dashboard panel

To access the Dashboard panel, in the navigation pane, click **Dashboard**.

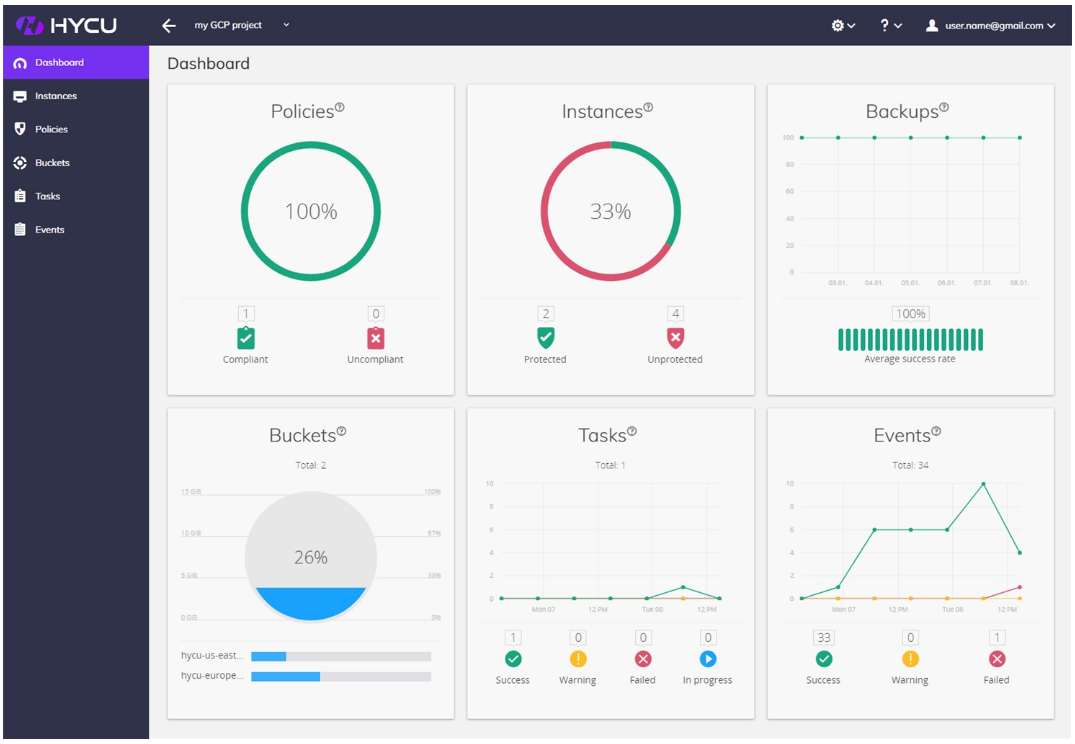


Figure 5–1: Dashboard in the WUI of HYCU for GCP

The following table describes what kind of information you can find within each widget.

Widget label	Description
Policies	Shows the percentage of policies that are compliant, and the exact number of compliant and uncompliant policies. A backup policy is considered compliant if all instances that have this policy assigned are compliant with the policy settings. For more information on policies, see “Defining your backup policy strategy” on page 25.
Instances	Shows the percentage of protected instances in your environment, and the exact number of protected and unprotected instances. An instance is considered protected if it has a backup policy assigned and if at least one backup image of the instance exists. For information about protecting instances (backup sources), see “Backing up instances” on page 41.
Backups	Shows the backup task success rate for the last seven days.
Buckets	Shows the number of existing buckets and their individual as well as joint storage capacity utilization. For information about setting up buckets , see “Setting up buckets” on page 36.
Tasks	Shows the number of tasks in the protected environment for the last 48 hours. The widget also shows how many tasks succeeded, failed, or are in progress or queued. For instructions on how to check the task status, see “Checking task statuses” on page 60.
Events	Shows the number of events in the protected environment for the last 48 hours. The widget also shows the number of events for each event severity. For instructions on how to view event details, see “Viewing events” on page 60.

Managing buckets

You can view bucket information, edit a bucket, deactivate or activate a bucket, or remove a bucket if you do not want to use it for storing backup images of protected data anymore.

> Accessing the Buckets panel
>
> To access the Buckets panel, in the navigation pane, click **Buckets**. Alternatively, in the Dashboard panel, click the **Buckets** widget title.

Viewing bucket information

You can view information about each bucket in the list of buckets in the Buckets panel. This allows you to have an overview of the general status of the buckets. The following information is available for each bucket:

Property name	Description
Name	Bucket name (globally unique). For information on how the automatic buckets are named, see "Objects created by the service" on page 84.
Location	Name of the Google Cloud Storage region in which the bucket resides.
Storage Class	Default object storage class of the bucket in the Google Cloud Storage service: Multi-regional, Regional, Nearline, or Coldline.
Status	Status of the bucket: • Active: You can use the bucket for backing up data, creating data archives, and restoring data. • Inactive: The bucket has been deactivated within HYCU for GCP. As long as it is not activated you can use it only for restoring data. • Inaccessible on GCP: Insufficient permissions are set on the bucket in the Google Cloud Storage service. HYCU for GCP cannot access the bucket. • Deleted from GCP: The bucket no longer exists in the Google Cloud Storage service. For instructions on how to change the status of active or inactive buckets, see "Deactivating and activating a bucket" on the next page.
Size Limit	Maximum amount of the bucket storage space (expressed in MiB, GiB, or TiB) that is allowed to be used by backup images created by HYCU for GCP. The amount represents a soft limit, therefore actual usage may exceed it.
Health	Health status of the bucket: • The ? icon: Indicates one of the following: – The bucket health has not been determined yet. – The bucket is inactive. • The ✓ icon: The bucket is in a healthy state. Utilization of storage space for backup images in the bucket is less than 90 percent of the configured size limit. • The ! icon: Utilization of storage space for backup images in

Property name	Description
	the bucket is over 90 percent and under 100 percent of the configured size limit. • The ⊗ icon: Indicates one of the following: – The bucket storage space occupied by backup images exceeds the configured size limit. – The bucket is not accessible due to an I/O error, insufficient permissions, or some other reason.
Utilization	Ratio (expressed in percentage) between the bucket storage space occupied by backup images and the configured size limit.
Automatic	Indicator of whether the bucket was created automatically by HYCU for GCP (✓) or not (✕).

To open the Details section where you can find more details about the bucket, click the desired bucket.

Editing a bucket

Editing a bucket means changing the value of the bucket's Size Limit property. This property represents a soft limit.

To edit a bucket, follow these steps:

1. In the Buckets panel, select the bucket that you want to edit, and then click ✎ **Edit**. The Edit Bucket dialog box appears.
2. Edit the value in the Size text box or select another unit of measurement from the drop-down list as required.
3. Click **Save**.

Deactivating and activating a bucket

Deactivation of a bucket makes the bucket unavailable for backup operations in HYCU for GCP. The bucket remains registered with HYCU for GCP with all the contained backup images intact. Restore of data from the bucket is still possible.

> Note You cannot deactivate buckets that were created automatically by HYCU for GCP.

You can deactivate a bucket when the following precondition is fulfilled:

– The bucket is not selected for the `Custom Bucket` option of any backup policy.

After deactivating a bucket, the bucket cannot be selected for the `Custom Bucket` option of a backup policy until it is activated again.

To deactivate or activate a bucket, follow these steps:

1. In the Buckets panel, select the bucket that you want to deactivate or activate.
2. Change the status of the selected bucket: click **Deactivate** or **Activate**.
3. *Only for deactivation.* Click **Yes** to confirm that you want to deactivate the selected bucket.

Removing a bucket

Removal of a bucket deregisters the bucket from HYCU for GCP. After deregistration, the bucket and its contained data other than backup images continue to be available in your Google Cloud Platform project.

> Note You cannot remove buckets that were created automatically by HYCU for GCP.

You can remove a bucket when both preconditions are fulfilled:

- The bucket contains no backup images.
- The bucket is not specified in the `Custom Bucket` option of any backup policy.

After removing a bucket, no backup operations that include this bucket are possible anymore.

To remove a bucket, follow these steps:

1. In the Buckets panel, select the bucket that you want to remove, and then click **Remove**.
2. Click **Yes** to confirm that you want to remove the selected bucket.

Managing backup policies

You can view backup policy information, edit backup policy properties, or delete a backup policy if you do not want to use it for protecting data anymore.

Accessing the Policies panel

To access the Policies panel, in the navigation pane, click **Policies**. Alternatively, in the Dashboard panel, click the **Policies** widget title.

Viewing backup policy information

You can view information about each backup policy in the list of backup policies in the Policies panel. This allows you to have an overview of the general status of the backup policies. The following information is available for each backup policy:

Property name	Description
Name	Backup policy name.
Compliancy	Compliancy status of the backup policy:

Property name	Description
	• The ✓ icon: The backup policy is compliant. • The ⊗ icon: The backup policy is uncompliant. • The ? icon: Backup policy compliancy is undefined. The policy is not assigned to any instance, or this is the "exclude" policy.
Instance Count	Total number of instances that have the particular backup policy assigned to them.
Description	Description of the backup policy, for example, how often backup is performed, how long backup images are retained, how many snapshots are kept.

To open the Details section where you can find more details about the backup policy, click the desired backup policy.

Creating Backup policies

See “Creating custom backup policies” on page 28.

Editing backup policies

To edit a backup policy, follow these steps:

1. In the Policies panel, select the backup policy that you want to edit, and then click ✎ **Edit**. The Edit Policy dialog box appears.
2. Edit the selected backup policy as required. For detailed information about backup policy properties, see “Creating custom backup policies” on page 28.
3. Click **Save**.

Deleting backup policies

To delete a backup policy, follow these steps:

1. In the Policies panel, select the backup policy that you want to delete, and then click 🗑 **Delete**.
2. Click **Yes** to confirm that you want to delete the selected backup policy.

Viewing instance details

You can view the details about each instance in the Details section of the Instances panel. The following information is available for each instance:

Property name	Description
Details	Shows the following information about the selected instance: – Virtual hardware and guest operating system properties – Instance location and current status – Time since last successful backup, backup success rate – Policy compliance rate of the restore points – Policy assignor—account that assigned the backup policy: a user account (when the assignment is made through the HYCU for GCP web user interface) or a service account (when the assignment is made from the Google Compute Engine service based on instance custom metadata tags)
Restore point	Shows the following information for each restore point: • Date and time when the restore point was created. • Available entities of the restore point, which determine your possibilities for the restore: ○ SNAP or S : Snapshot. Displayed if a snapshot of the instance (or an instance disk) exists. Snapshots allow faster completion of restore tasks. ○ BCKP or B : Backup image in a bucket. Displayed if backup data is stored in a bucket. ○ COPY or C : Copy of backup image. Displayed if a copy of the backup image (snapshot or backup data in a bucket) exists in another bucket. ○ ARCH or A : Archive. Displayed if a data archive exists in a bucket for the restore point. ○ CTLG or C : Catalog. Displayed if the disk catalog exists in a bucket. Disk catalogs enable restore of individual files or folders.
Compliancy	Shows compliancy status of each restore point: • The ✓ icon: The restore point is compliant. • The ✗ icon: The restore point is uncompliant. • The ? icon: Instance compliancy is undefined. The instance either has no policy assigned or the "exclude" policy is assigned to it. Note By pausing on a compliancy status icon, additional information about the backup is shown:

	– Backup frequency in the backup policy that triggered the backup. – The time period since previous successful backup.
Backup status	Shows backup status of the instance. For more information, see "Viewing the backup status of instances" below.
Restore status	Shows a progress bar indicating the progress of instance restore. Note By double-clicking a progress bar, you are directed to the Tasks panel where you can check details about the related task.

Viewing the backup status of instances

The Backup status of your instance determines whether it is possible to restore it.

Backup status	Restorability	Notes
✓ (Done)	✓	n/a
! (Done with errors)	✓	[1] An indicator of any of the following: – Not all instance disks were backed up successfully, therefore the instance can only be partially restored. If backup of a boot disk failed, you may be unable to start the instance after the restore. – Disk catalog creation failed. You cannot restore individual files or folders. – Creation of a copy of the backup image failed.
○ (Expired)	×	n/a
○ (Inaccessible on GCP)	×	*Only if snapshot is not available due to backup policy configuration.* Access permissions on all Google Cloud Storage buckets where the backup data is stored are not sufficient.
○ (Deleted from GCP)	×	*Only if snapshot is not available due to backup policy configuration.* Backup data is not available because buckets were deleted from the Google Cloud Platform project.

> Note By pausing on a backup status icon, additional information about the backup image is shown: consistency state, backup duration, size of backup data on a bucket, names of the containing Google Cloud Storage buckets, and backup ID.

Performing manual backups

HYCU for GCP backs up your data automatically after you assign a backup policy to the selected instances. However, you can also back up your data manually at any time, for example, for testing purposes or in the event when an automatic backup fails.

Prerequisites

- A backup policy other than the "exclude" backup policy is assigned to the instance.

Considerations

- When the assigned backup policy uses a backup window, manual backups may prevent the scheduled backup for the same instance from starting within the defined time frame. If this happens, the instance becomes uncompliant with the policy settings until the next backup window or the next manual backup.

Procedure

To perform a manual backup, follow these steps:

1. In the Instances panel, select which instances you want to back up.
2. Click **Backup** to invoke the backup of the selected instances.
3. Click **Yes** to confirm that you want to start the manual backup.

> Tip In the navigation pane, click **Tasks** to check the overall progress of the backup.

Manually marking restore points as expired

If you do not want to keep an existing restore point for potential data restore anymore, you can mark it as expired. Each restore point represents data that was backed up at a specified point in time.

> Important Marking a restore point as expired cannot be undone.

> ### Accessing the Instances panel
>
> To access the Instances panel, in the navigation pane, click **Instances**. Alternatively, in the Dashboard panel, click the **Instances** widget title.

To mark a restore point as expired, follow these steps:

1. In the Instances panel, select the corresponding instance.
2. In the Details section that appears at the bottom of the screen, select the restore point that you want to mark as expired.

3. Click **Expire**. The Expire dialog box appears.
4. Click **Yes** to confirm that you want the selected restore point to be marked as expired.

After you mark the restore points as expired, the HYCU for GCP cleaning process removes expired backup images from their buckets in the Google Cloud Storage service, and deletes the corresponding snapshots from the Google Compute Engine service (if they still exist).

Checking task statuses

You can use the Tasks panel to check the overall status of tasks.

> ### Accessing the Tasks panel
>
> To access the Tasks panel, in the navigation pane, click **Tasks**. Alternatively, in the Dashboard panel, click the **Tasks** widget title.

In the Tasks panel, you can do the following:

- Check the status of tasks that are currently running.
- Check the status of completed and stopped tasks.
- Check more details about a specific task in the Details section that appears at the bottom of the screen after you select the task.
- Generate a report about a specific task by selecting it, and then clicking **View Report**. To copy the report to the clipboard, in the Task Report dialog box that opens, click **Copy to clipboard**.
- Abort a currently running task by selecting it, and then clicking **Abort Task**.

The following table shows the task information:

Task information	Description
Description	Summary of the task (for example, running a backup, performing a restore, restoring individual files or folders).
Status	Current status of a task (for example, Ready, a progress bar indicating the Running status, Done, Done With Errors, Failed, or Aborted).
Started	Time when the task was started.
Finished	Time when the task finished.

Viewing events

The Events panel enables you to view all events that occurred in your environment, to check details about the selected event, and to list events that match the specified filter.

> ### Accessing the Events panel
>
> To access the Events panel, in the navigation pane, click **Events**. Alternatively, in the

> Dashboard panel, click the **Events** widget title.

The following information is available for each event:

Severity	Severity level of the event: • ✓ (Info): Events representing regular service operation. • ! (Warning): Potentially harmful situations that do not represent an immediate threat to service operation. • ✗ (Error): Errors that immediately affect service operation.
Message	Description of the event.
Category	Solution functional area to which the event belongs: • System: Events not related to any other category; they take place regardless of your interaction with HYCU for GCP. • Policies: Events related to backup policy management. • Backup: Events that take place during backup, notifications about skipped backup tasks. • Restore: Events that take place during restore. • Targets: Events related to bucket management. • Credentials: Events related to assignment of credentials to instances running Microsoft Windows.
Timestamp	Event creation date and time.

To open the Details section where you can find the event summary and more details about the event, click the desired event.

Filtering and sorting data in panels

HYCU for GCP enables you to filter data in the panels so you can easily find what you need. Each panel contains different filtering options and it can display only the entries that meet the specified filter criteria. For example, filtering the data in the Instances panel helps you to focus only on the instances that you are interested in or responsible for.

In addition, you can sort data in the panels by any parameter whose values are displayed in a particular table (in the overview pane). For example, sorting data in the Policies panel by the Compliancy parameter helps you easily track uncompliant backup policies.

How to filter data in panels

To filter data in panels, follow these steps:

1. Go to the web user interface panel of interest.
2. Click **Filters**. The Filters side pane opens.
3. Specify your filter criteria.
4. Click **Apply Filters**.

Depending on the panel the contents of which you want to filter, see one of the following sections for information on the available filtering options:

- “Filtering options in the Instances panel” below
- “Filtering options in the Policies panel” on the next page
- “Filtering options in the Buckets panel” on the next page
- “Filtering options in the Tasks panel” on the next page
- “Filtering options in the Events panel” on page 64

Filtering options in the Instances panel

In the Filters side panel, select one or more filtering options:

Filtering option	Action
Search	Enter a search term. You can filter by the instance name.
Policies	From the drop-down list, select the backup policies that are assigned to the instances.
Compliancy	Select one or more options to filter by the compliancy status: • **Success**: Instance is compliant. • **Failure**: Instance is not compliant. • **Undefined**: The "exclude" backup policy is assigned to the instance, or the instance does not have a backup policy assigned.
Protection	Select one or more options to filter by the protection status: • **Yes**: Instance is protected. • **No**: Instance is not protected. • **Deleted**: Instance no longer exists, but at least one of its backup images does. • **Undefined**: The "exclude" backup policy is assigned to the instance.

Filtering options in the Policies panel

In the Filters side panel, select one or more filtering options:

Filtering option	Action
Search	Enter a search term. You can filter by the name of the backup policy.
Compliancy	Select one or more options to filter by the compliancy status: • **Success**: All instances that the backup policy is assigned to are compliant. • **Failure**: Not all instances that the backup policy is assigned to are compliant. • **Undefined**: The backup policy is not assigned to any instance or this is the "exclude" backup policy.

Filtering options in the Buckets panel

In the Filters side panel, select one or more filtering options:

Filtering option	Action
Search	Enter a search term. You can filter by the bucket name.
Storage class	Select one or more options to filter by the Google Cloud Platform storage class: • **Regional** • **Coldline** • **Nearline** • **Multi-Regional**
Health	Select one or more options to filter by the status of the bucket: • **Ok** • **Warning** • **Error** • **Undefined**

Filtering options in the Tasks panel

In the Filters side panel, select one or more filtering options:

Filtering option	Action
Search	Enter a search term. You can filter by the task name or the task ID.

Filtering option	Action
Status	Select one or more options to filter by the status of the task: • **Done** • **Ready** • **Running** • **Failed** • **Done With Errors** • **Aborted**

Filtering options in the Events panel

In the Filters side panel, select one or more filtering options:

Filtering option	Action
Message	Enter a text string to filter the list to include only the messages with the specified string.
Category	From the drop-down list, select items to filter the list to include only the selected event categories.
Username	From the drop-down, select the user name.
Severity	Select one or more options to filter by the event severity: • **Success** • **Warning** • **Failed**

How to sort data in panels

To sort data in panels, follow these steps:

1. Go to the web user interface panel of interest.
2. Click the column heading of the property that you want to sort the data by.

   The ⌃ icon appears in the heading cell, indicating that the column data is sorted in ascending order.
3. Click the column heading again to toggle the sort order.

   The ⌄ icon appears in the heading cell, indicating that the column data is sorted in descending order.

Chapter 6

Administering

While using HYCU for GCP, you can perform different tasks to administer and customize the solution for your data protection needs.

In order to...	Follow instructions in...
Understand how user permissions in HYCU for GCP are defined.	Section "Managing users" below
Change the organization account when needed.	Section "Changing the organization account" on the next page
Configure project service accounts.	Section "Configuring project service accounts" on page 67
Be notified about different kinds of events in HYCU for GCP.	Section "Configuring event notifications" on page 69
Hide instances from HYCU for GCP.	Section "Excluding instances from synchronization" on page 71

If for whatever reason you decide that you no longer want to use HYCU for GCP, you can easily stop using it. For information on properly doing so, see "Ceasing service use" on page 79.

Managing users

This section provides information on managing HYCU for GCP users. HYCU for GCP does not provide means of direct user management. The service indirectly determines which user accounts are allowed to can take specific actions based on:

- The billing account selected while you subscribe to the solution.
- Sets of permissions that are granted the corresponding Google Accounts in the Google Cloud Platform service suite.

The following table lists different goals and their corresponding preconditions.

With a specific Google Account, you can...	Provided that...
Sign in to the web user interface	The Google Account can see at least

	one of the scoped Google Cloud Platform projects.
See your Google Cloud Platform projects	The projects are linked to the billing account selected for the service subscription.
Protect your Google Cloud Platform projects	The Google Account has the required roles granted in the following services of the Google Cloud Platform service suite: – Google Compute Engine – Google Cloud Storage

For more information on the required preconditions, see section "Extent of data protection" on page 13 and the *HYCU Backup and Recovery as a Service for GCP Release Notes*, section *Service requirements*.

Changing the organization account

This section describes the steps that you must perform to change the organization account. Such a change is required in the foreseen event when the Google Account that is set as the current organization account is going to (either change applies):

- Lose the Billing Account Viewer (`roles/billing.viewer`) role on the billing account of the service subscription.
- Cease to exist.

If such an event happens without prior and proper change of the organization account, HYCU for GCP is no longer able to retrieve information about scoped projects. It effectively results in reduced or no data protection activities, and eventually in your inability to sign in to the WUI.

> ⚠ Important A Google Account qualifies to be used as the new organization account when it (both conditions apply):
> – Has access to any Google Cloud Platform project linked to the billing account.
> – Has at least the Billing Account Viewer (`roles/billing.viewer`) role granted on the billing account.

> Accessing the Organization Account dialog box
>
> To access the Organization Account dialog box, click ⚙ **Administration** in the toolbar, and then select **Organization Account**.

To change the organization account, follow these steps:

1. In the Account list, select the user account that you want to set as the organization account. This list includes the following:

   - User accounts that signed in to the web user interface of HYCU for GCP at least once.
   - User accounts that were manually added to the list.

   If needed, click «, ‹, ›, or » to browse through parts of the list.

   > Tip With a large list of user accounts, to quickly locate the desired user account, enter a search criterion into the Search text box.

2. If a qualified user account is not present in the list, add it. Click + **Add** and allow the pop-up window to appear. Specify user name of the Google Account, enter the corresponding password, and click **Next**.
3. Click **Assign**.

Configuring project service accounts

This section describes the steps that you must perform to configure project service accounts in HYCU for GCP. Project service account is a Google Cloud Platform service account that is used for identification of automated requests to HYCU for GCP within a Google Cloud Platform project. Such requests must be authenticated similarly to those that you invoke interactively through the solution's web user interface. For more information about Google Cloud Platform service accounts, see the Understanding service accounts | Cloud Identity and Access Management Documentation | Google Cloud webpage.

When configured in HYCU for GCP, the project service account becomes a property of one Google Cloud Platform project within HYCU for GCP and facilitates data protection activities for that project. A project service account enables additional features in HYCU for GCP:

- Policy assignment from the Google Cloud Platform services
- Use of the HYCU for GCP application programming interface (API)

> Important A service account becomes effective only after it is imported into HYCU for GCP *and* assigned to a project.

Prerequisites

- The service account must have the following roles granted in the Google Cloud Platform service suite:
  - Compute Admin (`roles/compute.admin`), Storage Admin (`roles/storage.admin`), and Service Account User (`roles/iam.serviceAccountUser`) on the project with your protected instances.
  - *Only if you plan to use the HYCU for GCP API.* Service Account Token Creator (`roles/iam.serviceAccountTokenCreator`) on the service account itself.
  - *Only for cloning into non-original projects by using the HYCU for GCP API.* Compute Admin (`roles/compute.admin`) and Service Account User (`roles/iam.serviceAccountUser`) on the projects where you plan to clone your instances to.

See the following sections for the corresponding instructions:

- “Importing service accounts” below
- “Configuring webhook-based notifications” on page 70

Importing service accounts

Importing a service account makes it available to HYCU for GCP for assigning to a project.

Prerequisites

- The service account is configured in the Google Cloud Platform service suite.
- You have access to a valid JSON file which stores the service account information, including its private key.

> Accessing the Service Accounts dialog box
>
> To access the Service Account dialog box, click ⚙ **Administration** in the toolbar, and then select **Service Accounts**.

To import a service account into HYCU for GCP, do the following:

1. In the Service Accounts dialog box, click + **Add**.
2. Click **Browse**. In the Choose File to Upload dialog box, browse for and then select the JSON file with the service account information. Click **Open**.
3. Review the file contents and then click **Upload**.

A confirmation message indicates successful import of the service account.

> Note It may happen that a successfully imported service account does not appear in the service account list. This occurs when the service account belongs to the Google Cloud Platform project to which the user account you are using to sign in does not have access to. However, the service account is stored for potential use at a later time.

To delete an imported service account, in the Service Accounts dialog box, select its entry from the list of service accounts. If needed, click «, ‹, ›, or » to browse through parts of the list. Click 🗑 to delete the selected service account from HYCU for GCP.

> Caution Before deleting a service account, make sure that it is not assigned to any project linked to the billing account of your HYCU for GCP subscription.

Assigning imported service accounts to projects

Assigning a service account to a project allows using it for identification of automated requests to HYCU for GCP within that project. After such assignment, additional HYCU for GCP features are enabled for the project.

Prerequisites

- The service account is imported into HYCU for GCP.
- On the target project, the service account is granted any Google Cloud Platform role that includes the `resourcemanager.projects.get` permission. Most of the predefined

roles, for example, the Compute Admin and Storage Admin roles, include this permission.

- The target Google Cloud Platform project is selected in the HYCU for GCP web user interface.

> ### Accessing the Assign Service Account dialog box
>
> To access the Assign Service Account dialog box, click ⚙ **Administration** in the toolbar, and then select **Project Service Account**.

To assign a service account to a Google Cloud Platform project, do the following:

1. In the Service Accounts list, select the service account that you want to assign. If needed, click «, ‹ , › , or » to browse through parts of the list.
2. Click **Assign** to assign the selected service account.

A confirmation message indicates successful assignment of the service account to the selected project.

To unassign an imported service account from the currently selected project, in the Assign Service Account dialog box, select its entry from the list of service accounts, and then click **Unassign**.

Configuring event notifications

Notifications in HYCU for GCP are a convenient way of informing about events that occur in your data protection environment. They help you automate monitoring and make your supervision of the data protection activities more efficient. Properly configured notifications enable you to always react in time in situations that require doing so. HYCU for GCP supports two notification transmission methods which you can use independently:

- Email messages
- Webhooks

You configure notifications through a series of notification rules. Each rule defines who should be informed about what kind of events. For this purpose, a rule always includes at least one recipient, one or more categories (functional areas of HYCU for GCP), and one or more statuses (event severity levels) for which the notification should be sent.

For each email-based notification rule, you must specify:

- An email subject line
- Event categories of interest
- Event statuses of interest
- One or more recipients

For each webhook-based notification rule, you must specify:

- A name for the rule
- Event categories of interest
- Event statuses of interest

– Receiving endpoint URL
– *Only if the receiving endpoint requires sender's identification.* Secret token (webhook verification signature)

> ⚠ Important Configured notification rules are effective within the selected Google Cloud Platform project. Each project therefore needs its own configuration of event notifications.

See the following sections for the corresponding instructions:

- "Configuring email-based notifications" below
- "Configuring webhook-based notifications" below

Configuring email-based notifications

This section lists the steps that you must perform to configure email-based notifications.

> Accessing the Notifications dialog box
>
> To access the Notifications dialog box, click **Events** in the navigation pane, and then click 🔔 **Notifications** in the toolbar.

To configure email notifications, follow these steps:

1. In the Notifications dialog box, the Email messages tab is preselected. Click + **New** to create a new notification rule.
2. In the Subject text box, enter text for the email subject line.
3. From the Category drop-down list, select one or more categories. To include all categories, click **Select All**. For description of categories, see section "Viewing events" on page 60.
4. From the Status drop-down list, select one or more statuses. To include all statuses, click **Select All**. For description of statuses, see section "Viewing events" on page 60.
5. In the Email address text box, enter one or more recipients (valid email addresses), separated by space characters.
6. Review the supplied data and click **Save**.

   > Note An email notification rule becomes effective immediately after its configuration is saved.

7. Repeat steps 1 to 6 for each additional notification rule that you need.
8. Click **Close**.

To edit or delete an already configured notification rule, select its entry from the list of email notifications, and then click ✎ **Edit** or 🗑 **Delete** as appropriate.

Configuring webhook-based notifications

This section lists the steps that you must perform to configure webhook-based notifications.

> Accessing the Notifications dialog box
>
> To access the Notifications dialog box, click **Events** in the navigation pane, and then click **Notifications** in the toolbar.

To configure webhook notifications, follow these steps:

1. In the Notifications dialog box, click the **Webhooks** tab.
2. click + **New** to create a new notification rule.
3. In the Name text box, enter a name for the rule.
4. From the Category drop-down list, select one or more categories. To include all categories, click **Select All**. For description of categories, see section "Viewing events" on page 60.
5. From the Status drop-down list, select one or more statuses. To include all statuses, click **Select All**. For description of statuses, see section "Viewing events" on page 60.
6. In the Post URL text box, enter a valid URL of the endpoint the callbacks should be sent to. The URL should match one of the following formats, depending on the actual endpoint address:

   ```
   https://<Host>
   https://<Host>/<Path>
   ```

7. *Only if the receiving endpoint requires sender's identification.* In the Secret text box, enter a valid secret token for authentication. If the receiving endpoint does not perform authentication, the token is ignored.
8. Review the supplied data and then click **Save**.

   > Note A webhook notification rule becomes effective immediately after its configuration is saved.

9. Repeat steps 1 to 6 for each additional notification rule that you need.
10. Click **Close**.

To edit or delete an already configured notification rule, select its entry from the list of webhook notifications, and then click ✎ **Edit** or **Delete** as appropriate.

Excluding instances from synchronization

This section provides information on how to make selected instances invisible to HYCU for GCP.

The needs of your environment may require that some instances are not protected by HYCU for GCP. For example, your Google Cloud Platform projects may include managed instance groups and employ an autoscaler. To leave some instance unprotected, you can exclude them from synchronization so that they are not detected by HYCU for GCP. Undetected instances cannot be assigned backup policies in any way.

To exclude some instances from synchronization in HYCU for GCP, do the following:

1. Choose a Google Cloud Platform project to which instances that you want to leave unprotected belong to.
2. Within the project, chose an instance and add it the "hycu-instance-sync" custom metadata tag in the Google Compute Engine service. Use the following data:

Key	Value
hycu-instance-sync	false

   Custom metadata tags can be added from the Google Cloud Platform Console, the gcloud command line, or by using the Google Cloud Platform API. For instructions, see the Storing and Retrieving Instance Metadata | Compute Engine Documentation | Google Cloud webpage.
3. Repeat step 2 for each additional instance that you want to make invisible to HYCU for GCP.
4. Sign in to the web user interface of HYCU for GCP.
5. Select the same Google Cloud Platform project as you did in step 1 of the procedure. For instructions on selecting projects in HYCU for GCP, see “Selecting a different Google Cloud Platform project” on page 25.
6. In the navigation pane, click 🖵 **Instances**.
7. Click 🗘 **Synchronize** or wait until the next instance synchronization cycle.

   In the Instances panel, the names of the instances that you excluded from synchronization are not present.

Chapter 7

Troubleshooting

If you encounter problems while using HYCU for GCP, you can often solve them yourself. This chapter contains information that may help you in such cases. To get assistance from HYCU Customer Support straight away, see "Getting assistance" on page 76.

We recommend that you use a troubleshooting flow depicted in the following figure.

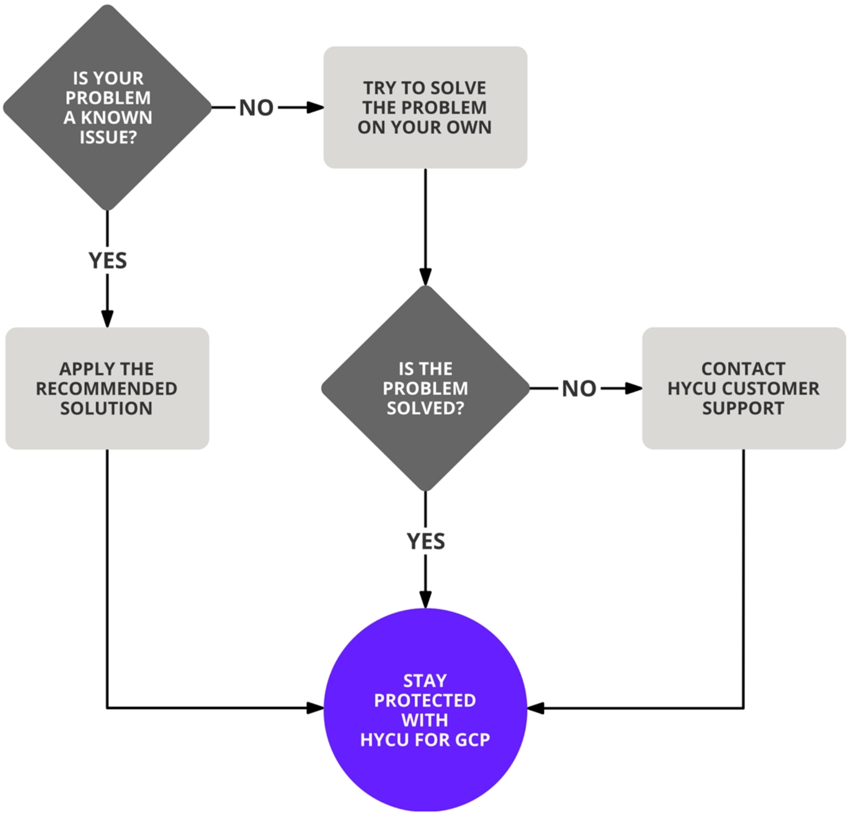

IS YOUR PROBLEM A KNOWN ISSUE?
NO
TRY TO SOLVE THE PROBLEM ON YOUR OWN
YES
APPLY THE RECOMMENDED SOLUTION
IS THE PROBLEM SOLVED?
NO
CONTACT HYCU CUSTOMER SUPPORT
YES
STAY PROTECTED WITH HYCU FOR GCP

Figure 7–1: Overview of the troubleshooting process

General troubleshooting guidelines

When investigating an issue, first verify that:

- All subscription and usage prerequisites are fulfilled, and you performed configuration according to the provided instructions.

- You are not running into a known service limitation. For a list of the limitations, see the *HYCU Backup and Recovery as a Service for GCP Release Notes*.
- Your issue is not related to third-party services (Google Cloud Platform). Otherwise, contact the respective service provider for assistance.
- The affected Google Cloud Platform instances are not running out of memory or storage space.

Problems and solutions

This section lists symptoms of common problems that you may encounter while using HYCU for GCP, together with proposed actions – resolution steps.

Missing Google Cloud Platform projects

Symptoms

In the web user interface, not all of your Google Cloud Platform projects are listed in the project selection dialog box.

Possible resolution steps

The missing projects are not linked to the Google Cloud Platform billing account that was selected in the process of subscribing to the service.

Consult your organization's data protection administrator to choose between the following resolutions:

- In the Google Cloud Platform service suite, link the missing projects to the billing account that was selected for the HYCU for GCP subscription. For instructions, see the Modify a Project's Billing Settings | Cloud Billing Documentation | Google Cloud webpage.
- Subscribe to HYCU for GCP again. In the process, choose the billing account which your missing projects are linked to.

Missing Google Cloud Storage buckets

Symptoms

In the web user interface, when you try to add a user-created bucket to HYCU for GCP, the Bucket drop-down list in the bucket selection dialog box is empty.

Possible resolution steps

In the Google Cloud Storage service, grant your Google Account the `roles/storage.admin` role on the problematic Google Cloud Platform project.

See also the *HYCU Backup and Recovery as a Service for GCP Release Notes*, section *Service requirements*, subsection *Prerequisites for using the service*.

Backup policy assignment failures

Symptoms

After adding the `hycu-policy` metadata tag to an instance in the Google Compute Engine service, no backup policy is assigned to the instance in HYCU for GCP.

The symptom may indicate one of the following:

- No service account is assigned to the affected project in HYCU for GCP.
- The backup policy that is specified for the metadata tag value does not exist.

Possible resolution steps

Find the corresponding entry in the event log to identify the root cause of the problem:

1. In the web user interface of HYCU for GCP, go to the Events panel and search for the following error message:

   ```
   Failed to assign a policy
   ```

2. Click the message entry, check the Message details section for the root cause of the problem, and act accordingly.

Snapshot creation failures

Symptoms

Whenever a backup task for any instance in a specific Google Cloud Platform project is started, the snapshot creation task fails and reports an error.

Possible resolution steps

In the Google Compute Engine service, grant your Google Account the `roles/compute.admin` role on the problematic Google Cloud Platform project.

See also the *HYCU Backup and Recovery as a Service for GCP Release Notes*, section *Service requirements*, subsection *Prerequisites for using the service*.

Inability to restore an instance during backup

Symptoms

While a backup task for an instance is running, you are unable to start a restore task to restore or even just clone the instance.

Possible resolution steps

In HYCU for GCP, one task can run at a time for a particular instance. If you are in a hurry to perform a restore after a data loss or to prepare an instance clone, abort the backup task and then invoke the restore task. Afterward, perform a manual backup for the instance.

Task progress indicator stuck at 0% forever

Symptoms

When you invoke a backup task, its child task for creating disk catalog never makes any progress.

After you invoke a backup task or a restore task, the task gets started but it never makes any progress.

Possible resolution steps

Check if the Google Cloud Platform project that the instance belongs to has the Cloud Pub/Sub API enabled. If it does not, enable the API for the project through the Google Cloud Platform Console.

File-level restore ending with errors or failing

Symptoms

When a restore of individual files or folders completes, the status of the corresponding task is set to `Done With Errors` or `Failed`. Closer inspection reveals that some or all of your selected objects have not been restored.

Possible resolution steps

Most probably the original volume no longer exists. In this case, restore your files or folders to an alternate location on the original instance or to an available bucket.

Inability to change the project or to sign in

Symptoms

Although you have access to multiple Google Cloud Platform projects, there is only the currently selected project available in the Select Google Cloud Platform Project dialog box.

After your web user interface session ends, you are unable to sign in again.

Possible resolution steps

Most probably the Google Account that is used as the organization account lost the required role on the billing account of the service subscription. Contact HYCU Customer Support.

For information on how to prevent the problem from reoccurring, see section "Changing the organization account" on page 66.

Getting assistance

Depending on the required type of assistance, do the following:

- If you need assistance with service evaluation, contact HYCU Customer Support. See section "Support" below.
- If you are already past your free trial period, you have a valid service subscription, and you:
  - Require information about service pricing, see chapter "Service pricing" on page 15.
  - Have an operational issue with the service, see section "Support" below.

Support

If you have an issue with the service, collect the following information before contacting HYCU Customer Support:

- Symptoms that you noticed and the expected behavior
- Date and time when the symptoms appeared first
- Information about recurrence of the problem

The listed pieces of information are required by HYCU Customer Support so that a support engineer can efficiently investigate the issue from the very beginning. When you have the information ready, do one of the following:

- *Preferred.* On the HYCU Customer Support webpage, submit your request (support case) with the information included.
- Send an email with the included information to support@hycu.com.

HYCU Customer Support will contact you shortly.

Getting additional information and latest updates

For additional information about HYCU for GCP, visit the Backup & Recovery for Google Cloud Platform | HYCU webpage.

For the most up-to-date documentation, go to the HYCU Backup and Recovery as a Service for GCP – HYCU Customer Support webpage.

Before contacting HYCU Customer Support

If you cannot solve your issue, report it. Before contacting HYCU Customer Support, make sure that you:

- Perform the general checks. For details, see section "General troubleshooting guidelines" on page 73.
- Verify that your problem is not documented in this chapter. For more information, see section "Problems and solutions" on page 74.
- Collect relevant information that might be required to send to HYCU Customer Support.

For details, see sections “Customer Support” on page 86 and “Getting assistance” on page 76.

HYCU Customer Support will provide you with further instructions.

> Note HYCU Customer Support is not qualified to solve issues with third-party services.

For information on how to reach HYCU Customer Support, see part “HYCU Customer Support and information” on page 86.

Chapter 8

Ceasing service use

At any time, you can decide to cease using HYCU for GCP to protect instances in your projects in the Google Cloud Platform service suite. In this case, you must complete a proper process to eliminate unnecessary costs, keep tight control over access to your Google Account, and cancel service subscription. The process helps you achieve three goals:

1. Stop being charged for the service that you no longer require. For guidance on achieving it, see section "Stopping service charges" below.
2. Prevent further service access to your Google Account. For guidance on achieving it, see section "Preventing account access" on page 82.
3. Unsubscribe from the service. For guidance on achieving it, see section "Canceling service subscription" on page 82.

Stopping service charges

Protection of your Google Cloud Platform data with HYCU for GCP is billed by Google through one or more billing accounts that your projects are linked to. To avoid unnecessary charges for the backup and recovery service, perform the following procedures in the suggested order. Each procedure affects one share of the total data protection cost.

Step	To stop being charged for...	Do the following...
1.	Backup and recovery service cost	In HYCU for GCP, unassign backup policies from all protected instances. For instructions, see "Unassigning backup policies" on the next page.
2.	Backup image storage cost	Remove all backup images from the Google Cloud Storage service. For instructions, see "Removing backup images" on the next page.
3.	Snapshot storage cost	Remove all snapshots created by HYCU for GCP from the Google Compute Engine service (if they exist). For instructions, see "Removing snapshots" on page 81.

Note If you skip the procedures 2 and 3, the costs of backup image storage and

> snapshot storage are still eliminated. This happens automatically, but at a later time.
>
> Alternatively, you can manually mark backup images and their corresponding snapshots as expired. For instructions, see "Manually marking restore points as expired" on page 59.

Unassigning backup policies

To unassign backup policies from all instances of your protected Google Cloud Platform projects, follow these steps:

1. Sign in to the web user interface of HYCU for GCP.
2. Select a Google Cloud Platform project. For instructions, see "Selecting a different Google Cloud Platform project" on page 25.
3. In the web user interface, In the navigation pane, click 🖥 **Instances**.
4. Select all instances, and then click 🛡 **Policies**.
5. Click **Unassign**.
6. Click **Yes** to confirm that you want to unassign the policies from the selected instances.
7. Repeat steps 2 to 7 for each additional Google Cloud Platform project that is protected with HYCU for GCP.

Removing backup images

Removal of backup images of all instances in your protected Google Cloud Platform projects includes:

– Deletion of buckets that were created automatically by HYCU for GCP
– Removal of backup images from your previously existing buckets

> Accessing the Google Cloud Platform Console
>
> To access the Google Cloud Platform Console , open a web browser, go to the Google Cloud including GCP & G Suite — Try Free | Google Cloud webpage, and click **Sign in**. Then sign in with your Google Account.

To delete buckets that were created automatically by HYCU for GCP, follow these steps:

1. In the toolbar of the Google Cloud Platform Console, click ⁂. The Select a project dialog box appears.
2. In the Select a project dialog box, click **ALL** and then click a project name in the Name column.
3. For each automatic bucket, follow instructions on the Deleting Buckets | Cloud Storage Documentation | Google Cloud webpage.

   For information on how automatic buckets are named, see "Objects created by the service" on page 84.

4. Repeat the procedure for each additional Google Cloud Platform project that is protected with HYCU for GCP.

To remove backup images created by HYCU for GCP from your previously existing buckets, follow these steps:

1. Open the Google Cloud Storage browser.
2. In the toolbar of the Google Cloud Platform Console, click ⁂. The Select a project dialog box appears.
3. In the Select a project dialog box, click **ALL**, and then click a project name in the Name column.
4. In the Name column, click the name of your bucket, and then click **hycu/**.
5. Select the checkbox next to the **backups/** folder name, and then click **Delete**.
6. In the overlay window that appears, confirm you want to delete the folder and its contents by clicking **Delete**.
7. For each additional bucket (in the same Google Cloud Platform project) that contains backup images, repeat steps 4 to 6 of this procedure.
8. Repeat steps 2 to 7 for each additional Google Cloud Platform project that is protected with HYCU for GCP.

Removing snapshots

You can remove snapshots created by HYCU for GCP from either the Google Cloud Platform Console or the gcloud command line. For information on how the snapshots are named, see "Objects created by the service" on page 84.

Removing snapshots from the Google Cloud Platform Console

> ### Accessing the Google Cloud Platform Console
>
> To access the Google Cloud Platform Console , open a web browser, go to the Google Cloud including GCP & G Suite — Try Free | Google Cloud webpage, and click **Sign in**. Then sign in with your Google Account.

To remove snapshots of all instances in your protected Google Cloud Platform projects, follow these steps:

1. Open the Google Compute Engine browser, and then click **Snapshots**.
2. In the toolbar of the Google Cloud Platform Console, click ⁂. The Select a project dialog box appears.
3. In the Select a project dialog box, click **ALL**, and then click a project name in the Name column.
4. Select the checkbox of the snapshot you want to delete.
5. Repeat step 4 for each additional snapshot that should be deleted.

6. Click **Delete**.
7. In the overlay window that appears, confirm you want to delete the snapshots by clicking **Delete**.
8. Repeat steps 2 to 7 for each additional Google Cloud Platform project that is protected with HYCU for GCP.

Removing snapshots from the gcloud command line

For instructions, see the Restoring and Deleting Persistent Disk Snapshots | Compute Engine Documentation | Google Cloud webpage.

Preventing account access

When you subscribed to HYCU for GCP, you granted the solution (a third-party app from the perspective of Google) access to your Google Account. After you stop using the solution, you must remove the access permission.

Follow these steps:

1. Open a web browser, go to the Sign in & security page of the Google website, and click **Sign in**.
2. Sign in with your Google Account.
3. Locate the Apps with account access section and click **MANAGE APPS**.
4. Click **HYCU Data Protection**, and then click **REMOVE ACCESS**.
5. Click **OK** to confirm revocation of the access permission.

For general information on permissions to access your Google Account, see the Third-party sites & apps with access to your account - Google Account Help webpage.

Canceling service subscription

Once you unsubscribe from the service, you lose data protection for your Google Cloud Platform projects that are covered by your subscription.

Prerequisites for canceling subscription

Before you unsubscribe from HYCU for GCP, make sure that the following prerequisites are fulfilled:

- You are signed in to Google with a Google Account that is granted the Billing Account Administrator (`roles/billing.admin`) role on the billing account of the service subscription.
- Your currently selected project in the Google Cloud Platform Console is linked to the billing account of the service subscription.

Cancellation procedure

To cancel subscription to HYCU for GCP, follow these steps:

1. Open a web browser and go to the HYCU | Marketplace - Google Cloud Platform webpage.
2. Click **Cancel service**.
3. In the Cancel HYCU subscription dialog box, click **CANCEL SUBSCRIPTION** to confirm your choice.

Appendix A

Objects created by the service

To provide data protection, HYCU for GCP creates specific objects (referred to as *HYCU objects*) in your Google Cloud Platform projects. Some of these objects actually protect original data (snapshots, backup images, automatic buckets), some are the result of a restore (restored files on an instance disk or in a bucket), and others are auxiliary objects that exist only for the duration of a task. All these objects are visible in the Google Cloud Platform user interfaces.

> Caution Apart from the restored files and unless specifically instructed to do so, never rename or delete any HYCU objects through the Google Platform Console or the gcloud command line.

The following table lists names or locations of objects that are created during a backup or restore task, and are preserved afterward.

Table A–1: Permanent HYCU objects

Object type	Name or location path template
Snapshot	`hycu-snap-<TaskID>-<DiskName>`
Automatic bucket	`hycu-<CloudStorageRegionName>-<UUID>`
Bucket folder with one of the following: a backup image, a copy of a backup image, a data archive.	`hycu/backups/<ProjectName>/<InstanceName>/<TaskID>`
Renamed original file (at the original location on the instance)	`<OriginalFileName>.hycu.orig[.<OriginalFileExtension>]`
Renamed restored file (at the original location on an instance)	

`<OriginalFileName>.hycu.restored[.<OriginalFileExtension>]`
Bucket folder with restored individual files or folders
`hycu/restores/<ProjectName>/<InstanceName>/<TaskID>/<DiskName>/<VolumeName>/<PathName>`

The following table lists names of auxiliary objects that exist only for the duration of a task.

Table A–2: Temporary HYCU objects

Object type
Name template
Temporary disk
`hycu-disk-tmp-<TaskID>-<OriginalDiskName>`
Temporary instance[1]
`hycu-instance-tmp-<TaskType>-<TaskID>-<UUID>`

[1] Applicable scenarios: instance rediscovery after access credentials assignment or disk cataloging enablement, backup tasks when disk cataloging is enabled, restore tasks

HYCU Customer Support and information

Use the communication channels listed in this section if you need:

- Help with the service subscription process
- Assistance while using the service
- Additional information about this service
- Information about other HYCU products and services

Customer Support

Should you require additional information or assistance while using the service, contact the vendor that arranged its subscription for you.

If you have subscribed to the service yourself, and are experiencing a problem, search for a solution on the following webpage:
support.hycu.com

In the absence of an article addressing your problem, ask HYCU Customer Support for assistance: on the webpage, sign in with a valid user account, click **Submit a request**, and then fill in the request form. You should have received user account information by email after subscribing to the service.

Important: Before submitting a request to the Customer Support department, have the following information ready:

- Symptoms
- Sequence of events leading to the problem
- Actions that you performed
- Messages that you received (a description with the date and time)

For a complete list of pieces of required support information, check troubleshooting sections in the service documentation.

Company website and video channel

For more information about our company and other products and services we offer, visit HYCU website at:
www.hycu.com

For additional product- or service-related information, watch videos on the HYCU channel on YouTube:
www.youtube.com/c/HYCUInc

General information

For questions related to product or service business, subscription to this service, purchase of other HYCU products, or subscription to other HYCU services, send an email to:
info@hycu.com

Feedback

For comments or suggestions about this service, including its documentation, send an email to:
info@hycu.com

We will be glad to hear from you!

www.hycu.com

HYCU