© 2022 Veeam Software.

All rights reserved. All trademarks are the property of their respective owners.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means, without written permission from Veeam Software (Veeam). The information contained in this document represents the current view of Veeam on the issue discussed as of the date of publication and is subject to change without notice. Veeam shall not be liable for technical or editorial errors or omissions contained herein. Veeam makes no warranties, express or implied, in this document. Veeam may have patents, patent applications, trademark, copyright, or other intellectual property rights covering the subject matter of this document. All other trademarks mentioned herein are the property of their respective owners. Except as expressly provided in any written license agreement from Veeam, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

**NOTE**

Read the End User Software License Agreement before using the accompanying software programs. Using any part of the software indicates that you accept the terms of the End User Software License Agreement.
# Contents

**CONTACTING VEEAM SOFTWARE** ................................................................................................................................. 6  
**ABOUT THIS GUIDE** ................................................................................................................................................. 7  
**WELCOME TO VEEAM BACKUP FOR GOOGLE CLOUD** ................................................................................................. 8  
**INTEGRATION WITH VEEAM BACKUP & REPLICATION** ................................................................................................. 9  
**PLANNING AND PREPARATION** .................................................................................................................................. 10  
  - **Ports** ............................................................................................................................................................................. 10  
  - **Service Account Permissions** ..................................................................................................................................... 11  
    - **Default Permissions** .............................................................................................................................................. 11  
    - **Repository Permissions** ......................................................................................................................................... 11  
    - **Worker Permissions** ............................................................................................................................................... 12  
    - **Snapshot Permissions** ........................................................................................................................................... 16  
    - **Backup Permissions** ............................................................................................................................................... 18  
    - **Restore Permissions** ............................................................................................................................................... 21  
  - **Google Cloud APIs** .................................................................................................................................................... 24  
**LICENSING** ................................................................................................................................................................. 25  
  - **Installing and Removing License** ................................................................................................................................ 26  
  - **Viewing License Information** .................................................................................................................................... 28  
  - **Revoking License Units** ............................................................................................................................................. 29  
**ARCHITECTURE OVERVIEW** ......................................................................................................................................... 30  
**DEPLOYMENT** ............................................................................................................................................................. 34  
  - **Installing Veeam Backup for Google Cloud** .................................................................................................................. 34  
  - **After You Install** ........................................................................................................................................................ 37  
  - **Uninstalling Veeam Backup for Google Cloud** ........................................................................................................... 39  
**ACCESSING VEEAM BACKUP FOR GOOGLE CLOUD** ................................................................................................. 42  
**CONFIGURING VEEAM BACKUP FOR GOOGLE CLOUD** ................................................................................................. 44  
  - **Managing Projects** ...................................................................................................................................................... 45  
    - **Adding Projects** .................................................................................................................................................... 45  
    - **Editing Projects** .................................................................................................................................................... 49  
    - **Removing Projects** ................................................................................................................................................ 50  
  - **Managing Permissions** ................................................................................................................................................ 51  
    - **Adding User Accounts** ........................................................................................................................................... 52  
    - **Editing User Accounts** ......................................................................................................................................... 55  
    - **Changing User Passwords** ................................................................................................................................... 56  
    - **Enabling Multi-Factor Authentication** ................................................................................................................... 57  
  - **Managing Repositories** ............................................................................................................................................. 58  
    - **Adding Backup Repositories** .................................................................................................................................. 58
Contacting Veeam Software

At Veeam Software we value feedback from our customers. It is important not only to help you quickly with your technical issues, but it is our mission to listen to your input and build products that incorporate your suggestions.

Customer Support

Should you have a technical concern, suggestion or question, visit the Veeam Customer Support Portal to open a case, search our knowledge base, reference documentation, manage your license or obtain the latest product release.

Company Contacts

For the most up-to-date information about company contacts and office locations, visit the Veeam Contacts Webpage.

Online Support

If you have any questions about Veeam products, you can use the following resources:

- Full documentation set: veeam.com/documentation-guides-datasheets.html
- Veeam R&D Forums: forums.veeam.com
About This Guide

This guide is designed for IT professionals who plan to use Veeam Backup for Google Cloud. The guide includes system requirements, licensing information and step-by-step deployment instructions. It also provides a comprehensive set of features to ensure easy execution of protection and disaster recovery tasks in Google Cloud environments.
Welcome to Veeam Backup for Google Cloud

Veeam Backup for Google Cloud is a solution developed for protection and disaster recovery tasks for Google Cloud environments. With Veeam Backup for Google Cloud, you can perform the following operations:

- Create image-level backups and cloud-native snapshots of VM instances.
- Create image-level backups and cloud-native snapshots of Cloud SQL instances.
- Keep the backed-up data in cost-effective, long-term Google Cloud storage buckets.
- Restore entire Cloud SQL instances, specific Cloud SQL databases, entire VM instances, individual persistent disks, and guest OS files and folders.
Integration with Veeam Backup & Replication

Google Cloud Plug-in for Veeam Backup & Replication extends the Veeam Backup & Replication functionality and allows you to add Veeam Backup for Google Cloud appliances to the Veeam Backup & Replication infrastructure. With Google Cloud Plug-in for Veeam Backup & Replication, you can manage data protection and disaster recovery operations from the Veeam Backup & Replication console. For more information, see the Integration with Veeam Backup & Replication Guide.
Planning and Preparation

Before you start using Veeam Backup for Google Cloud, consider the following requirements:

- **Network ports that must be open for data transmission**
- **Permissions that must be granted to service accounts used for Veeam Backup for Google Cloud operations**
- **Google Cloud APIs to which Veeam Backup for Google Cloud must have outbound internet access**

## Ports

The following network ports must be open to ensure proper communication of components in the Veeam Backup for Google Cloud infrastructure.

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Protocol</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workstation web browser</td>
<td>Backup appliance</td>
<td>TCP</td>
<td>443</td>
<td>Required to access the Web UI component from a user workstation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP</td>
<td>13140</td>
<td>Required to communicate with the REST API service running on the backup appliance.</td>
</tr>
<tr>
<td>Worker instance</td>
<td>TCP 443</td>
<td></td>
<td></td>
<td>Required to access the File-Level Restore browser running on a worker instance during the file-level recovery process.</td>
</tr>
<tr>
<td>Backup appliance</td>
<td>Ubuntu Security Update Repository (security.ubuntu.com)</td>
<td>HTTP</td>
<td>80</td>
<td>Required to get OS security updates.</td>
</tr>
<tr>
<td></td>
<td>Veeam Update Notification Server (repository.veeam.com)</td>
<td>TCP</td>
<td>443</td>
<td>Required to download information on available product updates.</td>
</tr>
<tr>
<td>SMTP server</td>
<td>TCP 587</td>
<td></td>
<td></td>
<td>Required to send email notifications.</td>
</tr>
</tbody>
</table>

**Note:** You cannot use the TCP port 25 that is most commonly used by SMTP servers — the port is always blocked by Google Compute Engine. For more information, see Google Cloud documentation.
Service Account Permissions

Google Cloud Identity and Access Management (IAM) roles that Veeam Backup for Google Cloud uses to perform data protection and disaster recovery operations must have permissions to access Google Cloud services and resources.

Default Permissions

Veeam Backup for Google Cloud requires a service account in each Google Cloud project where data protection and disaster recovery tasks will be performed. To allow Veeam Backup for Google Cloud to access Google Cloud services and resources that you want to protect, service accounts used by Veeam Backup for Google Cloud must have the following minimal set of permissions:

```
compute.disks.addResourcePolicies
compute.disks.get
compute.instances.get
compute.resourcePolicies.create
compute.resourcePolicies.get
compute.resourcePolicies.use
compute.zones.get
serviceusage.services.list
compute.projects.get
```

Repository Permissions

To allow Veeam Backup for Google Cloud to create a backup repository in a Google Cloud storage bucket and to access the repository when performing backup and restore operations, the service account associated with the Google Cloud project in which this bucket resides must have the following permissions:

```
storage.buckets.list
storage.buckets.get
storage.objects.create
storage.objects.delete
storage.objects.list
storage.objects.get
storage.hmacKeys.create
storage.hmacKeys.list
storage.hmacKeys.get
resourcemanager.projects.get
serviceusage.services.list
storage.buckets.getIamPolicy
storage.buckets.setIamPolicy *
compute.projects.get
```

* Veeam Backup for Google Cloud will use the `storage.buckets.setIamPolicy` permission only to grant access to repositories while performing SQL backup operations.
Worker Permissions

To allow Veeam Backup for Google Cloud to create a worker instance in a Google Cloud project and to access the instance when performing backup and restore operations, the service account associated with the project must have the following permissions:

VM Backup and Restore Permissions

```plaintext
compute.regions.list
compute.disks.list
compute.instances.get
compute.instances.list
compute.snapshots.get
compute.snapshots.list
compute.zones.get
compute.zones.list
compute.globalOperations.get
compute.zoneOperations.get
compute.regionOperations.get
resourcemanager.projects.get
compute.projects.get
compute.firewalls.list
compute.snapshots.getIamPolicy
compute.networks.list
compute.subnetworks.list
resourcemanager.projects.getIamPolicy
resourcemanager.projects.setIamPolicy *
iam.serviceAccounts.actAs
compute.disks.create
compute.disks.createSnapshot
compute.disks.delete
compute.disks.setLabels
compute.instances.attachDisk
compute.instances.create
compute.instances.delete
compute.instances.detachDisk
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.instances.setLabels
compute.instances.setTags
compute.routes.list
compute.regions.get
compute.snapshots.create
compute.snapshots.setLabels
compute.snapshots.setIamPolicy
compute.snapshots.delete
pubsub.subscriptions.consume
pubsub.subscriptions.create
pubsub.subscriptions.delete
pubsub.subscriptions.list
pubsub.subscriptions.get
```
logging.sinks.get
logging.sinks.delete
logging.sinks.list
pubsub.topics.attachSubscription
pubsub.topics.detachSubscription
pubsub.topics.create
pubsub.topics.delete
pubsub.topics.list
pubsub.topics.get
pubsub.topics.publish
compute.machineTypes.get
compute.machineTypes.list
compute.subnetworks.get
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.disks.use
serviceusage.services.list

* Veeam Backup for Google Cloud will use the resourcemanager.projects.setIamPolicy permission only to assign the
cloudsql.instances.get and cloudsql.instances.restoreBackup permissions to service accounts while
performing backup operations.

**IMPORTANT**

To allow Veeam Backup for Google Cloud to connect a created worker instance to a Shared VPC network, the
service account associated with the Google Cloud project where the instance belongs must also have either
the compute.networkUser role for the whole Shared VPC host project, or the compute.networkViewer
role for the whole host project plus compute.networkUser for specific subnets in the host project.

To learn how to provide access to Shared VPC networks, see Google Cloud documentation.
Cloud SQL Backup and Restore Permissions

compute.regions.list
compute.disks.list
compute.instances.get
compute.instances.list
compute.snapshots.get
compute.snapshots.list
compute.zones.get
compute.zones.list
compute.globalOperations.get
compute.zoneOperations.get
compute.regionOperations.get
resourcemanager.projects.get
compute.projects.get
compute.firewalls.list
compute.snapshots.getIamPolicy
compute.networks.list
compute.subnetworks.list
resourcemanager.projects.getIamPolicy
resourcemanager.projects.setIamPolicy *
iam.serviceAccounts.actAs
compute.disks.create
compute.disks.createSnapshot
compute.disks.delete
compute.disks.setLabels
compute.instances.attachDisk
compute.instances.create
compute.instances.delete
compute.instances.detachDisk
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.instances.setLabels
compute.instances.setTags
compute.routes.list
compute.regions.get
compute.snapshots.create
compute.snapshots.setLabels
compute.snapshots.setIamPolicy
compute.snapshots.delete
pubsub.subscriptions.consume
pubsub.subscriptions.create
pubsub.subscriptions.delete
pubsub.subscriptions.list
pubsub.subscriptions.get
logging.sinks.get
logging.sinks.delete
logging.sinks.list
pubsub.topics.attachSubscription
pubsub.topics.detachSubscription
pubsub.topics.create
pubsub.topics.delete
pubsub.topics.list
pubsub.topics.get
pubsub.topics.publish
compute.machineTypes.get
compute.machineTypes.list
compute.subnetworks.get
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.disks.use
serviceusage.services.list
cloudsql.databases.list
cloudsql.instances.create
cloudsql.instances.delete
cloudsql.instances.export
cloudsql.instances.get
cloudsql.instances.list
cloudsql.instances.listServerCas
cloudsql.users.create
cloudsql.users.list
compute.projects.get
Snapshot Permissions

To allow Veeam Backup for Google Cloud to create and manage cloud-native snapshots of Google Cloud instances, the service account associated with the Google Cloud project managing instances that you want to protect must have the following permissions.

VM Snapshot Permissions

```python
compute.addresses.list
calculate.firewalls.list
calculate.regions.list
calculate.disks.list
calculate.disks.createSnapshot
calculate.disks.get
calculate.instances.get
calculate.instances.list
calculate.networks.list
calculate.projects.get
calculate.snapshots.create
calculate.snapshots.delete
calculate.snapshots.get
calculate.snapshots.list
calculate.subnetworks.list
calculate.routes.list
calculate.zones.list
calculate.globalOperations.list
calculate.globalOperations.get
calculate.zoneOperations.get
calculate.regionOperations.get
resourceManager.projects.get
calculate.snapshots.setLabels
logging.sinks.create
logging.sinks.delete
logging.sinks.get
logging.sinks.list
logging.sinks.update
pubsub.subscriptions.create
pubsub.subscriptions.delete
pubsub.subscriptions.get
pubsub.subscriptions.list
pubsub.subscriptions.consume
pubsub.topics.attachSubscription
pubsub.topics.create
pubsub.topics.delete
pubsub.topics.detachSubscription
pubsub.topics.get
pubsub.topics.getIamPolicy
pubsub.topics.list
pubsub.topics.setIamPolicy
pubsub.topics.update
```
Cloud SQL Snapshot Permissions

cloudsql.backupRuns.create
cloudsql.backupRuns.delete
cloudsql.backupRuns.get
cloudsql.backupRuns.list
cloudsql.databases.list
cloudsql.instances.get
cloudsql.instances.list
compute.regions.list
compute.zones.list
logging.sinks.create
logging.sinks.delete
logging.sinks.get
logging.sinks.get
logging.sinks.list
pubsub.subscriptions.consume
pubsub.subscriptions.create
pubsub.subscriptions.delete
pubsub.subscriptions.get
pubsub.subscriptions.list
pubsub.subscriptions.list
pubsub.topics.attachSubscription
pubsub.topics.create
pubsub.topics.delete
pubsub.topics.detachSubscription
pubsub.topics.get
pubsub.topics.getIamPolicy
pubsub.topics.list
pubsub.topics.setIamPolicy
serviceusage.services.list
compute.projects.get
 Backup Permissions

To allow Veeam Backup for Google Cloud to perform backup operations, the service account associated with the Google Cloud project managing instances that you want to protect must have the following permissions.

VM Backup Permissions

```plaintext
compute.addresses.list
compute.regions.list
compute.disks.list
compute.disks.createSnapshot
compute.disks.get
compute.instances.get
compute.instances.list
compute.snapshots.create
compute.snapshots.delete
compute.snapshots.get
compute.snapshots.list
compute.snapshots.getIamPolicy
compute.snapshots.setIamPolicy
compute.snapshots.setLabels
compute.subnetworks.list
compute.routes.list
compute.machineTypes.get
compute.zones.list
compute.globalOperations.list
compute.globalOperations.get
compute.zoneOperations.get
compute.regionOperations.get
compute.projects.get
compute.regions.get
compute.networks.list
compute.firewalls.list
resourcemanager.projects.get
resourcemanager.projects.getIamPolicy
logging.sinks.create
logging.sinks.delete
logging.sinks.get
logging.sinks.list
logging.sinks.update
pubsub.subscriptions.create
pubsub.subscriptions.delete
pubsub.subscriptions.get
pubsub.subscriptions.list
pubsub.subscriptions.consume
pubsub.topics.attachSubscription
pubsub.topics.create
pubsub.topics.delete
pubsub.topics.detachSubscription
pubsub.topics.get
pubsub.topics.getIamPolicy
pubsub.topics.list
```
IMPORTANT

To allow Veeam Backup for Google Cloud to back up a VM instance connected to a Shared VPC network, the service account associated with the project where the instance belongs must also have either the `compute.networkUser` role for the whole Shared VPC host project, or the `compute.networkViewer` role for the whole host project plus `compute.networkUser` for specific subnets in the host project.

To learn how to provide access to Shared VPC networks, see Google Cloud documentation.
Cloud SQL Backup Permissions

cloudsql.backupRuns.create
cloudsql.backupRuns.delete
cloudsql.backupRuns.get
cloudsql.backupRuns.list
cloudsql.databases.list
cloudsql.instances.export
cloudsql.instances.get
cloudsql.instances.list
cloudsql.instances.listServerCas
cloudsql.instances.update
cloudsql.users.list
compute.regions.list
compute.zones.list
logging.sinks.create
logging.sinks.delete
logging.sinks.get
logging.sinks.get
logging.sinks.list
pubsub.subscriptions.consume
pubsub.subscriptions.create
pubsub.subscriptions.delete
pubsub.subscriptions.get
pubsub.subscriptions.list
pubsub.subscriptions.list
pubsub.topics.attachSubscription
pubsub.topics.create
pubsub.topics.delete
pubsub.topics.detachSubscription
pubsub.topics.get
pubsub.topics.getIamPolicy
pubsub.topics.list
pubsub.topics.setIamPolicy
serviceusage.services.list
compute.projects.get
Restore Permissions

To allow Veeam Backup for Google Cloud to perform restore operations, the service account associated with the Google Cloud project that will be used to manage the restored instances must have the following permissions.

VM Restore Permissions

```
compute.addresses.list
compute.disks.create
compute.disks.get
compute.disks.setLabels
compute.disks.use
compute.disks.delete
compute.disks.useReadOnly
compute.firewalls.list
compute.globalOperations.list
compute.globalOperations.get
compute.instances.create
compute.instances.delete
compute.instances.get
compute.instances.setLabels
compute.instances.setMachineResources
compute.instances.setMetadata
compute.instances.setMinCpuPlatform
compute.instances.setScheduling
compute.instances.setServiceAccount
compute.instances.setTags
compute.instances.start
compute.instances.stop
compute.instances.updateDisplayDevice
compute.instances.updateNetworkInterface
compute.instances.setDeletionProtection
compute.machineTypes.list
compute.networks.list
compute.projects.get
compute.regionOperations.get
compute.regions.get
compute.regions.list
compute.snapshots.create
compute.snapshots.delete
compute.snapshots.get
compute.snapshots.getIamPolicy
compute.snapshots.list
compute.snapshots.setLabels
compute.snapshots.useReadOnly
compute.subnetworks.list
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zones.get
compute.zones.list
iam.serviceAccounts.actAs
```
iamb.serviceAccounts.list
resourcemanager.projects.get
cloudkms.cryptoKeys.list
cloudkms.keyRings.list
compute.addresses.use
compute.addresses.useInternal
compute.disks.list
compute.instances.list
compute.routes.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.cryptoKeys.getIamPolicy
serviceusage.services.list

**IMPORTANT**

- To allow Veeam Backup for Google Cloud to perform restore to the original location while source VM instances still exist there, you must also add the permission `compute.instances.setIamPolicy`. The ability to rename VM instances is currently in pre-GA state. For more information, see Google Cloud documentation.

- To allow Veeam Backup for Google Cloud to connect a restored VM instance to a Shared VPC network, the service account associated with the project where the instance belongs must also have either the `compute.networkUser` role for the whole Shared VPC host project, or the `compute.networkViewer` role for the whole host project plus `compute.networkUser` for specific subnets in the host project.
To learn how to provide access to Shared VPC networks, see Google Cloud documentation.
Cloud SQL Restore Permissions

cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.list
cloudsql.backupRuns.get
cloudsql.instances.create
cloudsql.instances.get
cloudsql.instances.import
cloudsql.instances.restoreBackup
compute.firewalls.list
compute.networks.list
compute.projects.get
compute.regions.list
compute.routes.list
compute.subnetworks.list
compute.zones.list
cloudsql.backupRuns.list
cloudsql.databases.create
cloudsql.databases.list
cloudsql.instances.list
cloudsql.users.create
cloudsql.users.list
pubsub.subscriptions.consume
pubsub.subscriptions.create
pubsub.subscriptions.delete
pubsub.subscriptions.get
pubsub.subscriptions.list
pubsub.topics.attachSubscription
pubsub.topics.create
pubsub.topics.delete
pubsub.topics.detachSubscription
pubsub.topics.get
pubsub.topics.list
serviceusage.services.list
cloudsql.backupRuns.create
cloudsql.backupRuns.delete
cloudsql.databases.get
Google Cloud APIs

The backup appliance and worker instances must have outbound internet access to the following Google Cloud APIs:

- Compute Engine API
- Service Usage API
- IAM Service Account Credentials API
- Identity and Access Management (IAM) API
- Cloud Resource Manager API
- Cloud Billing API
- Pub/Sub API
- Cloud Key Management Service API
- Cloud Logging API
Licensing

Veeam Backup for Google Cloud is licensed by the number of protected instances. An instance is defined as a single Google Cloud resource — a VM instance or Cloud SQL instance. An instance is considered to be protected if it has a restore point (snapshot or backup) created by a backup policy during the past 31 days. Each protected instance consumes one license unit from the license scope. However, if an instance has only snapshots created manually, it does not consume any license units.

**NOTE**
If an instance has not been backed up within the past 31 days, Veeam Backup for Google Cloud automatically revokes the license unit from the instance. If you need to manually revoke a license unit, follow the instructions provided in section *Revoking License Units*.

Veeam Backup for Google Cloud is available in 2 license editions:

- **Free License**
  By default, Veeam Backup for Google Cloud operates in the *Free* edition that allows you to protect up to 10 instances free of charge.

- **BYOL (Bring Your Own License)**
  The *BYOL* (Bring Your Own License) edition is a subscription-based license that expires at the end of the subscription term. The maximum number of instances managed by Veeam Backup for Google Cloud depends on the number of units specified in your license. To learn how to obtain the license, contact a Veeam sales representative at *Sales Inquiry*.

  When the license expires, Veeam Backup for Google Cloud offers a grace period to ensure a smooth license update and to provide sufficient time to install a new license file. The duration of the grace period is 30 days after the expiration of the license. During this period, you can perform all types of data protection and disaster recovery operations. After the grace period is over, Veeam Backup for Google Cloud stops processing all instances and disables all scheduled backup policies. You must update your license before the end of the grace period.

  To learn how to install and update the license, see *Installing and Removing License*.

**NOTE**
Veeam Backup & Replication licensing is applied to Veeam Backup for Google Cloud appliances managed by standalone Veeam Backup & Replication servers. For more information, see the *Integration with Veeam Backup & Replication Guide*.
Installing and Removing License

NOTE
This section applies only to the BYOL edition of Veeam Backup for Google Cloud.

Installing License

To install or update a license installed on the backup appliance, do the following:

1. Switch to the Configuration page.
2. Navigate to License > License Info.
3. Click Install license.
4. In the Upload File window, click Browse to browse to a license file, and then click Upload.
Removing License

To remove a license installed on the backup appliance if you no longer need it, do the following:

1. On the License Info tab, click Remove License.
2. In the Remove License window, click Yes to confirm that you want to remove the license.

After you remove the license, Veeam Backup for Google Cloud will automatically switch back to the Free edition. In this case, according to the FIFO (first-in first-out) queue, only the first 10 instances registered in the configuration database will remain protected. You can revoke license units from these instances as described in section Revoking License Units.
Viewing License Information

To view details on the license that is currently installed on the backup appliance, do the following:

1. Switch to the Configuration page.
2. Navigate to License > License Info.

The License Info tab provides general information on the Veeam Backup for Google Cloud license:

- **Status** — the license status. The status depends on the license edition, the number of days remaining until license expiration and the number of days remaining in the grace period (if any).

- **Instances** — the total number of protected instances that consume license units. Each instance that has a restore point created in the past 31 days is considered to be protected and consumes one license unit. To view the list of instances that consume license units, switch to the License Usage tab.

- **Expiration Date** — the date when the license will expire.

- **License Type** — the license edition (Free, Subscription).

**NOTE**

Subscription is the name of the BYOL license in Veeam Backup for Google Cloud.

- **License ID** — the unique identification number of the provided license file (required for contacting the Veeam Customer Support Team).

- **Licensed To** — the name of an organization to which the license was issued.

- **Support ID** — the unique identification number of the support contract (required for contacting the Veeam Customer Support Team).
Revoking License Units

By default, Veeam Backup for Google Cloud automatically revokes a license unit from a protected instance if no new restore points have been created by the backup policy during the past 31 days. However, you can manually revoke license units from protected instances — this can be helpful, for example, if you remove a number of instances from a backup policy and do not want to protect them anymore.

To revoke a license unit from an instance, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **License > License Usage**.
3. Select the instance that you no longer want to protect.
4. Click **Revoke License**.
5. In the **Revoke License** window, click **Yes** to confirm that you want to revoke the license unit.
Architecture Overview

The Veeam Backup for Google Cloud infrastructure includes the following components:

- **Backup appliance**
- **Backup repositories**
- **Worker instances**

### Backup Appliance

The backup appliance is a Linux-based VM instance where Veeam Backup for Google Cloud is installed. The backup appliance performs the following administrative activities:

- Manages infrastructure components.
- Coordinates snapshot creation, backup and recovery tasks.
- Controls backup policy scheduling.
- Generates daily reports and email notifications.

The backup appliance also maintains the configuration database that stores data collected from the Veeam Backup for Google Cloud infrastructure for the existing backup policies, protected VM instances and Cloud SQL instances, deployed worker instances, connected Google Cloud projects and so on.

### Backup Repositories

A backup repository is a Google Cloud storage bucket where Veeam Backup for Google Cloud stores backups of protected VM instances and Cloud SQL instances.

To communicate with a backup repository, Veeam Backup for Google Cloud uses **Veeam Data Mover** — the service that runs on a worker instance and that is responsible for data processing and transfer. When a backup policy addresses the backup repository, the Veeam Data Mover establishes a connection with the repository to enable data transfer.

**IMPORTANT**

Backup files are stored in backup repositories in the native Veeam format and must be modified neither manually nor by 3rd party tools. Otherwise, Veeam Backup for Google Cloud may fail to restore the backed-up data.

### Encryption on Repositories

For enhanced data security, Veeam Backup for Google Cloud allows you to enable encryption at the repository level. Veeam Backup for Google Cloud uses the same encryption standards as Veeam Backup & Replication to encrypt backup files stored in backup repositories. To learn what encryption standards Veeam Backup & Replication uses to encrypt its data, see the Veeam Backup & Replication User Guide, section **Encryption Standards**.

To learn how to enable encryption at the repository level, see **Enabling Data Encryption**.
Limitations for Repositories

To use a storage bucket as a target location for backups, you must connect to a project in which this bucket resides, as described in section Adding Backup Repositories.

Veeam Backup for Google Cloud allows you to store backups only in the Standard Storage and Archive Storage classes. The Nearline Storage and Coldline Storage classes are not supported. For more information on storage classes offered by Cloud Storage, see Google Cloud documentation.

Worker Instances

A worker instance is an auxiliary Linux-based VM instance that is responsible for the interaction between the backup appliance and other components of the Veeam Backup for Google Cloud infrastructure. Worker instances process backup workload and distribute backup traffic when transferring data to and from backup repositories.

Veeam Backup for Google Cloud automatically deploys a worker instance in Google Cloud for the duration of a backup or restore process, and removes it immediately as soon as the process is over. To minimize cross-region traffic charges and to speed up the data transfer, depending on the performed operation, Veeam Backup for Google Cloud deploys the worker instance in the following location:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Worker Instance Location</th>
<th>Default Worker Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating image-level backups of VM instances</td>
<td>Google Cloud region in which a processed VM instance resides</td>
<td>e2-highcpu-8, with an additional empty standard persistent (pd-standard) disk up to 4000 GB in size</td>
</tr>
<tr>
<td>Creating image-level backups of Cloud SQL instances</td>
<td>Google Cloud region in which a target standard backup repository resides</td>
<td>e2-highcpu-8</td>
</tr>
<tr>
<td>Creating image-level backups of Cloud SQL instances using a staging server</td>
<td>Google Cloud region in which a source Cloud SQL instance resides</td>
<td>db-n1-standard-4</td>
</tr>
<tr>
<td>Creating archived image-level backups of VM instances</td>
<td>Google Cloud region in which a processed VM instance resides</td>
<td>e2-standard-4</td>
</tr>
<tr>
<td>Creating archived image-level backups of Cloud SQL instances</td>
<td>Google Cloud region in which a target standard backup repository resides</td>
<td>e2-standard-4</td>
</tr>
<tr>
<td>Performing health check for created restore points</td>
<td>Google Cloud region in which a target standard backup repository resides</td>
<td>e2-standard-4</td>
</tr>
<tr>
<td>Applying retention policy settings to created restore points</td>
<td>Google Cloud region in which a backup repository with backed-up data resides</td>
<td>e2-highcpu-8</td>
</tr>
</tbody>
</table>
Worker instances are deployed based on worker configurations and profiles that can be created either automatically by Veeam Backup for Google Cloud, or manually by the user as described in section Managing Workers.

**IMPORTANT**

For Veeam Backup for Google Cloud to deploy the number of worker instances required for a backup or restore process, you must have enough resource quotas allocated between your projects. To learn how to check your quotas, see [Google Cloud documentation](https://cloud.google.com/).  

**Worker Instance Components**

A worker instance uses the following components:

- **Veeam Data Mover** — the service that performs data processing tasks. During backup, the Veeam Data Mover retrieves data from snapshots and stores the retrieved data to backup repositories. During restore, the Veeam Data Mover transfers backed-up data from backup repositories to the target location.

- **File-Level Restore Browser** — the web service that allows you to find and save files and folders of a backed-up VM instance to a local machine. The File-Level Restore browser is installed automatically on every worker instance that is launched for file-level recovery.

For more information on recovering files of VM instances with the File-Level Restore browser, see [Performing File-Level Recovery](https://www.veeam.com/).
Security Certificates for Worker Instances

Veeam Backup for Google Cloud uses self-signed TLS certificates to establish secure communication between the web browser on a user workstation and the File-Level Restore browser running on a worker instance during the file-level recovery process. A self-signed certificate is generated automatically on the worker instance when the recovery session starts.
Deployment

Veeam Backup for Google Cloud comes as an image of a Linux-based VM that you can deploy from Google Cloud Marketplace.

Installing Veeam Backup for Google Cloud

Veeam Backup for Google Cloud is installed on a VM instance that is created in Google Cloud during the product installation.

To install Veeam Backup for Google Cloud, do the following:

1. Log in to Google Cloud Marketplace using credentials of a Google account that has the Editor role granted. To learn how to manage user roles in the Google Cloud Console, see Google Cloud documentation.

2. Click Explore the marketplace.

3. In the search field, enter Veeam Backup for Google Cloud and press [Enter] on the keyboard.

4. In the list of search results, click Veeam Backup for Google Cloud to open the product overview page.

5. Click Launch.

6. On the New Veeam Backup for Google Cloud deployment page, configure the following installation settings:
   a. Select a project where the VM instance running Veeam Backup for Google Cloud will belong.

   IMPORTANT

   Make sure that Google Cloud APIs listed in the Planning and Preparation section are enabled for the selected project. Otherwise, Veeam Backup for Google Cloud deployment may fail or cause unexpected errors. To learn how to enable APIs for Google Cloud projects, see Google Cloud documentation.
b. In the **Deployment name** field, enter a name for the new Veeam Backup for Google Cloud deployment.

The deployment will include the VM instance running Veeam Backup for Google Cloud, the Google Cloud service account used by the VM instance to access Google Cloud APIs, firewall rules defined to allow traffic to and from the VM instance, and other configuration details specified during installation.

c. From the **Zone** drop-down list, select an availability zone within a Google Cloud region in which the VM instance running Veeam Backup for Google Cloud will reside.

To learn how to configure availability and redundancy settings for Google Cloud resources, see [Google Cloud documentation](https://cloud.google.com/).

d. In the **Machine type** section, specify the number of vCPUs and the amount of memory on Compute Engine that will be allocated to the VM instance running Veeam Backup for Google Cloud.

The recommended hardware requirement for a VM instance running Veeam Backup for Google Cloud is an n1-standard-2 instance with 2 vCPUs and 7.5 GB RAM.

e. In the **Disks** section, specify the size of a boot disk that will be attached to the VM instance running Veeam Backup for Google Cloud, and the size of an additional data disk where the application database and logs will be stored.
f. In the **Networking** section, specify a VPC network and a subnet to which the VM instance running Veeam Backup for Google Cloud will be connected.

For a VPC network and a subnet to be displayed in the lists of available networks, they must be created in the Google Cloud Console for the region specified at step 6c, as described in [Google Cloud documentation](https://cloud.google.com).

**IMPORTANT**

Consider the following:

- The specified VPC network and subnet must have the outbound internet access to Google Cloud APIs listed in the **Planning and Preparation** section. Otherwise, Veeam Backup for Google Cloud will not work properly.
- The specified VPC network and subnet must allow the inbound internet access from a local machine that you plan to use to work with Veeam Backup for Google Cloud.

To learn how to enable internet access for VPC networks and subnets, see [Google Cloud documentation](https://cloud.google.com).

If there are no firewall rules that allow inbound HTTPS traffic in the specified network, you must select the **Allow HTTPS traffic from the internet** and specify the allowed IP address ranges explicitly.

If you want to connect to Veeam Backup for Google Cloud through SSH or use the Veeam Backup for Google Cloud REST API, you must select the **Allow SSH traffic from the internet** or **Allow public API traffic from the internet** check box and specify the allowed IP address ranges.

**TIP**

The IPv4 address ranges must be specified in the CIDR notation (for example, `12.23.34.0/24`). To let all IPv4 addresses access the VM instance running Veeam Backup for Google Cloud, you can enter `0.0.0.0/0`. However, note that allowing access from all IPv4 addresses is unsafe and thus not recommended in production environments.

g. Click **Deploy** to begin installation.
After installation completes, the **Suggested next steps** section will display a link to the Veeam Backup for Google Cloud interface. Click the link to proceed to the **initial configuration** required to start working with Veeam Backup for Google Cloud.

### After You Install

To start working with Veeam Backup for Google Cloud, you must perform the initial configuration of the backup appliance:

1. In a web browser, navigate to the Veeam Backup for Google Cloud web address.
   
   The address consists of a public IPv4 address or DNS hostname of the backup appliance. Note that the website is available over HTTPS only.

   **IMPORTANT**

   Internet Explorer is not supported. To access Veeam Backup for Google Cloud, use Microsoft Edge (version 40 or later), Mozilla Firefox (version 56 or later) or Google Chrome (version 62 or later).

2. Read and accept the Veeam license agreement, Veeam licensing policy, 3rd party components and software license agreements. If you reject the terms and conditions, you will not be able to continue installation.

3. In the **Instance ID** field, specify the unique numeric identifier of the VM instance running Veeam Backup for Google Cloud to prove that you are the owner of this VM instance.

   To obtain the ID assigned to the VM instance upon creation, you can either look it up on the **Instances** page in the Google Cloud Console, or send a query to the metadata server API using the gcloud command-line tool. To learn how to retrieve instance metadata, see Google Cloud documentation.

4. Create the Default Administrator account whose credentials you will use for your first login to Veeam Backup for Google Cloud.

   **NOTE**

   To increase the security of the Default Administrator account, it is recommended that you enable multi-factor authentication (MFA) for the account after you first log in to Veeam Backup for Google Cloud. To learn how to enable MFA, see Enabling Multi-Factor Authentication.
5. Log in to Veeam Backup for Google Cloud with the credentials of the Default Administrator account, as described in section Accessing Veeam Backup for Google Cloud.

You will immediately receive a warning in the notification area notifying that the service account used to install Veeam Backup for Google Cloud does not have the permissions required to perform data protection tasks for the project specified during the product installation. To eliminate the warning, do the following:

a. Click the link in the notification area.

Alternatively, you can switch to the Configuration page, navigate to Permissions > Projects, select the project and click Edit.

b. In the Edit Project wizard, at the Service Account step, click Generate and download script. Veeam Backup for Google Cloud will generate a gcloud script — run this script using the gcloud command-line tool to assign all the necessary permissions to the service account.

The account under which you run the script must have the permissions both to get and set project IAM policies and to create custom IAM roles (for example, it can have the iam.securityAdmin and iam.roleAdmin roles assigned). To learn what permissions and roles are required to create custom roles in IAM, see Google Cloud documentation.

At the Summary step of the wizard, review configuration information and click Finish to confirm the changes.

c. If you want Veeam Backup for Google Cloud to collect data on Shared VPC networks for the project where the backup appliance belongs, the service account must also have the permissions described in Service Account Permissions.

TIP
You can click Check Permissions to ensure that the account now has all the permissions required to perform data protection tasks for the project.

Note that it may take some time for Google Cloud to apply the changes to the account, and the permission check may display the permissions as missing right after you click Check Permissions. To work around the issue, try checking permissions once again in 5–10 minutes.
Uninstalling Veeam Backup for Google Cloud

Veeam Backup for Google Cloud creates a number of resources while operating in Google Cloud, and these resources are not removed from the Google Cloud infrastructure automatically when you uninstall the solution. That is why you must perform the following steps to uninstall Veeam Backup for Google Cloud:

1. Locate and save the unique numeric identifier of the VM instance running Veeam Backup for Google Cloud — you will need it later.
   
   To obtain the ID, you can either look it up on the **Instances** page in the Google Cloud Console, or send a query to the metadata server API using the gcloud command-line tool. To learn how to retrieve instance metadata, see Google Cloud documentation.

2. Save the names of Google Cloud projects that have ever been added to Veeam Backup for Google Cloud — you will need it later.
   
   To obtain the names, you can look them up on the **Permissions > Projects** page in the Veeam Backup for Google Cloud UI.

3. Log in to **Google Cloud Marketplace** using credentials of the Google account that you used to install Veeam Backup for Google Cloud.

4. Navigate to **Your products**.

5. Click **Veeam Backup for Google Cloud** to open the product overview page.

6. Click **Delete**.

7. Wait until Veeam Backup for Google Cloud is removed from your organization domain.

8. Navigate to **IAM & Admins > IAM**.

   In the list of permissions, locate the **deleted:serviceAccount:veeam** member, and then unassign all existing roles from this member.

In the list of roles, locate the role with the ID of the VM instance that was running Veeam Backup for Google Cloud in its name, and then delete this role.

**NOTE**

It may take up to one week for the role to be deleted.


In the list of logs router sinks, locate all sinks with the Cloud Pub/Sub topic type created by Veeam Backup for Google Cloud (these sinks will have the ID of the VM instance that was running Veeam Backup for Google Cloud in their names), and then delete these sinks.

11. Navigate to Pub/Sub > Subscriptions.

In the list of subscriptions, locate all subscriptions created by Veeam Backup for Google Cloud (these subscriptions will have the ID of the VM instance that was running Veeam Backup for Google Cloud in their names), and then delete these subscriptions.
12. Navigate to **Pub/Sub > Topics**. In the list of topics, locate all topics created by Veeam Backup for Google Cloud (these topics will have the ID of the VM instance that was running Veeam Backup for Google Cloud in their names), and then delete these topics.

13. Repeat steps 8–12 for each project that has ever been added to Veeam Backup for Google Cloud.
Accessing Veeam Backup for Google Cloud

To access Veeam Backup for Google Cloud, do the following:

1. In a web browser, navigate to the Veeam Backup for Google Cloud web address.

   **IMPORTANT**
   Internet Explorer is not supported. To access Veeam Backup for Google Cloud, use Microsoft Edge (latest version), Mozilla Firefox (latest version) or Google Chrome (latest version).

   The address consists of a public IPv4 address or DNS hostname of the backup appliance. Note that the website is available over HTTPS only.

   **NOTE**
   The web browser may display a warning notifying that the connection is untrusted. To eliminate the warning, you can replace the TLS certificate that is currently used to secure traffic between the browser and the backup appliance with a trusted TLS certificate. To learn how to replace certificates, see Replacing Web Certificates.

2. In the **Username** and **Password** fields, specify credentials of an authorized user account.

   If you log in for the first time, use credentials of the Default Administrator account that was created after the product installation. In future, you can add other user accounts to grant access to Veeam Backup for Google Cloud. For more information, see Managing Permissions.

   **TIP**
   If you do not remember the password, you can reset it. To do that, click the **Forgot password?** link and follow the instructions provided in this Veeam KB article.

3. Select the **Remain logged in** check box to save the specified credentials in a persistent browser cookie so that your session does not expire after 60 minutes of inactivity.

   If you select this check box, you will be logged in for 24 hours and will not have to provide credentials every time you access Veeam Backup for Google Cloud in a new browser session.

4. Click **Log in**.

   If multi-factor authentication (MFA) is enabled for the user, Veeam Backup for Google Cloud will prompt you to enter a code to verify the user identity. In the **Verification code** field, enter the temporary six-digit code generated by the authentication application running on your trusted device. Then, click **Log in**.
Logging Out

To log out, at the top right corner of the Veeam Backup for Google Cloud window, click the user name and then click **Log out**.
Configuring Veeam Backup for Google Cloud

To start working with Veeam Backup for Google Cloud, perform a number of steps for its configuration:

1. Add projects to get access to Google Cloud resources that you want to protect.
2. [Optional] Add users to control access to Veeam Backup for Google Cloud.
3. Add backup repositories.
4. Create worker configurations.

**NOTE**

Even after you add projects that manage your Google Cloud resources and configure all the necessary settings, Veeam Backup for Google Cloud will populate neither the list of VM instances nor the list of Cloud SQL instances on the Resources page — unless you create backup policies and specify regions where the instances belong, as described in sections Performing VM Backup and Performing SQL Backup.
Managing Projects

For each data protection and disaster recovery operation performed for a Google Cloud resource, you must specify a service account that has access to the resource and a set of permissions that determine what operations are allowed for the resource.

Particularly, Veeam Backup for Google Cloud uses service accounts to perform the following tasks:

- To access projects that manage Google Cloud resources.
- To synchronize the Google Cloud environment data with the configuration data stored on the backup appliance.
- To create and remove snapshots of VM instances.
- To create and remove snapshots of Cloud SQL instances.

Adding Projects

To add a new project, do the following:

1. Launch the Add Project wizard.
2. Select the project and specify permissions for its resources.
3. Specify a service account to access the project.
4. Finish working with the wizard.
Step 1. Launch Add Project Wizard

To launch the Add Project wizard, do the following:

1. Switch to the Configuration page.
2. Navigate to Permissions > Projects.
3. Click Add.

![Add Project Wizard](image)

Step 2. Select Project

At the Project Info step of the wizard, specify the unique identifier of a project that manages the resources that you want to protect, and choose data protection tasks that Veeam Backup for Google Cloud will be able to perform for the project.

You can find the project ID on the Dashboard page in the Google Cloud Console. For more information, see Google Cloud documentation.

![Select Project](image)
Step 3. Specify Service Account Name

At the **Service Account** step of the wizard, choose whether you want Veeam Backup for Google Cloud to access the selected project using an existing or a newly created service account.

- To use an already existing service account, use the **Account name** field to enter the name of the account. To check whether the specified account has all the necessary permissions required to perform data protection tasks for the project, click **Check Permissions**. For more information on the required permissions, see **Service Account Permissions**.

  You can view the list of all service accounts associated with the project on the the **Service Accounts** page in the Google Cloud Console. For more information, see Google Cloud documentation.

- To create a new service account, enter a name for the account in the **Account name** field, and click **Generate and download script**. Veeam Backup for Google Cloud will generate a gcloud script that you can run in your Google Cloud Console to create an account with the specified name and to assign all the necessary permissions.

  The following characters are not supported: `\ / " ' [ ] : | < > + = ; , ? * @ _ .` For more information on naming restrictions for Google Cloud service accounts, see Google Cloud documentation.
Step 4. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.
Editing Projects

For each project, you can modify settings configured while adding the project:

1. Switch to the Configuration page.
2. Navigate to Permissions > Projects.
3. Select the project and click Edit.
4. Complete the Edit Project wizard:
   a. To modify the list of tasks that Veeam Backup for Google Cloud can perform for the project, follow the instructions provided in section Adding Projects (step 2).
   b. To choose another service account or to create a new account to access the project, follow the instructions provided in section Adding Projects (step 3).

**NOTE**

The service account that is used to access the project where the backup appliance belongs (that is, the project specified during the product installation) can only be changed in the Google Cloud Console, as described in Google Cloud documentation.

   c. At the Summary step of the wizard, review configuration information and click Finish to confirm the changes.
Removing Projects

Veeam Backup for Google Cloud allows you to permanently remove a project from the configuration database if you no longer need it:

1. Switch to the **Configuration** page.
2. Navigate to **Permissions > Projects**.
3. Select the project and click **Remove**.

**NOTE**

You cannot remove a project that is used by any backup policy, backup repository or worker configuration. **Disable and remove all the related policies, remove all the related repositories, remove all the related worker configurations** — and then try removing the project again.
Managing Permissions

Veeam Backup for Google Cloud controls access to its functionality with the help of user roles. A role defines what operations users can perform and what range of data is available to them in the Veeam Backup for Google Cloud UI.

There are 3 roles that you can assign to users working with Veeam Backup for Google Cloud:

- **Portal Administrator** — can perform all configuration actions, can manage user roles, and can also act as a Portal Operator and Restore Operator.

- **Portal Operator** — can create, edit and start backup policies, manage the protected data, perform all restore operations and view session statistics.

- **Restore Operator** — can only perform restore operations and view session statistics.

The following table describes the functionality available to users with different roles in the Veeam Backup for Google Cloud UI.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Functionality</th>
<th>Portal Administrator</th>
<th>Portal Operator</th>
<th>Restore Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overview</strong></td>
<td>Dashboard</td>
<td>Full</td>
<td>Full</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Resources</strong></td>
<td>Infrastructure</td>
<td>Full</td>
<td>Full</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Policies</strong></td>
<td>Backup policies</td>
<td>Full</td>
<td>Full</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Protected Data</strong></td>
<td>Restore</td>
<td>Full</td>
<td>Full</td>
<td>Execute</td>
</tr>
<tr>
<td></td>
<td>File-level recovery</td>
<td>Full</td>
<td>Full</td>
<td>Execute</td>
</tr>
<tr>
<td></td>
<td>Remove</td>
<td>Full</td>
<td>Full</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Session Logs</strong></td>
<td>Session logs</td>
<td>Full</td>
<td>Full</td>
<td>Read</td>
</tr>
<tr>
<td></td>
<td>Stop session execution</td>
<td>Full</td>
<td>Full</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Configuration</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Permissions</strong></td>
<td>Projects, portal users</td>
<td>Full</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>and SMTP accounts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Repositories</strong></td>
<td>Backup repositories</td>
<td>Full</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Workers</strong></td>
<td>Worker instances</td>
<td>Full</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Adding User Accounts

To add a new user account, do the following:

1. Launch the Add Account wizard.
2. Specify an account name and description.
3. Specify a password.
4. Finish working with the wizard.

---

<table>
<thead>
<tr>
<th>Tab</th>
<th>Functionality</th>
<th>Portal Administrator</th>
<th>Portal Operator</th>
<th>Restore Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td>General settings</td>
<td>Full</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>License</strong></td>
<td>Licensing</td>
<td>Full</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Support Information</strong></td>
<td>Updates and logs</td>
<td>Full</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Step 1. Launch Add Account Wizard

To launch the **Add Account** wizard, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Permissions > Portal Users**.
3. Click **Add**.

![Add Account Wizard](image)

Step 2. Specify Account Name and Description

At the **Account Info** step of the wizard, use the **Name** and **Description** fields to enter a name for the new user account and to provide a description for future reference.

The maximum length of the account name is 32 characters. The following characters are supported: lowercase Latin letters, numeric characters, underscores and dashes. The following characters are not supported: `/ * [ ] : | > + = ; , ? * @ & $ .`
Step 3. Specify Password

At the General Settings step of the wizard, choose a role for the user account and specify a password that the user will use to access Veeam Backup for Google Cloud.

![Password Entry Screen]

Step 4. Finish Working with Wizard

At the Summary step of the wizard, review summary information and click Finish.

![Summary Step Screen]
Editing User Accounts

For each user account, you can modify settings configured while adding the account:

1. Switch to the **Configuration** page.
2. Navigate to **Permissions > Portal Users**.
3. Select the account and click **Edit**.
4. Complete the **Edit Account** wizard:
   a. At the **Account Info** step, provide a new description for the account.
   b. At the **General Settings** step, choose a new role for the account.
   c. At the **Summary** step, review summary information and click **Finish** to confirm the changes.
Changing User Passwords

For each user account, you can change the password specified while adding the account:

1. Switch to the **Configuration** page.
2. Navigate to **Permissions > Portal Users**.
3. Select the account and click **Change Password**.
4. In the **Change Password** window, enter the currently used password, enter and confirm a new password, and then click **Apply**.

![Change Password Window](image-url)
Enabling Multi-Factor Authentication

Multi-factor authentication (MFA) in Veeam Backup for Google Cloud is based on the Time-based One-Time Password (TOTP) method that requires the user to verify their identity by providing a temporary six-digit code generated by an authentication application running on a trusted device.

To enable MFA for a user account, do the following:

1. Switch to the Configuration page.
2. Navigate to Permissions > Portal Users.
3. Select the account and click MFA > Enable.
4. Follow the instructions provided in the Enabling MFA window:
   a. Install a supported authentication application on a trusted device. To view the list of authentication applications supported by Veeam Backup for Google Cloud, click See the full list of compatible apps.
   b. Scan the displayed QR code using the camera of the trusted device.
   c. Enter a verification code generated by the authentication application.
   d. Click Apply.

**NOTE**

Only Google Authenticator is fully supported by Veeam Backup for Google Cloud.
Managing Repositories

Veeam Backup for Google Cloud uses Google Cloud storage buckets as target locations for image-level backups of VM instances and Cloud SQL instances. To add a storage bucket to Veeam Backup for Google Cloud, configure a backup repository.

**IMPORTANT**
A backup repository must not be managed by multiple backup appliances simultaneously. Retention sessions running on different backup appliances may corrupt backup files stored in the repository, which may result in unpredictable data loss.

Adding Backup Repositories

To add a new backup repository, do the following:

1. Launch the Add Repository wizard.
2. Specify a repository name and description.
3. Specify a project for the repository.
4. Configure repository settings.
5. Enable encryption for the repository.
6. Finish working with the wizard.
Step 1. Launch Add Repository Wizard

To launch the Add Repository wizard, do the following:

1. Switch to the Configuration page.
2. Navigate to Repositories.
3. Click Add.

Step 2. Specify Repository Name and Description

At the Repository Info step of the wizard, use the Name and Description fields to enter a name for the new backup repository and to provide a description for future reference. The maximum length of the name is 127 characters; the following characters are not supported: / " ' [ ] : | < > = ; , ? * @ _.
Step 3. Specify Project

At the **Project** step of the wizard, do the following:

1. From the **Project** drop-down list, select a project where the new backup repository will belong.

   For a project to be displayed in the **Project** list, it must be added to Veeam Backup for Google Cloud as described in section **Adding Projects**.

2. Use the **Access Key** and **Secret key** fields to provide a Hash-based Message Authentication Code (HMAC) key associated with the service account that is used to access the project. Veeam Backup for Google Cloud will use the HMAC key to authenticate requests to the backup repository.

   You can create the necessary HMAC key beforehand in the Google Cloud Console as described in [Google Cloud documentation](https://cloud.google.com). Alternatively, you can click **Generate HMAC Credentials** to create a new HMAC key and associate it with the service account without closing the **Add Repository** wizard.
Step 4. Configure Repository Settings

At the **Storage Bucket** step of the wizard, do the following:

1. In the **Storage bucket** section, click **Choose bucket**.
   
   In the Choose storage bucket window, select a storage bucket that will be used as a target location for image-level backups of VM instances and Cloud SQL instances, and click **Apply**.
   
   For a storage bucket to be displayed in the **Available Buckets** list, it must be created for the selected project in the Google Cloud Console as described in Google Cloud documentation.

2. In the **Folder** section, choose whether you want to use an existing subdirectory inside the selected storage bucket or to create a new one to group backups stored in the bucket.
   
   - To use an existing subdirectory, select the **Use existing folder** option and click **Choose folder**. In the Choose folder window, select the necessary subdirectory and click **Apply**.
     
     For a subdirectory to be displayed in the **Available Folders** list, it must be created under the `/Veeam/Backup` path using gsutil commands as described in Google Cloud documentation.

   - To create a new subdirectory, select the **Create new folder** option and specify a name for the subdirectory. The maximum length of the name is 127 characters; the following characters are not supported: `\ / " ' [ ] : | < > + = ; , ? * @ & _`.

3. [This step applies only if you have selected the **Create new folder** option] In the **Storage class** section, select a storage class for the backup repository — it can be either the Standard Storage or Archive Storage class:
   
   - To store backups in a high-performance, short-term storage that you plan to access frequently, select **Standard**.
   
   - To store backups in a cost-effective, long-term storage that you plan to access less than once a year, select **Archive**.

   For the full description of Google Cloud storage classes, see Google Cloud documentation.

**NOTE**

If the selected subdirectory already contains backups created by the Veeam backup service, Veeam Backup for Google Cloud will import the backed-up data to the configuration database. You can then use this data to perform all disaster recovery operations described in section **Performing Restore**.

By default, Veeam Backup for Google Cloud applies retention settings saved in the backup metadata to the imported backups. However, if the selected subdirectory contains backups of resources that you plan to protect by a backup policy with the created repository specified as a backup target, Veeam Backup for Google Cloud will rewrite the saved retention settings and will apply to the imported backups new retention settings configured for that backup policy.

   - To create a new subdirectory, select the **Create new folder** option and specify a name for the subdirectory. The maximum length of the name is 127 characters; the following characters are not supported: `\ / " ' [ ] : | < > + = ; , ? * @ & _`.

**IMPORTANT**

If you select the **Archive** option, you must also enable backup archiving for any policy that will store backups in this repository. For more information, see **Performing VM Backup** and **Performing SQL Backup**.
Step 5. Enable Encryption

At the Encryption step of the wizard, use the Enable encryption check box to choose whether you want to encrypt backup files stored in the selected storage bucket. If you enable encryption, specify a password that will be used to encrypt data.
Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.

As soon as you click **Finish**, Veeam Backup for Google Cloud will start adding the new backup repository to the infrastructure. To track the progress, click **Go to Sessions** in the **Session Info** window to proceed to the Session Logs page.
Editing Backup Repositories

For each backup repository, you can modify settings configured while adding the repository to the Veeam Backup for Google Cloud infrastructure:

1. Switch to the Configuration page.
2. Navigate to Repositories.
3. Select the repository and click Edit.
4. Complete the Edit Repository wizard:
   a. To provide a new name and description for the repository, follow the instructions provided in section Adding Backup Repositories (step 2).
   b. To enable or disable encryption for the repository, follow the instructions provided in section Adding Backup Repositories (step 7).
   c. At the Summary step of the wizard, review summary information and click Finish to confirm the changes.

As soon as you click Finish, Veeam Backup for Google Cloud will start modifying the backup repository settings. To track the progress, click Go to Sessions in the Session Info window to proceed to the Session Logs page.
Removing Backup Repositories

Veeam Backup for Google Cloud allows you to permanently remove backup repositories from the infrastructure. When you remove a backup repository, Veeam Backup for Google Cloud unassigns the repository from the target storage bucket folder so that the folder is no longer used as a repository.

NOTE

Even though the storage bucket folder is no longer used as a repository, Veeam Backup for Google Cloud preserves all backup files previously stored in the repository and keeps these files in Google Cloud Storage. You can assign the folder to a new backup repository so that Veeam Backup for Google Cloud imports the backed-up data to the configuration database. In this case, you will be able to perform all disaster recovery operations described in section Performing Restore.

If you no longer need the backed-up data, you can remove it as described in section Removing Backups and Snapshots.

To remove a backup repository from the Veeam Backup for Google Cloud infrastructure, do the following:

1. Switch to the Configuration page.
2. Navigate to Repositories.
3. Select the repository and click Remove.

NOTE

You cannot remove a backup repository that is used by any backup policy or by a scheduled configuration backup. Modify the settings of all the related policies to remove references to the repository, change the configuration backup schedule — and then try removing the repository again.
Managing Workers

To perform most data protection and disaster recovery operations (such as creating image-level backups in backup repositories and restoring backed-up data), Veeam Backup for Google Cloud uses worker instances.

Each worker instance is deployed in a specific Google Cloud region for the duration of the backup or restore process. For more information on regions in which Veeam Backup for Google Cloud deploys worker instances, see Architecture Overview.

Managing Worker Configurations

A configuration is a group of network settings that Veeam Backup for Google Cloud uses to deploy worker instances in a specific Google Cloud region to perform data protection and disaster recovery operations. Veeam Backup for Google Cloud deploys one worker instance per each VM instance or Cloud SQL instance added to a backup policy or restore task.

By default, Veeam Backup for Google Cloud deploys worker instances with the same network configurations as those specified for the processed instances. However, to optimize infrastructure costs and to ensure better performance of backup and restore processes, you can add worker configurations to specify network settings for each region in which worker instances will be deployed.

NOTE
You can tell worker instances from other VM instances running in your environment by their names — all worker instances deployed by Veeam Backup for Google Cloud will have the word worker, the name of a related backup policy, and a GUID in their names.

Adding Worker Configurations

To add a new worker configuration, do the following:

1. Choose a project where worker instances will be deployed.
2. Launch the Add Worker Configuration wizard.
3. Specify general settings for the worker configuration.
4. Specify network settings for the worker configuration.
5. Finish working with the wizard.
Step 1. Choose Project for Worker Instances

**IMPORTANT**

It is recommended that you allocate a single specific project just for your worker instances so that you do not breach Google Cloud quota limits. That is why after you choose a project, do not try to change it by clicking the link in the **Project** section. Otherwise, all the created worker configurations will be removed automatically as soon as you choose another project.

To choose a project where worker instances will be created, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Workers > Network**.
3. Click the link in the **Project** section.
4. In the **Choose Project** window, select the necessary project and click **Apply**.
Step 2. Launch Add Worker Configuration Wizard

To launch the Add Worker Configuration wizard, click Add in the Worker configurations section.

Step 3. Specify General Settings

At the Region step of the wizard, select a region where new worker instances will operate and an availability zone for which you want to configure network settings.
Step 4. Specify Network Settings

At the Network step of the wizard, do the following:

1. Select a VPC network and a subnet to which you want to connect worker instances created based on the new worker configuration.

   For a VPC network and a subnet to be displayed in the lists of available networks, they must be created for the region specified at step 3 in the Google Cloud Console as described in Google Cloud documentation.

   **IMPORTANT**
   - A route whose destination IP address range is 0.0.0.0/0 and whose next hop is the default internet gateway must exist for the selected VPC network. To learn how to add and remove routes for a network, see Google Cloud documentation.
   - The selected subnet must have Private Google Access enabled. To learn how to enable Private Google Access for a subnet, see Google Cloud documentation.
   - If you plan to back up Cloud SQL instances using a staging server, the selected VPC network must have private services access configured. To learn how to configure private services access for a VPC network, see Google Cloud documentation.
   - If you want to connect worker instances created based on the worker configuration to a Shared VPC network, the service account specified for the project selected at step 1 must have the permissions described in Worker Permissions.

2. Select a firewall rule that will be used to control traffic between resources in the specified VPC network.

   For a firewall rule to be displayed in the list of available rules, it must be created in the Google Cloud Console as described in Google Cloud documentation.

   **IMPORTANT**
   If you plan to perform file-level recovery, the selected firewall rule must allow HTTPS traffic to all VM instances on the specified VPC network. To learn how to create firewall rules that allow HTTPS connections, see Google Cloud documentation.
# Step 5. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.

![Configuration Interface](image)

**Summary**

Review configured settings and click Finish to exit the wizard.

<table>
<thead>
<tr>
<th>Region</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Region</strong></td>
<td><strong>VPC</strong></td>
</tr>
<tr>
<td>Asia-northwest1 (Tokyo)</td>
<td>rele-45</td>
</tr>
</tbody>
</table>

**Verification checks**

- Google Private Access is enabled (required for backup): **OK**
- Port 80 for HTTPS (traffic is open) required for SSL (http is disabled): **OK**
- Private services access is enabled (required for Cloud SQL backup): **OK**
Editing Worker Configurations

For each worker configuration, you can modify settings specified while adding the worker configuration to the Veeam Backup for Google Cloud infrastructure:

1. Switch to the **Configuration** page.
2. Navigate to **Workers > Network**.
3. Select the worker configuration and click **Edit**.
4. Complete the **Edit Worker Configuration** wizard:
   a. To modify the VPC network and subnet to which the related worker instances are connected, and to change the firewall rule associated with the specified network, follow the instructions provided in section **Adding Worker Configurations** (step 4).
   b. At the **Summary** step of the wizard, review configuration information and click **Finish** to confirm the changes.

**NOTE**

If there are any worker instances created based on the selected configuration that are currently involved in a backup or restore process, the changes will be applied only when the process completes.
Removing Worker Configurations

Veeam Backup for Google Cloud allows you to permanently remove worker configurations from the infrastructure if you no longer need them. When you remove a worker configuration, Veeam Backup for Google Cloud does not remove currently running worker instances that have been created based on this configuration — these instances are removed only when the related operations complete.

To remove a worker configuration from the Veeam Backup for Google Cloud infrastructure, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Workers > Network**.
3. Select the worker configuration and click **Remove**.

**NOTE**

If there are any worker instances created based on the selected configuration that are currently involved in a backup or restore process, these instances will be removed only when the process completes.
Managing Worker Profiles

A profile is the machine type of a worker instance that Veeam Backup for Google Cloud deploys in a specific Google Cloud region to perform a backup or archive operation. Veeam Backup for Google Cloud deploys one worker instance per each Google Cloud resource (whether it is a VM instance or a Cloud SQL instance) added to a backup policy.

There are 3 types of worker profiles in Veeam Backup for Google Cloud:

- **Primary** — a profile that Veeam Backup for Google Cloud uses for creating image-level backups if the regional disk quota has not been reached yet.
- **Secondary** — a profile that Veeam Backup for Google Cloud uses for creating image-level backups if you have run or about to run out of the regional disk quota.
- **Archiving** — a profile that Veeam Backup for Google Cloud uses for creating archived backups.

Out of the box, Veeam Backup for Google Cloud comes with the default set of worker profiles where the primary profile is e2-highcpu-8, the secondary profile is e2-highcpu-2, and the archiving profile is e2-standard-4. However, to boost operational performance and to guarantee that you do not breach Google Cloud quota limits, you can add custom sets of worker profiles to specify machine types of VM instances that will operate as worker instances in different regions.

Adding Worker Profiles

To add a new custom set of worker profiles for one or more regions, do the following:

1. Launch the Add Worker Profiles wizard.
2. Choose the necessary regions.
3. Choose the default, secondary and archiving profiles for worker instances in these regions.
4. Finish working with the wizard.
Step 1. Launch Add Worker Profiles Wizard

To launch the **Add Worker Profiles** wizard, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Workers > Profile**.
3. Click **Add**.

Step 2. Choose Regions

At the **Regions** step of the wizard, select regions for which you want to specify worker profiles.
Step 3. Choose Worker Profiles

At the Worker Profiles step of the wizard, choose profiles that will be used to deploy workers in the selected regions. To help you choose, tables in the Choose machine type sections will provide information on the number of vCPU cores and the amount of system RAM for each available machine type.

**IMPORTANT**

Due to technical limitations, the list of available machine types is automatically filtered to show:

- For the primary profile, only those machine types that allow mounting persistent disks with at least 4 TB of total disk space attached.
- For the archiving profile, only those machine types that come with at least 8 GB RAM.

For the full description of machine types that can be used to deploy VM instances in Google Cloud, see [Google Cloud documentation](https://cloud.google.com/).
Step 4. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.

As soon as you click **Finish**, Veeam Backup for Google Cloud will create a separate set of worker profiles for each of the selected regions.
Editing Worker Profiles

For each set of worker profiles created for a Google Cloud region, you can modify settings specified while creating the profile set:

1. Switch to the **Configuration** page.
2. Navigate to **Workers > Profile**.
3. Select the profile set and click **Edit**.
4. Complete the **Edit Worker Profiles** wizard:
   a. To change profiles that will be used to deploy workers in the selected region, follow the instructions provided in section **Adding Worker Profiles** (step 3).
   b. At the **Summary** step of the wizard, review configuration information and click **Finish** to confirm the changes.

**NOTE**

If there are any worker instances that are currently involved in a backup or archive process in the selected region, the changes will be applied only when the process completes.

<table>
<thead>
<tr>
<th>Worker Profiles</th>
<th>Review configured settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td></td>
</tr>
<tr>
<td>Regions</td>
<td></td>
</tr>
<tr>
<td>Backup and restore operations</td>
<td></td>
</tr>
<tr>
<td>Primary profile</td>
<td>e3-highcpu4</td>
</tr>
<tr>
<td>Secondary profile</td>
<td>e3-highmem-4</td>
</tr>
<tr>
<td>Archiving</td>
<td></td>
</tr>
<tr>
<td>Archiving profile</td>
<td>n3-standard-4</td>
</tr>
</tbody>
</table>
Removing Worker Profiles

Veeam Backup for Google Cloud allows you to permanently remove sets of worker profiles if you no longer need them. When you remove a profile set, Veeam Backup for Google Cloud does not remove currently running worker instances that have been created based on this set — these instances are removed only when the related operations complete.

**NOTE**
After you remove a profile set, all worker instances that Veeam Backup for Google Cloud will further use to perform backup and archive operations in the region specified in the set will be deployed with the default profiles.

To remove a profile set from the Veeam Backup for Google Cloud infrastructure, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Workers > Profile**.
3. Select the profile set and click **Remove**.
Configuring General Settings

Veeam Backup for Google Cloud allows you to configure general settings that are applied to all performed operations and deployed infrastructure components:

- Define for how long obsolete snapshots and session records will be retained.
- Provide certificates to secure connections between Veeam Backup for Google Cloud infrastructure components.
- Configure notification settings for automated delivery of reports.
- Change the time zone set on the backup appliance.
Configuring Global Retention Settings

You can configure global retention settings to specify for how long the following data will be retained in the configuration database:

- Obsolete snapshots
- Session records

Configuring Retention Settings for Obsolete Snapshots

If an instance (whether it is a VM instance or a Cloud SQL instance) is no longer processed by a backup policy (for example, it was removed from the backup policy or the backup policy no longer exists), its cloud-native snapshots become obsolete. These snapshots are removed from the configuration database according to their own retention settings.

**NOTE**

Global retention settings apply to all cloud-native snapshots created by the Veeam backup service. If an instance is still processed by a backup policy, but some of its cloud-native snapshots are older than the number of days (or months) specified in the global retention settings, these cloud-native snapshots will be removed from the configuration database.

To configure retention settings for obsolete snapshots, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **General > Retention**.
3. In the **Obsolete snapshots retention** section, select either of the following options:
   - Select the **Never** option if you do not want Veeam Backup for Google Cloud to remove obsolete snapshots.
   - Select the **After** option if you want to specify the number of days (or months) during which Veeam Backup for Google Cloud will keep obsolete snapshots in the configuration database. The number must be between 90 and 36135.
     
     If you select this option, Veeam Backup for Google Cloud will remove obsolete instance snapshots from the configuration database as soon as the specified period of time is over — even if the instances are still processed by backup policies.
4. Click **Save**.

**NOTE**

When Veeam Backup for Google Cloud removes an obsolete snapshot from the configuration database, it also removes the snapshot from the Google Cloud infrastructure.
Configuring Retention Settings for Session Records

Veeam Backup for Google Cloud stores records for all sessions of performed data protection and disaster recovery operations in the configuration database on the additional data disk attached to the backup appliance. These session records are removed from the configuration database according to their own retention settings.

To configure retention settings for session records, do the following:

1. In the **Session logs retention** section, select either of the following options:
   - Select the **Keep all session logs** option if you do not want Veeam Backup for Google Cloud to remove session records.
   - Select the **Keep session logs only for last** option if you want to specify the number of days (or months) during which Veeam Backup for Google Cloud will keep session records in the configuration database.
     
     If you select this option, Veeam Backup for Google Cloud will remove all session records that are older than the specified time limit.

2. Click **Save**.

**IMPORTANT**

Retaining all session records in the configuration database may overload the data disk. By default, the disk comes with 20 GB of storage capacity. If you choose not to remove session records at all, consider increasing the disk space to avoid runtime problems.
Configuring Global Notification Settings

You can specify email notification settings for automated delivery of backup policy results and daily reports. Every daily report contains cumulative statistics for all backup policy and snapshot retention sessions run within the past 24-hour period.

To connect an SMTP server that will be used for sending email notifications:

1. Switch to the Configuration page.
2. Navigate to General > Email.
3. Select the Enable email notifications check box.
4. In the SMTP server field, enter a DNS name of the SMTP server. All email notifications (including test messages) will be sent by this SMTP server.
5. Click Advanced to specify an account that will be used when authenticating against the SMTP server and to configure other connection settings.

   In the Advanced SMTP Settings window:
   
   a. In the SMTP Port field, specify a communication port for SMTP traffic. The default SMTP port is 587.
   b. In the Timeout field, specify a connection timeout for responses from the SMTP server.
   c. For an SMTP server with SSL/TLS support, select the Connect using SSL check box to enable SSL data encryption.
   d. If your SMTP server requires authentication, select the This SMTP server requires authentication check box and choose the necessary account from the Connect as drop-down list.

      For an account to be displayed in the Connect as list, it must be added to the configuration database as described in section Adding SMTP Accounts. If you have not set up an account beforehand, click Add and follow the steps of the Add Account wizard.

   e. Click Apply.

6. In the From field, enter an email address of the notification sender. This email address will be displayed in the From field of notifications.
7. In the To field, enter an email address of a recipient. Use a semicolon to separate multiple recipient addresses.

   For each particular policy, you can specify additional recipients. For more information, see Creating Backup Policies.

NOTE
If you specify the same email recipient in both backup policy notification and global notification settings, Veeam Backup for Google Cloud will send each notification to this recipient twice.
8. In the Subject field, specify a subject for notifications. You can use the following runtime variables:
   - %JobName% — a backup policy name.
   - %JobResult% — a backup policy result.
   - %ObjectCount% — the number of instances in a backup policy.
   - %Issues% — the number of instances in a backup policy that encountered any issues (errors and warnings) while being processed.

9. In the Notify immediately on policy section, choose whether you want to receive email notifications in case backup policies complete successfully, complete with warnings or complete with errors.

10. To receive daily reports, select the Send daily report at check box and specify the exact time when the reports will be sent.

11. Click Save.

TIP

Veeam Backup for Google Cloud allows you to send a test message to check whether you have configured the settings correctly. To do that, click Send Test Email. A test message will be sent to the specified email address.
Adding SMTP Accounts

To add an account that will be used to connect to an SMTP server, do the following:

1. Launch the Add Account wizard.
2. Specify an account display name and description.
3. Provide credentials.
4. Finish working with the wizard.

Step 1. Launch Add Account Wizard

To launch the Add Account wizard, do the following:

1. Switch to the Configuration page.
2. Navigate to Permissions > SMTP Accounts.
3. Click Add.
Step 2. Specify Account Name and Description

At the **Account Info** step of the wizard, use the **Name** and **Description** fields to enter a name for the new SMTP account and to provide a description for future reference. The maximum length of the name is 255 characters.

![Add Account](image)

Step 3. Provide Credentials

At the **Account** step of the wizard, specify credentials of a user account that will be used to authenticate against the SMTP server.

![Add Account](image)
Step 4. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.
Editing SMTP Accounts

For each SMTP account, you can modify settings configured while creating the account:

1. Switch to the **Configuration** page.
2. Navigate to **Permissions > SMTP Accounts**.
3. Select the account and click **Edit**.
4. Complete the **Edit Account** wizard:
   a. To provide a new name and description for the account, follow the instructions provided in section **Adding SMTP Accounts** (step 2).
   b. To specify credentials of another user account to be used to authenticate against the SMTP server, follow the instructions provided in section **Adding SMTP Accounts** (step 3).
   c. At the **Summary** step of the wizard, review summary information and click **Finish** to confirm the changes.
Replacing Security Certificates

To establish secure data communications between the backup appliance and web browsers running on user workstations, Veeam Backup for Google Cloud uses Transport Layer Security (TLS) certificates.

When you install Veeam Backup for Google Cloud, it automatically generates a default self-signed certificate. You can replace this default certificate with your own self-signed certificate or with a certificate obtained from a Certificate Authority (CA). To replace the currently used TLS certificate, do the following:

1. Switch to the Configuration page.
2. Navigate to General > Certificate.
3. Click Replace Certificate.
4. Complete the Replace Certificate wizard:
   a. At the Certificate Source step of the wizard, do the following:
      - Select the Re-create the self-signed certificate option if you want to replace the existing certificate with a new self-signed certificate automatically generated by Veeam Backup for Google Cloud.
      - Select the Upload a new certificate option if you want to upload a certificate that you obtained from a CA or generated using a 3rd party tool.
   b. [This step applies only if you have selected the Upload a new certificate option] At the Upload Certificate step of the wizard, browse to the certificate that you want to install, and provide a password for the certificate file.

   **NOTE**
   Only .PFX and .P12 files are supported.
   
   c. At the Summary step of the wizard, review summary information and click Finish.
Changing Time Zone

Veeam Backup for Google Cloud runs daily reports and performs all data protection and disaster recovery operations according to the time zone set on the backup appliance.

Since the backup appliance is deployed on a VM instance in Google Cloud, the time zone is set to Coordinated Universal Time (UTC) by default. However, you can change the time zone if required. For example, you may want the time on the backup appliance to match the time on the workstation from which you access Veeam Backup for Google Cloud.

To change the time zone set on the backup appliance:

1. Switch to the **Configuration** page.
2. Navigate to **General > Time Zone**.
3. Select the necessary time zone from the **Time zone** drop-down list.
4. Click **Save**.

**NOTE**

You cannot change the time zone if any data protection or disaster recovery session is currently running. Wait for all the running sessions to complete or stop them manually — and then try changing the time zone again.
Performing Configuration Backup and Restore

You can back up and restore the configuration database that stores data collected from Veeam Backup for Google Cloud for the existing backup policies, protected VM instances and Cloud SQL instances, deployed worker instances, connected Google Cloud projects, logged session records and so on. If the backup appliance goes down for some reason, you can reinstall it and quickly restore its configuration from a configuration backup. You can also use a configuration backup to migrate the configuration of one backup appliance to another backup appliance in the Google Cloud infrastructure.

It is recommended that you regularly perform configuration backup for every backup appliance present in the Google Cloud infrastructure. Periodic configuration backups reduce the risk of data loss and minimize the administrative overhead costs in case any problems with the backup appliances occur.

You can run configuration backup manually on demand, or instruct Veeam Backup for Google Cloud to do it automatically on a regular basis.
Performing Configuration Backup Manually

While performing configuration backup, Veeam Backup for Google Cloud exports data from the configuration database and saves it to a backup file in a backup repository. To back up the configuration database of the backup appliance manually, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **General > Configuration Backup**.
3. In the **Overview** section, click **Take Backup Now**.
4. In the **Create Manual Backup** window, select a repository where the configuration backup will be stored, and click **Create**.

For a backup repository to be displayed in the **Repository** list, it must be added to Veeam Backup for Google Cloud as described in section **Adding Backup Repositories**. The **Repository** list shows only backup repositories of the **Standard** storage class that have encryption enabled.

As soon as you click **Create**, Veeam Backup for Google Cloud will start creating a new backup file in the selected repository. To track the progress, click **Go to Sessions** in the **Session Info** window to proceed to the **Session Logs** page.
Performing Configuration Backup Automatically

While performing configuration backup, Veeam Backup for Google Cloud exports data from the configuration database and saves it to a backup file in a backup repository. To instruct Veeam Backup for Google Cloud to back up the configuration database of the backup appliance automatically by schedule, do the following:

1. Switch to the Configuration page.
2. Navigate to General > Configuration Backup.
3. In the Backup schedule section, set the Enable scheduling toggle to On.
4. Click Choose in the Repository field, and use the list of available repositories in the Choose Repository window to select a repository where configuration backups will be stored.
   
   For a backup repository to be displayed in the list of available repositories, it must be added to Veeam Backup for Google Cloud as described in section Adding Backup Repositories. The list shows only backup repositories of the Standard storage class that have encryption enabled.
5. In the Keep restore points for field, specify the number of days for which you want to keep restore points in the selected backup repository.
6. In the Create daily backup at field, choose whether configuration backups will be created every day, on weekdays (Monday through Friday), or on specific days.
7. Click Save.
Exporting Configuration Backup Data

Once Veeam Backup for Google Cloud creates a successful configuration backup, you can export the configuration backup file and use it to restore configuration data on another backup appliance.

To export the configuration backup file, do the following:

1. Switch to the Configuration page.
2. Navigate to General > Configuration Backup.
3. Use either of the following options:
   a. To export the last successful configuration backup:
      i. In the Overview section, click Export Last Backup.
      ii. In the Export Last Backup window, specify a password that will be used to encrypt the exported file, provide a hint for the specified password, and click Export.
   b. To export a specific configuration backup file:
      i. In the Configuration restore section, click Available Restore Points.
      ii. In the Available Restore Points window, select the necessary backup and click Export Backup.
      iii. In the Export Backup window, specify a password that will be used to encrypt the exported file, provide a hint for the specified password, and click Export.

As soon as you click Export, Veeam Backup for Google Cloud will save the exported backup file to the default download directory on the local machine.
Restoring Configuration Data

Veeam Backup for Google Cloud offers restore of the configuration database that can be helpful in the following situations:

- The configuration database got corrupted, and you want to recover data from a configuration backup.
- You want to roll back the configuration database to a specific point in time.
- The backup appliance got corrupted, and you want to recover its configuration from a configuration backup.
- The backup appliance went down, and you want to apply its configuration to a new backup appliance.

IMPORTANT
Before you start the restore process, stop all backup policies that are currently running.

To restore the configuration database, do the following:

1. Launch the Configuration Restore wizard.
2. Choose a backup file.
3. Review the backup file info.
4. Choose restore options.
5. Track the restore progress.
6. View the results of verification steps.
7. Finish working with the wizard.
Step 1. Launch Configuration Restore Wizard

To launch the **Configuration Restore** wizard, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **General > Configuration Backup**.
3. In the **Configuration restore** section, click **Restore**.
Step 2. Choose Backup File

At the **Backup File** step of the wizard, choose whether you want to use an exported backup file or a backup file stored in a backup repository:

- If you want to use a file stored in a backup repository, select the **Use backup file from repository** option and do the following:
  
  a. Click **Choose** in the **Repository** field, and use the list of available repositories in the **Choose repository** window to select the repository where the necessary configuration backup file is stored.
  
  For a backup repository to be displayed in the **Repository** list, it must be added to Veeam Backup for Google Cloud as described in section **Adding Backup Repositories**. The list shows only backup repositories that store configuration backup files.
  
  b. Click **Choose** in the **Backup file** field, and select the necessary file in the **Choose backup file** window.

- If you want to use a file that was exported from this or another backup appliance, select the **Use imported backup file** option and do the following:
  
  a. Click **Choose** in the **Backup file** field.
  
  b. In the **Import backup file** window, browse to the necessary backup file, provide a password that was used to encrypt the file, and click **Import**.

**IMPORTANT**

The size of an uploaded backup file must not exceed 10 GB. To upload a file of a bigger size, open a support case.
Step 3. Review Backup File Info

Veeam Backup for Google Cloud will analyze the content of the selected backup file and display the following information:

- File information — the date and time when the backup file was created.
- Product information — the version of Veeam Backup for Google Cloud that was installed on the initial backup appliance and the version of the File-Level Recovery Service that was running on the appliance.
- Product configuration — configuration data saved in the file (such as the number of configured backup policies, added user accounts, created backup repositories, logged session records and so on).

At the File Content step of the wizard, review the provided information and click Next to confirm that you want to use the selected file to restore the configuration data.
Step 4. Choose Restore Options

By default, Veeam Backup for Google Cloud restores only configuration data for the existing infrastructure components, created backup policies and configured global settings. At the **Restore Options** step of the wizard, you can choose whether you want to restore session logs and user accounts of the initial backup appliance as well.

**IMPORTANT**

After you click **Restore**, the restore process will start. You will not be able to halt the process or edit the restore settings.
Step 5. Track Restore Progress

Veeam Backup for Google Cloud will display the results of every step performed while executing the configuration restore. At the **Restore** step of the wizard, wait for the restore process to complete and click **Next**.
Step 6. View Configuration Check Results

After the restore process is over, Veeam Backup for Google Cloud will run a number of verification checks to confirm that the configuration data has been restored successfully. At the Configuration Check step of the wizard, wait for the verification checks to complete and click Next.

**TIP**

If Veeam Backup for Google Cloud encounters an issue while performing a verification check, the Result column will display a description of the issue, and the Action column will provide instructions on how to resolve it. After you resolve the issue, click Recheck to ensure the backup appliance is now fully functional.

Note that some issues are displayed for informational purposes only and do not require any action at this point.

![Configuration Check Results](image-url)
Step 7. Finish Working with Wizard

At the **Restore Result** step of the wizard, click **Finish** to finalize the process of configuration data restore.
Viewing Available Resources

After you create a backup policy to protect a specific type of Google Cloud resources (VM instances or Cloud SQL instances), Veeam Backup for Google Cloud rescans Google Cloud regions specified in the policy settings and populates the resource list on the **Resources** page with all resources of that type residing in these regions. If a region is no longer specified in any backup policy, Veeam Backup for Google Cloud removes all resources residing in the region from the list of available resources.

The **Resources** page displays Google Cloud resources that can be protected by Veeam Backup for Google Cloud. Each resource is represented with a set of properties, such as:

- **Instance** — the name of the resource.
- **Policy** — the name of the backup policy that protects the resource (if any).
- **Region** — the region in which the resource resides.
- **Project** — the project that manages the resource.
- **Restore Points** — the number of restore points created for the resource (if any).
- **Latest Restore Point** — the date and time of the most recent restore point created for the resource (if any).
- **Destination** — the type of restore points created for the resource (if any).

On the **Resources** page, you can also perform the following actions:

- Manually create cloud-native snapshots of VM instances and Cloud SQL instances. For more information, see sections **Performing VM Backup** and **Performing SQL Backup**.
- Add Cloud SQL instances to the existing backup policies. For more information, see **Adding Resources to Policies**.

---

**Image Description:**
- **VM** and **Cloud SQL** tabs are shown.
- Several VM instances and Cloud SQL instances are listed with details such as instance name, type, project, region, latest restore point, and destination.
- Options to perform actions like 'Take Snapshot Now' and 'Stop' are visible.

---

104 | Veeam Backup for Google Cloud Platform | User Guide
Adding Resources to Policies

If you want to include additional resources in the existing backup policies, you can either edit the backup policy settings or quickly add the resources to the policies on the Resources page.

To add a Cloud SQL instance to a backup policy, do the following:

1. **Switch to the Cloud SQL tab** and select the necessary instance.

   For a Cloud SQL instance to be displayed in the list of available instances, the Google Cloud region in which the instance resides must be specified in any of the configured backup policies, and the service account specified in the backup policy settings must have permissions to access the instance.

2. **Click Add to Policy.**

3. **In the Add to Policy window,** select a backup policy that will protect the instance, and click **Add.**

   For a backup policy to be displayed in the list of available policies, the Google Cloud region in which the selected instance resides must be specified in the backup source settings, and the service account used by Veeam Backup for Google Cloud to perform backup must have permissions to access the instance.

4. **In the Results window,** click **OK.**
Performing Backup

With Veeam Backup for Google Cloud, you can protect Google Cloud resources in the following ways:

- **Create cloud-native snapshots of VM instances**
  A cloud-native snapshot includes point-in-time snapshots of persistent disks attached to the processed VM instance. Snapshots of persistent disks (also referred to as PD snapshots) are taken using native Google Cloud capabilities.

- **Create image-level backups of VM instances**
  In addition to cloud-native snapshots, you can protect your VM instances with image-level backups. An image-level backup captures the whole image of the processed VM instance (including OS data, application data and so on) at a specific point in time. The backup is saved as multiple files to a storage bucket in the native Veeam format.

- **Create cloud-native snapshots of Cloud SQL instances**
  A cloud-native snapshot is a point-in-time snapshot of the processed Cloud SQL instance. Snapshots of Cloud SQL instances are taken using native Google Cloud capabilities. By default, cloud-native snapshots are stored in the multi-region that is located geographically close to the region in which the original instance resides.

**NOTE**
Cloud-native snapshots of Cloud SQL instances are referred to as backups in Google Cloud documentation. However, since all ‘backups’ of a Cloud SQL instance are automatically deleted after you remove the instance itself, ‘backups’ of Cloud SQL instances are referred to as snapshots in this guide. In terms of Veeam logic, backups are independent files that are stored in backup repositories and that are not affected by any actions performed with the original instances whatsoever.

- **Create image-level backups of Cloud SQL instances**
  In addition to cloud-native snapshots, you can protect your Cloud SQL instances with image-level backups. An image-level backup captures the whole image of the processed Cloud SQL instance (including the instance configuration, databases, triggers, stored procedures and users) at a specific point in time. The backup is saved as multiple files to a storage bucket in the native Veeam format.

**NOTE**
Veeam Backup for Google Cloud allows you to protect MySQL instances only. PostgreSQL and SQL Server instances are not supported. For more information on types of Cloud SQL instances, see Google Cloud documentation.

To schedule data protection tasks to run automatically, create backup policies. For VM instances and Cloud SQL instances residing in any of the regions added to the backup policies, you can also take cloud-native snapshots manually when needed — for more information, see Creating VM Snapshots Manually and Creating SQL Snapshots Manually.
How Backup Works

Veeam Backup for Google Cloud does not install agent software inside instances to retrieve data. To back up both VM instances and Cloud SQL instances, Veeam Backup for Google Cloud uses native Google Cloud capabilities. During every backup session, Veeam Backup for Google Cloud creates a cloud-native snapshot for each instance added to a backup policy. The cloud-native snapshot is further used to create an image-level backup of the instance.

VM Instance Backup

Veeam Backup for Google Cloud performs VM instance backup in the following way:

1. Creates snapshots of persistent disks that are attached to the processed VM instance.
   
   PD snapshots are assigned resource labels upon creation. Keys and values of resource labels contain encrypted metadata that helps Veeam Backup for Google Cloud identify the related PD snapshots and treat them as a single unit — a cloud-native snapshot.

2. If you enable image-level backup for the backup policy, Veeam Backup for Google Cloud performs the following operations:
   
   a. Deploys a worker instance in a Google Cloud region in which the processed VM instance resides.
      
      By default, Veeam Backup for Google Cloud deploys worker instances with the same network configurations as those specified for the processed VM instances. However, you can add specific worker configurations. For more information, see Managing Workers.
   
   b. Re-creates the persistent disks from the cloud-native snapshot created at step 1 and attaches them to the worker instance.
      
      Note that the cloud-native snapshot used as a source for image-level backup is not a temporary snapshot — when the backup session completes, this snapshot remains in the snapshot chain and is deleted later according to the specified policy scheduling settings.
   
   c. Reads data from the persistent disks on the worker instance, transfers the data to the target standard backup repository and stores it in the native Veeam format.
      
      Veeam Backup for Google Cloud encrypts and compresses data saved to storage buckets. For more information, see Enabling Data Encryption.
   
   d. Removes the worker instance when the backup session completes.

3. If you enable the backup archiving mechanism, Veeam Backup for Google Cloud performs the following operations:
   
   a. Deploys a worker instance in a Google Cloud region in which the processed VM instance resides.
   
   b. Retrieves data from the target standard backup repository and transfers it to the target archive backup repository.
   
   c. Removes the worker instance when the archive session completes.
Cloud SQL Instance Backup

When processing a Cloud SQL instance added to a backup policy, Veeam Backup for Google Cloud can create a restore point of the instance and transfer the point directly to a backup repository, or can copy the instance to a staging server first, create a restore point and then transfer it to a repository. In the latter case, Veeam Backup for Google Cloud will also process all transaction logs of the copied instance to create a transactionally consistent backup. This guarantees the consistency of the instance state during recovery but could increase costs associated with cross-region data transfer.

Veeam Backup for Google Cloud performs SQL instance backup in the following way:

1. Creates a cloud-native snapshot of the processed Cloud SQL instance.
2. If you enable image-level backup for the backup policy and choose to perform backup using a staging server, Veeam Backup for Google Cloud performs the following operations:
   a. Launches a staging server instance in a Google Cloud region in which the source Cloud SQL instance resides.
   b. Reverts the staging server instance to the cloud-native snapshot created at step 1.
      Note that the cloud-native snapshot used as a source for image-level backup is not a temporary snapshot — when the backup session completes, this snapshot remains in the snapshot chain and is deleted later according to the specified policy scheduling settings.
   
   **IMPORTANT**
   Veeam Backup for Google Cloud launches staging server instances without public IP addresses. To allow backup operations to complete successfully, you must configure private services access for these instances manually, as described in Google Cloud documentation.
3. Exports databases of the processed Cloud SQL instance to a SQL dump file in the Temp folder of the storage bucket where the target standard backup repository resides.
   For more information on SQL dump files, see Google Cloud documentation.
4. Deploys a worker instance in a Google Cloud region in which the target standard backup repository is located.
   By default, Veeam Backup for Google Cloud deploys worker instances with the same network configurations as those specified for the processed Cloud SQL instances. However, you can add specific worker configurations. For more information, see Managing Workers.
5. Exports triggers, stored procedures and users of the processed the Cloud SQL instance to the SQL dump file in the Temp folder of the storage bucket.
6. Removes the staging server instance (if launched at step 2).
7. Reads data from the SQL dump file, transfers the data to the target standard backup repository and stores it in the native Veeam format.
8. Removes the worker instance and the files from the Temp folder when the backup session completes.
9. If you enable the backup archiving mechanism, Veeam Backup for Google Cloud performs the following operations:
   a. Deploys a worker instance in a Google Cloud region in which the target standard backup repository is located.
   b. Retrieves data from the target standard backup repository and transfers it to the target archive backup repository.
   c. Removes the worker instance when the archive session completes.
Snapshot Chain

During every backup session, Veeam Backup for Google Cloud creates a cloud-native snapshot of each instance (whether it is a VM instance or a Cloud SQL instance) added to a backup policy. The cloud-native snapshot itself is a collection of point-in-time snapshots that Veeam Backup for Google Cloud creates using native Google Cloud capabilities.

A sequence of cloud-native snapshots created during a set of backup sessions makes up a snapshot chain. Veeam Backup for Google Cloud builds the snapshot chain in the following way:

1. During the first backup session, Veeam Backup for Google Cloud creates a snapshot of all instance data and saves it in the region in which the processed instance resides. This snapshot becomes a starting point in the snapshot chain.
   
   The creation of the first snapshot may take significant time to complete since Veeam Backup for Google Cloud copies the whole image of the instance.

2. During subsequent backup sessions, Veeam Backup for Google Cloud creates snapshots that contain only those data blocks that have changed since the previous backup session.
   
   The creation of subsequent snapshots typically takes less time to complete, compared to the first snapshot in the chain. Note, however, that the completion time still depends on the amount of processed data.

   For more information on how incremental VM and Cloud SQL snapshots work, see Google Cloud Compute Engine documentation and Google Cloud SQL documentation.

Each cloud-native snapshot in the snapshot chain contains metadata. Metadata stores information about the protected instance and the backup policy that created the snapshot. Veeam Backup for Google Cloud uses metadata to identify outdated snapshots, to load the configuration of source instances during recovery operations, and so on.

Cloud-native snapshots act as independent restore points for backed-up instances. If you remove any snapshot, it will not break the snapshot chain — you will still be able to roll back instance data to any existing restore point.

The number of cloud-native snapshots kept in the snapshot chain is defined by retention policy settings. For more information, see Retention Policy for Snapshots.
Backup Chain

If you enable image-level backups for a backup policy, Veeam Backup for Google Cloud creates a new backup file in a backup repository during every backup session. A sequence of backup files created during a set of backup sessions makes up a standard backup chain.

The standard backup chain includes backup files of the following types:

- **Full** — a full backup file stores a copy of the full instance image.
- **Incremental** — incremental backup files store incremental changes of the instance image.

To create a standard backup chain for a VM instance protected by a backup policy, Veeam Backup for Google Cloud implements the forever forward incremental backup method:

1. During the first backup session, Veeam Backup for Google Cloud copies the full instance image and creates a full backup file in the backup repository. The full backup file becomes a starting point in the standard backup chain.
2. During subsequent backup sessions, Veeam Backup for Google Cloud copies only those data blocks that have changed since the previous backup session, and stores these data blocks to incremental backup files in the backup repository. The content of each incremental backup file depends on the content of the full backup file and the preceding incremental backup files in the standard backup chain.

Full and incremental backup files act as restore points for backed-up instances that let you roll back instance data to the necessary state. To recover an instance to a specific point in time, the chain of backup files created for the instance must contain a full backup file and a set of incremental backup files dependent on the full backup file.

**NOTE**

In version 3.0, the forever forward incremental backup method is not implemented for Cloud SQL instances — during every backup session Veeam Backup for Google Cloud creates a full backup file in the standard backup chain. The issue will be addressed in a future release.

If some file in the standard backup chain is missing, you will not be able to roll back to the necessary state. For this reason, you must not delete individual backup files from the backup repository manually. Instead, you must specify retention policy settings that will let you maintain the necessary number of backup files in the backup repository. For more information, see Retention Policy for Backups.
Archive Backup Chain

If you enable backup archiving for a backup policy, Veeam Backup for Google Cloud creates a new backup file in an archive repository during every archive session. A sequence of backup files created during a set of archive sessions makes up an archive backup chain.

The archive backup chain includes backup files of the following types:

- **Full** — a full archive backup file stores a copy of the full instance image.
- **Incremental** — incremental archive backup files store incremental changes of the instance image.

To create an archive backup chain for an VM instance protected by a backup policy, Veeam Backup for Google Cloud implements the forever forward incremental backup method:

1. During the first archive session, Veeam Backup for Google Cloud detects backed-up data that is stored in the full backup file and all incremental backup files existing in the standard backup chain, creates a full archive backup file with all the data, and copies this file to the archive repository. The full archive backup file becomes a starting point in the archive chain.

2. During subsequent archive sessions, Veeam Backup for Google Cloud checks the standard backup chain to detect data blocks that have changed since the previous archive session, creates incremental archive backup files with only those changed blocks, and copies these files to the archive repository. The content of each incremental archive backup file depends on the content of the full archive backup file and the preceding incremental archive backup files in the archive backup chain.

Full and incremental archive backup files act as restore points for backed-up instances that let you roll back instance data to the necessary state. To recover an instance to a specific point in time, the chain of backup files created for the instance must contain a full archive backup file and a set of incremental archive backup files.

**NOTE**

In version 3.0, the forever forward incremental backup method is not implemented for Cloud SQL instances — during every backup session Veeam Backup for Google Cloud creates a full backup file in the standard backup chain. The issue will be addressed in a future release.

If some file in the archive backup chain is missing, you will not be able to roll back to the necessary state. For this reason, you must not delete individual backup files from the archive repository manually. Instead, you must specify retention policy settings that will let you maintain the necessary number of backup files in the archive repository. For more information, see Retention Policy for Archived Backups.
Retention Policy

Cloud-native snapshots and image-level backups created by backup policies are not kept forever — they are removed according to retention policy settings specified while creating the policies as described in sections Creating VM Policies and Creating SQL Policies.

Depending on the data protection scenario, retention policy can be specified:

- **In restore points** — for cloud-native snapshots.
  The snapshot chain can contain only the allowed number of restore points. If the number of allowed restore points is exceeded, Veeam Backup for Google Cloud removes the earliest restore point from the snapshot chain. For more information, see Retention Policy for Snapshots.

- **In days/months/years** — for image-level backups.
  Restore points in the backup chain (either standard or archive) can be stored in the configuration database only for the allowed period of time. If a restore point is older than the specified time limit, Veeam Backup for Google Cloud removes it from the backup chain. For more information, see Retention Policy for Backups and Retention Policy for Archived Backups.

You can also specify retention settings for snapshots that become obsolete. For more information, see Configuring Global Retention Settings.

Retention Policy for Snapshots

For cloud-native snapshots, Veeam Backup for Google Cloud retains the number of latest restore points defined in backup scheduling settings as described in sections Creating VM Policies and Creating SQL Policies.

During every successful backup session, Veeam Backup for Google Cloud creates a new restore point. If Veeam Backup for Google Cloud detects that the number of restore points in the snapshot chain exceeds the retention limit, it removes the earliest restore point from the chain. For more information on the snapshot deletion process, see Google Cloud documentation.

![Diagram of retention policy for snapshots](image)

**NOTE**

Retention policy settings configured when creating backup policies do not apply to cloud-native snapshots created manually. To learn how to remove these snapshots, see Removing Backups and Snapshots.
Retention Policy for Backups

For image-level backups, Veeam Backup for Google Cloud retains restore points for the number of days defined in backup scheduling settings as described in sections Creating VM Policies and Creating SQL Policies.

To track and remove outdated restore points from a standard backup chain, Veeam Backup for Google Cloud performs the following actions once a day:

1. Veeam Backup for Google Cloud checks the configuration database to detect standard backup repositories that contain outdated restore points.

2. If an outdated restore point exists in a backup repository, Veeam Backup for Google Cloud deploys a worker instance in a Google Cloud region in which the repository with backed-up data resides.

3. Veeam Backup for Google Cloud transforms the standard backup chain in the following way:
   a. Rebuilds the full backup file to include there data of the incremental backup file that follows the full backup file. To do that, Veeam Backup for Google Cloud injects into the full backup file data blocks from the earliest incremental backup file in the chain. This way, the full backup 'moves' forward in the standard backup chain.

   ![Injecting data blocks diagram]

   b. Removes the earliest incremental backup file from the chain as redundant — this data has already been injected into the full backup file.

   ![Removing redundant backup diagram]
4. Veeam Backup for Google Cloud repeats step 2 for all other outdated restore points found in the standard backup chain until all the restore points are removed. As data from multiple restore points is injected into the rebuilt full backup file, Veeam Backup for Google Cloud ensures that the standard backup chain is not broken and that you will be able to recover your data when needed.

5. Removes the worker instance when the retention session completes.

**NOTES**

- Each worker instance can process only one retention task at a time, and Veeam Backup for Google Cloud can simultaneously deploy maximum 10 worker instances to process retention tasks. If the number of retention tasks that must be processed by worker instances is more than the specified limit, the tasks exceeding this limit are queued.
- In version 3.0, the forever forward incremental backup method is not implemented for Cloud SQL instances — during every backup session Veeam Backup for Google Cloud creates a full backup file in the standard backup chain. If Veeam Backup for Google Cloud detects an outdated restore point in a backup repository, it removes the earliest restore point from the backup chain. The issue will be addressed in a future release.
Retention Policy for Archived Backups

For archived backups, Veeam Backup for Google Cloud retains restore points for the number of days defined in backup scheduling settings as described in sections Creating VM Policies and Creating SQL Policies.

To track and remove outdated restore points from an archive backup chain, Veeam Backup for Google Cloud performs the following actions once a day:

1. Veeam Backup for Google Cloud checks the configuration database to detect archive backup repositories that contain outdated restore points.

2. If an outdated restore point exists in a backup repository, Veeam Backup for Google Cloud deploys a worker instance in a Google Cloud region in which the repository with backed-up data resides.

3. Veeam Backup for Google Cloud transforms the archive backup chain in the following way:
   a. Rebuilds the full archive backup file to include there data of the incremental archive backup file that follows the full archive backup file. To do that, Veeam Backup for Google Cloud injects into the full archive backup file data blocks from the earliest incremental archive backup file in the chain. This way, the full archive backup 'moves' forward in the archive backup chain.

   ![Diagram](image1.png)

   b. Removes the earliest incremental archive backup file from the chain as redundant — this data has already been injected into the full archive backup file.

   ![Diagram](image2.png)
4. Veeam Backup for Google Cloud repeats step 2 for all other outdated restore points found in the archive backup chain until all the restore points are removed. As data from multiple restore points is injected into the rebuilt full archive backup file, Veeam Backup for Google Cloud ensures that the archive backup chain is not broken and that you will be able to recover your data when needed.

5. Removes the worker instance when the retention session completes.

NOTES
- Each worker instance can process only one retention task at a time, and Veeam Backup for Google Cloud can simultaneously deploy maximum 10 worker instances to process retention tasks. If the number of retention tasks that must be processed by worker instances is more than the specified limit, the tasks exceeding this limit are queued.
- In version 3.0, the forever forward incremental backup method is not implemented for Cloud SQL instances — during every backup session Veeam Backup for Google Cloud creates a full backup file in the standard backup chain. If Veeam Backup for Google Cloud detects an outdated restore point in a backup repository, it removes the earliest restore point from the backup chain. The issue will be addressed in a future release.
Performing VM Backup

To produce cloud-native snapshots and image-level backups of VM instances, Veeam Backup for Google Cloud runs backup policies. A backup policy is a collection of settings that define the way backup operations are performed: what data to back up, where to store backups, when to start the backup process, and so on.

One backup policy can be used to process multiple VM instances within different regions, but you can back up each VM instance with one backup policy at a time. If a VM instance is added to more than one backup policy, it will be processed only by a backup policy that has the highest priority. Other backup policies will skip this VM instance from processing. For information on how to set a priority for a backup policy, see Setting Backup Policy Priority.

To schedule data protection tasks to run automatically, create backup policies. For each protected VM instance, you can also take a cloud-native snapshot manually when needed.

Creating Backup Policies

To create a backup policy, do the following:

1. Launch the Add VM Policy wizard.
2. Specify a backup policy name and description.
3. Configure backup source settings.
4. Configure backup target settings.
5. Create a schedule for the backup policy.
6. Enable label assignment.
7. Specify automatic retry, health check and notification settings for the backup policy.
8. Review the estimated cost of protecting the selected VM instances.
9. Finish working with the wizard.
Step 1. Launch Add VM Policy Wizard

To launch the Add VM Policy wizard, do the following:

1. Navigate to Policies > VM.
2. Click Add.

Step 2. Specify Backup Policy Name and Description

At the Policy Info step of the wizard, use the Name and Description fields to enter a name for the new backup policy and to provide a description for future reference. The maximum length of the name is 127 characters; the following characters are not supported: \ / ' " [ ] : | < > + = ; , ? * @ & _.

NOTE

When Veeam Backup for Google Cloud runs a backup policy, it adds the first 18 characters of the policy name to the names of snapshots created by the policy.
Step 3. Configure Backup Source Settings

At the Sources step of the wizard, specify the following backup source settings:

1. Choose a project where VM instances that you plan to back up belong.
2. Choose regions in which VM instances that you plan to back up reside.
3. Select VM instances to back up.

Step 3a. Choose Project

In the Project section of the Sources step of the wizard, choose a project that manages resources that you want to protect.

For a project to be displayed in the list of available projects, it must be added to Veeam Backup for Google Cloud as described in section Adding Projects.

**IMPORTANT**

It is recommended that you check whether the service account used to access the selected project has all the required permissions to perform data protection tasks. To do that, click Check Permissions.
Step 3b. Choose Regions

In the **Regions** section of the **Sources** step of the wizard, choose regions in which VM instances that you want to protect reside.

1. Click **Choose regions**.
2. In the **Choose regions** window, select the necessary regions, click **Add** to include them in the backup policy, and then click **Apply**.
Step 3c. Select VM Instances

In the **Resources** section of the **Sources** step of the wizard, specify the backup scope — select VM instances that Veeam Backup for Google Cloud will back up:

1. Click **Choose resources to protect**.

2. In the **Choose resources** window, choose whether you want to back up all VM instances from the regions selected at **step 3b**, or only specific VM instances.

   If you select the **All resources** option, Veeam Backup for Google Cloud will regularly check for new VM instances launched in the selected regions and automatically update the backup policy settings to include these instances in the backup scope.

   If you select the **Specific resources** option, you must also specify the instances explicitly:

   a. Use the **Resource type** drop-down list to choose whether you want to add individual VM instances or Google Cloud labels to the backup scope.

      If you select the **Label** option, Veeam Backup for Google Cloud will back up only those VM instances that reside in the selected regions under specific labels.

   b. Use the **Name** list to find the necessary resource, and then click **Include** to add the resource to the backup scope.

      For a resource to be displayed in the list of available resources, it must reside in a region that has ever been specified in any backup policy. Otherwise, the only option to discover available resources is to click **Browse** and wait for Veeam Backup for Google Cloud to populate the resource list.

      **TIP**

      You can simultaneously add multiple resources to the backup scope. To do that, click **Browse**, select check boxes next to the necessary VM instances or labels in the list of available resources, and then click **Protect**.

      If the list does not show the resources that you want to back up, click **Rescan** to launch the data collection process. As soon as the process is over, Veeam Backup for Google Cloud will update the resource list.

      If you add a label to the backup scope, Veeam Backup for Google Cloud will regularly check for new VM instances assigned the added label and automatically update the backup policy settings to include these instances in the scope. However, this applies only to VM instances from the regions selected at **step 3b**. If you select a label assigned to VM instances from other regions, these instances will not be protected by the backup policy. To work around the issue, either go back to step 3b and add the missing regions, or create a new backup policy.

3. To save changes made to the backup policy settings, click **Apply**.

   **TIP**

   As an alternative to selecting the **Specific resources** option and specifying the resources explicitly, you can select the **All resources** option and exclude a number of resources from the backup scope. To do that, click **Exclude resources** and specify the VM instances or labels that you do not want to back up — the procedure is the same as described for including resources in the backup scope.

   Mind that if a resource appears both in the list of included and excluded resources, Veeam Backup for Google Cloud will still not process the resource because the list of excluded resources has a higher priority.
### Specify source settings

Choose a project to add regions to, and then choose resources to protect by clicking the Create Policy button. The project and regions you choose will be used when you select resources to protect.

#### Project

To learn more about by Veeam Backup for Google Cloud, visit Google Cloud.

#### Region

Specify one or more regions. You can either choose regions from a list or enter a list of region names.

### Choose resources

#### Specific resources

- **Resource type:** Name
- **Include:**

#### Protected resources cp

<table>
<thead>
<tr>
<th>Resource ID</th>
<th>ID</th>
<th>Value</th>
<th>Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>653919714770334922</td>
<td>--</td>
<td>--</td>
<td>us-west1</td>
</tr>
<tr>
<td>7037420641167631457</td>
<td>--</td>
<td>--</td>
<td>us-east1</td>
</tr>
<tr>
<td>2422236943432078323</td>
<td>--</td>
<td>--</td>
<td>us-west2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Apply</th>
<th>Cancel</th>
</tr>
</thead>
</table>

Step 4. Configure Backup Target Settings

By default, backup policies create only cloud-native snapshots of processed instances. At the Targets step of the wizard, you can instruct Veeam Backup for Google Cloud to create image-level backups of the selected VM instances:

1. Set the Enable backups toggle to On.
2. Click Choose repository.
3. In the Choose repository window, select a standard backup repository where the created image-level backups will be stored.
   
   For a standard backup repository to be displayed in the Repository list, it must be added to Veeam Backup for Google Cloud as described in section Adding Backup Repositories. The Repository list shows only backup repositories of the Standard storage class.

3. To save changes made to the backup policy settings, click Apply.

You can also enable the backup archiving mechanism to instruct Veeam Backup for Google Cloud to store backed-up data in a low-cost, long-term archive storage:

1. Select the Enable backup archiving check box.
2. Click Choose repository.
3. In the Choose repository window, select an archive backup repository where the archived data will be stored.
   
   For an archive backup repository to be displayed in the Repository list, it must be added to Veeam Backup for Google Cloud as described in section Adding Backup Repositories. The Repository list shows only backup repositories of the Archive storage class.

4. To save changes made to the backup policy settings, click Apply.

For more information on the backup archiving mechanism, see Enabling Backup Archiving.
Step 5. Specify Policy Scheduling Options

At the Schedule step of the wizard, you can instruct Veeam Backup for Google Cloud to start the backup policy automatically according to a specific backup schedule. The backup schedule defines how often data of the VM instances added to the backup policy will be backed up.

To help you implement a comprehensive backup strategy, Veeam Backup for Google Cloud allows you to create schedules of the following types:

- **Daily** — the backup policy will create restore points repeatedly throughout a day on specific days.
- **Weekly** — the backup policy will create restore points once a day on specific days.
- **Monthly** — the backup policy will create restore points once a month on a specific day.
- **Yearly** — the backup policy will create restore points once a year on a specific day.

Combining multiple schedule types together allows you to retain restore points for longer periods of time — for more information, see Enabling Harmonized Scheduling. Combining multiple schedule types together also allows you to archive backups — for more information, see Enabling Backup Archiving.

Specifying Daily Schedule

To create a daily schedule for the backup policy, at the Schedule step of the wizard, do the following:

1. Set the **Daily schedule** toggle to **On** and click **Edit Daily Settings**.
2. In the **Create daily schedule** section, select hours when the backup policy will create cloud-native snapshots and image-level backups. Use the **Run at** drop-down list to choose whether you want the backup policy to run every day, on weekdays (Monday through Friday) or on specific days.

   If you want to protect VM instance data more frequently, you can instruct the backup policy to create multiple cloud-native snapshots per hour. To do that, click the link to the right of the **Snapshots** hour selection area, and specify the number of cloud-native snapshots that the backup policy will create within an hour.

**NOTE**

Veeam Backup for Google Cloud does not create image-level backups independently from cloud-native snapshots. That is why when you select hours for image-level backups, the same hours are automatically selected for cloud-native snapshots. To learn how Veeam Backup for Google Cloud performs backup, see How Backup Works.

3. In the **Configure daily retention** section, configure retention policy settings for the daily schedule:
   - For cloud-native snapshots, specify the number of restore points that you want to keep in a snapshot chain. If the restore point limit is exceeded, Veeam Backup for Google Cloud removes the earliest restore point from the chain. For more information, see Retention Policy for Snapshots.
   - For image-level backups, specify the number of days (or months) for which you want to keep restore points in a backup chain. If a restore point is older than the specified time limit, Veeam Backup for Google Cloud removes the restore point from the chain. For more information, see Retention Policy for Backups.

4. To save changes made to the backup policy settings, click **Apply**.
Specifying Weekly Schedule

To create a weekly schedule for the backup policy, at the Schedule step of the wizard, do the following:

1. Set the Weekly schedule toggle to On and click Edit Weekly Settings.

2. In the Create weekly schedule section, select days when the backup policy will create cloud-native snapshots and image-level backups. Use the Create restore points at drop-down list to schedule a specific time for the backup policy to run.

**NOTE**

Veeam Backup for Google Cloud does not create image-level backups independently from cloud-native snapshots. That is why when you select days for image-level backups, the same days are automatically selected for cloud-native snapshots. To learn how Veeam Backup for Google Cloud performs backup, see How Backup Works.

4. In the Configure weekly retention section, configure retention policy settings for the weekly schedule:
   - For cloud-native snapshots, specify the number of restore points that you want to keep in a snapshot chain.
     If the restore point limit is exceeded, Veeam Backup for Google Cloud removes the earliest restore point from the chain. For more information, see Retention Policy for Snapshots.
   - For image-level backups, specify the number of days (or months) for which you want to keep restore points in a backup chain.
     If a restore point is older than the specified time limit, Veeam Backup for Google Cloud removes the restore point from the chain. For more information, see Retention Policy for Backups.

5. To save changes made to the backup policy settings, click Apply.
Specifying Monthly Schedule

To create a monthly schedule for the backup policy, at the Schedule step of the wizard, do the following:

1. Set the Monthly schedule toggle to On and click Edit Monthly Settings.

2. In the Choose monthly backup target section, select months when the backup policy will create cloud-native snapshots and image-level backups. Use the Create restore points at and Run on drop-down lists to schedule a specific time and day for the backup policy to run.

**NOTE**

Veeam Backup for Google Cloud does not create image-level backups independently from cloud-native snapshots. That is why when you select months for image-level backups, the same months are automatically selected for cloud-native snapshots. To learn how Veeam Backup for Google Cloud performs backup, see How Backup Works.

3. In the Configure monthly retention section, configure retention policy settings for the monthly schedule:
   - For cloud-native snapshots, specify the number of restore points that you want to keep in a snapshot chain.
     
     If the restore point limit is exceeded, Veeam Backup for Google Cloud removes the earliest restore point from the chain. For more information, see Retention Policy for Snapshots.
   - For image-level backups, specify the number of days (or months) for which you want to keep restore points in a backup chain.
     
     If a restore point is older than the specified time limit, Veeam Backup for Google Cloud removes the restore point from the chain. For more information, see Retention Policy for Backups.

4. To save changes made to the backup policy settings, click Apply.
TIP

If you have enabled backup archiving at the Targets step of the wizard, and want to store monthly backups in an archive backup repository, set the Send backups to archive toggle to On, and follow the instructions provided in section Enabling Backup Archiving.
Specifying Yearly Schedule

[This step applies only if you have instructed Veeam Backup for Google Cloud to create image-level backups at the Targets step of the wizard]

To create a yearly schedule for the backup policy, at the Schedule step of the wizard, do the following:

1. Set the Yearly schedule toggle to On and click Edit Yearly Settings.

2. In the Create yearly schedule section, specify a day, month and time when the backup policy will create image-level backups.

   For example, if you select First, Friday, January and 06:00 PM, the backup policy will run every first Friday of January at 06:00 PM.

3. In the Keep backups for field, specify the number of years for which you want to keep restore points in a backup chain.

   If a restore point is older than the specified time limit, Veeam Backup for Google Cloud removes the restore point from the chain. For more information, see Retention Policy for Backups.

4. To save changes made to the backup policy settings, click Apply.

TIP

If you have enabled backup archiving at the Targets step of the wizard, and want to store yearly backups in an archive backup repository, set the Send backups to archive toggle to On, and follow the instructions provided in section Enabling Backup Archiving.
Enabling Harmonized Scheduling

When you combine multiple types of schedules, Veeam Backup for Google Cloud applies the harmonization mechanism that allows you to leverage restore points for long-term retentions instead of taking a new restore point every time. The mechanism simplifies the backup schedule, optimizes the backup performance and reduces the cost of retaining restore points.

With harmonized scheduling, Veeam Backup for Google Cloud can keep restore points created according to a daily, weekly or monthly schedule for longer periods of time:

- Cloud-native snapshots can be kept for weeks and months.
- Image-level backups can be kept for weeks, months and years.

For Veeam Backup for Google Cloud to use the harmonization mechanism, there must be specified at least 2 different schedules: one schedule will control the regular creation of restore points, while another schedule will control the process of retaining restore points. In terms of harmonized scheduling, Veeam Backup for Google Cloud re-uses restore points created according to a more-frequent schedule (daily, weekly or monthly) to achieve the desired retention for less-frequent schedules (weekly, monthly and yearly). Each restore point is marked with a flag of the related schedule type: the (Daily) flag is used to mark restore points created daily, (Weekly) — weekly, (Monthly) — monthly, and (Yearly) — yearly. Veeam Backup for Google Cloud uses these flags to control the retention period for the created restore points. Once a flag of a less-frequent schedule is assigned to a restore point, this restore point can no longer be removed — it is kept for the period defined in the retention settings. When the specified retention period is over, the flag is unassigned from the restore point. If the restore point does not have any other flags assigned, it is removed according to the retention settings of a more-frequent schedule.

NOTE

Restore points created according to a more-frequent schedule and less-frequent schedules compose a single backup or snapshot chain. This means that regardless of flags assigned to restore points, Veeam Backup for Google Cloud adds the restore points to the chain as described in sections Backup Chain and Snapshot Chain.

Consider the following example. You want a backup policy to create cloud-native snapshots of your critical workloads 3 times a day, to keep 3 daily snapshots in the snapshot chain, and also to retain one of the created snapshots for 2 weeks. In this case, you create 2 schedules when configuring the backup policy settings — daily and weekly:

1. In the daily scheduling settings, you select hours and days when snapshots will be created (for example, 7:00 AM, 9:00 AM, and 11:00 AM; Weekdays), and specify a number of daily restore points to retain (for example, 3).

   Veeam Backup for Google Cloud will propagate these settings to the schedule with a lower frequency (which is the weekly schedule in our example).
2. In the weekly scheduling settings, you specify which one of the snapshots created by the daily schedule will be kept for a longer period, and choose for how long you want to keep the selected snapshot.

For example, if you want to keep the daily restore point created at 7:00 AM on Monday for 2 weeks, you select 7:00 AM, Monday and specify 2 restore points to retain in the weekly schedule settings.
According to the specified scheduling settings, Veeam Backup for Google Cloud will create cloud-native snapshots in the following way:

1. On the first weekday (Monday), a backup session will start at 7:00 AM to create the first restore point. The restore point will be marked with the (Daily) flag as it was created according to the daily schedule.
   Since 7:00 AM, Monday is specified in the weekly scheduling settings, Veeam Backup for Google Cloud will assign the (Weekly) flag to this restore point.

2. On the same day (Monday), after backup sessions run at 9:00 AM and 11:00 AM, the created restore points will be marked with the (Daily) flag.

3. On the next weekday (Tuesday), after a backup session runs at 7:00 AM, the created restore point will be marked with the (Daily) flag.
   By the moment the backup session completes, the number of restore points with the (Daily) flag will exceed the retention limit specified in the daily scheduling settings. However, Veeam Backup for Google Cloud will not remove the earliest restore point (7:00 AM, Monday) with the (Daily) flag from the snapshot chain as this restore point is also marked with a flag of a less-frequent schedule. Instead, Veeam Backup for Google Cloud will unassign the (Daily) flag from the restore point. This restore point will be kept for the retention period specified in the weekly scheduling settings (that is, for 2 weeks).

4. On the same day (Tuesday), after a backup session runs at 9:00 AM, the number of restore points with the (Daily) flag will exceed the retention limit once again. Veeam Backup for Google Cloud will remove from the snapshot chain the restore point created at 9:00 AM on Monday as no flags of a less-frequent schedule are assigned to this restore point.
5. Veeam Backup for Google Cloud will continue creating restore points for the next week in the same way as described in steps 1–4.

6. On week 3, after a backup session runs at 7:00 AM on Monday, the number of weekly restore points will exceed the retention limit. Veeam Backup for Google Cloud will unassign the (Weekly) flag from the earliest weekly restore point. Since no other flags are assigned to this restore point, Veeam Backup for Google Cloud will remove this restore point from the snapshot chain.
Enabling Backup Archiving

When you combine multiple types of schedules, you can enable the archiving mechanism to instruct Veeam Backup for Google Cloud to store backed-up data in the low-cost, long-term Google Cloud archival storage. The mechanism is the most useful in the following cases:

- Your data retention policy requires that you keep rarely accessed data in an archive.
- You want to reduce data-at-rest costs and to save space in the high-cost, short-term Google Cloud standard storage.

With backup archiving, Veeam Backup for Google Cloud can retain backup files created according to a daily, weekly or monthly schedule for longer periods of time:

- To enable monthly archiving, you must configure a daily or a weekly schedule (or both).
- To enable yearly archiving, you must configure a daily, a weekly or a monthly schedule (or all three).

For Veeam Backup for Google Cloud to use the archiving mechanism, there must be specified at least 2 different schedules: one schedule will control the regular creation of backup files, while another schedule will control the process of copying backup files to an archive repository. Backup chains created according to these two schedules will be completely different — for more information, see Backup Chain and Archive Backup Chain.

Consider the following example. You want a backup policy to create image-level backups of your critical workloads once a week, to keep the backed-up data in a standard repository for 3 weeks, and also to keep backups created once in 2 months in an archive repository for a year. In this case, you create 2 schedules when configuring the backup policy settings — weekly and monthly:

1. In the policy target settings, you set the Enable backups toggle to On, select a standard repository that will store standard backups, and select an archive repository that will store archived data.
2. In the weekly scheduling settings, you select hours and days when backups will be created (for example, 7:00 AM, Monday), and specify a number of days for which Veeam Backup for Google Cloud will retain backups (for example, 21 days).

Veeam Backup for Google Cloud will propagate these settings to the archive schedule (which is the monthly schedule in our example).

3. In the monthly scheduling settings, you enable the archiving mechanism by setting the Send backups to archive toggle to On, specify when Veeam Backup for Google Cloud will create archive backup files, and choose for how long you want to keep the created backups in the archive repository.

For example, January, March, May, July, September, November, 12 months and First Monday.

**IMPORTANT**

- When you enable backup archiving, you become no longer able to create a schedule of the same frequency for standard backups. By design, these two functionalities are mutually exclusive.
- If you enable backup archiving, it is recommended that you set the Snapshots to keep value to 0, to reduce unexpected snapshot charges.
- If you enable backup archiving, it is recommended that you set the Keep archives for value to at least 12 months (or 365 days), since the minimum storage duration of the Google Cloud archival storage is 365 days.
- If you select the On day option, harmonized scheduling cannot be guaranteed. Plus, to support the On day option, Veeam Backup for Google Cloud will require to create an additional temporary restore point if there are no other schedules planned to run on that day. However, the temporary restore point will be removed by the Backup Retention process from the Google Cloud infrastructure during approximately 24 hours, to reduce unexpected infrastructure charges.
According to the specified scheduling settings, Veeam Backup for Google Cloud will create image-level backups in the following way:

1. On the first Monday of February, a backup session will start at 7:00 AM to create the first restore point in the standard backup chain. Veeam Backup for Google Cloud will store this restore point as a full backup file in the standard repository.

2. On the second and third Mondays of February, Veeam Backup for Google Cloud will create restore points at 7:00 AM and add them to the standard backup chain as incremental backup files in the standard repository.
3. On the fourth Monday of February, Veeam Backup for Google Cloud will create a new restore point at 7:00 AM. By the moment the backup session completes, the earliest restore point in the standard backup chain will get older than the specified retention limit. That is why Veeam Backup for Google Cloud will rebuild the full backup file and remove from the chain the restore point created on the first Monday.

For more information on how Veeam Backup for Google Cloud transforms standard backup chains, see *Retention Policy for Backups*.

4. On the first Monday of March, a backup session will start at 7:00 AM to create another restore point in the standard backup chain. At the same time, the earliest restore point in the standard backup chain will get older than the specified retention limit again. That is why Veeam Backup for Google Cloud will rebuild the full backup file again and remove from the chain the restore point created on the second Monday.

After the backup session completes, an archive session will create a restore point with all the data from the standard backup chain. Veeam Backup for Google Cloud will copy this restore point as a full archive backup file to the archive repository.
5. Up to May, Veeam Backup for Google Cloud will continue adding new restore points to the standard backup chain and deleting outdated backup files from the standard repository, according to the specified weekly scheduling settings.

On the first Monday of May, an archive session will create a restore point with only that data that has changed since the previous archive session in March. Veeam Backup for Google Cloud will copy this restore point as an incremental archive backup file to the archive repository.

6. Up to the first Monday of February of the next year, Veeam Backup for Google Cloud will continue adding new restore points to the standard backup chain and deleting outdated backup files from the standard repository, according to the specified weekly scheduling settings. Veeam Backup for Google Cloud will also continue adding new restore points to the archive backup chain, according to the specified monthly settings.

By the moment the archive session completes, the earliest restore point in the archive backup chain will get older than the specified retention limit. That is why Veeam Backup for Google Cloud will rebuild the full archive backup file and remove from the chain the restore point created on the first Monday of March of the previous year.

For more information on how Veeam Backup for Google Cloud transforms archive backup chains, see Retention Policy for Archived Backups.
Step 6. Enable Label Assignment

At the **Labels** step, you can instruct Veeam Backup for Google Cloud to assign labels to cloud-native snapshots created by the backup policy:

1. Click either the **Labels will not be copied from source disks** or **Custom labels will not be assigned** link.

2. In the **Choose labels to assign** window, choose whether you want to assign to snapshots of the selected VM instances already existing labels from source persistent disks and your own custom labels.

   If you set the **Assign custom labels** toggle to **On**, you must also specify the labels explicitly. To do that, use the **Name** and **Value** fields to specify a name and a value for the new custom label, and then click **Add**. Note that you cannot add more than 5 custom labels.

3. To save changes made to the backup policy settings, click **Apply**.
Step 7. Configure General Settings

At the Settings step of the wizard, you can enable automatic retries, schedule health checks and specify notification settings for the backup policy.

Automatic Retry Settings

To instruct Veeam Backup for Google Cloud to run the backup policy again if it fails on the first try, do the following:

1. In the Retries section of the step, select the Automatically retry failed policy check box.
2. In the field to the right of the check box, specify the maximum number of attempts to run the backup policy. The time interval between retries is 15 minutes.

When retrying backup policies, Veeam Backup for Google Cloud processes only those VM instances that failed to be backed up during the previous attempt.

**NOTE**

The automatic retry settings apply only to backup policies that run according to specific schedules — these settings do not apply to policies started manually.

Health Check Settings

If you have enabled creation of image-level backups at step 4, you can instruct Veeam Backup for Google Cloud to periodically perform a health check for all restore points created by the backup policy. During the health check, Veeam Backup for Google Cloud performs an availability check for data blocks in backup files in the whole standard backup chain, and a cyclic redundancy check (CRC) for metadata to verify its integrity. The health check helps you ensure that the restore points are consistent and that you will be able to restore data using these restore points.

To instruct Veeam Backup for Google Cloud to perform a monthly health check, do the following:

1. In the Health check section of the step, set the Enable health check toggle to On.
2. Use the Run on drop-down lists to schedule a specific day for the health check to run.

**NOTE**

Veeam Backup for Google Cloud performs the health check during the last policy session that runs on the day when the health check is scheduled. If another backup policy session runs on the same day, Veeam Backup for Google Cloud will not perform the health check during that session. For example, if the backup policy is scheduled to run multiple times on Saturday, and the health check is also scheduled to run on Saturday, the health check will only be performed during the last policy session on Saturday.
Notification Settings

To instruct Veeam Backup for Google Cloud to send email notifications for the backup policy, do the following:

1. In the Notifications section of the step, set the Enable notifications toggle to On.
   
   If you set the toggle to Off, Veeam Backup for Google Cloud will send notifications according to the configured global notification settings.

2. In the Email field, specify an email address of a recipient. Use a semicolon to separate multiple recipient addresses.

3. Use the Notify on list to choose whether you want Veeam Backup for Google Cloud to send email notifications in case the backup policy completes successfully, completes with warnings or completes with errors.

4. Select the Suppress notifications until the last retry check box to receive a notification about the final backup policy result.

   If you do not select the check box, Veeam Backup for Google Cloud will send a notification for every backup policy retry.

**NOTE**

If you specify the same email recipient in both backup policy notification and global notification settings, Veeam Backup for Google Cloud will send each notification to this recipient twice.
Step 8. Review Estimated Cost

[This step applies only if you have created a schedule for the backup policy at the Schedule step of the wizard]

At the Cost Estimation step of the wizard, review the approximate monthly cost of Google Cloud services that Veeam Backup for Google Cloud will require to protect the VM instances added to the backup policy. The total estimated cost includes the following:

- The cost of creating and maintaining cloud-native snapshots of the VM instances.
  
  For each VM instance included in the backup policy, Veeam Backup for Google Cloud takes into account the total size and the number of persistent disks attached, the number of restore points to be kept in the snapshot chain, and the configured scheduling settings.

- The cost of creating and storing in backup repositories image-level backups of the VM instances.
  
  For each VM instance included in the backup policy, Veeam Backup for Google Cloud takes into account the total size and the number of persistent disks attached, the number of restore points to be kept in the backup chain, and the configured scheduling and health check settings.

- The cost of transferring the VM instance data between Google Cloud regions during data protection operations (for example, if a protected VM instance and the target storage bucket reside in different regions).
  
  - The cost of sending API requests to Google Cloud during data protection operations.

The estimated cost may occur to be significantly higher due to the backup frequency, cross-region data transfer and snapshot charges. To reduce the cost, you can try the following workarounds:

- To avoid additional costs related to cross-region data transfer, select a backup repository that resides in the same region as VM instances that you plan to back up.

- To reduce high snapshot charges, adjust the snapshot retention settings to keep less restore points in the snapshot chain.

- To optimize the cost of storing backups, modify the scheduling settings to run the backup policy less frequently, or specify an archive repository for long-term retention of restore points.

**TIP**

You can save the cost estimation as a .CSV or .XML file. To do that, click Export to and select the necessary format.
Step 9. Finish Working with Wizard

At the Summary step of the wizard, review configuration information and click Finish.
Creating Snapshots Manually

Veeam Backup for Google Cloud allows you to manually create snapshots of VM instances. Each snapshot is saved to the same region in which the protected VM instance resides.

**NOTE**

Veeam Backup for Google Cloud does not include snapshots created manually in the snapshot chain and does not apply the configured retention policy settings to these snapshots. This means that the snapshots are kept in your Google Cloud environment unless you remove them manually, as described in section Removing Backups and Snapshots.

To manually create a cloud-native snapshot of a VM instance, do the following:

1. Navigate to **Resources > VM**.
2. Select the necessary instance and click **Take Snapshot Now**.
   
   For a VM instance to be displayed in the list of available instances, it must reside in any of the regions added to a backup policy as described in section Creating Backup Policies.

3. In the **Take Snapshot Now** window, choose whether you want to assign labels to the created snapshot:
   
   - To assign already existing labels from the source persistent disk attached to the selected VM instance, select the **Copy labels from source disks** check box.
   
   - To assign your own custom labels, select the **Add custom labels** check box and specify the labels explicitly. To do that, use the **Name** and **Value** fields to specify a key and a value for the new custom label, and then click **Add**.

   To save changes made to the snapshot settings, click **Take Snapshot**.
Performing SQL Backup

To produce cloud-native snapshots and image-level backups of Cloud SQL instances, Veeam Backup for Google Cloud runs backup policies. A backup policy is a collection of settings that define the way backup operations are performed: what data to back up, where to store backups, when to start the backup process, and so on.

One backup policy can be used to process multiple Cloud SQL instances within different regions, but you can back up each instance with one backup policy at a time. If a Cloud SQL instance is added to more than one backup policy, it will be processed only by a backup policy that has the highest priority. Other backup policies will skip this instance from processing. For information on how to set a priority for a backup policy, see Setting Backup Policy Priority.

To schedule data protection tasks to run automatically, create backup policies. For each protected Cloud SQL instance, you can also take a cloud-native snapshot manually when needed.

Creating Backup Policies

To create a backup policy, do the following:

1. Launch the Add Cloud SQL Policy wizard.
2. Specify a backup policy name and description.
3. Configure backup source settings.
4. Configure backup target settings.
5. Create a schedule for the backup policy.
6. Choose whether you want to use a staging server to perform backup.
7. Specify automatic retry, health check and notification settings for the backup policy.
8. Review the estimated cost of protecting the selected Cloud SQL instances.
9. Finish working with the wizard.
Step 1. Launch Add Cloud SQL Policy Wizard

To launch the **Add Cloud SQL Policy** wizard, do the following:

1. Navigate to **Policies > Cloud SQL**.
2. Click **Add**.

![Add Cloud SQL Policy Wizard](image)

Step 2. Specify Backup Policy Name and Description

At the **Policy Info** step of the wizard, use the **Name** and **Description** fields to enter a name for the new backup policy and to provide a description for future reference. The maximum length of the name is 127 characters; the following characters are not supported: \ / " ' [ ] : | < > + = ; , ? * @ & _ .

**NOTE**

When Veeam Backup for Google Cloud runs a backup policy, it adds the word **Veeam** to the descriptions of snapshots created by the policy.
Step 3. Configure Backup Source Settings

At the **Sources** step of the wizard, specify the following backup source settings:

1. Choose a project where Cloud SQL instances that you plan to back up belong.
2. Choose regions in which Cloud SQL instances that you plan to back up reside.
3. Select Cloud SQL instances to back up.

Step 3a. Choose Project

In the **Project** section of the **Sources** step of the wizard, choose a project that manages resources that you want to protect.

For a project to be displayed in the list of available projects, it must be added to Veeam Backup for Google Cloud as described in section **Adding Projects**.

**IMPORTANT**

It is recommended that you check whether the service account used to access the selected project has all the required permissions to perform data protection tasks. To do that, click **Check Permissions**.
Step 3b. Choose Regions

In the **Regions** section of the **Sources** step of the wizard, choose regions in which Cloud SQL instances that you want to protect reside.

1. Click **Choose regions**.
2. In the **Choose regions** window, select the necessary regions, click **Add** to include them in the backup policy, and then click **Apply**.

![Choose regions window screenshot](image-url)
Step 3c. Select Cloud SQL Instances

In the Resources section of the Sources step of the wizard, specify the backup scope — select Cloud SQL instances that Veeam Backup for Google Cloud will back up:

1. Click Choose resources to protect.
2. In the Choose resources window, choose whether you want to back up all Cloud SQL instances from the regions selected at step 3b, or only specific Cloud SQL instances.

If you select the All resources option, Veeam Backup for Google Cloud will regularly check for new Cloud SQL instances launched in the selected regions and automatically update the backup policy settings to include these instances in the backup scope.

If you select the Specific resources option, you must also specify the instances explicitly:

   a. Use the Resource type drop-down list to choose whether you want to add individual Cloud SQL instances or Google Cloud labels to the backup scope.

      If you select the Label option, Veeam Backup for Google Cloud will back up only those Cloud SQL instances that reside in the selected regions under specific labels.

   b. Use the search field to the right of the Resource type list to find the necessary resource, and then click Include to add the resource to the backup scope.

   For a resource to be displayed in the list of available resources, it must reside in a region that has ever been specified in any backup policy. Otherwise, the only option to discover available resources is to click Browse and wait for Veeam Backup for Google Cloud to populate the resource list.

TIP

You can simultaneously add multiple resources to the backup scope. To do that, click Browse, select check boxes next to the necessary Cloud SQL instances or labels in the list of available resources, and then click Protect.

If the list does not show the resources that you want to back up, click Rescan to launch the data collection process. As soon as the process is over, Veeam Backup for Google Cloud will update the resource list.

If you add a label to the backup scope, Veeam Backup for Google Cloud will regularly check for new Cloud SQL instances assigned the added label and automatically update the backup policy settings to include these instances in the scope. However, this applies only to Cloud SQL instances from the regions selected at step 3b. If you select a label assigned to Cloud SQL instances from other regions, these instances will not be protected by the backup policy. To work around the issue, either go back to step 3b and add the missing regions, or create a new backup policy.

3. To save changes made to the backup policy settings, click Apply.

TIP

As an alternative to selecting the Specific resources option and specifying the resources explicitly, you can select the All resources option and exclude a number of resources from the backup scope. To do that, click Exclude resources and specify the Cloud SQL instances or labels that you do not want to back up — the procedure is the same as described for including resources in the backup scope.

Mind that if a resource appears both in the list of included and excluded resources, Veeam Backup for Google Cloud will still not process the resource because the list of excluded resources has a higher priority.
Step 4. Configure Backup Target Settings

By default, backup policies create only cloud-native snapshots of processed instances. At the Targets step of the wizard, you can instruct Veeam Backup for Google Cloud to create image-level backups of the selected Cloud SQL instances:

1. Set the Enable backups toggle to On.
2. Click Choose repository.
3. In the Choose repository window, select a standard backup repository where the created image-level backups will be stored.
   
   For a standard backup repository to be displayed in the Repository list, it must be added to Veeam Backup for Google Cloud as described in section Adding Backup Repositories. The Repository list shows only backup repositories of the Standard storage class.
4. To save changes made to the backup policy settings, click Apply.

You can also enable the backup archiving mechanism to instruct Veeam Backup for Google Cloud to store backed-up data in a low-cost, long-term archive storage:

1. Select the Archives will be stored in check box.
2. Click Choose repository.
3. In the Choose repository window, select an archive backup repository where the archived data will be stored.
   
   For an archive backup repository to be displayed in the Repository list, it must be added to Veeam Backup for Google Cloud as described in section Adding Backup Repositories. The Repository list shows only backup repositories of the Archive storage class.
4. To save changes made to the backup policy settings, click Apply.
Step 5. Specify Policy Scheduling Options

At the Schedule step of the wizard, you can instruct Veeam Backup for Google Cloud to start the backup policy automatically according to a specific backup schedule. The backup schedule defines how often data of the Cloud SQL instances added to the backup policy will be backed up.

To help you implement a comprehensive backup strategy, Veeam Backup for Google Cloud allows you to create schedules of the following types:

- **Daily** — the backup policy will create restore points repeatedly throughout a day on specific days.
- **Weekly** — the backup policy will create restore points once a day on specific days.
- **Monthly** — the backup policy will create restore points once a month on a specific day.
- **Yearly** — the backup policy will create restore points once a year on a specific day.

Combining multiple schedule types together allows you to retain restore points for longer periods of time — for more information, see Enabling Harmonized Scheduling.

Specifying Daily Schedule

To create a daily schedule for the backup policy, at the Schedule step of the wizard, do the following:

1. Set the Daily schedule toggle to On and click Edit Daily Settings.

2. In the Create daily schedule section, select hours when the backup policy will create cloud-native snapshots and image-level backups. Use the Run at drop-down list to choose whether you want the backup policy to run every day, on weekdays (Monday through Friday) or on specific days.

   If you want to protect Cloud SQL instance data more frequently, you can instruct the backup policy to create multiple cloud-native snapshots per hour. To do that, click the link to the right of the Snapshots hour selection area, and specify the number of cloud-native snapshots that the backup policy will create within an hour.

   **NOTE**

   Veeam Backup for Google Cloud does not create image-level backups independently from cloud-native snapshots. That is why when you select hours for image-level backups, the same hours are automatically selected for cloud-native snapshots. To learn how Veeam Backup for Google Cloud performs backup, see How Backup Works.

3. In the Configure daily retention section, configure retention policy settings for the daily schedule:

   o For cloud-native snapshots, specify the number of restore points that you want to keep in a snapshot chain.
     
     If the restore point limit is exceeded, Veeam Backup for Google Cloud removes the earliest restore point from the chain. For more information, see Retention Policy for Snapshots.

   o For image-level backups, specify the number of days (or months) for which you want to keep restore points in a backup chain.
     
     If a restore point is older than the specified time limit, Veeam Backup for Google Cloud removes the restore point from the chain. For more information, see Retention Policy for Backups.

5. To save changes made to the backup policy settings, click Apply.
Specifying Weekly Schedule

To create a weekly schedule for the backup policy, at the Schedule step of the wizard, do the following:

1. Set the Weekly schedule toggle to On and click Edit Weekly Settings.

2. In the Create weekly schedule section, select days when the backup policy will create cloud-native snapshots and image-level backups. Use the Create restore points at drop-down list to schedule a specific time for the backup policy to run.

   **NOTE**

   Veeam Backup for Google Cloud does not create image-level backups independently from cloud-native snapshots. That is why when you select days for image-level backups, the same days are automatically selected for cloud-native snapshots. To learn how Veeam Backup for Google Cloud performs backup, see How Backup Works.

4. In the Configure weekly retention section, configure retention policy settings for the weekly schedule:
   
   o For cloud-native snapshots, specify the number of restore points that you want to keep in a snapshot chain.
     
     If the restore point limit is exceeded, Veeam Backup for Google Cloud removes the earliest restore point from the chain. For more information, see Retention Policy for Snapshots.

   o For image-level backups, specify the number of days (or months) for which you want to keep restore points in a backup chain.
     
     If a restore point is older than the specified time limit, Veeam Backup for Google Cloud removes the restore point from the chain. For more information, see Retention Policy for Backups.

5. To save changes made to the backup policy settings, click Apply.
Specifying Monthly Schedule

To create a monthly schedule for the backup policy, at the **Schedule** step of the wizard, do the following:

1. Set the **Monthly schedule** toggle to **On** and click **Edit Monthly Settings**.

2. In the **Choose monthly backup target** section, select months when the backup policy will create cloud-native snapshots and image-level backups. Use the **Create restore points at** and **Run on** drop-down lists to schedule a specific time and day for the backup policy to run.

**NOTE**

Veeam Backup for Google Cloud does not create image-level backups independently from cloud-native snapshots. That is why when you select months for image-level backups, the same months are automatically selected for cloud-native snapshots. To learn how Veeam Backup for Google Cloud performs backup, see **How Backup Works**.

3. In the **Configure monthly retention** section, configure retention policy settings for the monthly schedule:
   
   o For cloud-native snapshots, specify the number of restore points that you want to keep in a snapshot chain.
     
     If the restore point limit is exceeded, Veeam Backup for Google Cloud removes the earliest restore point from the chain. For more information, see **Retention Policy for Snapshots**.

   o For image-level backups, specify the number of days (or months) for which you want to keep restore points in a backup chain.
     
     If a restore point is older than the specified time limit, Veeam Backup for Google Cloud removes the restore point from the chain. For more information, see **Retention Policy for Backups**.

4. To save changes made to the backup policy settings, click **Apply**.
Specifying Yearly Schedule

[This step applies only if you have instructed Veeam Backup for Google Cloud to create image-level backups at the Targets step of the wizard]

To create a yearly schedule for the backup policy, at the Schedule step of the wizard, do the following:

1. Set the Yearly schedule toggle to On and click Edit Yearly Settings.

2. In the Create yearly schedule section, specify a day, month and time when the backup policy will create image-level backups.

   For example, if you select First, Friday, January and 06:00 PM, the backup policy will run every first Friday of January at 06:00 PM.

3. In the Keep backups for field, specify the number of years for which you want to keep restore points in a backup chain.

   If a restore point is older than the specified time limit, Veeam Backup for Google Cloud removes the restore point from the chain. For more information, see Retention Policy for Backups.

4. To save changes made to the backup policy settings, click Apply.

TIP

If you have enabled backup archiving at the Targets step of the wizard, and want to store yearly backups in an archive backup repository, set the Send backups to archive toggle to On.
Enabling Harmonized Scheduling

When you combine multiple types of schedules, Veeam Backup for Google Cloud applies the harmonization mechanism that allows you to leverage restore points for long-term retentions instead of taking a new restore point every time. The mechanism simplifies the backup schedule, optimizes the backup performance and reduces the cost of retaining restore points.

With harmonized scheduling, Veeam Backup for Google Cloud can keep restore points created according to a daily, weekly or monthly schedule for longer periods of time:

- Cloud-native snapshots can be kept for weeks and months.
- Image-level backups can be kept for weeks, months and years.

For Veeam Backup for Google Cloud to use the harmonization mechanism, there must be specified at least 2 different schedules: one schedule will control the regular creation of restore points, while another schedule will control the process of retaining restore points. In terms of harmonized scheduling, Veeam Backup for Google Cloud re-uses restore points created according to a more-frequent schedule (daily, weekly or monthly) to achieve the desired retention for less-frequent schedules (weekly, monthly and yearly). Each restore point is marked with a flag of the related schedule type: the (Daily) flag is used to mark restore points created daily, (Weekly) — weekly, (Monthly) — monthly, and (Yearly) — yearly. Veeam Backup for Google Cloud uses these flags to control the retention period for the created restore points. Once a flag of a less-frequent schedule is assigned to a restore point, this restore point can no longer be removed — it is kept for the period defined in the retention settings. When the specified retention period is over, the flag is unassigned from the restore point. If the restore point does not have any other flags assigned, it is removed according to the retention settings of a more-frequent schedule.

**NOTE**

Restore points created according to a more-frequent schedule and less-frequent schedules compose a single backup or snapshot chain. This means that regardless of flags assigned to restore points, Veeam Backup for Google Cloud adds the restore points to the chain as described in sections Backup Chain and Snapshot Chain.
Consider the following example. You want a backup policy to create cloud-native snapshots of your critical workloads 3 times a day, to keep 3 daily snapshots in the snapshot chain, and also to retain one of the created snapshots for 2 weeks. In this case, you create 2 schedules when configuring the backup policy settings — daily and weekly:

1. In the daily scheduling settings, you select hours and days when snapshots will be created (for example, 7:00 AM, 9:00 AM, and 11:00 AM; Weekdays), and specify a number of daily restore points to retain (for example, 3).

Veeam Backup for Google Cloud will propagate these settings to the schedule with a lower frequency (which is the weekly schedule in our example).
2. In the weekly scheduling settings, you specify which one of the snapshots created by the daily schedule will be kept for a longer period, and choose for how long you want to keep the selected snapshot.

For example, if you want to keep the daily restore point created at 7:00 AM on Monday for 2 weeks, you select 7:00 AM, Monday and specify 2 restore points to retain in the weekly schedule settings.

According to the specified scheduling settings, Veeam Backup for Google Cloud will create cloud-native snapshots in the following way:

1. On the first weekday (Monday), a backup session will start at 7:00 AM to create the first restore point. The restore point will be marked with the (Daily) flag as it was created according to the daily schedule.

   Since 7:00 AM, Monday is specified in the weekly scheduling settings, Veeam Backup for Google Cloud will assign the (Weekly) flag to this restore point.

2. On the same day (Monday), after backup sessions run at 9:00 AM and 11:00 AM, the created restore points will be marked with the (Daily) flag.

3. On the next weekday (Tuesday), after a backup session runs at 7:00 AM, the created restore point will be marked with the (Daily) flag.

   By the moment the backup session completes, the number of restore points with the (Daily) flag will exceed the retention limit specified in the daily scheduling settings. However, Veeam Backup for Google Cloud will not remove the earliest restore point (7:00 AM, Monday) with the (Daily) flag from the snapshot chain as this restore point is also marked with a flag of a less-frequent schedule. Instead, Veeam Backup for Google Cloud will unassign the (Daily) flag from the restore point. This restore point will be kept for the retention period specified in the weekly scheduling settings (that is, for 2 weeks).
4. On the same day (Tuesday), after a backup session runs at 9:00 AM, the number of restore points with the (Daily) flag will exceed the retention limit once again. Veeam Backup for Google Cloud will remove from the snapshot chain the restore point created at 9:00 AM on Monday as no flags of a less-frequent schedule are assigned to this restore point.

5. Veeam Backup for Google Cloud will continue creating restore points for the next week in the same way as described in steps 1–4.

6. On week 3, after a backup session runs at 7:00 AM on Monday, the number of weekly restore points will exceed the retention limit. Veeam Backup for Google Cloud will unassign the (Weekly) flag from the earliest weekly restore point. Since no other flags are assigned to this restore point, Veeam Backup for Google Cloud will remove this restore point from the snapshot chain.
Step 6. Specify Processing Options

At the Processing Options step of the wizard, choose whether you want to use a staging server to perform backup. To learn how Veeam Backup for Google Cloud uses staging servers to protect Cloud SQL instances, see How Backup Works.

ProtectingInstancesWithoutStagingServer

To back up the selected Cloud SQL instances without a staging server, do the following:

1. Select the Use production instance option.
2. Click Choose option.
3. In the Choose authentication option window, choose the database authentication method that will be used to authenticate against the production Cloud SQL instance.
   
   If you select the Cloud SQL User option, also specify credentials of a user that Veeam Backup for Google Cloud will use to access the instance. If you select the Cloud IAM option, Veeam Backup for Google Cloud will automatically detect the unique email address associated with the service account that will be used to access the instance — this is the service account that was specified when adding the project where the instance belongs to Veeam Backup for Google Cloud.

   IMPORTANT

   To be able to use the Cloud IAM option, you must configure Cloud SQL IAM database authentication for the instance in the Google Cloud console in advance, as described in Google Cloud documentation.

4. Click Apply.
Protecting Instances With Staging Server

To back up the selected Cloud SQL instances using a staging server, select the **Use staging server** option.

**NOTE**

When performing backup with a staging server, Veeam Backup for Google Cloud uses the Default Administrator account to send REST API requests to the Cloud SQL instances processed by the backup policy. That is why there is no need to specify credentials for authentication.
Step 7. Configure General Settings

At the **Settings** step of the wizard, you can enable automatic retries, schedule health checks and specify notification settings for the backup policy.

**Automatic Retry Settings**

To instruct Veeam Backup for Google Cloud to run the backup policy again if it fails on the first try, do the following:

1. In the **Retries** section of the step, select the **Automatically retry failed policy** check box.
2. In the field to the right of the check box, specify the maximum number of attempts to run the backup policy. The time interval between retries is 15 minutes.

When retrying backup policies, Veeam Backup for Google Cloud processes only those Cloud SQL instances that failed to be backed up during the previous attempt.

**NOTE**

The automatic retry settings apply only to backup policies that run according to specific schedules — these settings do not apply to policies **started manually**.

**Health Check Settings**

You can instruct Veeam Backup for Google Cloud to periodically perform a health check for all restore points created by the backup policy. During the health check, Veeam Backup for Google Cloud performs an availability check for data blocks in backup files in the whole standard backup chain, and a cyclic redundancy check (CRC) for metadata to verify its integrity. The health check helps you ensure that the restore points are consistent and that you will be able to restore data using these restore points.

To instruct Veeam Backup for Google Cloud to perform a monthly health check, do the following:

1. In the **Health check** section of the step, set the **Enable health check** toggle to **On**.
2. Use the **Run on** drop-down lists to schedule a specific day for the health check to run.

**NOTE**

Veeam Backup for Google Cloud performs the health check during the last policy session that runs on the day when the health check is scheduled. If another backup policy session runs on the same day, Veeam Backup for Google Cloud will not perform the health check during that session. For example, if the backup policy is scheduled to run multiple times on Saturday, and the health check is also scheduled to run on Saturday, the health check will only be performed during the last policy session on Saturday.
Notification Settings

To instruct Veeam Backup for Google Cloud to send email notifications for the backup policy, do the following:

1. In the **Notifications** section of the step, set the **Enable notifications** toggle to **On**.
   
   If you set the toggle to **Off**, Veeam Backup for Google Cloud will send notifications according to the configured **global notification settings**.

2. In the **Email** field, specify an email address of a recipient. Use a semicolon to separate multiple recipient addresses.

3. Use the **Notify on** list to choose whether you want Veeam Backup for Google Cloud to send email notifications in case the backup policy completes successfully, completes with warnings or completes with errors.

4. Select the **Suppress notifications until the last retry** check box to receive a notification about the final backup policy result.
   
   If you do not select the check box, Veeam Backup for Google Cloud will send a notification for every backup policy retry.

**NOTE**

If you specify the same email recipient in both backup policy notification and **global notification settings**, Veeam Backup for Google Cloud will send each notification to this recipient twice.
Step 8. Review Estimated Cost

[This step applies only if you have created a schedule for the backup policy at the Schedule step of the wizard]

At the Cost Estimation step of the wizard, review the approximate monthly cost of Google Cloud services that Veeam Backup for Google Cloud will require to protect the Cloud SQL instances added to the backup policy. The total estimated cost includes the following:

- The cost of creating and maintaining cloud-native snapshots of the Cloud SQL instances.
  For each Cloud SQL instance included in the backup policy, Veeam Backup for Google Cloud takes into account the amount of storage provisioned for the instance, the number of restore points to be kept in the snapshot chain, and the configured scheduling settings.

- The cost of creating and storing in backup repositories image-level backups of the Cloud SQL instances.
  For each Cloud SQL instance included in the backup policy, Veeam Backup for Google Cloud takes into account the amount of storage provisioned for the instance, the number of restore points to be kept in the backup chain, the specified processing options, and the configured scheduling and health check settings.

- The cost of transferring the Cloud SQL instance data between Google Cloud regions during data protection operations (for example, if a protected Cloud SQL instance and the target storage bucket reside in different regions).
  - The cost of sending API requests to Google Cloud during data protection operations.

The estimated cost may occur to be significantly higher due to the backup frequency, cross-region data transfer and snapshot charges. To reduce the cost, you can try the following workarounds:

- To avoid additional costs related to cross-region data transfer, select a backup repository that resides in the same region as Cloud SQL instances that you plan to back up.
- To reduce high snapshot charges, adjust the snapshot retention settings to keep less restore points in the snapshot chain.
- To optimize the cost of storing backups, modify the scheduling settings to run the backup policy less frequently, or specify an archive repository for long-term retention of restore points.

TIP
You can save the cost estimation as a .CSV or .XML file. To do that, click Export to and select the necessary format.
Step 9. Finish Working with Wizard

At the Summary step of the wizard, review configuration information and click Finish.
Creating Snapshots Manually

Veeam Backup for Google Cloud allows you to manually create snapshots of Cloud SQL instances. Each snapshot is saved to the same region in which the protected Cloud SQL instance resides.

**NOTE**

Veeam Backup for Google Cloud does not include snapshots created manually in the snapshot chain and does not apply the configured retention policy settings to these snapshots. This means that the snapshots are kept in your Google Cloud environment unless you remove them manually, as described in section Removing Backups and Snapshots.

To manually create a cloud-native snapshot of a Cloud SQL instance, do the following:

1. Navigate to **Resources > Cloud SQL**.
2. Select the necessary instance and click **Take Snapshot Now**.

   For a Cloud SQL instance to be displayed in the list of available instances, it must reside in any of the regions added to a backup policy as described in section Creating Backup Policies.
Editing Backup Policy Settings

For each backup policy, you can modify settings configured while creating the policy:

1. Navigate to Policies.
2. Switch to the necessary tab and select the backup policy.
3. Click Edit.
4. Complete the Edit Policy wizard:
   a. To provide a new name and description for the policy, follow the instructions provided in section Performing VM Backup (step 2) or Performing SQL Backup (step 2).
   b. To choose another project, to modify the list of regions in which instances that you plan to back up reside, or to add instances to the backup scope, follow the instructions provided in section Performing VM Backup (step 3a, step 3b or step 3c) or Performing SQL Backup (step 3a, step 3b or step 3c).

   IMPORTANT

   If you change the project that manages resources that you want to protect, it is recommended that you check whether the service account used to access the selected project has all the required permissions to perform data protection tasks. To do that, click Check Permissions.

   c. To instruct Veeam Backup for Google Cloud to create image-level backups, follow the instructions provided in section Performing VM Backup (step 4) or Performing SQL Backup (step 4).
   d. To modify the schedule configured for the policy, follow the instructions provided in section Performing VM Backup (step 5) or Performing SQL Backup (step 5).
   e. [This step applies only to VM backup policies] To assign labels to cloud-native snapshots, follow the instructions provided in section Performing VM Backup (step 6).
   [This step applies only to SQL backup policies] To choose whether you want to use a staging server to perform backup, follow the instructions provided in section Performing SQL Backup (step 6).
   f. To configure automatic retry, health check and notification settings, follow the instructions provided in section Performing VM Backup (step 7) or Performing SQL Backup (step 7).
   g. At the Summary step of the wizard, review configuration information and click Finish.
## Summary

### General settings
- **Name:** asia-east-policy
- **Description:** Protecting instances in asia-east regions
- **Regions:** 2 regions
- **Project:** NIO backup 2

### Protected resources
- **Instances:** 12 instances
- **Labels:**

### Snapshot settings
- **Snapshots enabled:** Yes
- **Copy snapshots from source disks:** No
- **Add custom labels:** No
- **Weekly retention:** Keep 7 weekly snapshots
- **Monthly retention:** Keep 7 monthly snapshots

### Backup settings
- **Backups enabled:** Yes
- **Archival enabled:** No
- **Weekly retention:** Keep weekly backup for 21 days (5 backups excluded)
- **Monthly retention:** Keep monthly backup for 30 days (9 backups excluded)

### Other settings
- **Automatic restore enabled:** Yes
Setting Backup Policy Priority

By default, Veeam Backup for Google Cloud runs backup policies in the order you create them. However, you can set the backup policy priority manually:

1. Navigate to Policies.
2. Switch to the necessary tab and click Priority.
3. In the Priority Order window, do the following:
   a. Select a backup policy in the list of existing policies.
   b. To move the policy up or down the list, use the Up and Down arrows.
   c. To save changes made to the priority order, click Apply.

**NOTE**

If an instance is included into multiple backup policies, it will be processed only by the backup policy that has the highest priority.
Enabling and Disabling Backup Policies

By default, Veeam Backup for Google Cloud runs all created backup policies according to the specified schedules. However, you can temporarily disable a backup policy so that Veeam Backup for Google Cloud does not run the backup policy automatically. You will still be able to manually start or enable the disabled backup policy at any time you need.

To enable or disable a backup policy, do the following:

1. Navigate to Policies.
2. Switch to the necessary tab and select the backup policy.
3. Click Enable or Disable.
Starting and Stopping Backup Policies

You can start a backup policy manually, for example, if you want to create an additional restore point in the snapshot or backup chain and do not want to modify the configured backup policy schedule. You can also stop a backup policy if processing of an instance is about to take too long, and you do not want the policy to have an impact on the production environment during business hours.

To start or stop a backup policy, do the following:

1. Navigate to **Policies**.
2. Switch to the necessary tab and select the backup policy.
3. Click **Start** or **Stop**.
Exporting and Importing Backup Policies

Veeam Backup for Google Cloud allows you to use settings of an existing backup policy as a template for creating other backup policies. You can export a backup policy to a .JSON file, modify the necessary settings in the file, and then import the policy to the same or a different backup appliance.

Exporting Backup Policies

To export a backup policy to a .JSON file, do the following:

1. Navigate to Policies.
2. Switch to the necessary tab and select the backup policy.
3. Click Advanced > Export Policy.

Veeam Backup for Google Cloud will save the backup policy settings as a single .JSON file to the default download directory on the local machine.
Importing Backup Policies

To import a backup policy from a .JSON file, do the following:

1. Click **Advanced > Import Policy**.

2. In the **Import Policy** window, specify a name for the imported backup policy, paste the content of the necessary .JSON file, and click **Import**.
Viewing Protected Resources

After a backup policy successfully creates a restore point of a Google Cloud resource according to the specified schedule, or after you create a snapshot of a resource manually, Veeam Backup for Google Cloud adds the resource to the resource list on the **Protected Data** page.

The **Protected Data** page displays Google Cloud resources that are already protected by Veeam Backup for Google Cloud. Each resource is represented with a set of properties, such as:

- **Instance** — the name of the resource.
- **Policy** — the name of the backup policy that protects the resource.
- **Restore Points** — the number of restore points created for the resource.
- **Latest Restore Point** — the date and time of the most recent restore point created for the resource.
- **Region** — the region in which the resource resides.
- **Database Version** — the database version installed on the Cloud SQL instance.
- **Instance Size** — the machine type of the VM instance.
- **Operating System** — the operating system running on the VM instance.
- **File-level Recovery URL** — the link to the File-Level Restore browser.

The link appears when Veeam Backup for Google Cloud starts a restore session to perform file-level recovery. The link contains a public DNS name of the worker instance hosting the File-Level Restore browser and authentication information used to access this worker instance.

On the **Protected Data** page, you can also perform the following actions:

- Remove restore points if you no longer need them. For more information, see Removing Backups and Snapshots.
- Restore data of backed-up VM instances and Cloud SQL instances. For more information, see sections Performing VM Restore and Performing SQL Restore.
Removing Backups and Snapshots

Veeam Backup for Google Cloud stores information on all protected Google Cloud resources in the configuration database. Even if a resource is no longer protected by any backup policy, information on the backed-up data will not be deleted from the database until Veeam Backup for Google Cloud automatically removes all restore points associated with this resource according to the retention settings saved in the backup metadata. If necessary, you can also remove the restore points manually.

**IMPORTANT**

Do not delete backup files from Google Cloud storage buckets in the Google Cloud Console. If some file in a backup chain is missing, you will not be able to roll back the resource data to the necessary state.

To remove restore points manually, do the following:

1. Navigate to Protected Data.
2. Switch to the necessary tab and select resources whose restore points you want to remove.
3. Click **Remove** and select either of the following options:
   - **Snapshots > All** — to remove all cloud-native snapshots created for the selected resources both by backup policies and manually.
   - **Snapshots > Created by Policy** — to remove all cloud-native snapshots created for the selected resources by backup policies.
   - **Snapshots > Created Manually** — to remove all cloud-native snapshots created for the selected resources manually.
   - **Backups > All** — to remove all image-level backups created for the selected resources.
   - **Backups > Standard** — to remove all image-level backups created in standard repositories for the selected resources.
   - **Backups > Archived** — to remove all image-level backups created in archive repositories for the selected resources.
   - **Snapshots and Backups** — to remove both cloud-native snapshots and image-level backups created for the selected resources.
Performing Restore

In various disaster recovery scenarios, Veeam Backup for Google Cloud allows you to perform the following operations using backed-up data:

- **Restore of VM instances** — restore VM instances from cloud-native snapshots or image-level backups to the original location or to a new location.
- **Restore of Cloud SQL instances** — restore Cloud SQL instances from cloud-native snapshots or image-level backups to the original location or to a new location.
Performing VM Restore

Veeam Backup for Google Cloud offers the following restore operations:

- **Instance restore** — start an entire VM instance from a restore point.
- **Disk restore** — restore persistent disks attached to a VM instance.
- **File-level recovery** — recover individual files and folders of a VM instance.

You can restore VM instance data to the most recent state or to any available restore point.

Performing Instance Restore

In case a disaster strikes, you can restore an entire VM instance from a cloud-native snapshot or image-level backup. Veeam Backup for Google Cloud allows you to restore one or more VM instances at a time, to the original location or to a new location.

**IMPORTANT**
When restoring a VM instance, Veeam Backup for Google Cloud recovers data from all zonal and regional persistent disks (standard, balanced, extreme and SSD) attached to the instance. However, due to technical reasons, when it comes to local SSDs (SCSI and NVMe), Veeam Backup for Google Cloud is able to recover only the configuration of these disks, which means that any data stored on the disks is lost during the restore process.

How Instance Restore Works

To restore a VM instance from a cloud-native snapshot, Veeam Backup for Google Cloud uses native Google Cloud capabilities. To restore a VM instance from an image-level backup, Veeam Backup for Google Cloud performs the following steps:

1. Deploys a worker instance in the Google Cloud region in which the restored VM instance will reside.
2. Creates empty persistent disks and attaches them to the worker instance.
   - The number of empty persistent disks equals the number of persistent disks attached to the backed-up VM instance.
3. Restores backed-up data to the empty persistent disks on the worker instance.
4. Takes cloud-native snapshots of the persistent disks with the restored data.
5. Creates disks from the snapshots in the target location.
6. Removes the worker instance and all the created snapshots from the Google Cloud environment.
7. Creates a VM instance in the target location.
8. Attaches the created persistent disks with the restored data to the VM instance.
9. [This step applies only if you perform restore to the original location and if the source VM instance is still present in the location] Powers off the source VM instance, renames the restored VM instance and then removes the source VM instance from the Google Cloud environment.
How to Perform Instance Restore

To restore a protected VM instance, do the following:

1. Launch the VM Instance Restore wizard.
2. Select a restore point.
3. Choose a restore mode.
4. Select a project.
5. Select a region and an availability zone.
6. Enable encryption.
7. Specify a new name and machine type for the instance.
8. Configure network settings.
9. Specify a restore reason.
10. Finish working with the wizard.

IMPORTANT

Before you start VM instance restore, make sure that network settings are configured for each region where worker instances will be deployed during the restore process. For information on how to configure network settings, see Adding Worker Configurations.
Step 1. Launch VM Instance Restore Wizard

To launch the **VM Instance Restore** wizard, do the following:

1. Navigate to **Protected Data > VM**.
2. Select the VM instance that you want to restore, and click **Restore > Instance Restore**.
Step 2. Select Restore Point

At the **Instances** step of the wizard, select a restore point that will be used to restore the selected VM instance. By default, Veeam Backup for Google Cloud uses the most recent valid restore point. However, you can restore the VM instance data to an earlier state.

To select a restore point, do the following:

1. Select the VM instance.
2. Click **Choose Restore Point**.
3. In the **Select restore point** window, select the necessary restore point and click **Apply**.

   To help you choose a restore point, Veeam Backup for Google Cloud provides the following information on each available restore point:

   - **Creation Time** — the date when the restore point was created.
   - **Size** — the size of the restore point.
   - **Destination** — the type of the restore point:
     - **Snapshot** — a cloud-native snapshot created by a backup policy.
     - **Manual Snapshot** — a cloud-native snapshot created manually.
     - **Backup** — an image-level backup created by a backup policy.
   - **Storage Class** — the storage class of a backup repository where the restore point is stored (applies only to image-level backups).
   - **Project** — a project that manages the protected VM instance.
   - **Region** — a region in which the protected VM instance resides.
   - **Retention** — a retention configured for the backup policy that created the restore point.
Step 3. Choose Restore Mode

At the **Restore Mode** step of the wizard, choose whether you want to restore the selected VM instance to the original or to a custom location.

**TIP**

If restore to the original location is not available, the wizard will display a message notifying that some of the selected VM instances have issues with the original settings. To learn what these issues are, click the **One or more VM instances** link in the message.
Step 4. Select Project

At the **Project** step of the wizard, select a project that will be used to manage the restored VM instance.

Veeam Backup for Google Cloud allows you to check whether the service account used to access the selected project has all the necessary permissions required to perform restore tasks for the project. To do that, click **Check Permissions**.

Veeam Backup for Google Cloud also allows you to generate a gcloud script that you can run in your Google Cloud Console to assign all the necessary restore permissions to the account. To do that, click **Generate and download script**.
Step 5. Select Region and Availability Zone

[This step applies only if you have selected the Restore to new location, or with different settings option at the Restore Mode step of the wizard]

At the Region step of the wizard, select a region where the restored VM instance will operate and an availability zone for which you want to configure network settings.
Step 6. Enable Encryption

[This step applies only if you have selected the Restore to new location, or with different settings option at the Restore Mode step of the wizard]

At the Encryption step of the wizard, choose whether persistent disks of the restored VM instance will be encrypted with Google Cloud Key Management Service (Cloud KMS) customer-managed encryption keys (CMEKs):

- If you do not want to encrypt persistent disks or want to apply the existing encryption scheme, select the Use original encryption scheme option.
- If you want to encrypt persistent disks, select the Use customer-managed encryption key from Google Cloud KMS option and choose the necessary CMEK from the Encryption key drop-down list.

For a CMEK to be displayed in the list of available encryption keys, it must be stored in the region selected at step 5.
Step 7. Specify Instance Name and Type

(This step applies only if you have selected the Restore to new location, or with different settings option at the Restore Mode step of the wizard)

At the Instance Settings step of the wizard, do the following:

1. Select the VM instance.
2. If you want to specify a new name and a new machine type for the restored VM instance, click Edit.

In the Configure settings window, specify the name and the machine type, and click Apply. To learn how to choose a machine type when creating a VM instance in Google Cloud, see Google Cloud documentation.

TIP

If Veeam Backup for Google Cloud is unable to restore the VM instance using the specified name for some reason, the wizard will display an error icon in the Instance column. To learn what this reason is, hover your mouse over the icon.
Step 8. Configure Network Settings

[This step applies only if you have selected the Restore to new location, or with different settings option at the Restore Mode step of the wizard]

At the Network Settings step of the wizard, do the following:

1. Select the VM instance.
2. Click Edit.
3. In the Edit network settings window, select a VPC network and a subnet to which the restored VM instance will be connected. You can also choose whether you want the restored VM instance to have the same reserved static external IP address and the same network labels as the source VM instance.

For a VPC network and a subnet to be displayed in the lists of available networks, they must be created for the region specified at step 5 in the Google Cloud Console as described in Google Cloud documentation.

**NOTE**

Veeam Backup for Google Cloud cannot assign a static external IP address to a restored VM instance if the source instance does not have the address reserved. To learn how to reserve static external IP addresses for VM instances, see Google Cloud documentation.
Step 9. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for restoring the VM instance. This information will be saved to the session history, and you will be able to reference it later.
Step 10. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.

**TIP**

If you want to start the restored VM instance as soon as the restore process completes, select the **Power on target VM instances after restore** check box.
Performing Disk Restore

In case a disaster strikes, you can restore corrupted persistent disks of a VM instance from a cloud-native snapshot or image-level backup. Veeam Backup for Google Cloud allows you to restore persistent disks to the original location or to a new location.

**IMPORTANT**

You can restore zonal and regional persistent disks of all types: standard (pd-standard), balanced (pd-balanced), extreme (pd-extreme) and SSD (pd-ssd). Restore of local SSDs (SCSI and NVMe) is not supported due to technical reasons.

How Disk Restore Works

To restore persistent disks from a cloud-native snapshot, Veeam Backup for Google Cloud uses native Google Cloud capabilities. To restore persistent disks from an image-level backup, Veeam Backup for Google Cloud performs the following steps:

1. Deploys a worker instance in the Google Cloud region in which the restored persistent disks will reside.
2. Creates empty persistent disks and attaches them to the worker instance.
   - The number of empty persistent disks equals the number of disks you want to restore.
3. Restores backed-up data to the empty persistent disks on the worker instance.
4. Takes cloud-native snapshots of the persistent disks with the restored data.
5. Creates disks from snapshots in the target location.
6. Removes the worker instance and all the created snapshots from the Google Cloud environment.

**NOTE**

Veeam Backup for Google Cloud does not attach the restored persistent disks to any VM instances — the disks are placed to the specified location as standalone persistent disks.
How to Perform Disk Restore

To restore persistent disks attached to a protected VM instance, do the following:

1. **Launch the Disk Restore wizard.**
2. **Select a restore point.**
3. **Choose a restore mode.**
4. **Select a project.**
5. **Select a region and an availability zone.**
6. **Enable encryption.**
7. **Specify new names for the disks.**
8. **Specify a restore reason.**
9. **Finish working with the wizard.**

**IMPORTANT**

Before you start disk restore, make sure that network settings are configured for each region where worker instances will be deployed during the restore process. For information on how to configure network settings, see **Adding Worker Configurations**.

Step 1. Launch Disk Restore Wizard

To launch the **Disk Restore** wizard, do the following:

1. **Navigate to Protected Data > VM.**
2. **Select the VM instance whose persistent disks you want to restore, and click Restore > Disk Restore.**
Step 2. Select Restore Point

At the Instances step of the wizard, select a restore point that will be used to restore persistent disks of the selected VM instance. By default, Veeam Backup for Google Cloud uses the most recent valid restore point. However, you can restore the disks to an earlier state.

To select a restore point, do the following:

1. Select the VM instance.
2. Click Choose Restore Point.
3. In the Select restore point window, select the necessary restore point and click Apply.
   
   To help you choose a restore point, Veeam Backup for Google Cloud provides the following information on each available restore point:
   
   - **Creation Time** — the date when the restore point was created.
   - **Size** — the size of the restore point.
   - **Destination** — the type of the restore point:
     - **Snapshot** — a cloud-native snapshot created by a backup policy.
     - **Manual Snapshot** — a cloud-native snapshot created manually.
     - **Backup** — an image-level backup created by a backup policy.
   - **Storage Class** — the storage class of a backup repository where the restore point is stored (applies only to image-level backups).
   - **Project** — a project that manages the protected VM instance.
   - **Region** — a region in which the protected VM instance resides.
   - **Retention** — a retention configured for the backup policy that created the restore point.

   **TIP**

   If you want to restore only specific persistent disks of the selected VM, you can exclude the unnecessary disks from the restore process. To do that, click Exclusions to open the Exclude disks from restore window, select check boxes next to the disks that you do not want to restore, and click Apply.
Step 3. Choose Restore Mode

At the Restore Mode step of the wizard, choose whether you want to restore persistent disks of the selected VM instance to the original or to a custom location.
TIP
If restore to the original location is not available, the wizard will display a message notifying that some of the selected disks have issues with the original settings. To learn what these issues are, click the One or more disks link in the message.
Step 4. Select Project

At the Project step of the wizard, select a project where the restored persistent disks will belong.

Veeam Backup for Google Cloud allows you to check whether the service account used to access the selected project has all the necessary permissions required to perform restore tasks for the project. To do that, click Check Permissions.

Veeam Backup for Google Cloud also allows you to generate a gcloud script that you can run in your Google Cloud Console to assign all the necessary restore permissions to the account. To do that, click Generate and download script.
Step 5. Select Region and Availability Zone

[This step applies only if you have selected the **Restore to new location, or with different settings** option at the **Restore Mode** step of the wizard]

At the **Region** step of the wizard, select a region and an availability zone to which the restored persistent disks will be placed.
Step 6. Enable Encryption

[This step applies only if you have selected the Restore to new location, or with different settings option at the Restore Mode step of the wizard]

At the Encryption step of the wizard, choose whether the restored persistent disks will be encrypted with Google Cloud Key Management Service (Cloud KMS) customer-managed encryption keys (CMEKs):

- If you do not want to encrypt the persistent disks or want to apply the existing encryption scheme, select the Use original encryption scheme option.

- If you want to encrypt the persistent disks, select the Use customer-managed encryption key from Google Cloud KMS option and choose the necessary CMEK from the Encryption key drop-down list.

For a CMEK to be displayed in the list of available encryption keys, it must be stored in the region selected at step 5.
Step 7. Specify Disk Names

[This step applies only if you have selected the Restore to new location, or with different settings option at the Restore Mode step of the wizard]

At the Disk Settings step of the wizard, you can specify a new name for each restored persistent disk:

1. Select the necessary disk and click Rename.
2. In the Rename disk window, specify a name for the disk and click Apply.

TIP

If Veeam Backup for Google Cloud is unable to restore the disk using the specified name for some reason, the wizard will display a warning icon in the Disk column. To learn what this reason is, hover your mouse over the icon.
Step 8. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for restoring the persistent disks. This information will be saved to the session history, and you will be able to reference it later.

Step 9. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.
Performing File-Level Recovery

In case a disaster strikes, you can recover corrupted or missing files of a VM instance from a cloud-native snapshot or image-level backup. Veeam Backup for Google Cloud allows you to download the necessary files and folders to a local machine using the File-Level Restore browser.

**IMPORTANT**

You can recover files and folders from the following file systems only:

- Microsoft Windows systems — FAT, FAT32, NTFS.
- Linux systems — ext2, ext3, ext4, XFS, Btrfs.

**How File-Level Recovery Works**

To recover files and folders of a backed-up VM instance, Veeam Backup for Google Cloud performs the following steps:

1. Deploys a worker instance in either of the following Google Cloud regions:
   - To restore files and folders from a cloud-native snapshot, the worker instance is deployed in the region in which the source VM instance resides.
   - To restore files and folders from an image-level backup, the worker instance is deployed in the region in which the storage bucket with backed-up data resides.

2. When restoring files and folders from a cloud-native snapshot, attaches persistent disks of the VM instance to the worker instance.
   When restoring files and folders from an image-level backup, the disks are not physically extracted from the backup — Veeam Backup for Google Cloud emulates their presence on the worker instance. The source backup itself remains in the read-only state.

3. Launches the File-Level Restore browser.
   The File-Level Restore browser displays the file system tree of the backed-up VM instance. In the browser, you select the necessary files and folders to restore.

4. Saves the selected files and folders to the local machine.

5. Removes the worker instance from the Google Cloud environment.
How to Perform File-Level Recovery

To recover files and folders of a protected VM instance, do the following:

1. Launch the File-Level Recovery wizard.
2. Select a restore point.
3. Specify a recovery reason.
4. Finish working with the wizard — start a recovery session.
5. Choose files and folders to recover.
6. Stop the recovery session.

IMPORTANT

• Before you start file-level recovery, make sure that network settings are configured for each region where worker instances will be deployed during the recovery process. For information on how to configure network settings, see Adding Worker Configurations.
• Make sure the machine where you plan to open the File-Level Restore browser is allowed to access the worker instances over the internet. To enable internet access for a worker instance, update the firewall rule specified in the instance network settings to add an inbound rule for HTTPS traffic on the port 443. For information on how to update firewall rules, see Google Cloud documentation.

Step 1. Launch File-Level Recovery Wizard

To launch the File-Level Recovery wizard, do the following:

1. Navigate to Protected Data > VM.
2. Select the VM instance whose files and folders you want to recover, and click File-Level Recovery.
Step 2. Select Restore Point

At the **Instances** step of the wizard, select a restore point that will be used to recover files and folders of the selected VM instance. By default, Veeam Backup for Google Cloud uses the most recent valid restore point. However, you can recover the items to an earlier state.

To select a restore point, do the following:

1. Select the VM instance.
2. Click **Choose Restore Point**.
3. In the **Select restore point** window, select the necessary restore point and click **Apply**.

To help you choose a restore point, Veeam Backup for Google Cloud provides the following information on each available restore point:

- **Creation Time** — the date when the restore point was created.
- **Size** — the size of the restore point.
- **Destination** — the type of the restore point:
  - *Snapshot* — a cloud-native snapshot created by a backup policy.
  - *Backup* — an image-level backup created by a backup policy.
- **Storage Class** — the storage class of a backup repository where the restore point is stored (applies only to image-level backups).
- **Project** — a project that manages the protected VM instance.
- **Region** — a region in which the protected VM instance resides.
- **Retention** — a retention configured for the backup policy that created the restore point.
Step 3. Specify Recovery Reason

At the **Reason** step of the wizard, specify a reason for recovering files and folders. This information will be saved to the session history, and you will be able to reference it later.
Step 4. Start Recovery Session

At the **Summary** step of the wizard, review summary information and click **Finish**.

As soon as you click **Finish**, Veeam Backup for Google Cloud will close the **File-level Recovery** wizard, start a recovery session and display the **FLR Running Sessions** window. During the recovery session, Veeam Backup for Google Cloud will deploy a worker instance and attach persistent disks of the processed VM instance to it.

<table>
<thead>
<tr>
<th>TIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you accidentally close the <strong>FLR Running Sessions</strong> window, navigate to <strong>Protected Data</strong> and click the link in the <strong>File-Level Recovery URL</strong> column to open the window again.</td>
</tr>
</tbody>
</table>

In the **FLR Running Sessions** window, you can track the progress of the recovery session. In the **URL** column of the window, Veeam Backup for Google Cloud will display a link to the File-Level Restore browser. You can use the link in either of the following ways:

- Click the link to open the File-Level Restore browser on your local machine while the recovery session is running.
- Copy the link, close the **FLR Running Sessions** window and open the File-Level Restore browser on another machine.

<table>
<thead>
<tr>
<th>IMPORTANT</th>
</tr>
</thead>
<tbody>
<tr>
<td>When you click <strong>Copy FLR URL</strong>, Veeam Backup for Google Cloud copies the following information to the clipboard:</td>
</tr>
</tbody>
</table>

- A link to the File-Level Restore browser that includes a public DNS name of the worker instance hosting the browser and authentication information used to access the browser.
- A thumbprint of a TLS certificate that is installed on the worker instance hosting the File-Level Restore browser.

To avoid a man-in-the-middle attack, before you start recovering files and folders, check that the certificate thumbprint displayed in the web browser from which you access the File-Level Restore browser matches the provided certificate thumbprint.
Step 5. Choose Items to Recover

In the File-Level Restore browser, you can find and recover items (files and folders) of the selected VM instance. All recovered items will be saved as a single .ZIP archive to the default download directory on a machine from which you access the browser.

1. In the File-Level Restore browser, navigate to a folder that contains the necessary files.
2. In the working area, select check boxes next to the files and click Add to Restore List.
3. Repeat steps 1-2 for all other folders whose files you want to recover.
4. Switch to the Restore List tab.
5. On the Restore List tab, review the list of items to recover, select check boxes next to the items, and click Download.
Step 6. Stop Recovery Session

After you finish working with the File-Level Restore browser, it is recommended that you stop the running recovery session so that Veeam Backup for Google Cloud can detach persistent disks of the processed VM instance from the deployed worker instance and remove the worker instance from the Google Cloud environment.

To stop the recovery session, click **Stop Recovery Session** in the **FLR Running Sessions** window. If you do not perform any actions in the File-Level Restore browser for 30 minutes, Veeam Backup for Google Cloud will stop the recovery session automatically.

**TIP**

If you accidentally close the **FLR Running Sessions** window, navigate to **Protected Data** and click the link in the **File-Level Recovery URL** column to open the window again.
Performing SQL Restore

Veeam Backup for Google Cloud offers the following restore operations:

- **Instance restore** — start an entire Cloud SQL instance from a restore point.
- **Database restore** — restore specific databases of a Cloud SQL instance from an image-level backup.

You can restore Cloud SQL instance data to the most recent state or to any available restore point.

Performing Instance Restore

In case a disaster strikes, you can restore an entire Cloud SQL instance from a cloud-native snapshot or image-level backup. Veeam Backup for Google Cloud allows you to restore one or more Cloud SQL instances at a time, to the original location or to a new location.

**NOTE**

Due to technical limitations in Google Cloud, Veeam Backup for Google Cloud does not support restore to the original location if the source Cloud SQL instance is still present in the location, if it has been recently deleted (less than a week ago), or if its name is reserved.

How SQL Restore Works

To restore a Cloud SQL instance from a cloud-native snapshot, Veeam Backup for Google Cloud first creates a Cloud SQL instance in the target location and then uses native Google Cloud capabilities to revert the instance to the snapshot.

To restore a Cloud SQL instance from an image-level backup, Veeam Backup for Google Cloud performs the following steps:

1. Creates a Cloud SQL instance in the target location.
2. Deploys a worker instance in the Google Cloud region in which the repository with backed-up data is located.
3. Exports databases, triggers, stored procedures and users of the processed the Cloud SQL instance to a SQL dump file in the Temp folder of the storage bucket where the backup repository resides.
   
   For more information on SQL dump files, see Google Cloud documentation.
4. Imports the exported databases, triggers, stored procedures and users to the created Cloud SQL instance.
5. Removes the worker instance from the Google Cloud environment.
How to Perform SQL Restore

To restore a protected Cloud SQL instance, do the following:

1. Launch the Cloud SQL Instance Restore wizard.
2. Select a restore point.
3. Choose a restore mode.
4. Select a project.
5. Select a region and an availability zone.
6. Specify a new name and machine type for the instance.
7. Configure network settings.
8. Configure security settings.
9. Enable flag assignment.
10. Specify a restore reason.
11. Finish working with the wizard.

**IMPORTANT**

Before you start Cloud SQL instance restore, make sure that network settings are configured for each region where worker instances will be deployed during the restore process. For information on how to configure network settings, see Adding Worker Configurations.

Step 1. Launch Cloud SQL Instance Restore Wizard

To launch the Cloud SQL Instance Restore wizard, do the following:

1. Navigate to Protected Data > Cloud SQL.
2. Select the Cloud SQL instance that you want to restore, and click Restore > Instance Restore.
Step 2. Select Restore Point

At the **Instances** step of the wizard, select a restore point that will be used to restore the selected Cloud SQL instance. By default, Veeam Backup for Google Cloud uses the most recent valid restore point. However, you can restore the instance data to an earlier state.

To select a restore point, do the following:

1. Select the Cloud SQL instance.
2. Click **Restore Point**.
3. In the **Choose restore point** window, select the necessary restore point and click **Apply**.

   To help you choose a restore point, Veeam Backup for Google Cloud provides the following information on each available restore point:

   - **Creation Time** — the date when the restore point was created.
   - **Size** — the size of the restore point (applies only to image-level backups).
   - **Destination** — the type of the restore point:
     - **Snapshot** — a cloud-native snapshot created by a backup policy.
     - **Manual Snapshot** — a cloud-native snapshot created manually.
     - **Backup** — an image-level backup created by a backup policy.
   - **Storage Class** — the storage class of a backup repository where the restore point is stored (applies only to image-level backups).
   - **Policy** — a backup policy that created the restore point.
   - **Region** — a region in which the protected Cloud SQL instance resides.
   - **Project** — a project that manages the protected Cloud SQL instance.
   - **Retention** — a retention configured for the backup policy that created the restore point.
<table>
<thead>
<tr>
<th>Creation Time</th>
<th>Size</th>
<th>Destination</th>
<th>Project</th>
<th>Retention</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/06/2022 20:51 PM</td>
<td>N/A</td>
<td>Snapshot</td>
<td>Veeam Backup 2</td>
<td>Daily</td>
</tr>
<tr>
<td>05/05/2022 02:34 PM</td>
<td>0 bytes</td>
<td>Manual snapshot</td>
<td>Veeam Backup 2</td>
<td>None</td>
</tr>
<tr>
<td>05/03/2022 00:19 PM</td>
<td>3.25 MB</td>
<td>Backup (pre):</td>
<td>Veeam Backup 2</td>
<td>Daily</td>
</tr>
<tr>
<td>05/02/2022 00:19 PM</td>
<td>N/A</td>
<td>Snapshot</td>
<td>Veeam Backup 3</td>
<td>Daily</td>
</tr>
<tr>
<td>05/02/2022 00:15 PM</td>
<td>2.25 MB</td>
<td>Backup (pre):</td>
<td>Veeam Backup 2</td>
<td>Daily</td>
</tr>
<tr>
<td>05/02/2022 00:15 PM</td>
<td>N/A</td>
<td>Snapshot</td>
<td>Veeam Backup 2</td>
<td>Daily</td>
</tr>
<tr>
<td>05/02/2022 23:19 PM</td>
<td>3.25 MB</td>
<td>Backup (pre):</td>
<td>Veeam Backup 2</td>
<td>Daily</td>
</tr>
<tr>
<td>05/03/2022 23:36 PM</td>
<td>3.25 MB</td>
<td>Backup (pre):</td>
<td>Veeam Backup 2</td>
<td>Daily</td>
</tr>
<tr>
<td>04/29/2022 23:51 PM</td>
<td>0 bytes</td>
<td>Manual snapshot</td>
<td>Veeam Backup 2</td>
<td>None</td>
</tr>
<tr>
<td>04/29/2022 19:38 PM</td>
<td>2.7 MB</td>
<td>Backup (pre):</td>
<td>Veeam Backup 2</td>
<td>Daily</td>
</tr>
<tr>
<td>04/25/2022 23:00 PM</td>
<td>2.7 MB</td>
<td>Backup (pre):</td>
<td>Veeam Backup 2</td>
<td>Daily</td>
</tr>
<tr>
<td>04/24/2022 20:17 PM</td>
<td>2.7 MB</td>
<td>Backup (pre):</td>
<td>Veeam Backup 2</td>
<td>Daily</td>
</tr>
<tr>
<td>04/23/2022 20:19 PM</td>
<td>2.7 MB</td>
<td>Backup (pre):</td>
<td>Veeam Backup 2</td>
<td>Daily</td>
</tr>
<tr>
<td>04/23/2022 00:19 PM</td>
<td>2.7 MB</td>
<td>Backup (pre):</td>
<td>Veeam Backup 3</td>
<td>Daily</td>
</tr>
<tr>
<td>04/23/2022 21:56 PM</td>
<td>3.4 MB</td>
<td>Backup (pre):</td>
<td>Veeam Backup 2</td>
<td>Daily</td>
</tr>
</tbody>
</table>
Step 3. Choose Restore Mode

At the Restore Mode step of the wizard, choose whether you want to restore the selected Cloud SQL instance to the original or to a custom location.

Note that the Restore to original location, with original settings option is available only if you have selected a restore point of the Backup type at the Restore Point step of the wizard.

TIP

If restore to the original location is not available, the wizard will display a message notifying that some of the selected Cloud SQL instances have issues with the original settings. To learn what these issues are, click the One or more instances link in the message.
Step 4. Select Project

At the **Project** step of the wizard, select a project that will be used to manage the restored Cloud SQL instance.

Veeam Backup for Google Cloud allows you to check whether the service account used to access the selected project has all the necessary permissions required to perform restore tasks for the project. To do that, click **Check Permissions**.

Veeam Backup for Google Cloud also allows you to generate a gcloud script that you can run in your Google Cloud Console to assign all the necessary restore permissions to the account. To do that, click **Generate Script**.
Step 5. Select Region and Availability Zone

(This step applies only if you have selected the Restore to new location, or with different settings option at the Restore Mode step of the wizard)

At the Region step of the wizard, select a region where the restored Cloud SQL instance will operate and an availability zone for which you want to configure network settings.

To configure the restored Cloud SQL instance for high availability, select the Multiple zones option, and choose a primary and a secondary zone where the restored Cloud SQL instance will be located within the selected region. The high availability configuration allows you to reduce downtime when a zone or the instance becomes unavailable. For more information on high availability in Google Cloud, see Google Cloud documentation.

TIP

If some of the restored Cloud SQL instances cannot be configured for high availability, the wizard will display a message notifying that the instances have issues with the original zone settings. To learn what these issues are, click the instances link in the message.
Step 6. Specify Instance Name and Type

[This step applies only if you have selected the Restore to new location, or with different settings option at the Restore Mode step of the wizard]

At the Instance Settings step of the wizard, do the following:

1. Select the Cloud SQL instance.

2. If you want to specify a new name and a new machine type for the restored Cloud SQL instance, or to configure storage settings for the instance, click Edit.

   In the Configure general settings window, specify the name and the machine type, and click Apply. To learn how to choose a machine type when creating a Cloud SQL instance in Google Cloud, see Google Cloud documentation.

   You can also choose a new storage type and manually increase storage capacity for the restored Cloud SQL instance. If you want Veeam Backup for Google Cloud to increase the storage capacity to fit the instance size automatically, select the Automatic increase check box. Note, however, that the amount of storage capacity allocated to an instance affects its cost. To learn how to configure storage settings when creating a Cloud SQL instance in Google Cloud, see Google Cloud documentation.

TIP

If Veeam Backup for Google Cloud is unable to restore the Cloud SQL instance using the specified name for some reason, the wizard will display an error icon in the Instance column. To learn what this reason is, hover your mouse over the icon.
Step 7. Configure Network Settings

[This step applies only if you have selected the Restore to new location, or with different settings option at the Restore Mode step of the wizard]

At the Network Settings step of the wizard, do the following:

1. Select the Cloud SQL instance.

2. Click Edit.

3. In the Edit network settings window, choose whether you want to configure public IP and private IP connectivity for the restored Cloud SQL instance.

   To connect the restored Cloud SQL instance to a VPC network with a private IP address, select the Private IP check box and specify a VPC network to which the instance will be connected. For a VPC network to be displayed in the lists of available networks, it must be created for the region specified at step 6 in the Google Cloud Console as described in Google Cloud documentation.

   IMPORTANT

   The specified VPC network must have private services access configured. To learn how to configure private services access for a VPC network, see Google Cloud documentation.

   To assign a public IPv4 address to the restored Cloud SQL instance and to accept connections to it from specific IP address ranges, set the Public IP toggle to On, and then use the Allowed network connections section to specify the allowed IP address ranges.

   TIP

   The IP address ranges must be specified in the CIDR notation (for example, 12.23.34.0/24). To let all IP addresses access the restored Cloud SQL instance, you can enter 0.0.0.0/0. However, note that allowing access from all IP addresses is unsafe and thus not recommended in production environments.

---

![Cloud SQL Instance Restore](image)
Step 8. Configure Security Settings

[This step applies only if you have selected the **Restore to new location, or with different settings** option at the **Restore Mode** step of the wizard]

At the **Security Settings** step of the wizard, choose whether you want to connect to the restored Cloud SQL instance using SSL only, and whether you want the instance data to be encrypted with Google Cloud Key Management Service (Cloud KMS) customer-managed encryption keys (CMEKs). To do that, select the Cloud SQL instance, click **Edit** and then do either of the following:

- **If you want to secure connections to the restored Cloud SQL instance, set the Allow only SSL connections toggle to **On**.**

  Since SSL connections use digital certificates to provide encrypted access, make sure you have obtained a Certificate Authority (CA) certificate, a client public key certificate, and a client private key — before you connect to the restored instance using SSL. For more information, see Google Cloud documentation.

- **If you do not want to encrypt the restored data or want to apply the existing encryption scheme, select the Use original encryption scheme option.**

- **If you want to encrypt the restored data, select the Use customer-managed encryption key from Google Cloud KMS option and choose the necessary CMEK from the Encryption key drop-down list.**

  For a CMEK to be displayed in the list of available encryption keys, it must be stored in the region selected at step 5.

**NOTE**

Due to **technical limitations in Google Cloud**, Veeam Backup for Google Cloud does not support data encryption with multi-regional and global region keys.
Step 9. Enable Flag Assignment

[This step applies only if you have selected the *Restore to new location, or with different settings* option at the *Restore Mode* step of the wizard]

At the **Flags** step of the wizard, you can instruct Veeam Backup for Google Cloud to modify flags set on databases of the restored Cloud SQL instance:

1. Select the Cloud SQL instance.
2. Click **Edit**.
3. In the **Configure flags** window, choose whether you want flags of the restored databases to have the same values as the source databases or new modified values.

   If you want to set a new value for a database flag, select the flag and click **Edit**. If you want to clear all flags to their original values, click **Reset to original**.

   To save changes made to the flag settings, click **Apply**.

![Configure Flags Window](image-url)
Step 10. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for restoring the Cloud SQL instance. This information will be saved to the session history, and you will be able to reference it later.

Step 11. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.
Performing Database Restore

In case a disaster strikes, you can restore corrupted databases of a Cloud SQL instance from an image-level backup. Veeam Backup for Google Cloud allows you to restore databases to the original location or to a new location.

NOTE

Due to technical limitations in Google Cloud, Veeam Backup for Google Cloud does not support restore to the original location if the source database is still present in the location.

How Database Restore Works

To restore a Cloud SQL database from an image-level backup, Veeam Backup for Google Cloud performs the following steps:

1. Creates a temporary snapshot of the Cloud SQL instance that will host the restored database.

   NOTE

   If Veeam Backup for Google Cloud fails to restore the database, the Cloud SQL instance will be reverted to the temporary snapshot.

2. Deploys a worker instance in the Google Cloud region in which the repository with backed-up data is located.

3. Exports files, triggers and stored procedures of the processed database to the `Temp` folder of the storage bucket where the backup repository resides.

   For more information on SQL dump files, see Google Cloud documentation.

4. Imports the exported database files, triggers and stored procedures to the created Cloud SQL instance.

5. Removes the worker instance from the Google Cloud environment.

6. Deletes the temporary snapshot.
How to Perform Database Restore

To restore databases of a protected Cloud SQL instance, do the following:

1. Launch the Database Restore wizard.
2. Select databases.
3. Choose a restore mode.
4. Select a project.
5. Configure target instance settings.
6. Specify a restore reason.
7. Finish working with the wizard.

IMPORTANT
Before you start Cloud SQL database restore, make sure that network settings are configured for each region where worker instances will be deployed during the restore process. For information on how to configure network settings, see Adding Worker Configurations.

Step 1. Launch Database Restore Wizard

To launch the Database Restore wizard, do the following:

1. Navigate to Protected Data > Cloud SQL.
2. Select the Cloud SQL instance whose databases you want to restore, and click Restore > Database Restore.
Step 2. Select Databases

At the Databases step of the wizard, click Add to select databases to restore, and then choose a restore point that will be used to restore the selected databases. By default, Veeam Backup for Google Cloud uses the most recent valid restore point. However, you can restore the backed-up data to an earlier state.

To select a restore point, do the following:

1. Select a database.
2. Click Restore Point.
3. In the Choose restore point window, select the necessary restore point and click Apply.

To help you choose a restore point, Veeam Backup for Google Cloud provides the following information on each available restore point:

- **Creation Time** — the date when the restore point was created.
- **Size** — the size of the restore point (applies only to image-level backups).
- **Destination** — the type of the restore point:
  - **Snapshot** — a cloud-native snapshot created by a backup policy.
  - **Backup** — an image-level backup created by a backup policy.
- **Storage Class** — the storage class of the backup repository where the restore point is stored (applies only to image-level backups).
- **Region** — a region in which the protected Cloud SQL instance resides.
- **Policy** — a backup policy that created the restore point.
- **Retention** — a retention configured for the backup policy that created the restore point.
Step 3. Choose Restore Mode

At the **Restore Mode** step of the wizard, choose whether you want to restore the selected databases to the original or to a custom location.

**TIP**

If restore to the original location is not available, the wizard will display a message notifying that some of the selected databases have issues with the original settings. To learn what these issues are, click the **One or more databases** link in the message.
Step 4. Select Project

[This step applies only if you have selected the **Restore to new location, or with different settings** option at the **Restore Mode** step of the wizard]

At the **Project** step of the wizard, select a project where the restored databases will belong.

Veeam Backup for Google Cloud allows you to check whether the service account used to access the selected project has all the necessary permissions required to perform restore tasks for the project. To do that, click **Check Permissions**.

Veeam Backup for Google Cloud also allows you to generate a gcloud script that you can run in your Google Cloud Console to assign all the necessary restore permissions to the account. To do that, click **Generate Script**.
Step 5. Configure Target Instance Settings

[This step applies only if you have selected the Restore to new location, or with different settings option at the Restore Mode step of the wizard]

At the Instance step of the wizard, choose a Cloud SQL instance that will host the restored databases. To do that, click the link in the Instance field, select the necessary Cloud SQL instance from the Choose Cloud SQL instance list, and click Apply.

For a Cloud SQL instance to be displayed in the list of available instances, it must belong to the project selected at step 4 and be running on a supported database engine. In Veeam Backup for Google Cloud v3.0, only the MySQL database engine is supported.

**TIP**

Veeam Backup for Google Cloud will perform a number of configuration checks for the selected databases. If any of the checks fail to complete successfully for a database, the wizard will display an error in the Checks column of the Databases to restore table. You can click the link to get more information on the error.
Step 6. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for restoring the Cloud SQL databases. This information will be saved to the session history, and you will be able to reference it later.

![Database Restore](image)

Step 7. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.

![Database Restore](image)
Enabling Data Encryption

For enhanced data security, Veeam Backup for Google Cloud allows you to encrypt backed-up data stored in Google Cloud storage buckets using Veeam encryption mechanisms. Additionally, Veeam Backup for Google Cloud supports native Google Cloud encryption — Google Cloud Key Management Service (Cloud KMS) customer-managed encryption keys (CMEKs).

**IMPORTANT**

Customer-supplied encryption keys (CSEKs) are not supported.

Storage Bucket Encryption

Veeam Backup for Google Cloud encrypts backup files stored in storage buckets the same way Veeam Backup & Replication encrypts backup files stored in backup repositories. To learn what algorithms Veeam Backup & Replication uses to encrypt backup files, see the Veeam Backup & Replication User Guide, section Encryption Standards.

To enable encryption for a backup repository added to the Veeam Backup for Google Cloud infrastructure, configure the repository settings as described in section Adding Backup Repositories. After you create a backup policy and specify the backup repository as a target location for image-level backups, as described in sections Performing VM Backup and Performing SQL Backup, Veeam Backup for Google Cloud performs the following steps:

1. Generates an encryption key to protect files stored in the backup repository, and stores the key in the configuration database on the backup appliance.
2. Uses the generated key to encrypt backed-up data transferred to the backup repository when running the backup policy.
Cloud KMS Encryption

Veeam Backup for Google Cloud allows you to back up and restore data of encrypted Cloud SQL instances and VM instances whose persistent disks are encrypted with Google Cloud KMS CMEKs. Additionally, you can encrypt unencrypted data and change CMEKs used to encrypt data when performing the following operations:

- Restoring entire VM instances to a new location
- Restoring persistent disks of VM instances to a new location
- Restoring entire Cloud SQL instances to a new location

Depending on the operation performed for an encrypted Cloud SQL instance or a VM instance that has encrypted persistent disks, the IAM role that Veeam Backup for Google Cloud uses for the operation may require specific permissions to access Google Cloud KMS resources:

- Creating cloud-native snapshots
- Creating image-level backups
- Restoring from cloud-native snapshots
- Restoring from image-level backups

**NOTE**

When you add a project to the Veeam Backup for Google Cloud infrastructure, you specify a service account that will be used to access the project. Veeam Backup for Google Cloud automatically grants this service account all the necessary IAM role permissions required to perform data protection and disaster recovery operations with Google Cloud resources. You can view and modify the list of granted permissions on the IAM page in the Google Cloud Console. For more information, see Google Cloud documentation.

Creating Cloud-Native Snapshots

The process of creating cloud-native snapshots of an encrypted Cloud SQL instance or a VM instance with encrypted persistent disks does not differ from the same process for an unencrypted Cloud SQL instance or a VM instance with unencrypted persistent disks. The IAM role used to encrypt the created snapshots does not require any additional permissions — Veeam Backup for Google Cloud encrypts these snapshots with the same CMEKs with which the source Cloud SQL instance or persistent disks of the source VM instance are encrypted.
Creating Image-Level Backups

The process of creating image-level backups of an encrypted Cloud SQL instance or a VM instance with encrypted persistent disks does not depend on the location where the worker instance processing the data is deployed. Regardless of whether the worker instance is deployed in the same Google Cloud project where the source Cloud SQL or VM instance belongs, Veeam Backup for Google Cloud performs the following steps:

- To back up a Cloud SQL instance:
  a. Takes a cloud-native snapshot of the Cloud SQL instance.
  b. Exports databases, triggers, stored procedures and users of the Cloud SQL instance to a storage bucket to read and further transfer the backed-up data to a backup repository.
     The IAM role used to encrypt the backed-up data requires permissions to access CMEKs with which the source Cloud SQL instance is encrypted.
  c. Removes the worker instance from the Google Cloud environment.

- To back up a VM instance:
  a. Takes a cloud-native snapshot of the VM instance.
  b. Creates persistent disks from the snapshot.
     To encrypt the created disks, Veeam Backup for Google Cloud requires permissions of an IAM role that can access the CMEK with which you want to encrypt these disks.
  c. Attaches the created persistent disks to the worker instance to read and further transfer the backed-up data to a backup repository.
     The IAM role used to encrypt the backed-up data requires permissions to access CMEKs with which persistent disks of the source VM instance are encrypted.
  d. Removes the worker instance from the Google Cloud environment.

**NOTE**
Every time before creating persistent disks from a cloud-native snapshot, Veeam Backup for Google Cloud checks whether the total size of pd-standard disks breaches the zone quota for the project where the worker instance is deployed. If the total disk size is less than 4000 GB, Veeam Backup for Google Cloud temporarily attaches an additional empty disk to the worker instance — but only for the duration of the backup process and if the quota allows attaching the disk. This allows Veeam Backup for Google Cloud to speed up the data transfer to reduce your backup costs.
Restoring from Cloud-Native Snapshots

The process of restoring a Cloud SQL or VM instance from an encrypted cloud-native snapshot does not differ depending on the location where the restored instance will reside. Regardless of whether the Cloud SQL or VM instance will be restored to the same Google Cloud project where the cloud-native snapshot belongs, Veeam Backup for Google Cloud performs the following steps:

- To restore a Cloud SQL instance:
  a. Creates a Cloud SQL instance in the target location.
     To encrypt the created instance, Veeam Backup for Google Cloud requires permissions of an IAM role that can access the CMEK with which you want to encrypt this instance.
  b. Exports databases, triggers, stored procedures and users of the Cloud SQL instance to a storage bucket to further import the data to the Cloud SQL instance.

- To restore a VM instance:
  a. Creates persistent disks from the cloud-native snapshot.
     To encrypt the created disks, Veeam Backup for Google Cloud requires permissions of an IAM role that can access the CMEK with which you want to encrypt these disks.
  b. Creates a VM instance in the target location.
  c. Attaches the created persistent disks with the restored data to the VM instance.
Restoring from Image-Level Backups

The process of restoring an encrypted Cloud SQL instance or a VM instance with encrypted persistent disks from an image-level backup does not differ depending on the location where the worker instance processing the data is deployed. Regardless of whether the worker instance is deployed in the same Google Cloud project where the restored Cloud SQL or VM instance will belong, Veeam Backup for Google Cloud performs the following steps:

- To restore a Cloud SQL instance:
  a. Creates a Cloud SQL instance in the target location.
     To encrypt the created instance, Veeam Backup for Google Cloud requires permissions of an IAM role that can access the CMEK with which you want to encrypt this instance.
  b. Exports databases, triggers, stored procedures and users of the Cloud SQL instance to a storage bucket to further import the data to the Cloud SQL instance.
  c. Removes the worker instance from the Google Cloud environment.

- To restore a VM instance:
  a. Creates persistent disks from the image-level backup, and attaches the disks to the worker instance to read and further restore the backed-up data to a target location.
     To encrypt the created disks, Veeam Backup for Google Cloud requires permissions of an IAM role that can access the CMEK with which you want to encrypt these disks.
  b. Takes cloud-native snapshots of the persistent disks with the restored data.
  c. Creates a VM instance in the target location.
  d. Creates persistent disks from the snapshots, and attaches the disks to the VM instance.
     To encrypt the created disks, Veeam Backup for Google Cloud requires permissions of an IAM role that can access the CMEK with which you want to encrypt these disks.
  e. Removes the worker instance from the Google Cloud environment.

**NOTE**

Every time before creating persistent disks from a cloud-native snapshot, Veeam Backup for Google Cloud checks whether the total size of pd-standard disks breaches the zone quota for the project where the worker instance is deployed. If the total disk size is less than 1500 GB, Veeam Backup for Google Cloud temporarily attaches an additional empty disk to the worker instance — but only for the duration of the restore process and if the quota allows attaching the disk. This allows Veeam Backup for Google Cloud to speed up the data transfer to reduce your restore costs.
Reviewing Dashboard

Veeam Backup for Google Cloud comes with an Overview dashboard that provides at-a-glance real-time overview of the protected Google Cloud resources and allows you to estimate the overall backup performance. The dashboard includes the following widgets:

- **Sessions in Last 24 Hours** — displays the number of all sessions started for data protection and disaster recovery operations (including system sessions) that completed successfully during the past 24 hours, the number of sessions that completed with warnings, the number of sessions that completed with errors, and the number of sessions that are currently running.

  To get more information on the sessions, click either View Session Logs or any of the widget rows. In the latter case, the Session Logs page will show only those sessions that have the same status as that clicked in the widget.

  For more information on the Session Logs page, see Viewing Session Statistics.

- **Successful Policy Tasks** — displays the number of snapshots, backups and archived backups successfully created by backup policies during a specific time period (the past 24 hours by default), and the number of attempts that were made to create these restore points.

  To specify the time period, click the link next to the Schedule icon. To get more information on the created snapshots, backups or archived backups, click any of the widget rows. In the latter case, the Session Logs page will show only those sessions during which Veeam Backup for Google Cloud created the same items as that clicked in the widget.

  For more information on the Session Logs page, see Viewing Session Statistics.

- **Top Policies** — shows top 8 backup policies for fluctuations in execution time (including retries). For each policy, the widget calculates the growth rate to detect whether it took less or more time for the policy to complete in comparison with the average runtime value for the previous 10 policy launches.

- **Protected Workloads** — displays the number of available Google Cloud resources that got protected by Veeam Backup for Google Cloud during a specific time period (the past 24 hours by default).

  To specify the time period, click the link next to the Schedule icon. To get more information on the protected resources, click any of the widget rows.

  For more information on the available resources, their properties and the actions you can perform for the resources, see Viewing Available Resources.

- **Storage Usage** — displays the amount of storage space that is currently consumed by backups and archived backups created by Veeam Backup for Google Cloud in storage buckets, the number of snapshots created for the protected resources, and the total size of all VM instance snapshots residing in Google Cloud Storage. The widget also calculates the ratio of the total amount of storage space used in the Standard Storage class to the total amount of storage space used in the Archive Storage class.

- **Bottlenecks Overview** — is designed to help you avoid possible backup bottlenecks.

  The widget analyzes the total amount of time waited to deploy worker instances during data protection operations in different Google Cloud regions, and displays the most problematic region (if any).

  The widget also analyzes the amount of disk quota across all regions to detect whether the quota has already been reached in any of the regions, and whether Veeam Backup for Google Cloud failed to deploy a worker instance with the primary profile in that region during a backup or restore process. For more information on machine types of VM instances that operate as worker instances, see Managing Worker Profiles.
The widget also analyzes memory usage on the backup appliance, and displays a warning if the memory usage keeps breaching the preconfigured threshold (80%) for 60 minutes in a row. If the problem persists, the only way to resolve the issue may be to change the machine type for the backup appliance as described in Google Cloud documentation.

To learn how to resolve a bottleneck, click the **How to resolve?** link in the widget row.
Viewing Session Statistics

For each performed data protection or disaster recovery operation, Veeam Backup for Google Cloud starts a new session and stores its records in the configuration database. You can track real-time statistics of all running and completed operations on the Session Logs page.

To view the full list of tasks executed during an operation, click the link in the Status column. To view the full list of Google Cloud resources processed during an operation, click the link in the Items column.

TIP

If you want to specify the time period during which Veeam Backup for Google Cloud will keep session records in the configuration database, follow the instructions provided in section Configuring Global Retention Settings.
Collecting Object Properties

You can export properties of objects managed by Veeam Backup for Google Cloud as a single .CSV or .XML file. To do that, navigate to the necessary tab and click Export. Veeam Backup for Google Cloud will save the file with the exported data to the default download directory on the local machine.

NOTE

Even if you try to export properties of a specific object, Veeam Backup for Google Cloud will still export all properties of all objects present on the currently opened tab.
Updating Veeam Backup for Google Cloud

Veeam Backup for Google Cloud allows you to check for new product versions and available package updates, download and install them right from the Web UI.

It is recommended that you timely install available updates to avoid issues while working with the product. For example, timely installed security updates may help you prevent potential security issues and reduce the risk of compromising sensitive data.
Checking for Updates

Veeam Backup for Google Cloud automatically notifies you about newly released product versions and package updates available for the operating system running on the backup appliance. However, you can check for the available updates manually if required:

1. Switch to the **Configuration** page.
2. Navigate to **Support Information**.
3. Switch to the **Updates** tab.
4. Click **Check and View Updates**.

If new updates are available, Veeam Backup for Google Cloud will display them on the **Updates** tab of the **Veeam Updater** page. To view detailed information on an update, select the check box next to the update and click **What’s new?**
Installing Updates

To download and install new product versions and available package updates, you can use either of the following options:

- **Install updates immediately**
- **Schedule update installation**

You can also **set a reminder to send update notifications**.

**IMPORTANT**

You can update the backup appliance using the Veeam updater service only. Updating of the backup appliance manually is not supported.

### Installing Updates

**IMPORTANT**

Before you install a product update, make sure all backup policies are stopped and restore tasks are finished. Otherwise, the update process will interrupt the running activities, which may result in data loss.

To download and install available product and package updates:

1. Open the **Veeam Updater** page:
   a. Switch to the **Configuration** page.
   b. Navigate to **Support Information**.
   c. Switch to the **Updates** tab.
   d. Click **Check and View Updates**.

2. On the **Veeam Updater** page, do the following:
   a. In the **Updates are available for this system** section, select check boxes next to the necessary updates.
   b. In the **Choose action** section, select the **Install updates now** option, select the **Reboot automatically after install if required** check box to allow Veeam Backup for Google Cloud to reboot the backup appliance if needed, and then click **Install Updates Now**.

**NOTE**

The updater may require you to read and accept the Veeam license agreement and the 3rd party components license agreement. If you reject the agreements, you will not be able to continue installation.
Veeam Backup for Google Cloud will download and install the updates; the results of the installation process will be displayed on the History tab. Keep in mind that it may take several minutes for the installation process to complete.

**NOTE**

When installing product updates, Veeam Backup for Google Cloud restarts all services running on the backup appliance, including the Web UI service. That is why Veeam Backup for Google Cloud will log you out when the update process completes.
Scheduling Update Installation

You can instruct Veeam Backup for Google Cloud to automatically download and install available product versions and package updates on a specific date at a specific time:

1. On the Veeam Updater page, in the Updates are available for this system section, select check boxes next to the necessary updates.

2. In the Choose action section, do the following:
   a. Select the Schedule updates installation option and configure the necessary schedule.

   **IMPORTANT**

   When selecting a date and time for the update installation, make sure no backup policies are scheduled to run on the selected time. Otherwise, the update process will interrupt the running activities, which may result in data loss.

   b. Select the Reboot automatically after install if required check box to allow Veeam Backup for Google Cloud to reboot the backup appliance if needed.

   c. Click Schedule Updates.

Veeam Backup for Google Cloud will automatically download and install the updates on the selected date at the selected time; the results of the installation process will be displayed on the History tab.
Setting Update Reminder

If you have not decided when to install available product versions and package updates, you can set an update reminder — instruct Veeam Backup for Google Cloud to send an update notification later.

To do that, on the Veeam Updater page, in the Choose action section, do the following:

1. Select the Remind me later option and choose when you want to receive the reminder.

   If you select the Next Week option, Veeam Backup for Google Cloud will send the reminder next Monday.

2. Click Remind me later.
Viewing Update History

To see the results of the update installation performed on the backup appliance, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Support Information**.
3. Switch to the **Updates** tab.
4. Click **Check and View Updates**.
5. On the **Veeam Updater** page, switch to the **History** tab.

For each date when an update was installed, the **Veeam Updater** page will display the name of the update and its status (whether the installation process completed successfully, completed with warnings or failed to complete).

To download logs for the installed updates, select the necessary date in the **Date** section, and click **View Full Log**. Veeam Backup for Google Cloud will save the logs as a single file to the default download directory on the local machine.
Getting Technical Support

If you have any questions or issues with Veeam Backup for Google Cloud, you can search for a resolution on Veeam R&D Forums or submit a support case in the Veeam Customer Support Portal.

When you submit a support case, it is recommended that you provide the Veeam Customer Support Team with the following information:

- **Version information for the product and its infrastructure components**
- **The error message or an accurate description of the problem you are facing**
- **Log files**

Viewing Product Details

To view the product details, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Support Information > Updates**.

The **About** section of the **Updates** tab displays the following information:

- **Product version** — the currently installed version of Veeam Backup for Google Cloud.
- **Project ID** — the unique identification number of the Google Cloud project where the VM instance running Veeam Backup for Google Cloud belongs.
- **Support ID** — the unique identification number of the Veeam support contract.
- **FLR service version** — the version of the File-Level Recovery Service currently running on the backup appliance.

**TIP**

You can click the link in the **Available Updates** section of the **Updates** tab to check for, download and install new product versions and available package updates. For more information, see Updating Veeam Backup for Google.
Downloading Logs

To download the product logs, do the following:

1. Switch to the **Download Logs** tab.

2. Click **Download Logs**.

3. In the **Download Logs** window, specify a time interval for which the logs will be collected:
   - Select the **Collect logs for the last** option if you want to collect data for a specific number of days in the past.
   - Select the **Collect logs for the time period from** option if you want to collect data for a specific period of time in the past.

   After you click **OK**, the logs will be saved locally in the default download folder as a single .ZIP archive.