Veeam Backup for Google
Cloud Platform

Version 1.0
User Guide
February, 2021
### Contents

- **CONTACTING VEEAM SOFTWARE** ................................................................. 6
- **ABOUT THIS GUIDE** .................................................................................... 7
- **WELCOME TO VEEAM BACKUP FOR GOOGLE CLOUD PLATFORM** .......... 8
- **SYSTEM REQUIREMENTS** ............................................................................ 9
- **LICENSING** ................................................................................................. 11
  - Installing and Removing License ................................................................. 12
  - Viewing License Information ....................................................................... 14
  - Revoking License Units.................................................................................. 15
- **ARCHITECTURE OVERVIEW** ..................................................................... 16
- **DEPLOYMENT** ............................................................................................. 18
  - Installing Veeam Backup for Google Cloud Platform ................................. 18
  - After You Install .......................................................................................... 20
  - Uninstalling Veeam Backup for Google Cloud Platform ............................... 22
- **ACCESSING VEEAM BACKUP FOR GOOGLE CLOUD PLATFORM** .......... 23
- **CONFIGURING VEEAM BACKUP FOR GOOGLE CLOUD PLATFORM** ........ 25
  - Managing Projects ....................................................................................... 26
    - Adding Projects .......................................................................................... 26
    - Editing Projects .......................................................................................... 29
    - Removing Projects ...................................................................................... 30
  - Managing Permissions ................................................................................... 31
    - Adding Backup Administrator Accounts ................................................. 31
    - Changing Backup Administrator Passwords .......................................... 34
    - Enabling Multi-Factor Authentication ..................................................... 35
  - Managing Repositories ................................................................................. 36
    - Adding Backup Repositories ..................................................................... 36
    - Editing Backup Repositories ..................................................................... 41
    - Removing Backup Repositories ............................................................... 42
  - Managing Workers ........................................................................................ 43
    - Adding Worker Configurations ............................................................... 43
    - Editing Worker Configurations ............................................................... 48
    - Removing Worker Configurations ........................................................... 49
  - Configuring General Settings ...................................................................... 50
    - Configuring Global Retention Settings ..................................................... 51
    - Configuring Global Notification Settings ................................................. 53
    - Replacing Security Certificates ............................................................... 58
    - Changing Time Zone .................................................................................. 59
# Veeam Backup for Google Cloud Platform | User Guide

## PERFORMING BACKUP

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>How Backup Works</td>
<td>61</td>
</tr>
<tr>
<td>How Backup Works</td>
<td>61</td>
</tr>
<tr>
<td>How Backup Works</td>
<td>61</td>
</tr>
<tr>
<td>How Backup Works</td>
<td>61</td>
</tr>
<tr>
<td>Snapshot Chain</td>
<td>62</td>
</tr>
<tr>
<td>Backup Chain</td>
<td>63</td>
</tr>
<tr>
<td>Retention Policy</td>
<td>64</td>
</tr>
<tr>
<td>Creating Backup Policies</td>
<td>66</td>
</tr>
<tr>
<td>Creating Backup Policies</td>
<td>66</td>
</tr>
<tr>
<td>Creating Backup Policies</td>
<td>66</td>
</tr>
<tr>
<td>Creating Backup Policies</td>
<td>66</td>
</tr>
<tr>
<td>Step 1. Launch Add Policy Wizard</td>
<td>67</td>
</tr>
<tr>
<td>Step 2. Specify Backup Policy Name and Description</td>
<td>67</td>
</tr>
<tr>
<td>Step 3. Configure Backup Source Settings</td>
<td>68</td>
</tr>
<tr>
<td>Step 4. Configure Backup Target Settings</td>
<td>71</td>
</tr>
<tr>
<td>Step 5. Specify Policy Scheduling Options</td>
<td>73</td>
</tr>
<tr>
<td>Step 6. Review Estimated Cost</td>
<td>81</td>
</tr>
<tr>
<td>Step 7. Specify Retry and Email Notification Settings</td>
<td>83</td>
</tr>
<tr>
<td>Step 8. Finish Working with Wizard</td>
<td>84</td>
</tr>
<tr>
<td>Editing Backup Policy Settings</td>
<td>85</td>
</tr>
<tr>
<td>Setting Backup Policy Priority</td>
<td>86</td>
</tr>
<tr>
<td>Exporting and Importing Backup Policies</td>
<td>87</td>
</tr>
<tr>
<td>Enabling and Disabling Backup Policies</td>
<td>89</td>
</tr>
<tr>
<td>Starting and Stopping Backup Policies</td>
<td>90</td>
</tr>
<tr>
<td>Creating Snapshots Manually</td>
<td>91</td>
</tr>
<tr>
<td>Removing Backups and Snapshots</td>
<td>92</td>
</tr>
<tr>
<td>Removing Snapshots Created Manually</td>
<td>93</td>
</tr>
</tbody>
</table>

## PERFORMING RESTORE

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performing Instance Restore</td>
<td>95</td>
</tr>
<tr>
<td>Performing Instance Restore</td>
<td>95</td>
</tr>
<tr>
<td>Step 1. Launch Instance Restore Wizard</td>
<td>97</td>
</tr>
<tr>
<td>Step 2. Select Restore Point</td>
<td>98</td>
</tr>
<tr>
<td>Step 3. Select Project</td>
<td>99</td>
</tr>
<tr>
<td>Step 4. Choose Restore Mode</td>
<td>100</td>
</tr>
<tr>
<td>Step 5. Select Region and Availability Zone</td>
<td>100</td>
</tr>
<tr>
<td>Step 6. Enable Encryption</td>
<td>101</td>
</tr>
<tr>
<td>Step 7. Specify Instance Name and Type</td>
<td>102</td>
</tr>
<tr>
<td>Step 8. Configure Network Settings</td>
<td>103</td>
</tr>
<tr>
<td>Step 9. Specify Restore Reason</td>
<td>104</td>
</tr>
<tr>
<td>Step 10. Finish Working with Wizard</td>
<td>104</td>
</tr>
<tr>
<td>Performing Disk Restore</td>
<td>105</td>
</tr>
<tr>
<td>Performing Disk Restore</td>
<td>105</td>
</tr>
<tr>
<td>Step 1. Launch Disk Restore Wizard</td>
<td>107</td>
</tr>
<tr>
<td>Step 2. Select Restore Point</td>
<td>108</td>
</tr>
<tr>
<td>Step 3. Select Project</td>
<td>109</td>
</tr>
<tr>
<td>Step 4. Choose Restore Mode</td>
<td>109</td>
</tr>
</tbody>
</table>
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 at www.veeam.com/support.html 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 www.veeam.com/contacts.html.

Online Support

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

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

This guide is designed for IT professionals who plan to use Veeam Backup for Google Cloud Platform. 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 Platform environments.
Welcome to Veeam Backup for Google Cloud Platform

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

- Create image-level backups and cloud-native snapshots of VM instances.
- Restore entire VM instances, individual persistent disks, and guest OS files and folders.
System Requirements

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

- **Network ports**
- **GCP APIs**

Network Ports

The following network ports must be open to ensure proper communication of components in the Veeam Backup for GCP 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>Worker instance</td>
<td>TCP 443</td>
<td></td>
<td></td>
<td>Required to access the File Level Recovery for Veeam Backup browser running on a worker instance during the file-level recovery process.</td>
</tr>
<tr>
<td>Backup appliance</td>
<td>Worker instance</td>
<td>SSH</td>
<td>22</td>
<td>Required to deploy the Worker service to worker instances.</td>
</tr>
<tr>
<td></td>
<td>RPC 643</td>
<td></td>
<td></td>
<td>Required to communicate with the Worker service running on worker instances.</td>
</tr>
<tr>
<td></td>
<td>TCP 9999</td>
<td></td>
<td></td>
<td>Required to perform file-level recovery.</td>
</tr>
<tr>
<td>Ubuntu Security Update Repository (security.ubuntu.com)</td>
<td>HTTP 80</td>
<td></td>
<td></td>
<td>Required to get OS security updates.</td>
</tr>
<tr>
<td>Veeam Update Notification Server (repository.veeam.com)</td>
<td>TCP 443</td>
<td></td>
<td></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](#).
GCP APIs

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

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

Veeam Backup for GCP is licensed by the number of protected VM instances. A VM 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 VM instance consumes 1 license unit. However, if a VM instance has only manually created snapshots, it does not consume any license units.

**NOTE**

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

Veeam Backup for GCP is available in 2 license editions:

- **Free License**
  
  By default, Veeam Backup for GCP operates in the *Free* edition that allows you to protect up to 10 VM 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 VM instances managed by Veeam Backup for GCP 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 GCP 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 GCP stops processing all VM 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.
Installing and Removing License

By default, Veeam Backup for GCP 1.0 comes with a Free license. To unlock the full product functionality, you must install a Bring Your Own License.

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 BYOL License

To remove a BYOL 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 Confirmation window, click Yes to confirm that you want to remove the license.

After you remove the license, Veeam Backup for GCP will automatically switch back to the Free edition. In this case, according to the FIFO (first-in first-out) queue, only the first 10 VM instances registered in the configuration database will remain protected. You can revoke license units from these VM 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 GCP 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 VM instances that consume license units. Each VM instance that has a restore point created in the past 31 days is considered to be protected and consumes 1 license unit. To view the list of VM 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, BYOL**).

- **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 GCP automatically revokes a license unit from a protected VM 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 VM instances — this can be helpful, for example, if you remove a number of VM instances from a backup policy and do not want to protect them anymore.

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

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

The Veeam Backup for GCP 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 GCP is installed. The backup appliance performs the following administrative activities:

- Manages infrastructure components.
- Coordinates snapshot creation, backup and recovery tasks.
- Controls backup policy scheduling.

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

**Backup Repositories**

A backup repository is a GCP storage bucket where Veeam Backup for GCP stores backups of VM instances.

To communicate with a backup repository, Veeam Backup for GCP 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.

**Encryption on Repositories**

For enhanced data security, Veeam Backup for GCP allows you to enable encryption at the repository level. Veeam Backup for GCP 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 GCP allows you to store backups only in the Standard Storage class. Nearline Storage, Coldline Storage and Archive 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 GCP infrastructure. Worker instances process backup workload and distribute backup traffic when transferring data to backup repositories.

Veeam Backup for GCP automatically deploys a worker instance to every processed VM instance and keeps the worker instance running for the duration of the backup or restore process. To minimize cross-region traffic charges and to speed up the data transfer, depending on the performed operation, Veeam Backup for GCP launches the worker instance in the following location:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Worker Instance Location</th>
<th>Default Worker Instance Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating image-level backups</td>
<td>GCP 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>VM instance restore</td>
<td>GCP region to which an VM instance is restored</td>
<td>e2-highcpu-4, with an additional empty standard persistent (pd-standard) disk up to 1500 GB in size</td>
</tr>
<tr>
<td>File-level restore from cloud-native snapshots</td>
<td>GCP region in which an original VM instance resides</td>
<td>e2-highcpu-2</td>
</tr>
<tr>
<td>File-level restore from image-level backups</td>
<td>GCP region in which a storage bucket with backed-up data resides</td>
<td>e2-highcpu-2</td>
</tr>
</tbody>
</table>

Worker instances are deployed based on worker configurations that can be created either automatically by Veeam Backup for GCP, or manually by the user as described in section Managing Workers.

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 Recovery for Veeam Backup Browser** — the web service that allows you to find and save files and folders of a backed-up instance to a local machine. The Veeam File-Level Recovery 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 Recovery for Veeam Backup browser, see Performing File-Level Recovery.

Security Certificates for Worker Instances

Veeam Backup for GCP uses self-signed TLS certificates to establish secure communication between the web browser on a user workstation and the File Level Recovery for Veeam Backup 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 GCP comes as an image of a Linux-based VM that you can deploy from Google Cloud Marketplace.

Installing Veeam Backup for Google Cloud Platform

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

To install Veeam Backup for GCP, do the following:

1. Log in to Google Cloud Marketplace using credentials of a GCP service account that you plan to use to install Veeam Backup for GCP.

   **IMPORTANT**

   The service account must be both enabled (to gain access to GCP resources) and granted the Service Account Admin role or the Editor basic role (to perform actions on the behalf of Veeam Backup for GCP). To learn how to enable GCP service accounts and grant roles to them, see Google Cloud documentation.

2. Click Explore Marketplace.


4. In the list of search results, click the necessary product edition to open the Veeam Backup for GCP overview page.

5. Click Launch.

6. On the New Veeam Backup for Google Cloud Platform deployment page, configure the following installation settings:

   a. Select a project where the VM instance running Veeam Backup for GCP will belong.

       **IMPORTANT**

       Make sure, that GCP APIs listed in System Requirements are enabled for the selected project. Otherwise, Veeam Backup for GCP deployment may fail or cause unexpected errors. To learn how to enable APIs for a Google Cloud project, see Google Cloud documentation.

   b. In the Deployment name field, enter a name for the new Veeam Backup for GCP deployment.

      The deployment will include the VM instance running Veeam Backup for GCP, the GCP service account used to deploy the VM instance, firewall rules created 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 GCP region in which the VM instance running Veeam Backup for GCP will reside.

      To learn how to configure availability and redundancy settings for GCP resources, see Google Cloud documentation.
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 GCP.

The recommended hardware requirement for a VM instance running Veeam Backup for GCP 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 GCP, 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 GCP will be connected.

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 6b in the Google Cloud Console as described in Google Cloud documentation.

**IMPORTANT**

Consider the following:

- The specified VPC network and subnet must have the outbound internet access to GCP APIs listed in System Requirements. Otherwise, Veeam Backup for GCP may not work efficiently and may cause unexpected errors.
- 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 GCP.

To learn how to enable internet access for VPC networks and subnets, see Google Cloud documentation.

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

**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 GCP, 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 Platform interface. Click the link to proceed to the initial configuration required to start working with Veeam Backup for GCP.
After You Install

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

1. In a web browser, navigate to the Veeam Backup for GCP 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 GCP, use Microsoft Edge (version 40 or later), Mozilla Firefox (version 56 or later) or Google Chrome (version 62 or later).

2. Read and accept both the Veeam license agreement and the 3rd party components license agreement. If you reject the agreements, you will not be able to continue installation.
   To read the terms of the license agreement for the 3rd party components, click **3rd party components license agreement**.

3. In the **Check Google Instance ID** field, specify the unique numeric identifier of the VM instance running Veeam Backup for GCP to prove that you are the owner of this VM instance.
   To obtain the ID assigned to the VM instance upon creation, you can 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 GCP.

   **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 GCP. To learn how to enable MFA, see Enabling Multi-Factor Authentication.

5. Log in to Veeam Backup for GCP with the credentials of the Default Administrator account, as described in section Accessing Veeam Backup for Google Cloud Platform.
   You will immediately receive a warning in the notification area notifying that the service account used to install Veeam Backup for GCP does not have the permissions required to perform data protection tasks for the project selected during the product installation. To eliminate the warning, do the following:
   a. Click the link in the notification area.
   b. In the **Edit Project** wizard, at the **Service Account** step, click **Generate and download script**. Veeam Backup for GCP 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 `iam.roles.create` permission granted. To learn what permissions and roles are required to create custom roles in IAM, see Google Cloud documentation.
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.

At the **Summary** step of the wizard, review configuration information and click **Finish** to confirm the changes.
Uninstalling Veeam Backup for Google Cloud Platform

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

1. Log in to Google Cloud Console using credentials of the GCP service account that you used to install Veeam Backup for GCP.
3. Click Veeam Backup for Google Cloud Platform to open the Veeam Backup for GCP overview page.
4. Click Delete.
5. Wait until Veeam Backup for GCP is removed from your organization domain.
6. 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.
7. Navigate to IAM & Admins > Roles.
   In the list of roles, locate the role with the ID of the VM instance that was running Veeam Backup for GCP 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 GCP (these sinks will have the ID of the VM instance that was running Veeam Backup for GCP in their names), and then delete these sinks.
Accessing Veeam Backup for Google Cloud Platform

To access Veeam Backup for GCP, do the following:

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

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

   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.

   If you log in for the first time, use credentials of the Default Administrator that was created after the product installation. In future, you can add other users to grant access to Veeam Backup for GCP. For more information, see Adding Backup Administrator Accounts.

3. Select the **Keep me logged in** check box to save the specified credentials in a persistent browser cookie so that you do not have to provide credentials every time you access Veeam Backup for GCP in a new browser session.
4. Click **Login**.

If **multi-factor authentication (MFA) is enabled** for the user, Veeam Backup for GCP 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 GCP window, click the user name and then click **Log out**.
Configuring Veeam Backup for Google Cloud Platform

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

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

**NOTE**

Even after you add projects that manage your GCP resources and configure all the necessary settings, Veeam Backup for GCP will not populate the list of VM instances on the *Instances* page — unless you create backup policies and specify regions where the VM instances belong, as described in section *Creating Backup Policies.*
Managing Projects

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

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

- To access projects that manage GCP resources.
- To synchronize the GCP environment data with the configuration data stored on the backup appliance.
- To create and remove VM instance snapshots.

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.

Step 2. Select Project

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

You can find the project name and ID on the Dashboard page in the Google Cloud Console. For more information, see Google Cloud documentation.
Step 3. Specify Service Account Name

At the Service Account step of the wizard, choose whether you want Veeam Backup for GCP 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.

  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 GCP 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 GCP service accounts, see Google Cloud documentation.

![Service Account Step](image)

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

![Edit Project](image)
Removing Projects

Veeam Backup for GCP 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

To allow different users to access Veeam Backup for GCP, you can create the Backup Administrator accounts for these users. Users that log in to Veeam Backup for GCP as Backup Administrators are allowed to perform all administrative activities and data protection tasks (for example, to configure settings, to back up VM instances, to restore backed-up data and so on).

Adding Backup Administrator Accounts

To add a new Backup Administrator 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.
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 > Backup 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 account and to provide a description for future reference.

The maximum length of the account name is 255 characters. The following characters are supported: lowercase Latin letters, numeric characters, underscores and dashes. The following characters are not supported: / \ * ' ] : | < > + = ; , ? * @ & . The dollar sign ($) can be used only as the last character of the name.
Step 3. Specify Password

At the **Credentials** step of the wizard, specify a password that the user will use to access Veeam Backup for GCP.

![Add Account](image)

**Account Info**

**Specify account credentials**

**Credentials**

- **Password:** ********
- **Repeat password:** ********

*The password must be at least 8 characters long. It must contain at least 1 numeric character (0-9), 1 uppercase letter (A-Z) and 1 lowercase letter (a-z). Monotonic sequences (such as 1234) are not allowed.*

![Next, Previous, Cancel buttons](image)

---

Step 4. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.
Changing Backup Administrator Passwords

For each Backup Administrator account, you can change the password specified while creating the account:

1. Switch to the **Configuration** page.
2. Navigate to **Permissions > Backup Accounts**.
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**.
Enabling Multi-Factor Authentication

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

To enable MFA for a user accessing Veeam Backup for GCP as a Backup Administrator, do the following:

1. Switch to the Configuration page.
2. Navigate to Permissions > Backup Accounts.
3. Select the account and click Enable MFA.
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 GCP, 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.
Managing Repositories

Veeam Backup for GCP uses GCP storage buckets as target locations to store backups of VM instances. To add a storage bucket to Veeam Backup for GCP, configure a backup repository.

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. Configure repository settings.
4. Enable encryption for the repository.
5. 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 Backup 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. Configure Repository Settings

At the Storage Bucket 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 GCP 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 GCP 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. 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.

3. 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 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.

   **TIP**

   It may take some time for Veeam Backup for GCP to retrieve information about existing storage buckets from Google Cloud Platform. To speed up the data collection process, click Rescan.

4. 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 backup files 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.

   **NOTE**

   If the selected subdirectory already contains backup files, Veeam Backup for GCP 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.
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: `\ / " ' { [ ] : | < > + = ; , ? * @ & _`.
Step 4. 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 5. 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 GCP 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 GCP infrastructure:

1. Switch to the **Configuration** page.
2. Navigate to **Backup 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 GCP 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 GCP allows you to permanently remove backup repositories from the infrastructure. When you remove a backup repository, Veeam Backup for GCP unassigns the repository from the target storage bucket so that the bucket is no longer used as a repository.

**NOTE**

Even though the storage bucket is no longer used as a repository, Veeam Backup for GCP preserves all backup files previously stored in the repository and keeps these files in Google Cloud Storage. You can assign the bucket to a new backup repository so that Veeam Backup for GCP 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 GCP infrastructure, do the following:

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

**NOTES**

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

Veeam Backup for GCP deploys one worker instance per each VM instance added to a backup policy or restore task. Veeam Backup for GCP comes with the default worker configuration that deploys worker instances with the same networking configurations as those specified for the processed VM instances.

To optimize infrastructure costs and to ensure better performance of the backup and restore processes, you can add custom worker configurations to specify network settings for each region in which worker instances will be deployed.

Adding Worker Configurations

To add a new worker configuration, do the following:

1. Choose a project where worker instances will be created.
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

The type of each deployed worker instance is selected based on the regional quota. To boost operational performance and to reduce GCP data transfer costs, the largest machine type that Veeam Backup for GCP may require when deploying a worker instance is e2-highcpu-8. That is why it is recommended that you allocate a single specific project just for your worker instances so that you do not breach GCP quota limits.

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

1. Switch to the Configuration page.
2. Navigate to Worker Configurations.
3. Click the link in the Project section.
4. In the Choose Project window, select the necessary project and click Apply.

IMPORTANT

After you choose a project, do not try to change it by clicking the link in the Project section. Otherwise, all created worker configurations will be removed automatically as soon as you choose another project.
Step 2. Launch Add Worker Configuration Wizard

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

Step 3. Specify General Settings

At the Region & Zone 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 Settings** 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](https://cloud.google.com/).

   **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](https://cloud.google.com/).
   - The selected subnet must have Private Google Access enabled. To learn how to enable Private Google Access for a subnet, see [Google Cloud documentation](https://cloud.google.com/).

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](https://cloud.google.com/).

   **Important**
   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](https://cloud.google.com/).

### Add Worker Configuration

<table>
<thead>
<tr>
<th>Region &amp; Zone</th>
<th>Specify network settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Settings</td>
<td>VPC network: yam-allregionsrules</td>
</tr>
<tr>
<td>Subnet: yam-us-wsec4</td>
<td></td>
</tr>
<tr>
<td>Firewall rule: yam-allregrule</td>
<td></td>
</tr>
</tbody>
</table>
Step 5. 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 GCP will start adding the new worker configuration to the infrastructure. To track the progress, click **Go to Sessions** in the **Session Info** window to proceed to the **Session Logs page**.
Editing Worker Configurations

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

1. Switch to the Configuration page.
2. Navigate to Worker Configurations.
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 Configuration (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 GCP allows you to permanently remove worker configurations from the infrastructure. When you remove a worker configuration, Veeam Backup for GCP also removes all worker instances that have been created based on this configuration.

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

1. Switch to the **Configuration** page.
2. Navigate to **Worker Configurations**.
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.
Configuring General Settings

Veeam Backup for GCP 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 must be retained.
- Provide certificates to secure connections between Veeam Backup for GCP 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 must be retained in the configuration database:

- Obsolete snapshots
- Session records

Configuring Retention Settings for Obsolete Snapshots

If a VM 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. Retention policy settings configured when creating backup policies do not apply to obsolete snapshots — these snapshots are removed from the configuration database according to their own retention settings.

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 GCP to remove obsolete snapshots.
   - Select the After option if you want to specify the number of days (or months) during which Veeam Backup for GCP must keep obsolete snapshots in the configuration database. The number must be between 90 and 36135.
     If you select this option, Veeam Backup for GCP will first wait for the specified period of time after a VM instance stops being processed by a backup policy, and then will remove its obsolete snapshots from the configuration database as soon as the period is over.
4. Click Save.
Configuring Retention Settings for Session Records

Veeam Backup for GCP stores records for all sessions of performed data protection and disaster recovery operations. 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 GCP 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 GCP must keep session records in the configuration database.

   If you select this option, Veeam Backup for GCP will remove all session records that are older than the specified time limit.

2. Click **Save**.
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 or an IP address 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. Do not use spaces after semicolons between the specified email 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 GCP will send each notification twice to this recipient.

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 VM instances in a backup policy.
   - %Issues% — the number of VM 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 must be sent.

11. Click **Save**.

**TIP**

Veeam Backup for GCP allows you to send a test message to check whether you have configured all 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 64 characters; the following characters are not supported: \ / " ' [ ] : | < > = ; , ? * @ & _.

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.

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 the 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 GCP uses Transport Layer Security (TLS) certificates.

When you install Veeam Backup for GCP, 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 GCP.
      - 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 if required.

   **NOTE**

   For certificates obtained from 3rd party tools, only .PFX files are supported.

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

To allow Veeam Backup for GCP to discover the newly installed certificate, restart the backup appliance.
Changing Time Zone

Veeam Backup for GCP 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 GCP.

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**.
Performing Backup

With Veeam Backup for GCP, you can protect VM instance data 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 GCP 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.

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.
How Backup Works

Veeam Backup for GCP does not install agent software inside VM instances to retrieve data. To back up VM instances, Veeam Backup for GCP uses capabilities of PD snapshots.

During every backup session, Veeam Backup for GCP creates a cloud-native snapshot of each VM instance added to a backup policy. The cloud-native snapshot is further used to create an image-level backup of the VM instance. Veeam Backup for GCP performs backup in the following way:

1. Veeam Backup for GCP creates snapshots of persistent disks that are attached to the processed VM instance.

2. PD snapshots are assigned resource labels upon creation. Keys and values of resource labels contain encrypted metadata that helps Veeam Backup for GCP identify the related PD snapshots and treat them as a single unit — a cloud-native snapshot.

3. If you enable image-level backup for the backup policy, Veeam Backup for GCP performs the following operations:
   a. Launches a worker instance in a GCP region where the processed VM instance resides.
   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 until the next image-level backup session.
   c. Reads data from the persistent disks on the worker instance, transfers the data to a GCP storage bucket and stores it in the native Veeam format.
      Veeam Backup for Google Cloud Platform 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.
Snapshot Chain

During every backup session, Veeam Backup for GCP creates a cloud-native snapshot of each VM instance added to a backup policy. The cloud-native snapshot itself is a collection of point-in-time snapshots that Veeam Backup for GCP creates using native GCP capabilities.

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

1. During the first backup session, Veeam Backup for GCP takes a snapshot of all VM instance data and saves it in the region where the processed VM 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 GCP copies the whole image of the VM instance.

2. During subsequent backup sessions, Veeam Backup for GCP takes snapshots of 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.

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

Cloud-native snapshots act as independent restore points for backed-up VM 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 a 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 GCP will create 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 backup chain.

The backup chain includes backup files of the following types:

- **Full** – a full backup file stores a copy of the full VM image.
- **Incremental** – incremental backup files store incremental changes of VM images.

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

1. During the first backup session, Veeam Backup for GCP copies the full VM image and creates a full backup file in the backup repository. The full backup file becomes a starting point in the backup chain.

2. During subsequent backup sessions, Veeam Backup for GCP 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 backup chain.

Full and incremental backup files act as restore points for backed-up VM instances that let you roll back instance data to the necessary state. To recover a VM 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.

If some file in the 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**.
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.

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 GCP 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 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 GCP removes it from the backup chain. For more information, see Retention Policy for 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 GCP retains the number of latest restore points defined in backup scheduling settings.

During every successful backup session, Veeam Backup for GCP creates a new restore point. If Veeam Backup for GCP detects that the number of restore points in the snapshot chain exceeds the retention limit, it removes the earliest restore point from the chain.

Mind Veeam Backup for GCP does not apply retention policy settings to cloud-native snapshots created manually. To learn how to remove these snapshots, see section Removing Snapshots Created Manually.
Retention Policy for Backups

For image-level backups, Veeam Backup for GCP retains restore points for the number of days defined in backup scheduling settings.

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

1. Veeam Backup for GCP checks the configuration database to detect GCP storage buckets that contain outdated restore points.

2. If an outdated restore point exists in a storage bucket, Veeam Backup for GCP transforms the backup chain in the following way:
   a. Veeam Backup for GCP rebuilds the full backup file to include the data of the incremental backup file that follows the full backup file. To do that, Veeam Backup for GCP 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 backup chain.

   ![Diagram 1](image1.png)

   b. Veeam Backup for GCP removes the earliest incremental backup file from the chain as redundant — this data has already been injected into the full backup file.

   ![Diagram 2](image2.png)

3. Veeam Backup for GCP repeats step 2 for all other outdated restore points found in the 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 GCP ensures that the backup chain is not broken and that you will be able to recover your data when needed.

   ![Diagram 3](image3.png)
Creating Backup Policies

To produce image-level backups of VM instances, Veeam Backup for GCP 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 backups must be stored, when the backup process must start 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 create a backup policy, do the following:

1. Launch the Add 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. Review the estimated cost of protecting the selected VM instances.
7. Specify automatic retry settings and notification settings for the backup policy.
8. Finish working with the wizard.
Step 1. Launch Add Policy Wizard

To launch the Add Policy wizard, do the following:

1. Navigate to Policies.
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 GCP runs a backup policy, it adds the first 20 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 where 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 GCP 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 **Specify region** section of the **Sources** step of the wizard, choose regions where 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 GCP will back up:

1. Click **Select 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 GCP 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 **Protect specific resources** option, you must also specify the instances explicitly:
     a. Use the **Type** drop-down list to choose whether you want to add individual VM instances or GCP labels to the backup scope.
        - If you select the **Label** option, Veeam Backup for GCP will back up only those VM instances that reside in the selected regions under specific labels.
     b. Use the search field to the right of the **Type** list to find the necessary resource, and then click **Protect** to add the resource to the backup scope.
        - Alternatively, you can click **Select resources from the global list**, select check boxes next to the necessary VM instances or labels in the list of available resources, and then click **Protect**.
TIP

It may take some time for Veeam Backup for GCP to access GCP resources and to populate the list of available VM instances or labels. To speed up the data collection process, click Rescan.

If you add a label to the backup scope, Veeam Backup for GCP 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.
Step 4. Configure Backup Target Settings

At the Targets step of the wizard, you can enable the following additional data protection scenarios:

- Assign labels to created cloud-native snapshots.
- Instruct Veeam Backup for GCP to create image-level backups.

Step 4a. Configure Snapshot Settings

If you want to assign labels to cloud-native snapshots of the selected VM instances, do the following:

1. Click the link in the Snapshot Settings section of the Targets step of the wizard.
2. In the Choose labels to assign window, choose whether you want to assign already existing labels from source persistent disks or your own custom labels.

   If you set the Add custom labels toggle to On, you must also specify the labels explicitly. To do that, use the Key and Value fields to specify a key and a value for the new custom label, and then click Add.

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

![Image of the Veeam Backup for Google Cloud Platform interface showing the Snapshot Settings section with options to assign labels and a click to apply changes.](image-url)
Step 4b. Configure Backup Settings

If you want to create image-level backups of the selected VM instances, do the following:

1. In the **Backup Settings** section of the **Targets** step of the wizard, set the **Enable backups** toggle to **On**.

2. In the **Choose repository** window, select a backup repository where the created image-level backups must be stored.

   For a backup repository to be displayed in the **Repository** list, it must be added to Veeam Backup for GCP as described in section **Adding Backup Repositories**.

3. To save changes made to the backup policy settings, click **Apply**.
Step 5. Specify Policy Scheduling Options

You can instruct Veeam Backup for GCP 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 must be backed up.

To help you implement a comprehensive backup strategy, Veeam Backup for GCP 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 archive restore points for longer periods of time. 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 retention** toggle to **On** and click **Configure daily settings**.
2. In the **Create daily schedule** window, select hours when the backup policy must create cloud-native snapshots and image-level backups.
   
   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 must create within an hour.

   **NOTE**

   Veeam Backup for GCP 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 GCP performs backup, see How Backup Works.

3. Use the **Run at** drop-down list to choose whether you want the backup policy to run everyday, on work days (Monday through Friday) or on specific days.

4. 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 GCP 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 GCP 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 retention toggle to On and click Configure weekly settings.

2. In the Create weekly schedule window, select weekdays when the backup policy must create cloud-native snapshots and image-level backups.

   **NOTE**
   
   Veeam Backup for GCP 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 GCP performs backup, see How Backup Works.

3. Use the Create restore points at drop-down list to schedule a specific time for the backup policy to run.

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 GCP 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 GCP 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 retention** toggle to *On* and click **Configure monthly settings**.

2. In the **Create monthly schedule** window, select months when the backup policy must create cloud-native snapshots and image-level backups.

**NOTE**

Veeam Backup for GCP 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 GCP performs backup, see *How Backup Works*.

3. 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.

4. In the **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 GCP 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 GCP 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 Yearly Schedule

[This step applies only if you have instructed Veeam Backup for GCP 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 retention** toggle to **On** and click **Edit yearly settings**.

2. In the **Create yearly schedule** window, specify a day, month and time when the backup policy must 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 GCP 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**.
Enabling Backup Archiving

You can archive restore points created according to the daily, weekly or monthly schedule for longer periods of time:

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

To archive restore points, you must create at least 2 different schedules: one schedule will control the regular creation of restore points, while another schedule will control the backup archiving process. In terms of backup archiving, Veeam Backup for GCP treats schedules of different types as tiers with the ascending priority: daily, weekly, monthly, yearly. When you configure multiple schedules, Veeam Backup for GCP first creates restore points according to the lower-tier schedule, and then archives one of the created restore points according to higher-tier schedules.

In the backup archiving scenario, each restore point is marked with a flag of the related schedule type: the (D) flag is used to mark restore points created daily, (W) — weekly, (M) — monthly, and (Y) — yearly. Veeam Backup for GCP uses these flags to control the retention period for archived backups. Once a flag of a higher-tier schedule is assigned to a restore point, this restore point can no longer be removed — it remains archived 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 lower-tier schedule.

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 to archive one of the created snapshots for 2 weeks. In this case, you must create 2 schedules when configuring the backup policy settings — daily and weekly:

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

Veeam Backup for GCP will propagate these settings to the schedule of a higher tier (which is the weekly schedule in our example).
2. In the weekly scheduling settings, you must specify which one of the snapshots created by the daily schedule must be archived, and choose for how long you want to archive the selected snapshot.

For example, if you want to archive the daily restore point created at 7:00 AM on Monday for 2 weeks, you must 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 GCP will create cloud-native snapshots in the following way:

1. On the first work day (Monday), a backup session will start at 7:00 AM to create the first restore point. The restore point will be marked with the (D) 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 GCP will treat this restore point as archived and will add the (W) flag to it.

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

By the moment the backup session completes, the number of restore points with the (D) flag will exceed the retention limit specified in the daily scheduling settings. However, Veeam Backup for GCP will not remove the earliest restore point (*7:00 AM, Monday*) with the (D) flag from the snapshot chain as this restore point is also marked with a flag of a higher-tier schedule. Instead, Veeam Backup for GCP will unassign the (D) flag from the restore point. This restore point will be archived 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 (D) flag will exceed the retention limit once again. Veeam Backup for GCP will remove from the snapshot chain the restore point created at 9:00 AM on Monday as no flags of a higher-tier schedule are assigned to this restore point.

5. Veeam Backup for GCP 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 archived restore points will exceed the retention limit. Veeam Backup for GCP will unassign the (W) flag from the earliest archived restore point. Since no other flags are assigned to this restore point, Veeam Backup for GCP will remove this restore point from the snapshot chain.
Step 6. 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 GCP resources that will be consumed 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 GCP takes into account the machine type, 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 GCP takes into account the machine type, the number of persistent disks attached, the number of restore points to be kept in the backup chain, and the configured scheduling settings.

- The cost of transferring the VM instance data between GCP regions during data protection operations (for example, if a protected VM instance and the target storage bucket reside in different regions).
  
  If you get a warning message regarding additional costs associated with cross-region data transfer, you can click View details to see available cost-effective options.

- 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, configure the scheduling settings to run the backup policy less frequently.

**TIP**

You can save the cost estimation as a .CSV or .XML file. To do that, click Export and select the necessary format.
## Review cost estimation

The information calculates the costs based on the configured target settings, the specified scheduling options, and the number of resources to protect.

Note: Veeam Backup for GCP makes predefined assumptions to calculate the cost, which means that the results should be used only as an approximation.

For more information on how Veeam Backup for GCP calculates the cost, see this Veeam KB article.

---

Estimated monthly cost: $125.56

<table>
<thead>
<tr>
<th>Instance</th>
<th>Snapshot</th>
<th>Backup</th>
<th>Traffic</th>
<th>Transact.</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>gce-standard-4c6</td>
<td>$5.67</td>
<td>$14.72</td>
<td>$6.15</td>
<td>$3.64</td>
<td>$33.18</td>
</tr>
<tr>
<td>gce-standard-8c</td>
<td>$11.24</td>
<td>$29.58</td>
<td>$6.15</td>
<td>$3.64</td>
<td>$53.61</td>
</tr>
<tr>
<td>gce-standard-8c</td>
<td>$11.24</td>
<td>$29.58</td>
<td>$6.15</td>
<td>$3.64</td>
<td>$53.61</td>
</tr>
</tbody>
</table>

---

Cost: $125.56
Step 7. Specify Retry and Email Notification Settings

At the **Retries and Notifications** step of the wizard, you can enable automatic retries and specify notification settings for the backup policy.

**Automatic Retry Settings**

To instruct Veeam Backup for GCP 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 60 seconds.

When retrying backup policies, Veeam Backup for GCP processes only those VMs 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.
Notification Settings

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

1. In the **Notifications** section of the step, set the **Enabled** toggle to **On**.
2. In the **Email** field, specify an email address of a recipient. Use a semicolon to separate multiple recipient addresses. Do not use spaces after semicolons between the specified email addresses.
3. Use the **Notify on** list to choose whether you want Veeam Backup for GCP 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 GCP 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 GCP will send each notification twice to this recipient.

Step 8. Finish Working with Wizard

At the **Summary** step of the wizard, review configuration information and click **Finish**.
Editing Backup Policy Settings

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

1. Navigate to Policies.
2. Select the backup policy and click Edit.
3. Complete the Edit Policy wizard:
   a. To provide a new name and description for the policy, follow the instructions provided in section Creating Backup Policies (step 2).
   b. To choose another project, to modify the list of regions where VM instances that you plan to back up reside, or to add VM instances to the backup scope, follow the instructions provided in section Creating Backup Policies (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 Permission check.

c. To assign labels to cloud-native snapshots, or to instruct Veeam Backup for GCP to create image-level backups, follow the instructions provided in section Creating Backup Policies (step 4a or step 4b).

d. To modify the schedule configured for the policy, follow the instructions provided in section Creating Backup Policies (step 5).

e. To configure automatic retry and notification settings, follow the instructions provided in section Creating Backup Policies (step 7).

f. At the Summary step of the wizard, review configuration information and click Finish.
Setting Backup Policy Priority

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

1. Navigate to Policies.
2. 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 a VM instance is included into multiple backup policies, it will be processed only by the backup policy that has the highest priority.
Exporting and Importing Backup Policies

Veeam Backup for GCP 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. Select the necessary backup policy and click Advanced > Export Policy.

Veeam Backup for GCP 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. On the Policies tab, 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 Apply.
Enabling and Disabling Backup Policies

By default, Veeam Backup for GCP runs all created backup policies according to the specified schedules. However, you can temporarily disable a backup policy so that Veeam Backup for GCP 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. Select the necessary backup policy, and 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 a VM 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. Select the necessary backup policy, and click Start or Stop.
Creating Snapshots Manually

Veeam Backup for GCP allows you to manually create snapshots of VM instances added to your backup policies. Each snapshot is saved to the same region where the protected VM instance resides.

**NOTE**

Veeam Backup for GCP 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 GCP environment unless you remove them manually, as described in section Removing Snapshots Created Manually.

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

1. Navigate to **Instances**.
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 be added to the backup policy as described in section Creating Backup Policies.
3. In the **Take Snapshot Now** wizard, 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, click **Add** and specify the labels explicitly. To do that, in the **Add Label** window, specify a key and a value for the new custom label, and then click **Apply**.

To save changes made to the snapshot settings, click **Finish** at the **Summary** step of the wizard.
Removing Backups and Snapshots

Veeam Backup for GCP applies the configured retention policy settings to automatically remove cloud-native snapshots and image-level backups created by backup policies. If necessary, you can also remove the backed-up data manually.

**IMPORTANT**

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

To remove backed-up data manually, do the following:

1. Navigate to Protected Data.
2. Select VM instances whose data you want to remove.
3. Click Remove and select either of the following options:
   - **Snapshots** — to remove all cloud-native snapshots created by backup policies.
   - **Snapshots > Manual** — to remove all cloud-native snapshots created manually.
   - **Snapshots > All** — to remove all cloud-native snapshots both by backup policies and manually.
   - **Backups** — to remove all image-level backups created for the selected VM instances.
   - **Snapshots and backups** — to remove both cloud-native snapshots and image-level backups created for the selected VM instances.
Removing Snapshots Created Manually

If you want to remove specific cloud-native snapshots created for a VM instance manually, do the following:

1. Navigate to Protected Data.
2. Select the necessary instance, and click the link in the Restore Points column.
3. In the Available Restore Points window, select a snapshot that you want to remove, and click Remove.
Performing Restore

Veeam Backup for GCP offers the following disaster recovery operations:

- **Instance Restore** — starts an entire VM instance from a restore point.
- **Disk Restore** — restores persistent disks attached to a VM instance.
- **File-Level Recovery** — recovers 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 GCP 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 GCP recovers data from all zonal and regional persistent disks (standard, balanced and SSD) attached to the instance. However, due to technical reasons, when it comes to local SSDs (SCSI and NVMe), Veeam Backup for GCP 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 GCP uses native GCP capabilities. To restore a VM instance from an image-level backup, Veeam Backup for GCP performs the following steps:

1. Launches a worker instance in the GCP region where 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 GCP 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 and removes it from the GCP environment.

How to Perform Instance Restore

To restore a protected VM instance, do the following:

1. Launch the Instance Restore wizard.
2. Select a restore point.
3. Select a project.
4. Choose a restore mode.
5. Select a region and 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 launched during the restore process. For information on how to configure network settings, see Adding Worker Configurations.
Step 1. Launch Instance Restore Wizard

To launch the Instance Restore wizard, do the following:

1. Navigate to Protected Data.
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 GCP 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 GCP 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.

<table>
<thead>
<tr>
<th>Creation Time</th>
<th>Size</th>
<th>Destination</th>
<th>Project</th>
<th>Region</th>
<th>Retention</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/29/2021 13:00:17 PM</td>
<td>6.11 GB</td>
<td>Snapshot</td>
<td>v3-backup</td>
<td>us-west-1</td>
<td>Daily</td>
</tr>
<tr>
<td>11/29/2021 13:00:14 PM</td>
<td>6.11 GB</td>
<td>Snapshot</td>
<td>v3-backup</td>
<td>us-west-1</td>
<td>Daily</td>
</tr>
<tr>
<td>11/27/2021 13:00:16 PM</td>
<td>6.11 GB</td>
<td>Snapshot</td>
<td>v3-backup</td>
<td>us-west-1</td>
<td>Daily</td>
</tr>
<tr>
<td>11/25/2021 13:00:15 PM</td>
<td>6.11 GB</td>
<td>Snapshot</td>
<td>v3-backup</td>
<td>us-west-1</td>
<td>Daily</td>
</tr>
</tbody>
</table>
Step 3. 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 GCP allows you to check whether the service account used to access the selected project has all the necessary permissions required to perform data protection tasks for the project. To do that, click **Check permissions**.

Veeam Backup for GCP 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 4. 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.

- **Restore to original location, with original settings**
  - Quickly restores the selected VM instance to its original location, with the same name and settings as the source instance.
- **Restore to new location, or with different settings**
  - Restores additional configuration steps to restore the selected VM instance to a new location or to use settings that differ from the source instance.

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 & Zone** 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 must 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 Google-managed encryption key** 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. Click Edit.
3. In the Configure settings window, specify a name and select a machine type for the restored VM instance. To learn how to choose a machine type when creating a VM instance in Google Cloud, see Google Cloud documentation.

To save changes made to the instance settings, click Apply.

![Instance Settings screen](image-url)
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 must 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 tags 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 GCP 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 instance 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 GCP 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) and SSD (pd-ssd). Restore of local SSDs (SCSI and NVMe) is not supported due to technical reasons.

How Volume-Level Restore Works

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

1. Launches a worker instance in the GCP region where 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 GCP environment.

NOTE
Veeam Backup for GCP 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. Select a project.
4. Choose a restore mode.
5. Select a region and 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 launched 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.
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 GCP 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 GCP 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.

   **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. Select Project

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

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

Veeam Backup for GCP 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 4. 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.
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 & Zone** step of the wizard, select a region to which the restored persistent disks will be placed, 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 the restored persistent disks must 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 Google-managed encryption key** 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** window, specify a name for the disk and click **Apply**.
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.

![Veeam Backup for Google Cloud Platform disk restore wizard](image)

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 GCP allows you to download the necessary files and folders to a local machine using the File Level Recovery for Veeam Backup 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 GCP performs the following steps:

1. Launches a worker instance in either of the following GCP regions:
   - To restore files and folders from a cloud-native snapshot, the worker instance is launched in the region where the source VM instance resides.
   - To restore files and folders from an image-level backup, the worker instance is launched in the region where the target storage bucket resides.

2. Attaches persistent disks of the VM instance to the worker instance.
   The disks are not physically extracted from the backup — Veeam Backup for GCP emulates their presence on the worker instance. The source backup itself remains in the read-only state.

3. Launches the File Level Recovery for Veeam Backup browser.
   The File Level Recovery for Veeam Backup 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. Detaches the persistent disks from the worker instance.

6. Removes the worker instance from the GCP 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 launched 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 Recovery for Veeam Backup 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.**
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 GCP 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 GCP 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.
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.

![File-Level Recovery wizard](image)

**TIP**

If you accidentally close the **File-Level Recovery Running Sessions** window, navigate to **Protected Data** and click the link in the **File-Level Recovery URL** column to open the window again.

Step 4. Start Recovery Session

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

As soon as you click **Start**, Veeam Backup for GCP 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 GCP will launch a worker instance and attach persistent disks of the processed VM instance to it.

**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.

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 GCP will display a link to the File Level Recovery for Veeam Backup browser. You can use the link in either of the following ways:

- Click the link to open the File Level Recovery for Veeam Backup 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 Recovery for Veeam Backup browser on another machine.
**IMPORTANT**

When you click **Copy FLR URL**, Veeam Backup for GCP copies the following information to the clipboard:

- A link to the File Level Recovery for Veeam Backup browser the 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 installed on the worker instance hosting the File Level Recovery for Veeam Backup 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 Recovery for Veeam Backup browser matches the provided certificate thumbprint.

<table>
<thead>
<tr>
<th>FLR Running Sessions - kk-test-backup3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Restore Point</strong></td>
<td><strong>URL</strong></td>
</tr>
</tbody>
</table>
Step 5. Choose Items to Recover

In the File Level Recovery for Veeam Backup browser, you can find and recover items (files and folders) of the selected VM instance. All recovered items are saved as a single .ZIP archive to the default download directory on a machine from which you access the browser.

To recover files from a specific folder, do the following:

1. In the File Level Recovery for Veeam Backup browser, navigate to the folder that contains the necessary files.
2. In the working area, select check boxes next to the files and click **Download**.

To recover files from multiple folders all at once, do the following:

1. In the File Level Recovery for Veeam Backup 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 Recovery List**.
3. Repeat steps 1-2 for all other folders whose files you want to recover.
4. Click **Pending Recovery**.
5. In the **Recovery List** window, review the list of items to recover and click **Download**.
Step 6. Stop Recovery Session

After you finish working with the File Level Recovery for Veeam Backup browser, it is recommended that you stop the running recovery session so that Veeam Backup for GCP can detach persistent disks of the processed VM instance from the launched worker instance and remove the worker instance from the GCP 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 Recovery for Veeam Backup browser for 30 minutes, Veeam Backup for GCP 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.
Enabling Data Encryption

For enhanced data security, Veeam Backup for GCP allows you to encrypt backed-up VM instance data stored in GCP storage buckets using Veeam encryption mechanisms. Additionally, Veeam Backup for GCP supports native GCP 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 GCP 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 GCP 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 section Creating Backup Policies, Veeam Backup for GCP performs the following steps:

1. Generates an encryption key to protect VM instance data 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 GCP allows you to back up and restore data of 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

Depending on the operation performed for a VM instance that has encrypted persistent disks, the IAM role that Veeam Backup for GCP 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 GCP infrastructure, you specify a service account that will be used to access the project. Veeam Backup for GCP automatically grants this service account all the necessary IAM role permissions required to perform data protection and disaster recovery operations with GCP 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 a VM instance with encrypted persistent disks does not differ from the same process for 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 GCP encrypts these snapshots with the same CMEKs with which persistent disks of the source VM instance are encrypted.

Creating Image-Level Backups

The process of creating image-level backups of a VM instance with encrypted persistent disks does not depend on the location where the worker instance processing the VM instance data is launched. Regardless of whether the worker instance is launched in the same GCP project where the source VM instance belongs, Veeam Backup for GCP performs the following steps:

1. Takes a cloud-native snapshot of the VM instance.
2. Creates persistent disks from the snapshot.  
   To encrypt the created disks, Veeam Backup for GCP requires permissions of an IAM role that can access the CMEK with which you want to encrypt these disks.
3. 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.
4. Removes the worker instance from the GCP environment.
NOTE
Every time before creating persistent disks from a cloud-native snapshot, Veeam Backup for GCP checks whether the total size of pd-standard disks breaches the zone quota for the project where the worker instance is launched. If the difference between the quota and the total disk size exceeds 4000 GB, Veeam Backup for GCP temporarily attaches an additional empty disk to the worker instance — but only for the duration of the backup process. This allows Veeam Backup for GCP to speed up the data transfer to reduce your backup costs.

Restoring from Cloud-Native Snapshots

The process of restoring a VM instance from an encrypted cloud-native snapshot does not differ depending on the location where the restored VM instance will reside. Regardless of whether the VM instance will be restored to the same GCP project where the cloud-native snapshot resides, Veeam Backup for GCP performs the following steps:

1. Creates persistent disks from the image-level backup.
   To encrypt the created disks, Veeam Backup for GCP requires permissions of an IAM role that can access the CMEK with which you want to encrypt these disks.
2. Creates a VM instance in the target location.
3. Attaches the created persistent disks with the restored data to the VM instance.

Restoring from Image-Level Backups

The process of restoring 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 VM instance data is launched. Regardless of whether the worker instance is launched in the same GCP project where the restored VM instance will reside, Veeam Backup for GCP performs the following steps:

1. Creates persistent disks from the snapshot, 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 GCP requires permissions of an IAM role that can access the CMEK with which you want to encrypt these disks.
2. Takes cloud-native snapshots of the persistent disks with the restored data.
3. Creates a VM instance in the target location.
4. Creates persistent disks from the snapshots, and attaches the disks to the VM instance.
   To encrypt the created disks, Veeam Backup for GCP requires permissions of an IAM role that can access the CMEK with which you want to encrypt these disks.
5. Removes the worker instance from the GCP environment.

NOTE
Every time before creating persistent disks from a cloud-native snapshot, Veeam Backup for GCP checks whether the total size of pd-standard disks breaches the zone quota for the project where the worker instance is launched. If the difference between the quota and the total disk size exceeds 1500 GB, Veeam Backup for GCP temporarily attaches an additional empty disk to the worker instance — but only for the duration of the restore process. This allows Veeam Backup for GCP to speed up the data transfer to reduce your restore costs.
Viewing Session Statistics

For each performed data protection or disaster recovery operation, Veeam Backup for GCP 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 VM instances 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 GCP must 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 GCP as a single .CSV or .XML file. To do that, navigate to the necessary tab and click Export. Veeam Backup for GCP 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 GCP will still export all properties of all objects present on the currently opened tab.
Updating Veeam Backup for Google Cloud Platform

Veeam Backup for GCP 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 performance 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 GCP 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. Navigate to Support.
2. On the Updates tab, click Check and View Updates.

If new updates are available, Veeam Backup for GCP will display them on the Updates tab of the Veeam Backup for GCP 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

Before you install a product update, make sure all backup policies are disabled 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 Backup for GCP Updater page:
   a. Navigate to Support.
   b. On the Updates tab, click Check and View Updates.

2. On the Veeam Backup for GCP 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 GCP 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 GCP 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 GCP restarts all services running on the backup appliance, including the Web UI service. That is why Veeam Backup for GCP will log you out when the update process completes.

Scheduling Update Installation

You can instruct Veeam Backup for GCP to automatically download and install available product versions and package updates on a specific date at a specific time:

1. On the **Veeam Backup for GCP 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.
   b. Select the **Reboot automatically after install if required** check box to allow Veeam Backup for GCP to reboot the backup appliance if needed.
   c. Click **Schedule Updates**.

Veeam Backup for GCP 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 GCP to send an update notification later.

To do that, on the **Veeam Backup for GCP 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 GCP 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. Navigate to Support.
2. On the Updates tab, click Check and View Updates.
3. On the Veeam Backup for GCP Updater page, switch to the History tab.

For each date when an update was installed, the Veeam Backup for GCP 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 GCP 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 GCP, 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.

The About section of the Updates tab displays the following information:

- **Product version** — the currently installed version of Veeam Backup for GCP.
- **Instance ID** — the unique identification number of the VM instance running Veeam Backup for GCP.
- **Support ID** — the unique identification number of the Veeam support contract.

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 must 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 log.zip archive.