Backing up on-premises ONTAP data to Google Cloud Storage

Cloud Manager

Tom Onacki
September 09, 2021

Table of Contents

Backing up on-premises ONTAP data to Google Cloud Storage

Complete a few steps to get started backing up data from your on-premises ONTAP systems to Google Cloud Storage.

TIP

In most cases you'll use Cloud Manager for all backup and restore operations. However, starting with ONTAP 9.9.1 you can initiate volume backup operations of your on-premises ONTAP clusters using ONTAP System Manager. See how to use System Manager to back up your volumes to the cloud using Cloud Backup.

A Beta feature released in January 2021 allows you to run compliance scans on the backed up volumes from your on-premises systems. Typically, compliance scans are free up to 1 TB of data, and then a cost for the service is applied for data over 1 TB. When combining Backup and Data Sense for your on-premises volumes, the cost for scans on those on-prem volumes is free. Learn more about how Cloud Data Sense can get your business applications and cloud environments privacy ready.

Quick start

Get started quickly by following these steps, or scroll down to the remaining sections for full details.

Verify support for your configuration

- You have discovered the on-premises cluster and added it to a working environment in Cloud Manager. See Discovering ONTAP clusters for details.
  - The cluster is running ONTAP 9.7P5 or later.
  - The cluster has a SnapMirror license — it is included as part of the Premium Bundle or Data Protection Bundle.
  - The cluster must have the required network connections to Google storage and to the Connector.
- The Connector must have the required network connections to Google storage and to the cluster.
- You have a valid Google subscription for the object storage space where your backups will be located.
- You have a Google account with an access key and secret key so the ONTAP cluster can back up and restore data.

Enable Cloud Backup on the system

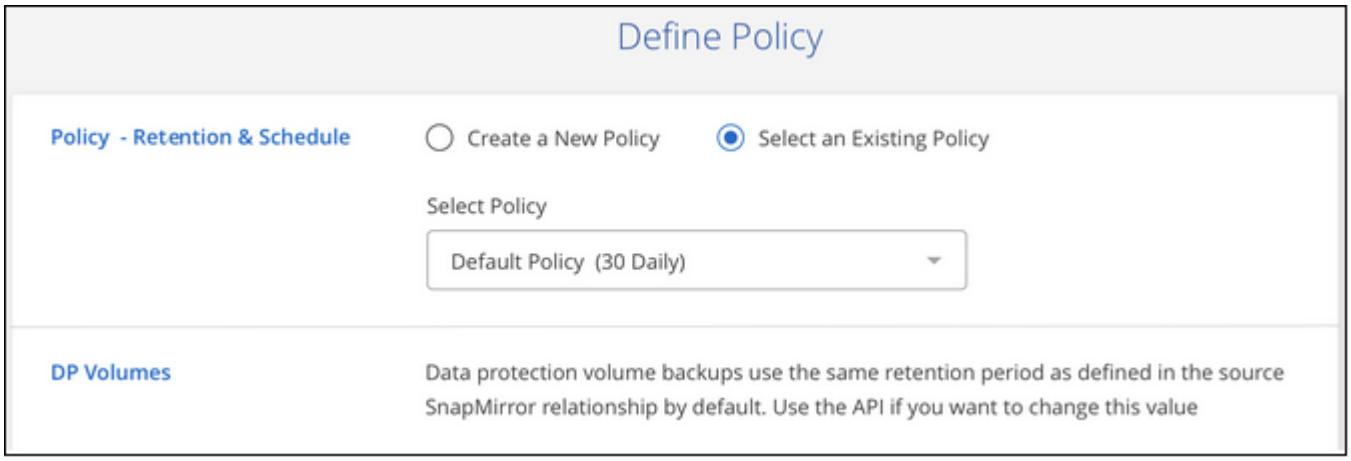
Select the working environment and click **Enable** next to the Backup & Compliance service in the right-panel, and then follow the setup wizard.

Select the cloud provider and enter the provider details

Select Google Cloud as your provider and then enter the provider details. You also need to specify the IPspace in the ONTAP cluster where the volumes reside.

Define the backup policy

The default policy backs up volumes every day and retains the most recent 30 backup copies of each volume. Change to hourly, daily, weekly, or monthly backups, or select one of the system-defined policies that provide more options. You can also change the number of backup copies to retain.



Select the volumes that you want to back up

Identify which volumes you want to back up from the cluster.

Activate Compliance scans on the backed up volumes (optional)

Choose whether you want to have Cloud Data Sense scan the volumes that are backed up in the cloud.

Restore your data, as needed

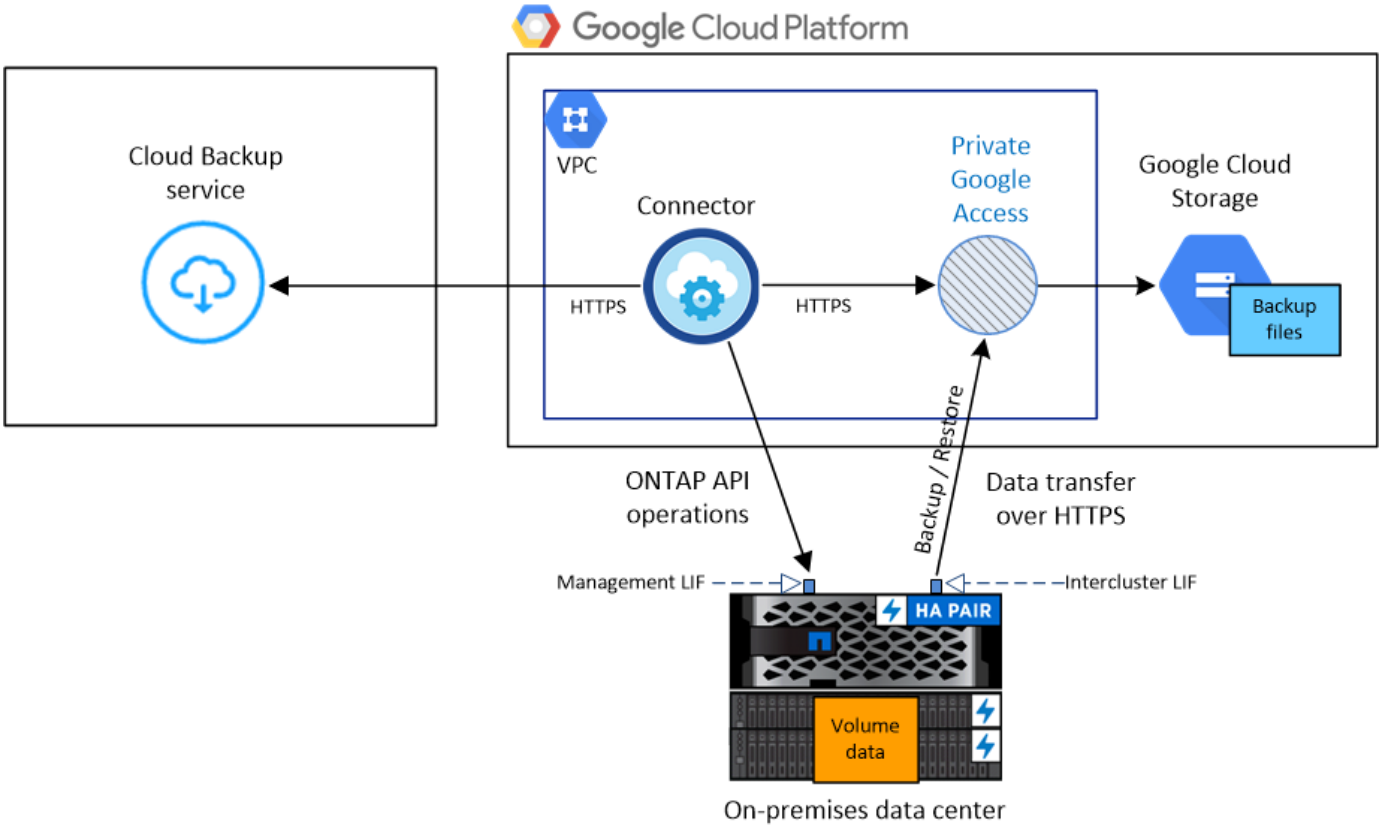
Restore a backup to a new volume. You can restore data to a Cloud Volumes ONTAP system in Google, or to an on-premises ONTAP system.

See Restoring volume data from backup files for details.

Requirements

Read the following requirements to make sure you have a supported configuration before you start backing up on-premises volumes to Google Cloud storage.

The following image shows each component and the connections that you need to prepare between them:



Note that the Cloud Restore instance is not shown in this diagram because single-file restore is not currently supported in GCP.

Preparing your ONTAP clusters

You need to discover your on-premises ONTAP clusters in Cloud Manager before you can start backing up volume data.

Learn how to discover a cluster.

ONTAP requirements

- ONTAP 9.7P5 and later.
- A SnapMirror license (included as part of the Premium Bundle or Data Protection Bundle).

  Note: The "Hybrid Cloud Bundle" is not required when using the Cloud Backup service.

  See how to manage your cluster licenses.

- Time and time zone are set correctly.

  See how to configure your cluster time.

Cluster networking requirements

- The ONTAP cluster initiates an HTTPS connection over port 443 from the intercluster LIF to Google Cloud storage for backup and restore operations.

ONTAP reads and writes data to and from object storage. The object storage never initiates, it just responds.

- ONTAP requires an inbound connection from the Connector to the cluster management LIF. The Connector can reside in a Google Cloud Platform VPC.
- An intercluster LIF is required on each ONTAP node that hosts the volumes you want to back up. The LIF must be associated with the *IPspace* that ONTAP should use to connect to object storage. Learn more about IPspaces.

  When you set up Cloud Backup, you are prompted for the IPspace to use. You should choose the IPspace that each LIF is associated with. That might be the "Default" IPspace or a custom IPspace that you created.

- The nodes' intercluster LIFs are able to access the internet.
- DNS servers have been configured for the storage VM where the volumes are located. See how to configure DNS services for the SVM.
- Note that if you use are using a different IPspace than the Default, then you might need to create a static route to get access to the object storage.
- Update firewall rules, if necessary, to allow Cloud Backup service connections from ONTAP to object storage through port 443 and name resolution traffic from the storage VM to the DNS server over port 53 (TCP/UDP).

Creating or switching Connectors

A Connector is required to back up data to the cloud, and the Connector must be in a Google Cloud Platform VPC when backing up data to Google Cloud storage. You can't use a Connector that's deployed on-premises. You'll either need to create a new Connector or make sure that the currently selected Connector resides in the correct provider.

- Learn about Connectors
- Creating a Connector in GCP
- Switching between Connectors

Preparing networking for the Connector

Ensure that the Connector has the required networking connections.

Steps

1. Ensure that the network where the Connector is installed enables the following connections:
   - An outbound internet connection to the Cloud Backup service over port 443 (HTTPS)
   - An HTTPS connection over port 443 to your Google Cloud storage
   - An HTTPS connection over port 443 to your ONTAP clusters
2. Enable Private Google Access on the subnet where you plan to deploy the Connector. Private Google Access is needed if you have a direct connection from your ONTAP cluster to the VPC and you want communication between the Connector and Google Cloud Storage to stay in your virtual private network.

   Note that Private Google Access works with VM instances that have only internal (private) IP addresses (no external IP addresses).

Supported regions

You can create backups from on-premises systems to Google Cloud storage in all regions where Cloud Volumes ONTAP is supported. You specify the region where the backups will be stored when you set up the service.

License requirements

Before your 30-day free trial of the Cloud Backup service expires, you need to subscribe to a pay-as-you-go (PAYGO) Cloud Manager Marketplace offering from Google, or purchase and activate a Cloud Backup BYOL license from NetApp. These licenses are for the account and can be used across multiple systems.

- For Cloud Backup PAYGO licensing, you'll need a subscription to the Google Cloud Manager Marketplace offering to continue using Cloud Backup. Billing for Cloud Backup is done through this subscription.
- For Cloud Backup BYOL licensing, you don't need a subscription. You need the serial number from NetApp that enables you to use the service for the duration and capacity of the license. Learn how to manage your BYOL licenses.

You need to have a Google subscription for the object storage space where your backups will be located.

A SnapMirror license is required on the cluster. Note that the "Hybrid Cloud Bundle" is not required when using Cloud Backup.

Preparing Google Cloud Storage for backups

When you set up backup, you need to provide storage access keys for a service account that has Storage Admin permissions. A service account enables Cloud Backup to authenticate and access Cloud Storage buckets used to store backups. The keys are required so that Google Cloud Storage knows who is making the request.

Steps

1. Create a service account that has the predefined Storage Admin role.
2. Go to GCP Storage Settings and create access keys for the service account:
   a. Select a project, and click **Interoperability**. If you haven't already done so, click **Enable interoperability access**.
   b. Under **Access keys for service accounts**, click **Create a key for a service account**, select the service account that you just created, and click **Create Key**.

      You'll need to enter the keys in Cloud Backup later when you configure the backup service.

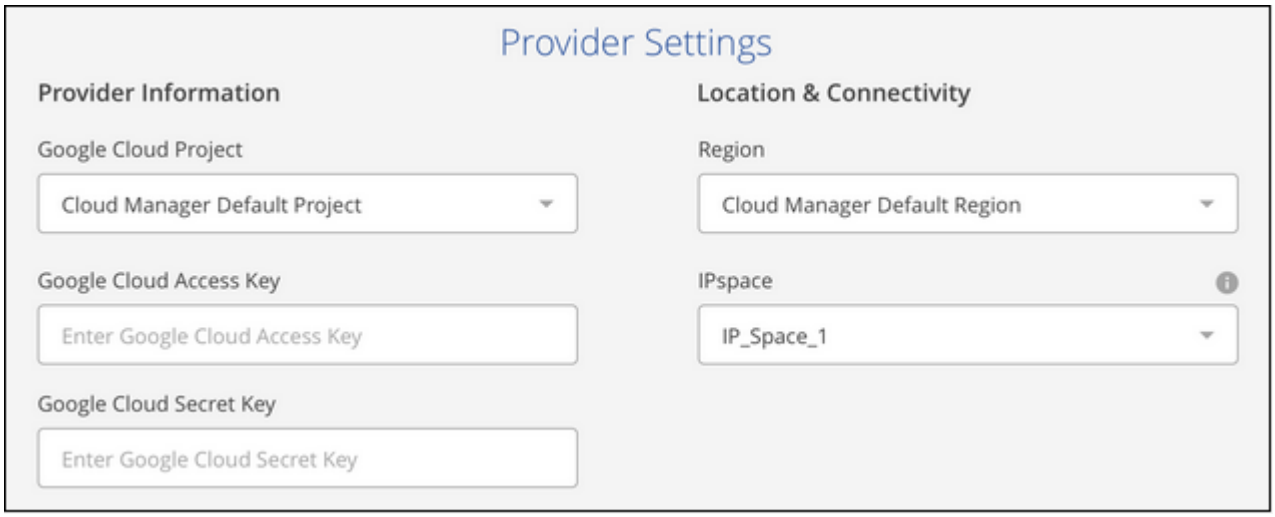
Enabling Cloud Backup

Enable Cloud Backup at any time directly from the on-premises working environment.

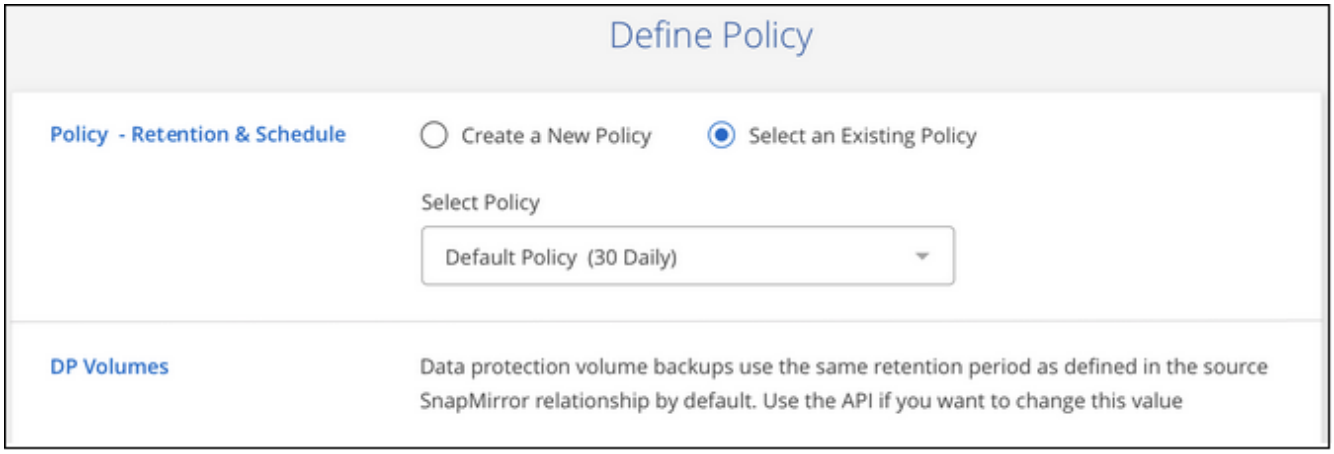
Steps

1. From the Canvas, select the working environment and click **Enable** next to the Backup & Compliance service in the right-panel.

2. Select Google Cloud as your provider and click **Next**.
3. Enter the provider details. Note that you can't change this information after the service has started.
   a. The Google Cloud Project where you want the Google Cloud Storage bucket to be created for backups. (The Project must have a Service Account that has the predefined Storage Admin role.)
   b. The Google Access Key and Secret Key used to store the backups.
   c. The Google region where the backups will be stored.
   d. The IPspace in the ONTAP cluster where the volumes you want to back up reside. The intercluster LIFs for this IPspace must have outbound internet access.



4. Click **Next** after you've entered the provider details.
5. In the *Define Policy* page, select an existing backup schedule and retention value, or define a new backup policy, and click **Next**.



See the list of existing policies.

6. Select the volumes that you want to back up.
   - To back up all volumes, check the box in the title row (Volume Name).
   - To back up individual volumes, check the box for each volume (Volume_1).

7. Click **Activate Backup** and Cloud Backup starts taking the initial backups of your volumes.

Result

Cloud Backup starts taking the initial backups of each selected volume and the Backup Dashboard is displayed so you can monitor the state of the backups.

What's next?

You can start and stop backups for volumes or change the backup schedule and you can restore entire volumes from a backup file.