Back up Cloud Volumes ONTAP data

Cloud Manager

NetApp
March 22, 2022

Table of Contents

Back up Cloud Volumes ONTAP data

Backing up Cloud Volumes ONTAP data to Amazon S3

Complete a few steps to get started backing up data from Cloud Volumes ONTAP to Amazon S3.

Quick start

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

1 **Verify support for your configuration**

- You're running Cloud Volumes ONTAP 9.6 or later in AWS.
- You have a valid cloud provider subscription for the storage space where your backups will be located.
- You have subscribed to the Cloud Manager Marketplace Backup offering, an AWS annual contract, or you have purchased and activated a Cloud Backup BYOL license from NetApp.
- The IAM role that provides the Cloud Manager Connector with permissions includes S3 permissions from the latest Cloud Manager policy.

2 **Enable Cloud Backup on your new or existing system**

- New systems: Cloud Backup is enabled by default in the working environment wizard. Be sure to keep the option enabled.
- Existing systems: Select the working environment and click **Enable** next to the Backup & Restore service in the right-panel, and then follow the setup wizard.

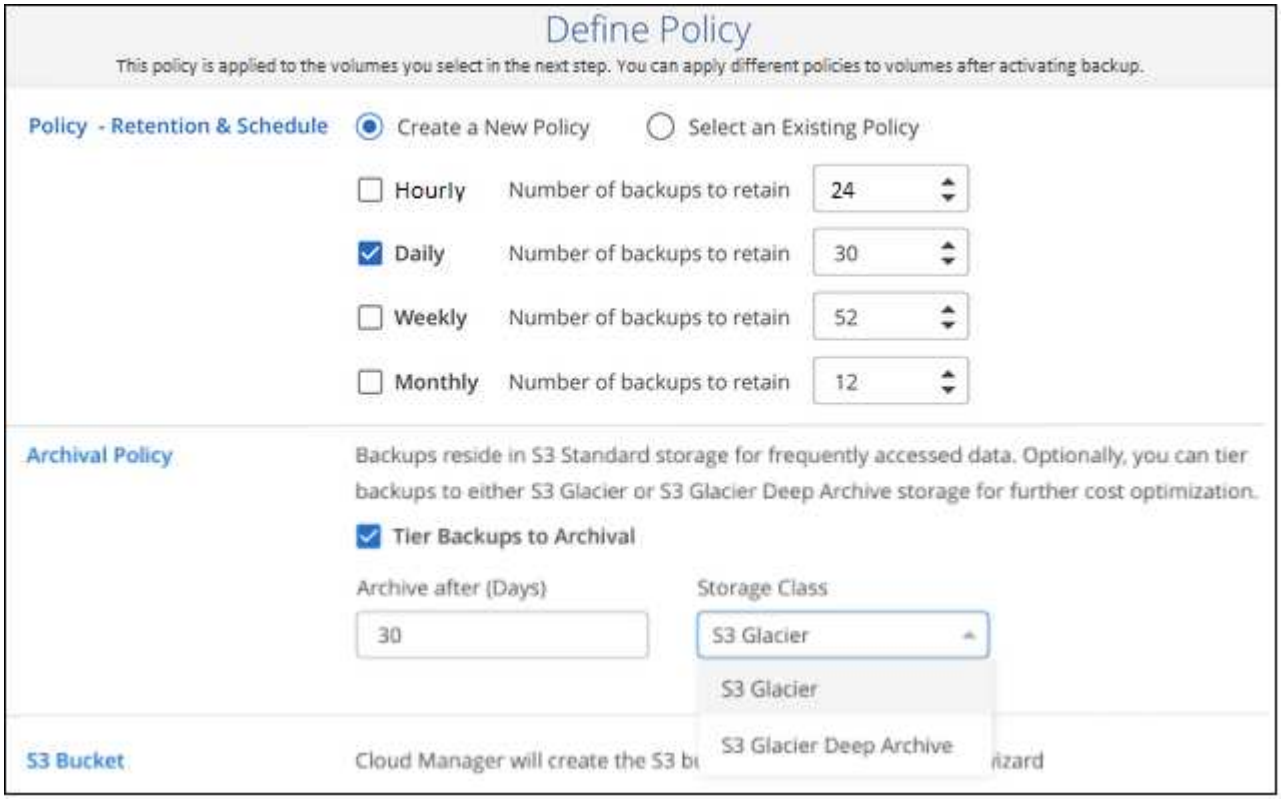
3 **Enter the provider details**

Select the AWS Account and the region where you want to create the backups. You can also choose your own customer-managed key for data encryption instead of using the default Amazon S3 encryption key.

4 Define the default 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 you want to retain.

Backups are stored in S3 Standard storage by default. If your cluster is using ONTAP 9.10.1 or greater, you can choose to tier backups to either S3 Glacier or S3 Glacier Deep Archive storage after a certain number of days for further cost optimization.



5 Select the volumes that you want to back up

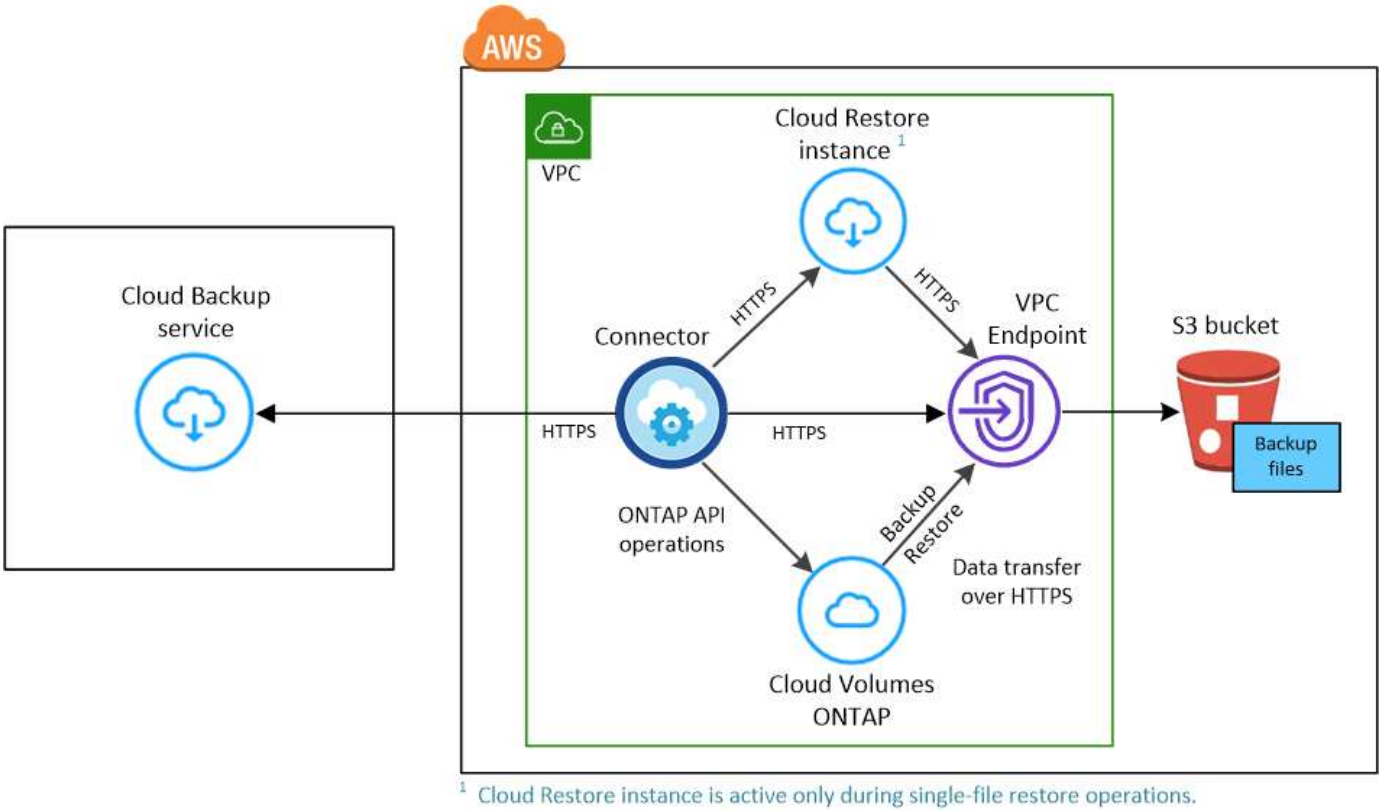
Identify which volumes you want to back up using the default backup policy in the Select Volumes page. If you want to assign different backup policies to certain volumes, you can create additional policies and apply them

to volumes later.

Requirements

Read the following requirements to make sure that you have a supported configuration before you start backing up volumes to S3.

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



When the Cloud Restore instance is deployed in the cloud, it is located in the same subnet as the Connector.

Supported ONTAP versions

Cloud Volumes ONTAP 9.6 and later.

License requirements

For Cloud Backup PAYGO licensing, a Cloud Manager subscription is available in the AWS Marketplace that enables deployments of Cloud Volumes ONTAP and Cloud Backup. You need to subscribe to this Cloud Manager subscription before you enable Cloud Backup. Billing for Cloud Backup is done through this subscription.

For an annual contract that enables you to back up both Cloud Volumes ONTAP data and on-premises ONTAP data, you need to subscribe from the AWS Marketplace page and then associate the subscription with your AWS credentials.

For an annual contract that enables you to bundle Cloud Volumes ONTAP and Cloud Backup, you must set up the annual contract when you create a Cloud Volumes ONTAP working environment. This option doesn't enable you to back up on-prem data.

For Cloud Backup BYOL licensing, 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.

And you need to have an AWS account for the storage space where your backups will be located.

Supported AWS regions

Cloud Backup is supported in all AWS regions where Cloud Volumes ONTAP is supported; including AWS GovCloud regions.

Required setup for creating backups in a different AWS account

By default, backups are created using the same account as the one used for your Cloud Volumes ONTAP system. If you want to use a different AWS account for your backups, you must log in to the AWS portal and link the two accounts.

Required information for using customer-managed keys for data encryption

You can choose your own customer-managed keys for data encryption in the activation wizard instead of using the default Amazon S3 encryption keys. In this case you'll need to have the encryption managed keys already set up. See how to use your own keys.

AWS Backup permissions required

The IAM role that provides Cloud Manager with permissions must include S3 permissions from the latest Cloud Manager policy.

Here are the specific permissions from the policy:

```
{
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
            ]
        },
```

AWS Restore permissions required

The following EC2 permissions are needed for the IAM role that provides Cloud Manager with permissions so that it can start, stop, and terminate the Cloud Restore instance:

```
            "Action": [
                "ec2:DescribeInstanceTypeOfferings",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
```

Required outbound internet access for AWS deployments

The Cloud Restore instance requires outbound internet access. If your virtual or physical network uses a proxy server for internet access, ensure that the instance has outbound internet access to contact the following endpoints.

Endpoints	Purpose
http://amazonlinux.us-east-1.amazonaws.com/2/extras/docker/stable/x86_64/4bf88ee77c395ffe1e0c3ca68530dfb3a683ec65a4a1ce9c0ff394be50e922b2/	CentOS package for the Cloud Restore Instance AMI.
http://cloudmanagerinfraprod.azurecr.io https://cloudmanagerinfraprod.azurecr.io	Cloud Restore Instance image repository.

Enabling Cloud Backup on a new system

Cloud Backup is enabled by default in the working environment wizard. Be sure to keep the option enabled.

See Launching Cloud Volumes ONTAP in AWS for requirements and details for creating your Cloud Volumes ONTAP system.

Steps

1. Click **Create Cloud Volumes ONTAP**.
2. Select Amazon Web Services as the cloud provider and then choose a single node or HA system.
3. Fill out the Details & Credentials page.
4. On the Services page, leave the service enabled and click **Continue**.

5. Complete the pages in the wizard to deploy the system.

Result

Cloud Backup is enabled on the system and backs up volumes every day and retains the most recent 30 backup copies.

What's next?

You can start and stop backups for volumes or change the backup schedule.
You can also restore entire volumes or individual files from a backup file to a Cloud Volumes ONTAP system in AWS, or to an on-premises ONTAP system.

Enabling Cloud Backup on an existing system

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

Steps

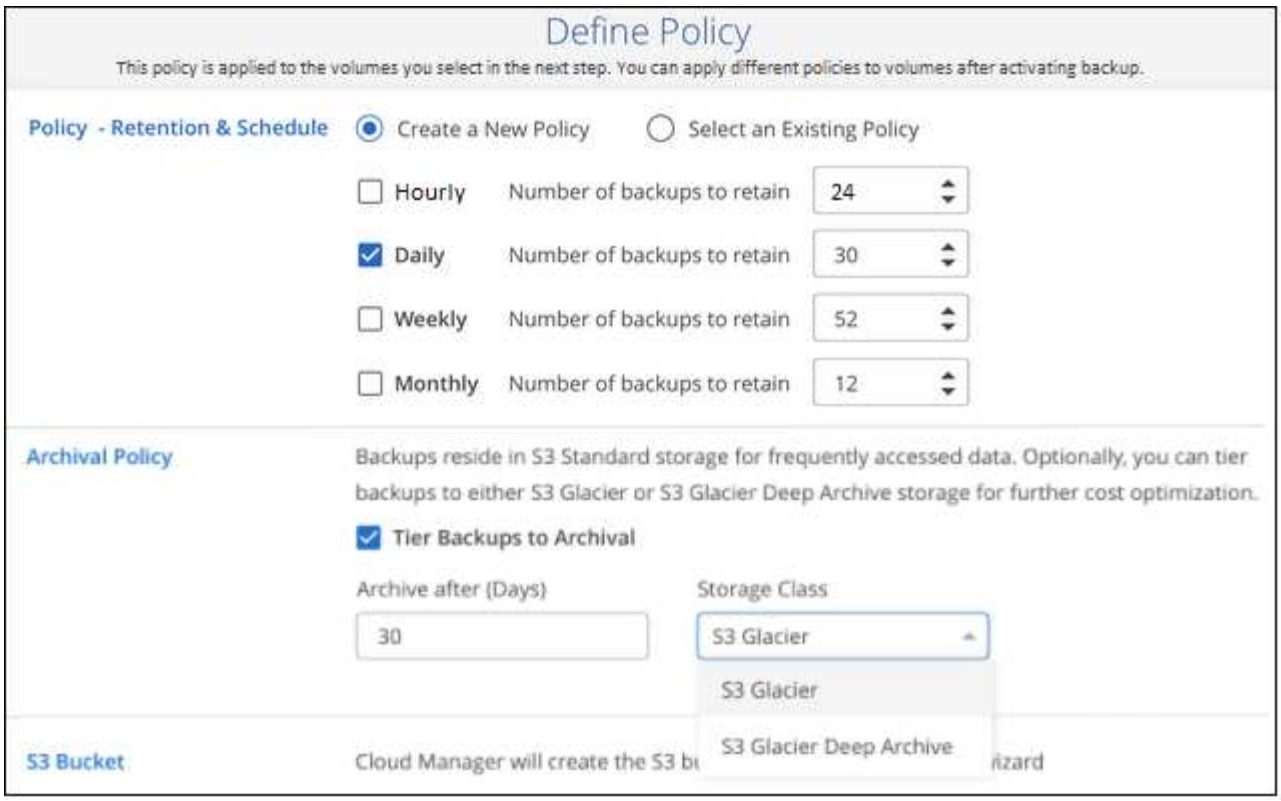
1. Select the working environment and click **Enable** next to the Backup & Restore service in the right-panel.

2. Select the provider details and click **Next**.
   a. The AWS Account used to store the backups. This can be a different account than where the Cloud Volumes ONTAP system resides.

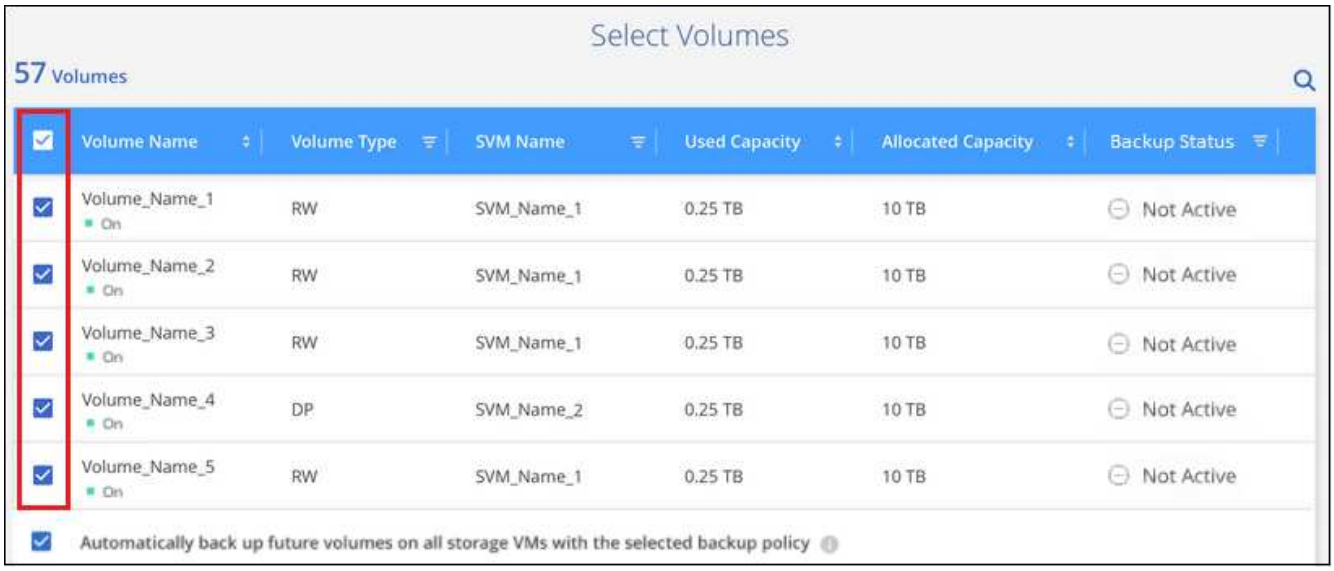
      If you want to use a different AWS account for your backups, you must log in to the AWS portal and link the two accounts.

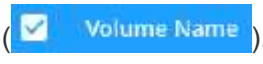
   b. The region where the backups will be stored. This can be a different region than where the Cloud Volumes ONTAP system resides.
   c. Whether you'll use the default Amazon S3 encryption keys or choose your own customer-managed keys from your AWS account to manage encryption of your data. (See how to use your own encryption keys).

3. Enter the default backup policy details and click **Next**.
   a. Define the backup schedule and choose the number of backups to retain. See the list of existing policies you can choose.
   b. When using ONTAP 9.10.1 and greater, you can choose to tier backups to either S3 Glacier or S3 Glacier Deep Archive storage after a certain number of days for further cost optimization. Learn more about using archival tiers.



4. Select the volumes that you want to back up using the default backup policy in the Select Volumes page. If you want to assign different backup policies to certain volumes, you can create additional policies and apply them to those volumes later.



   - To back up all volumes, check the box in the title row (

).
   - To back up individual volumes, check the box for each volume (

).

5. If you want all volumes added in the future to have backup enabled, just leave the checkbox for "Automatically back up future volumes…" checked. If you disable this setting, you'll need to manually enable backups for future volumes.
6. Click **Activate Backup** and Cloud Backup starts taking the initial backups of each selected volume.

Result

Cloud Backup starts taking the initial backups of each selected volume and the Volume 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.
You can also restore entire volumes or individual files from a backup file to a Cloud Volumes ONTAP system in AWS, or to an on-premises ONTAP system.

Backing up Cloud Volumes ONTAP data to Azure Blob storage

Complete a few steps to get started backing up data from Cloud Volumes ONTAP to Azure Blob storage.

Quick start

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

1 Verify support for your configuration

- You're running Cloud Volumes ONTAP 9.7P5 or later in Azure.
- You have a valid cloud provider subscription for the storage space where your backups will be located.
- You have subscribed to the Cloud Manager Marketplace Backup offering, or you have purchased and activated a Cloud Backup BYOL license from NetApp.

2 Enable Cloud Backup on your new or existing system

- New systems: Cloud Backup is enabled by default in the working environment wizard. Be sure to keep the option enabled.
- Existing systems: Select the working environment and click **Enable** next to the Backup & Restore service in the right-panel, and then follow the setup wizard.

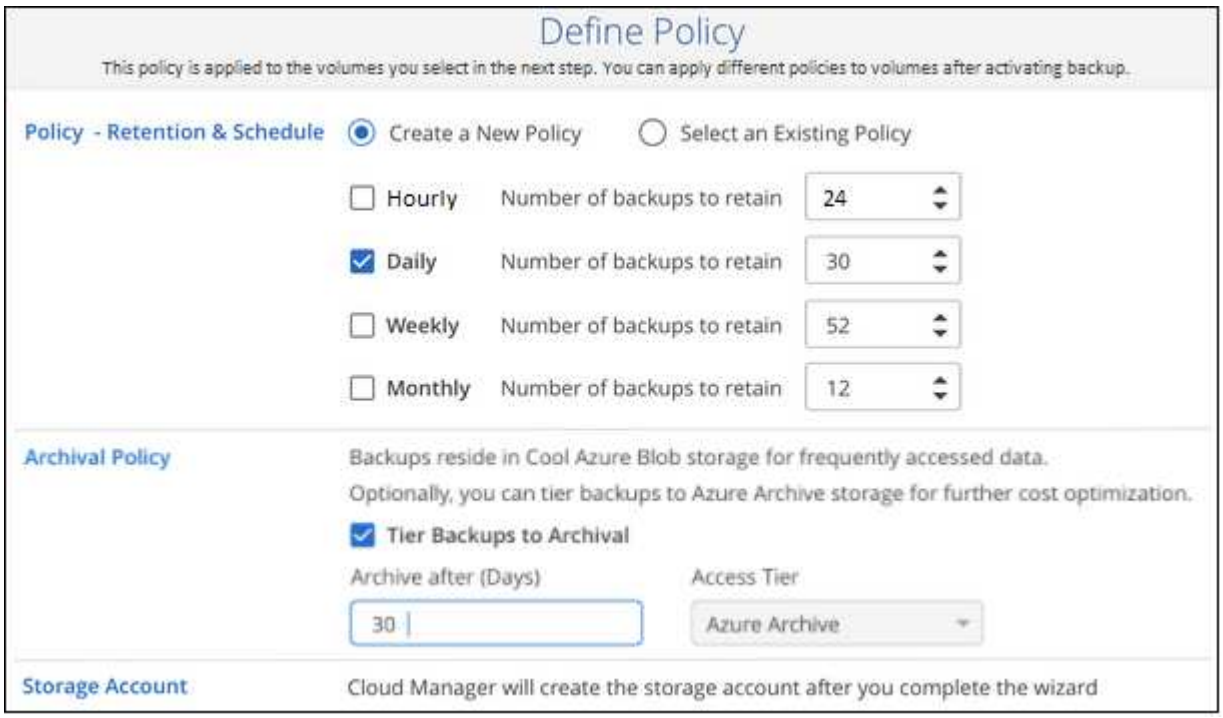
3 Enter the provider details

Select the provider subscription and region, and choose whether you want to create a new resource group or use an already existing resource group. You can also choose your own customer-managed keys for data encryption instead of using the default Microsoft-managed encryption key.

4 Define the default 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 you want to retain.

By default, backups are stored in the Cool access tier. If your cluster is using ONTAP 9.10.1 or greater, you can choose to tier backups to Azure Archive storage after a certain number of days for further cost optimization.



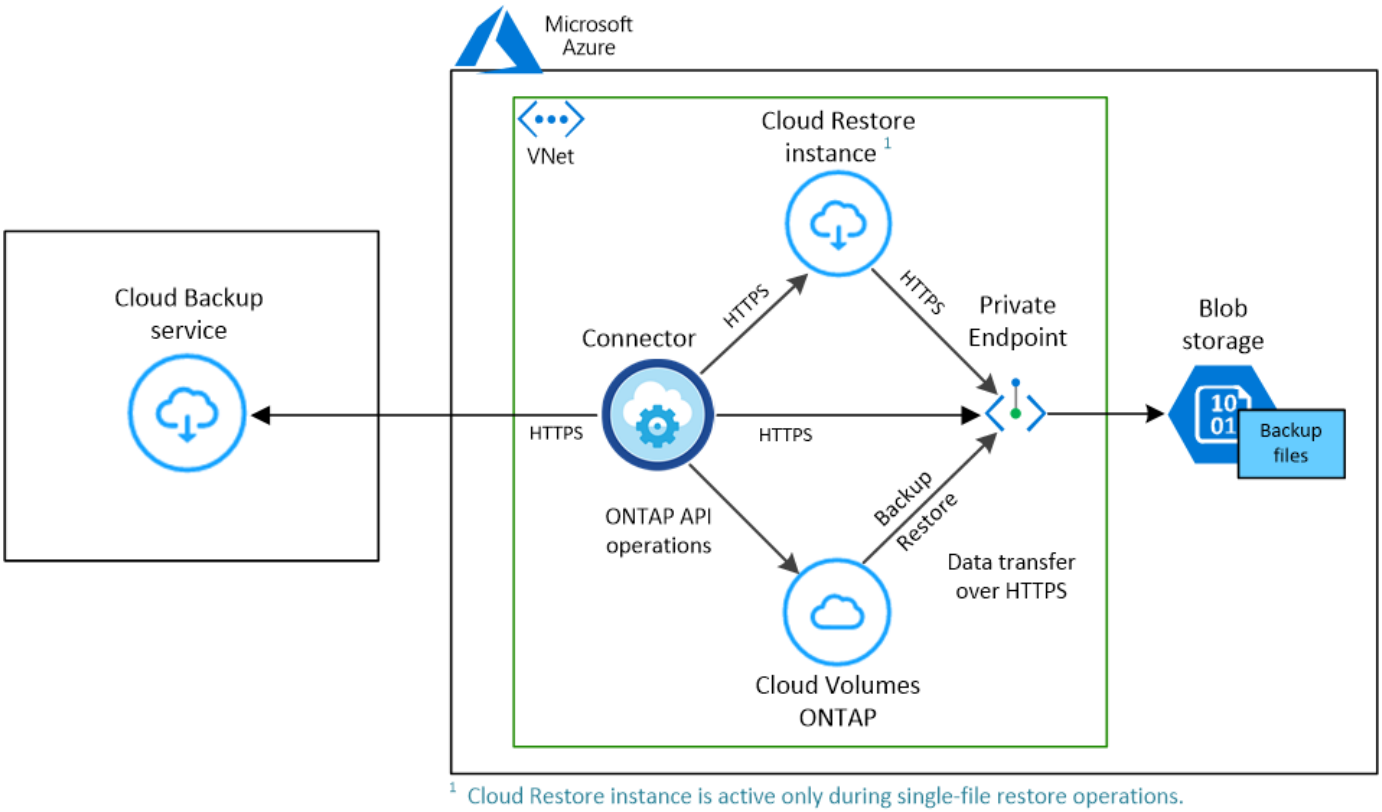
5 Select the volumes that you want to back up

Identify which volumes you want to back up using the default backup policy in the Select Volumes page. If you want to assign different backup policies to certain volumes, you can create additional policies and apply them to volumes later.

Requirements

Read the following requirements to make sure that you have a supported configuration before you start backing up volumes to Azure Blob storage.

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



[1] Cloud Restore instance is active only during single-file restore operations.

When the Cloud Restore virtual machine is deployed in the cloud, it is located in the same subnet as the Connector.

Supported ONTAP versions

Cloud Volumes ONTAP 9.7P5 and later.

License requirements

For Cloud Backup PAYGO licensing, a subscription through the Azure Marketplace is required before you enable Cloud Backup. Billing for Cloud Backup is done through this subscription. You can subscribe from the Details & Credentials page of the working environment wizard.

For Cloud Backup BYOL licensing, 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.

And you need to have a Microsoft Azure subscription for the storage space where your backups will be located.

Supported Azure regions

Cloud Backup is supported in all Azure regions where Cloud Volumes ONTAP is supported; including Azure Government regions.

Required setup for creating backups in a different Azure subscription

By default, backups are created using the same subscription as the one used for your Cloud Volumes ONTAP system. If you want to use a different Azure subscription for your backups, you must log in to the Azure portal and link the two subscriptions.

Required information for using customer-managed keys for data encryption

You can use your own customer-managed keys for data encryption in the activation wizard instead of using the default Microsoft-managed encryption keys. In this case you will need to have the Azure Subscription, Key Vault name, and the Key. See how to use your own keys.

Required outbound internet access for Azure deployments

The Cloud Restore virtual machine requires outbound internet access. If your virtual or physical network uses a proxy server for internet access, ensure that the instance has outbound internet access to contact the following endpoints.

Endpoints	Purpose
http://olcentgbl.trafficmanager.net https://olcentgbl.trafficmanager.net	Provides CentOS packages for the Cloud Restore virtual machine.
http://cloudmanagerinfraprod.azurecr.io https://cloudmanagerinfraprod.azurecr.io	Cloud Restore virtual machine image repository.

Enabling Cloud Backup on a new system

Cloud Backup is enabled by default in the working environment wizard. Be sure to keep the option enabled.

See Launching Cloud Volumes ONTAP in Azure for requirements and details for creating your Cloud Volumes ONTAP system.

If you want to pick the name of the resource group, **disable** Cloud Backup when deploying Cloud Volumes ONTAP. Follow the steps for enabling Cloud Backup on an existing system to enable Cloud Backup and choose the resource group.

Steps

1. Click **Create Cloud Volumes ONTAP**.
2. Select Microsoft Azure as the cloud provider and then choose a single node or HA system.
3. In the Define Azure Credentials page, enter the credentials name, client ID, client secret, and directory ID, and click **Continue**.
4. Fill out the Details & Credentials page and be sure that an Azure Marketplace subscription is in place, and click **Continue**.
5. On the Services page, leave the service enabled and click **Continue**.

6. Complete the pages in the wizard to deploy the system.

Result

Cloud Backup is enabled on the system and backs up volumes every day and retains the most recent 30 backup copies.

What's next?

You can start and stop backups for volumes or change the backup schedule.
You can also restore entire volumes or individual files from a backup file to a Cloud Volumes ONTAP system in Azure, or to an on-premises ONTAP system.

Enabling Cloud Backup on an existing system

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

Steps

1. Select the working environment and click **Enable** next to the Backup & Restore service in the right-panel.

2. Select the provider details and click **Next**.
   a. The Azure subscription used to store the backups. This can be a different subscription than where the Cloud Volumes ONTAP system resides.

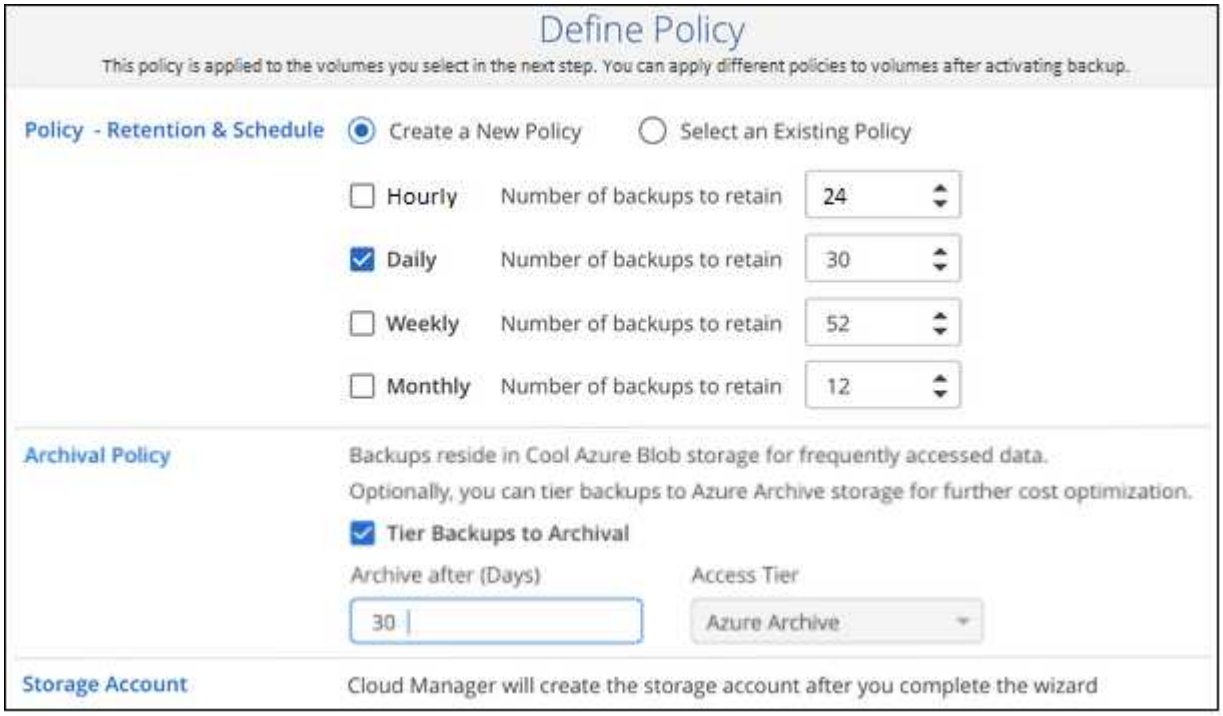
      If you want to use a different Azure subscription for your backups, you must log in to the Azure portal and link the two subscriptions.

   b. The region where the backups will be stored. This can be a different region than where the Cloud Volumes ONTAP system resides.
   c. The resource group that manages the Blob container - you can create a new resource group or select an existing resource group.
   d. Whether you'll use the default Microsoft-managed encryption key or choose your own customer-managed keys to manage encryption of your data. (See how to use your own keys).

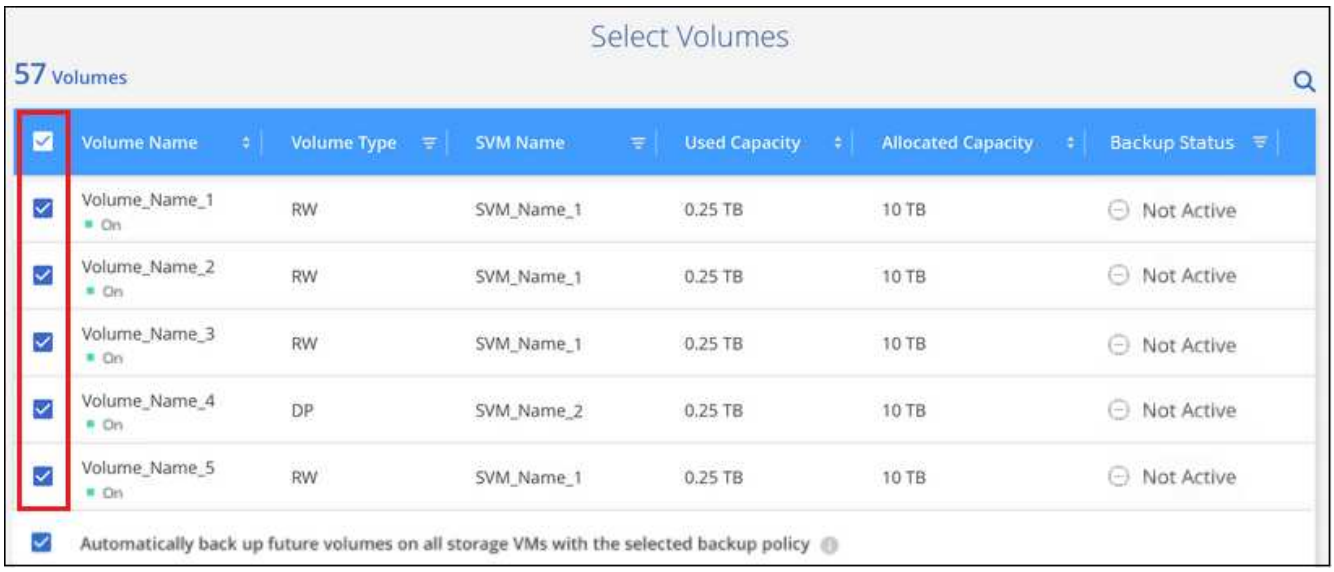
3. Enter the default backup policy details and click **Next**.

a. Define the backup schedule and choose the number of backups to retain. See the list of existing policies you can choose.

b. When using ONTAP 9.10.1 and greater, you can choose to tier backups to Azure Archive storage after a certain number of days for further cost optimization. Learn more about using archival tiers.



4. Select the volumes that you want to back up using the default backup policy in the Select Volumes page. If you want to assign different backup policies to certain volumes, you can create additional policies and apply them to those volumes later.



- 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).

5. If you want all volumes added in the future to have backup enabled, just leave the checkbox for "Automatically back up future volumes…" checked. If you disable this setting, you'll need to manually

enable backups for future volumes.

6. Click **Activate Backup** and Cloud Backup starts taking the initial backups of each selected volume.

Result

Cloud Backup starts taking the initial backups of each selected volume and the Volume 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.
You can also restore entire volumes or individual files from a backup file to a Cloud Volumes ONTAP system in Azure, or to an on-premises ONTAP system.

Backing up Cloud Volumes ONTAP data to Google Cloud Storage

Complete a few steps to get started backing up data from Cloud Volumes ONTAP to Google Cloud Storage.

Quick start

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

1 Verify support for your configuration

- You're running Cloud Volumes ONTAP 9.7P5 or later in GCP.
- You have a valid GCP subscription for the storage space where your backups will be located.
- You have a service account in your Google Cloud Project that has the predefined Storage Admin role.
- You have subscribed to the Cloud Manager Marketplace Backup offering, or you have purchased and activated a Cloud Backup BYOL license from NetApp.

2 Enable Cloud Backup on your new or existing system

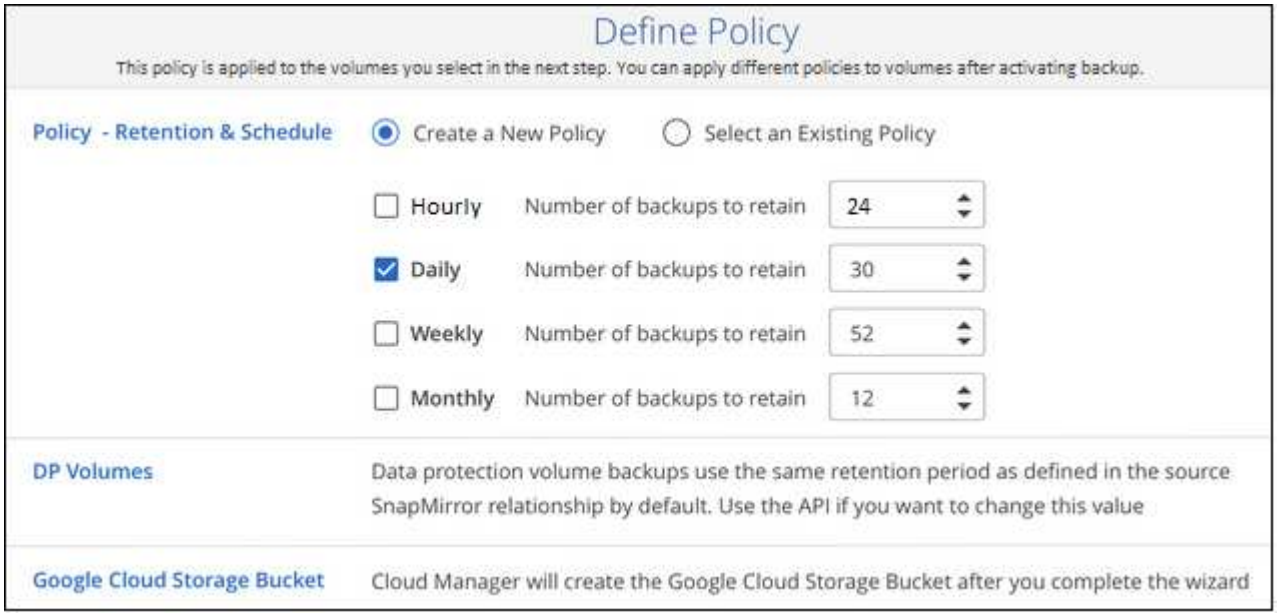
- New systems: Cloud Backup can be enabled when you complete the new working environment wizard.
- Existing systems: Select the working environment and click **Enable** next to the Backup & Restore service in the right-panel, and then follow the setup wizard.

3 Enter the provider details

Select the Google Cloud Project where you want the Google Cloud Storage bucket to be created for backups.

4 **Define the default 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 you want to retain.



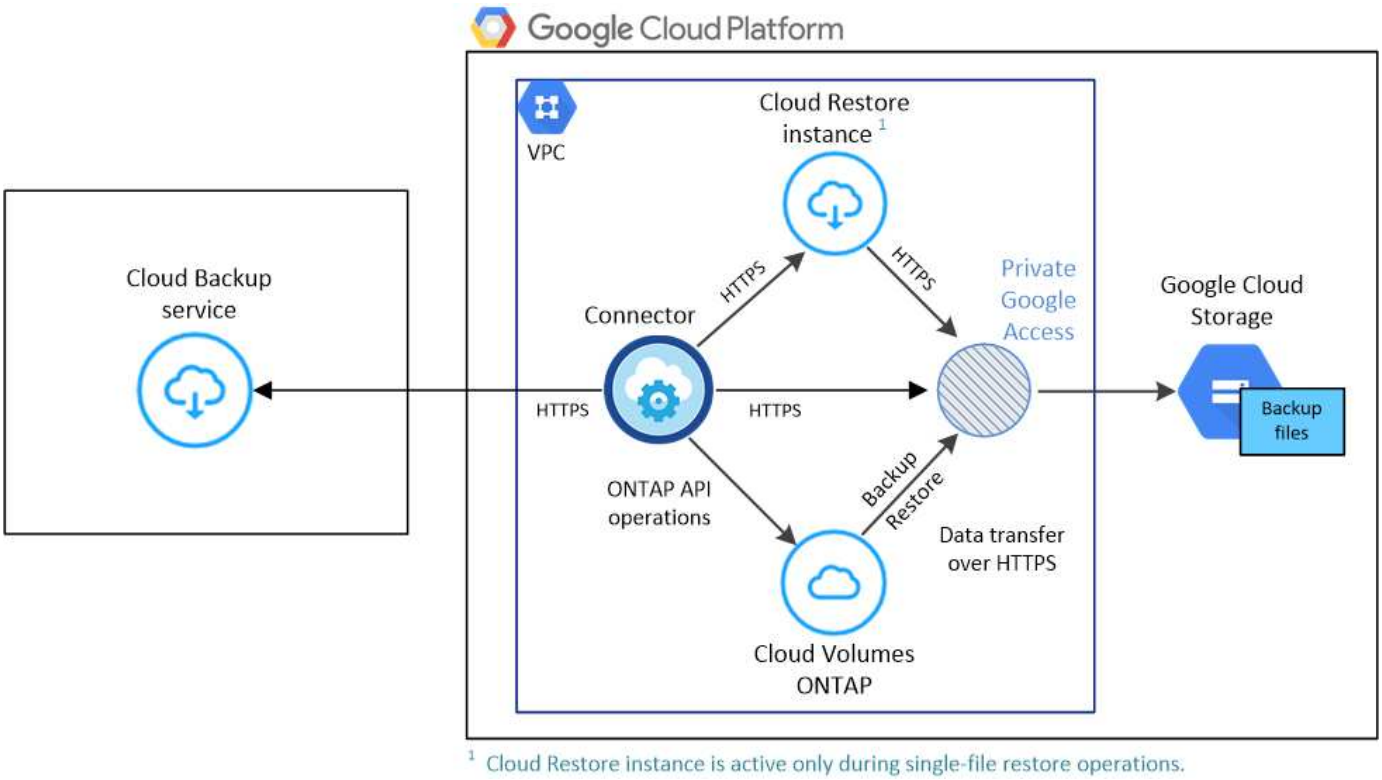
5 **Select the volumes that you want to back up**

Identify which volumes you want to back up using the default backup policy in the Select Volumes page. If you want to assign different backup policies to certain volumes, you can create additional policies and apply them to volumes later.

Requirements

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

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



Supported ONTAP versions

Cloud Volumes ONTAP 9.7P5 and later.

Supported GCP regions

Cloud Backup is supported in all GCP regions where Cloud Volumes ONTAP is supported.

License requirements

For Cloud Backup PAYGO licensing, a subscription through the GCP Marketplace is required before you enable Cloud Backup. Billing for Cloud Backup is done through this subscription. You can subscribe from the Details & Credentials page of the working environment wizard.

For Cloud Backup BYOL licensing, 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.

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

GCP Service Account

You need to have a service account in your Google Cloud Project that has the predefined Storage Admin role. Learn how to create a service account.

Enabling Cloud Backup on a new system

Cloud Backup can be enabled when you complete the working environment wizard to create a new Cloud Volumes ONTAP system.

You must have a Service Account already configured. If you don't select a service account when you create the Cloud Volumes ONTAP system, then you'll need to turn off the system and add the service account to Cloud Volumes ONTAP from the GCP console.

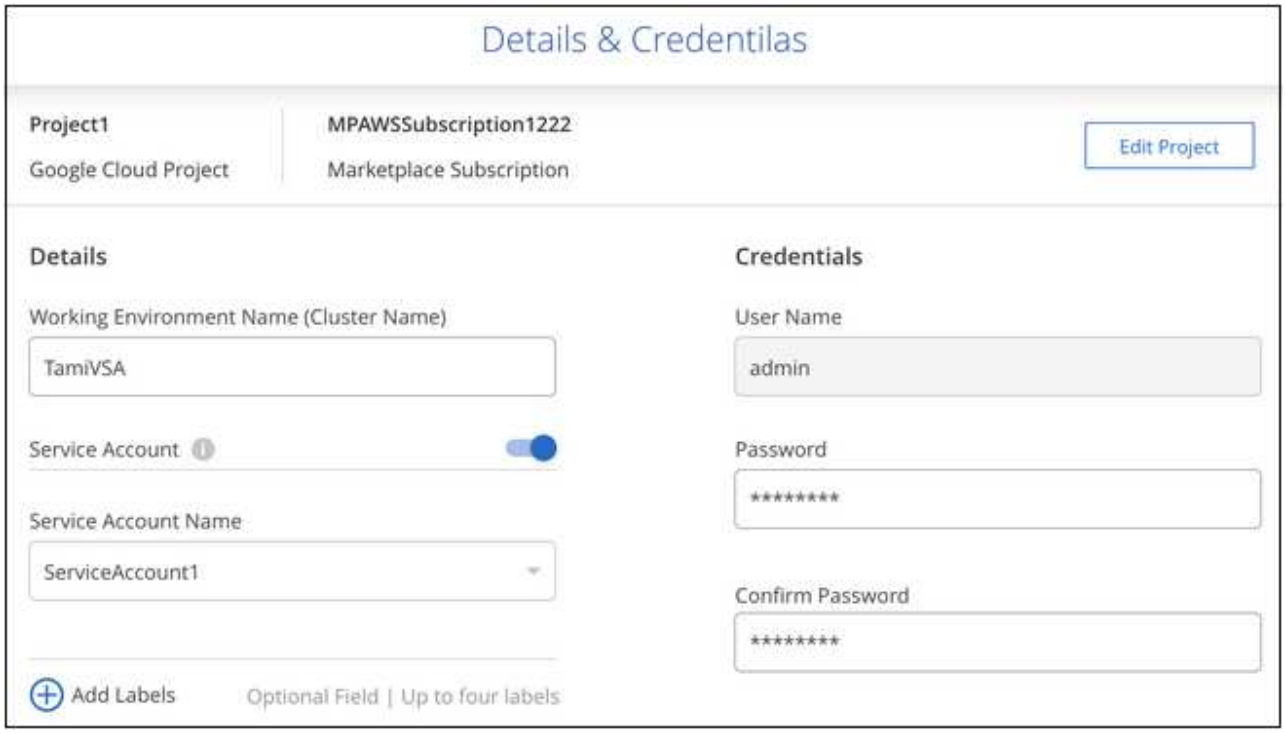
See Launching Cloud Volumes ONTAP in GCP for requirements and details for creating your Cloud Volumes

ONTAP system.

Steps

1. On the Working Environments page, click **Add Working Environment** and follow the prompts.
2. **Choose a Location**: Select **Google Cloud Platform**.
3. **Choose Type**: Select **Cloud Volumes ONTAP** (either single-node or high-availability).
4. **Details & Credentials**: Enter the following information:
   a. Click **Edit Project** and select a new project if the one you want to use is different than the default Project (where Cloud Manager resides).
   b. Specify the cluster name.
   c. Enable the **Service Account** switch and select the Service Account that has the predefined Storage Admin role. This is required to enable backups and tiering.
   d. Specify the credentials.

      Make sure that a GCP Marketplace subscription is in place.



5. **Services**: Leave the Cloud Backup service enabled and click **Continue**.

6. Complete the pages in the wizard to deploy the system as described in Launching Cloud Volumes ONTAP in GCP.

Result

Cloud Backup is enabled on the system and backs up the volume you created every day and retains the most recent 30 backup copies.

You can start and stop backups for volumes or change the backup schedule.
You can also restore entire volumes from a backup file to a Cloud Volumes ONTAP system in Google, or to an on-premises ONTAP system.

Enabling Cloud Backup on an existing system

You can enable Cloud Backup at any time directly from the working environment.

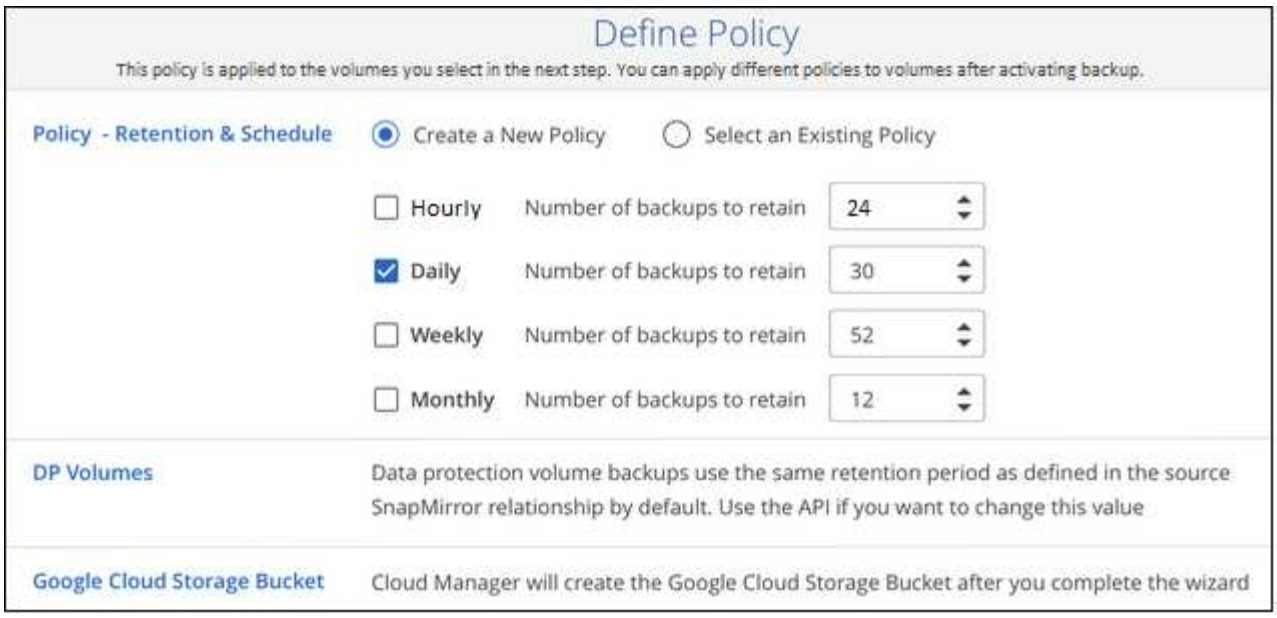
Steps

1. Select the working environment and click **Enable** next to the Backup & Restore service in the right-panel.

2. Select the Google Cloud Project and region where you want the Google Cloud Storage bucket to be created for backups, and click **Next**.

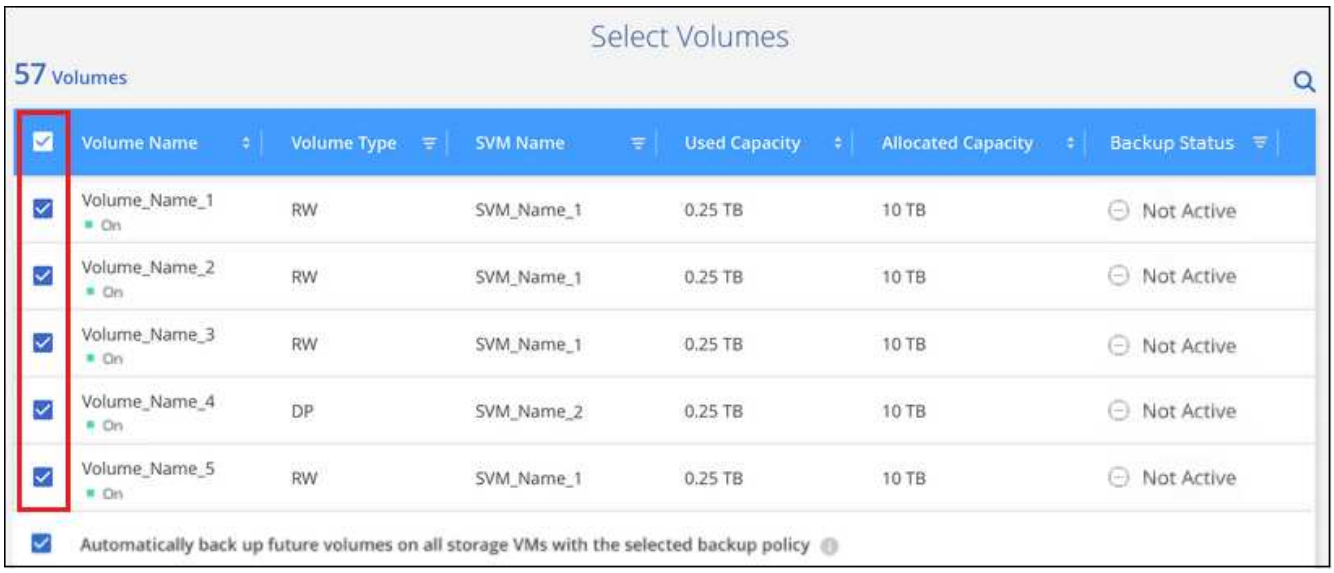
   Note that the Project must have a Service Account that has the predefined Storage Admin role.

3. In the *Define Policy* page, select the default backup schedule and retention value and click **Next**.



See the list of existing policies.

4. Select the volumes that you want to back up using the default backup policy in the Select Volumes page. If you want to assign different backup policies to certain volumes, you can create additional policies and apply them to those volumes later.



   - 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).

5. If you want all volumes added in the future to have backup enabled, just leave the checkbox for "Automatically back up future volumes…" checked. If you disable this setting, you'll need to manually enable backups for future volumes.
6. Click **Activate Backup** and Cloud Backup starts taking the initial backups of each selected volume.

Result

Cloud Backup starts taking the initial backups of each selected volume and the Volume 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.
You can also restore entire volumes from a backup file to a Cloud Volumes ONTAP system in Google, or to an on-premises ONTAP system.