Back up and restore Kubernetes data

Cloud Backup

NetApp
June 09, 2022

Table of Contents

Back up and restore Kubernetes data

Protect your Kubernetes cluster data using Cloud Backup

Cloud Backup provides backup and restore capabilities for protection and long-term archive of your Kubernetes cluster data. Backups are automatically generated and stored in an object store in your public or private cloud account.

When necessary, you can restore an entire *volume* from a backup to the same or different working environment.

Features

Backup features:

- Back up independent copies of your persistent volumes to low-cost object storage.
- Apply a single backup policy to all volumes in a cluster, or assign different backup policies to volumes that have unique recovery point objectives.
- Backup data is secured with AES-256 bit encryption at-rest and TLS 1.2 HTTPS connections in-flight.
- Support for up to 4,000 backups of a single volume.

Restore features:

- Restore data from a specific point in time.
- Restore a volume to the source system or to a different system.
- Restores data on a block level, placing the data directly in the location you specify, all while preserving the original ACLs.

Supported Kubernetes working environments and object storage providers

Cloud Backup enables you to back up Kubernetes volumes from the following working environments to object storage in the following public and private cloud providers:

Source Working Environment	Backup File Destination
Kubernetes cluster in AWS	Amazon S3
Kubernetes cluster in Azure	Azure Blob
Kubernetes cluster in Google	Google Cloud Storage

You can restore a volume from a Kubernetes backup file to the following working environments:

Backup File Location	Destination Working Environment
Amazon S3	Kubernetes cluster in AWS
Azure Blob	Kubernetes cluster in Azure
Google Cloud Storage	Kubernetes cluster in Google

Cost

There are two types of costs associated with using Cloud Backup: resource charges and service charges.

Resource charges

Resource charges are paid to the cloud provider for object storage capacity in the cloud. Since Cloud Backup preserves the storage efficiencies of the source volume, you pay the cloud provider object storage costs for the data *after* ONTAP efficiencies (for the smaller amount of data after deduplication and compression have been applied).

Service charges

Service charges are paid to NetApp and cover both the cost to *create* backups and to *restore* volumes, from those backups. You pay only for the data that you protect, calculated by the source logical used capacity (*before* ONTAP efficiencies) of volumes which are backed up to object storage. This capacity is also known as Front-End Terabytes (FETB).

There are two ways to pay for the Backup service. The first option is to subscribe from your cloud provider, which enables you to pay per month. The second option is to purchase licenses directly from NetApp. Read the Licensing section for details.

Licensing

Cloud Backup is available in two licensing options: Pay As You Go (PAYGO), and Bring Your Own License (BYOL). A 30-day free trial is available if you don't have a license.

Free trial

When using the 30-day free trial, you are notified about the number of free trial days that remain. At the end of your free trial, backups stop being created. You must subscribe to the service or purchase a license to continue using the service.

Backup files are not deleted when the service is disabled. You'll continue to be charged by your cloud provider for object storage costs for the capacity that your backups use unless you delete the backups.

Pay-as-you-go subscription

Cloud Backup offers consumption-based licensing in a pay-as-you-go model. After subscribing through your cloud provider's marketplace, you pay per GB for data that's backed up—there's no up-front payment. You are billed by your cloud provider through your monthly bill.

You should subscribe even if you have a free trial or if you bring your own license (BYOL):

- Subscribing ensures that there's no disruption of service after your free trial ends.

  When the trial ends, you'll be charged hourly according to the amount of data that you back up.

- If you back up more data than allowed by your BYOL license, then data backup continues through your pay-as-you-go subscription.

  For example, if you have a 10 TB BYOL license, all capacity beyond the 10 TB is charged through the PAYGO subscription.

You won't be charged from your pay-as-you-go subscription during your free trial or if you haven't exceeded

your BYOL license.

Learn how to set up a pay-as-you-go subscription.

Bring your own license

BYOL is term-based (12, 24, or 36 months) *and* capacity-based in 1 TB increments. You pay NetApp to use the service for a period of time, say 1 year, and for a maximum amount capacity, say 10 TB.

You'll receive a serial number that you enter in the Cloud Manager Digital Wallet page to enable the service. When either limit is reached, you'll need to renew the license. The Backup BYOL license applies to all source systems associated with your Cloud Manager account.

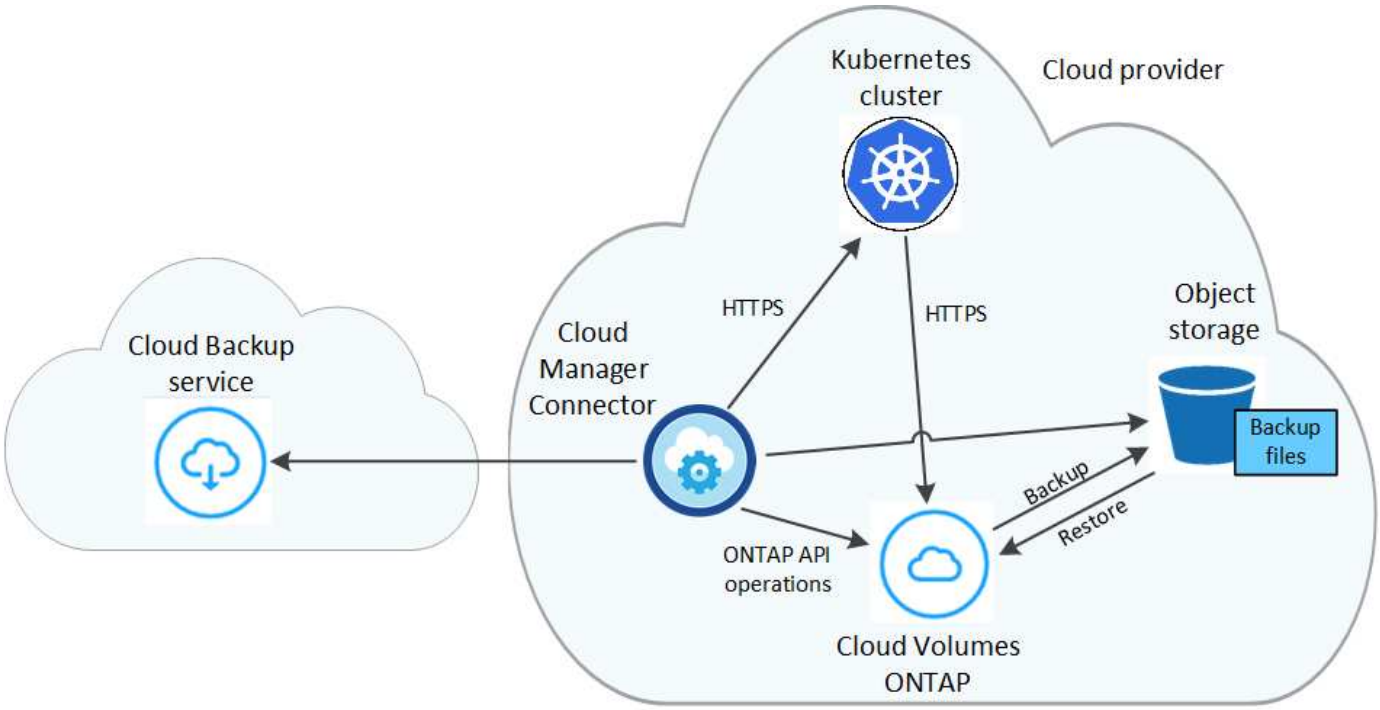
Learn how to manage your BYOL licenses.

How Cloud Backup works

When you enable Cloud Backup on a Kubernetes system, the service performs a full backup of your data. After the initial backup, all additional backups are incremental, which means that only changed blocks and new blocks are backed up. This keeps network traffic to a minimum.

Any actions taken directly from your cloud provider environment to manage or change backup files may corrupt the files and will result in an unsupported configuration.

The following image shows the relationship between each component:



Supported storage classes or access tiers

- In AWS, backups start in the *Standard* storage class and transition to the *Standard-Infrequent Access* storage class after 30 days.
- In Azure, backups are associated with the *Cool* access tier.

- In GCP, backups are associated with the *Standard* storage class by default.

Customizable backup schedule and retention settings per cluster

When you enable Cloud Backup for a working environment, all the volumes you initially select are backed up using the default backup policy that you define. If you want to assign different backup policies to certain volumes that have different recovery point objectives (RPO), you can create additional policies for that cluster and assign those policies to other volumes.

You can choose a combination of hourly, daily, weekly, and monthly backups of all volumes.

Once you have reached the maximum number of backups for a category, or interval, older backups are removed so you always have the most current backups.

Supported volumes

Cloud Backup supports Persistent volumes (PVs).

Limitations

- When creating or editing a backup policy when no volumes are assigned to the policy, the number of retained backups can be a maximum of 1018. As a workaround you can reduce the number of backups to create the policy. Then you can edit the policy to create up to 4000 backups after you assign volumes to the policy.
- Ad-hoc volume backups using the **Backup Now** button aren't supported on Kubernetes volumes.

Backing up Kubernetes persistent volume data to Amazon S3

Complete a few steps to get started backing up data from your persistent volumes on EKS Kubernetes clusters to Amazon S3 storage.

Quick start

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

Review prerequisites

- You have discovered the Kubernetes cluster as a Cloud Manager working environment.
  - Trident must be installed on the cluster, and the Trident version must be 21.1 or greater.
  - All PVCs that will be used to create persistent volumes that you want to back up must have "snapshotPolicy" set to "default".
  - The cluster must be using Cloud Volumes ONTAP on AWS for its' backend storage.
  - The Cloud Volumes ONTAP system must be running ONTAP 9.7P5 or later.
- 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.

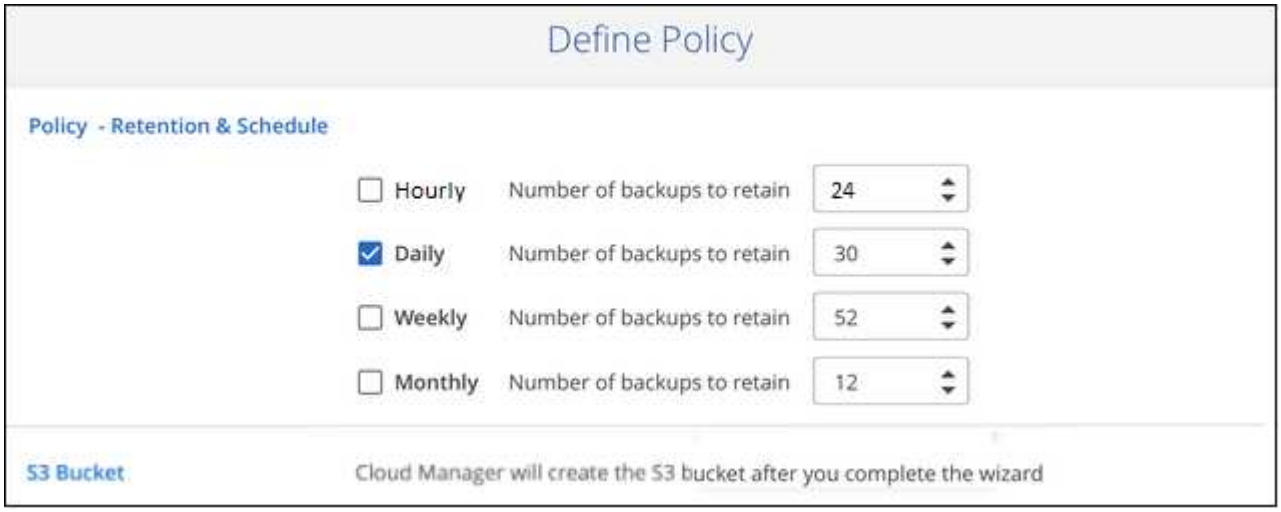
- The IAM role that provides the Cloud Manager Connector with permissions includes S3 permissions from the latest Cloud Manager policy.

2 Enable Cloud Backup on your existing Kubernetes cluster

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

3 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 you want to retain.



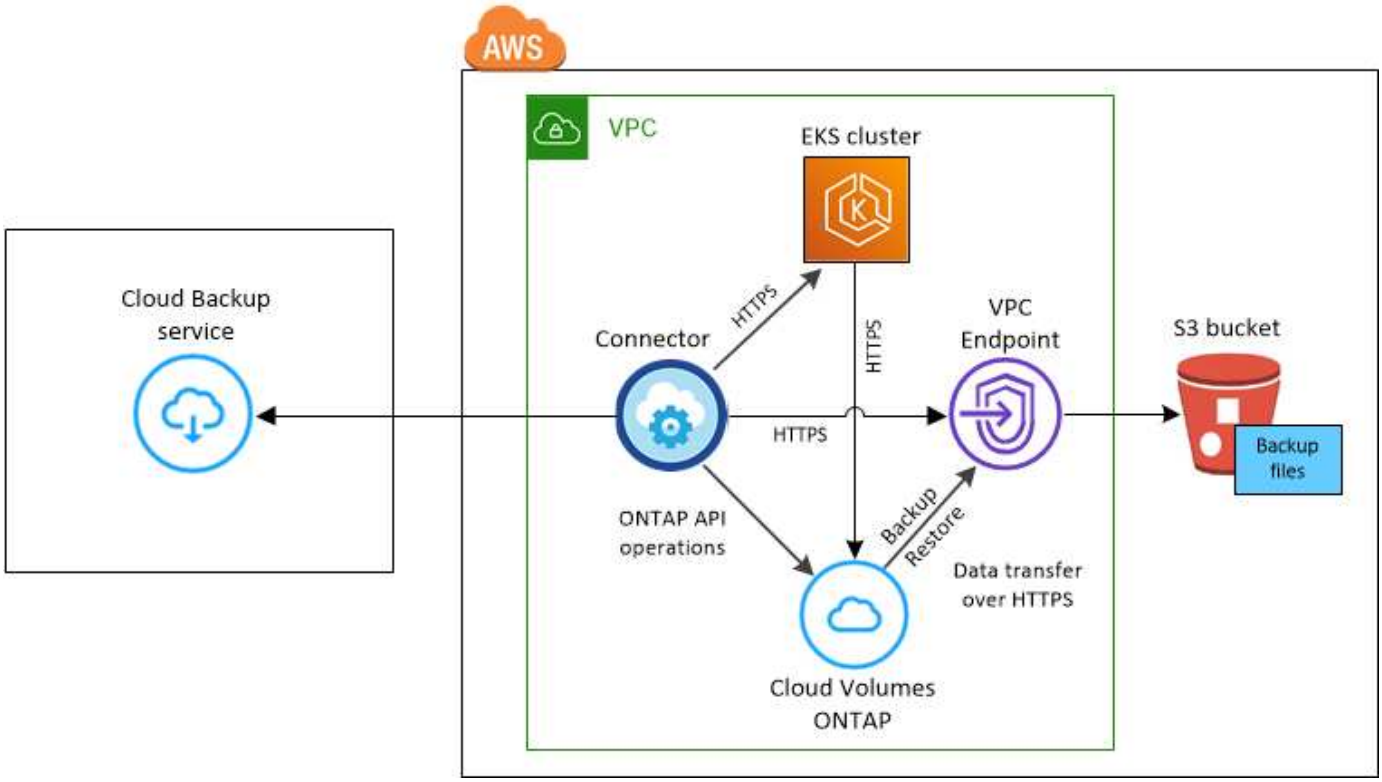
4 Select the volumes that you want to back up

Identify which volumes you want to back up in the Select Volumes page. An S3 bucket is created automatically in the same AWS account and Region as the Cloud Volumes ONTAP system, and the backup files are stored there.

Requirements

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

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



Note that the VPC Endpoint is optional.

Kubernetes cluster requirements

- You have discovered the Kubernetes cluster as a Cloud Manager working environment. See how to discover the Kubernetes cluster.
- Trident must be installed on the cluster, and the Trident version must be a minimum of 21.1. See how to install Trident or how to upgrade the Trident version.
- The cluster must be using Cloud Volumes ONTAP on AWS for its' backend storage.
- The Cloud Volumes ONTAP system must be in the same AWS region as the Kubernetes cluster, and it must be running ONTAP 9.7P5 or later (ONTAP 9.8P11 and later is recommended).

  Note that Kubernetes clusters in on-premises locations are not supported. Only Kubernetes clusters in cloud deployments that are using Cloud Volumes ONTAP systems are supported.

- All Persistent Volume Claim objects that will be used to create the persistent volumes that you want to back up must have "snapshotPolicy" set to "default".

  You can do this for individual PVCs by adding `snapshotPolicy` under annotations:

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: full
  annotations:
    trident.netapp.io/snapshotPolicy: "default"
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1000Mi
  storageClassName: silver
```

You can do this for all PVCs associated with a particular backend storage by adding the `snapshotPolicy` field under defaults in the `backend.json` file:

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas-advanced
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  backendName: tbc-ontap-nas-advanced
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-nas-advanced-secret
  limitAggregateUsage: 80%
  limitVolumeSize: 50Gi
  nfsMountOptions: nfsvers=4
  defaults:
    spaceReserve: volume
    exportPolicy: myk8scluster
    snapshotPolicy: default
    snapshotReserve: '10'
  deletionPolicy: retain
```

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.

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 S3 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-*"
            ]
        },
```

Enabling Cloud Backup

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

Steps

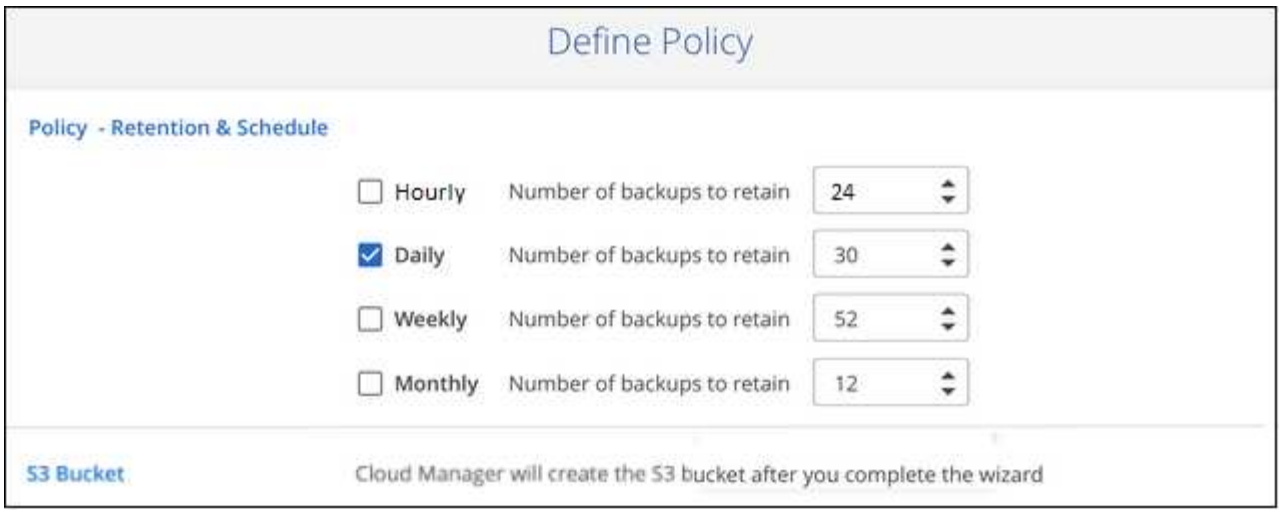
1. Select the working environment and click **Enable** next to the Backup & Restore service in the right-panel.

   If the Amazon S3 destination for your backups exists as a working environment on the Canvas, you can drag the Kubernetes cluster onto the Amazon S3 working environment to initiate the setup wizard.

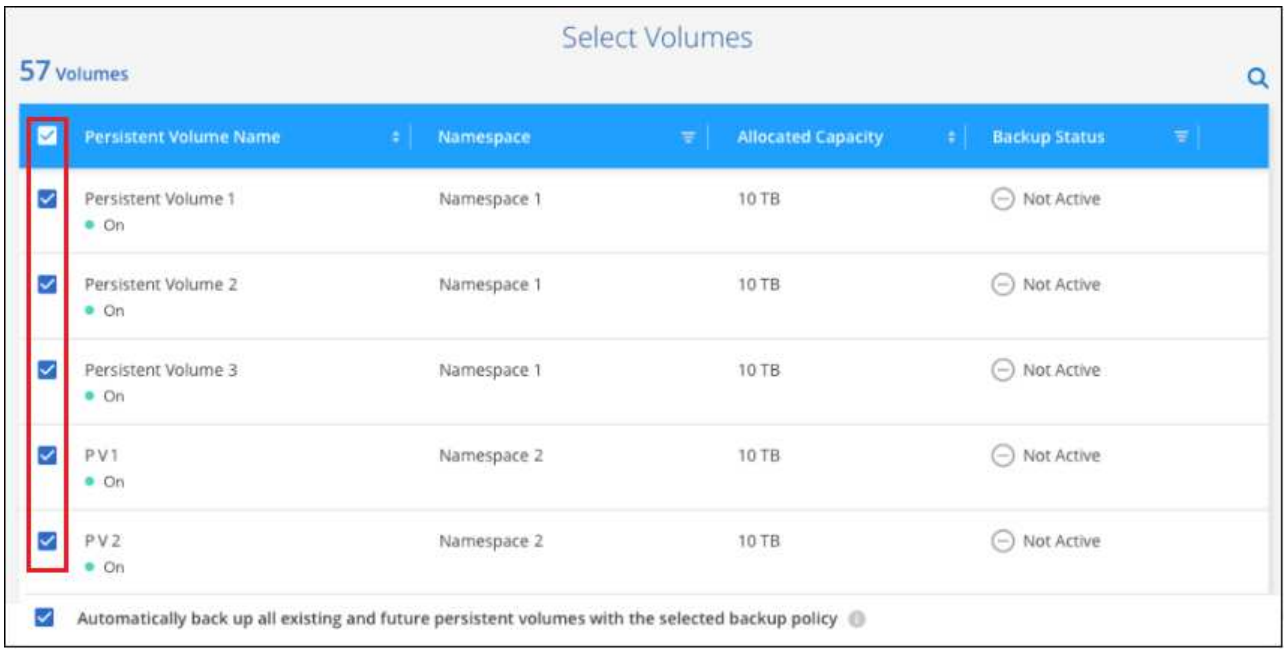
   

2. Enter the backup policy details and click **Next**.

   You can define the backup schedule and choose the number of backups to retain.



3. Select the persistent 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).



4. If you want all current and future volumes 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.
5. Click **Activate Backup** and Cloud Backup starts taking the initial backups of each selected volume.

Result

An S3 bucket is created automatically in the same AWS account and Region as the Cloud Volumes ONTAP system, and the backup files are stored there.

The Kubernetes 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 as a new volume on the same or different Kubernetes cluster in AWS (in the same region).

Backing up Kubernetes persistent volume data to Azure Blob storage

Complete a few steps to get started backing up data from your persistent volumes on AKS Kubernetes clusters to Azure Blob storage.

Quick start

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

1 Review prerequisites

- You have discovered the Kubernetes cluster as a Cloud Manager working environment.
  - Trident must be installed on the cluster, and the Trident version must be 21.1 or greater.
  - All PVCs that will be used to create persistent volumes that you want to back up must have "snapshotPolicy" set to "default".
  - The cluster must be using Cloud Volumes ONTAP on Azure for its' backend storage.
  - The Cloud Volumes ONTAP system must be running ONTAP 9.7P5 or later.
- 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 existing Kubernetes cluster

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

3 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 you want to retain.

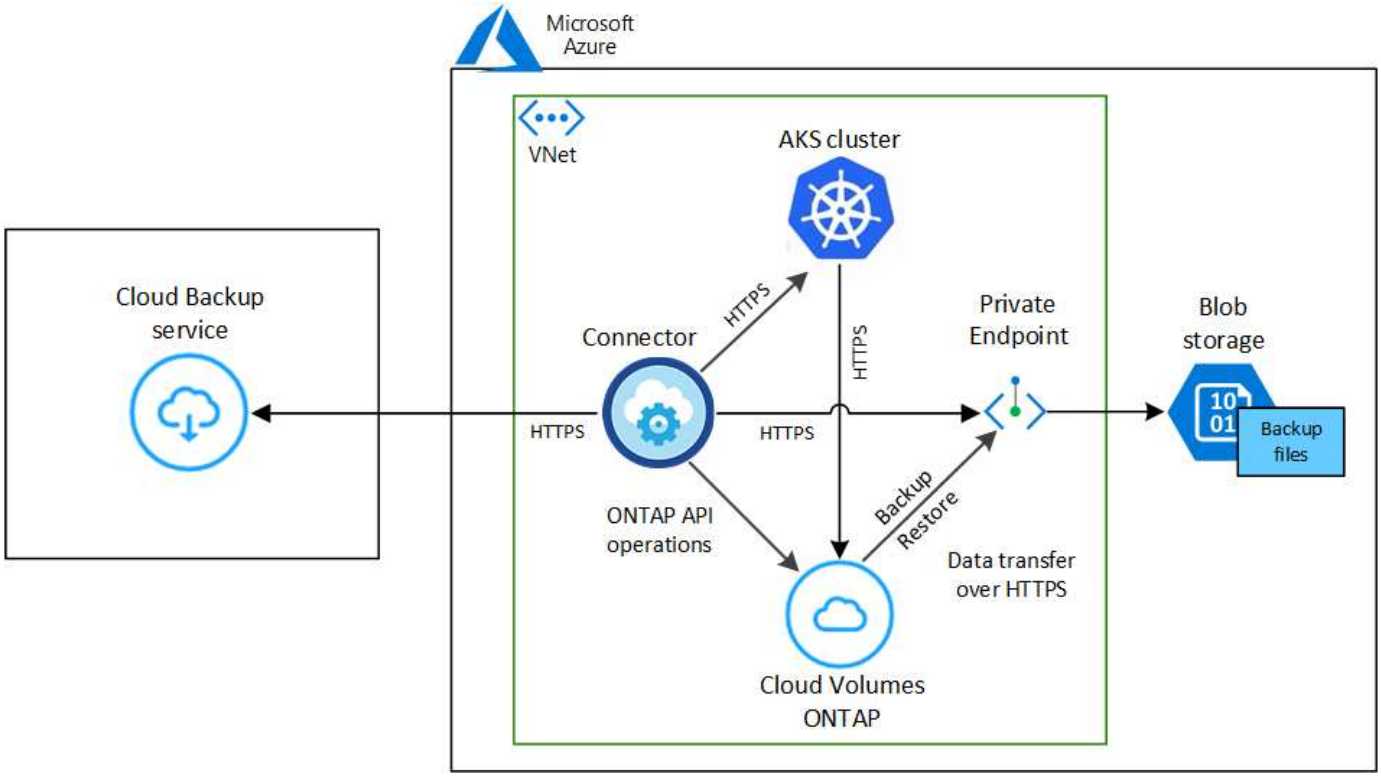
4 **Select the volumes that you want to back up**

Identify which volumes you want to back up in the Select Volumes page. The backup files are stored in a Blob container using the same Azure subscription and Region as the Cloud Volumes ONTAP system.

Requirements

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

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



Note that the Private Endpoint is optional.

Kubernetes cluster requirements

- You have discovered the Kubernetes cluster as a Cloud Manager working environment. See how to discover the Kubernetes cluster.
- Trident must be installed on the cluster, and the Trident version must be a minimum of 21.1. See how to install Trident or how to upgrade the Trident version.
- The cluster must be using Cloud Volumes ONTAP on Azure for its' backend storage.
- The Cloud Volumes ONTAP system must be in the same Azure region as the Kubernetes cluster, and it must be running ONTAP 9.7P5 or later (ONTAP 9.8P11 and later is recommended).

  Note that Kubernetes clusters in on-premises locations are not supported. Only Kubernetes clusters in cloud deployments that are using Cloud Volumes ONTAP systems are supported.

- All Persistent Volume Claim objects that will be used to create the persistent volumes that you want to back up must have "snapshotPolicy" set to "default".

  You can do this for individual PVCs by adding `snapshotPolicy` under annotations:

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: full
  annotations:
    trident.netapp.io/snapshotPolicy: "default"
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1000Mi
  storageClassName: silver
```

  You can do this for all PVCs associated with a particular backend storage by adding the `snapshotPolicy` field under defaults in the `backend.json` file:

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas-advanced
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  backendName: tbc-ontap-nas-advanced
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-nas-advanced-secret
  limitAggregateUsage: 80%
  limitVolumeSize: 50Gi
  nfsMountOptions: nfsvers=4
  defaults:
    spaceReserve: volume
    exportPolicy: myk8scluster
    snapshotPolicy: default
    snapshotReserve: '10'
  deletionPolicy: retain
```

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.

Enabling Cloud Backup

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

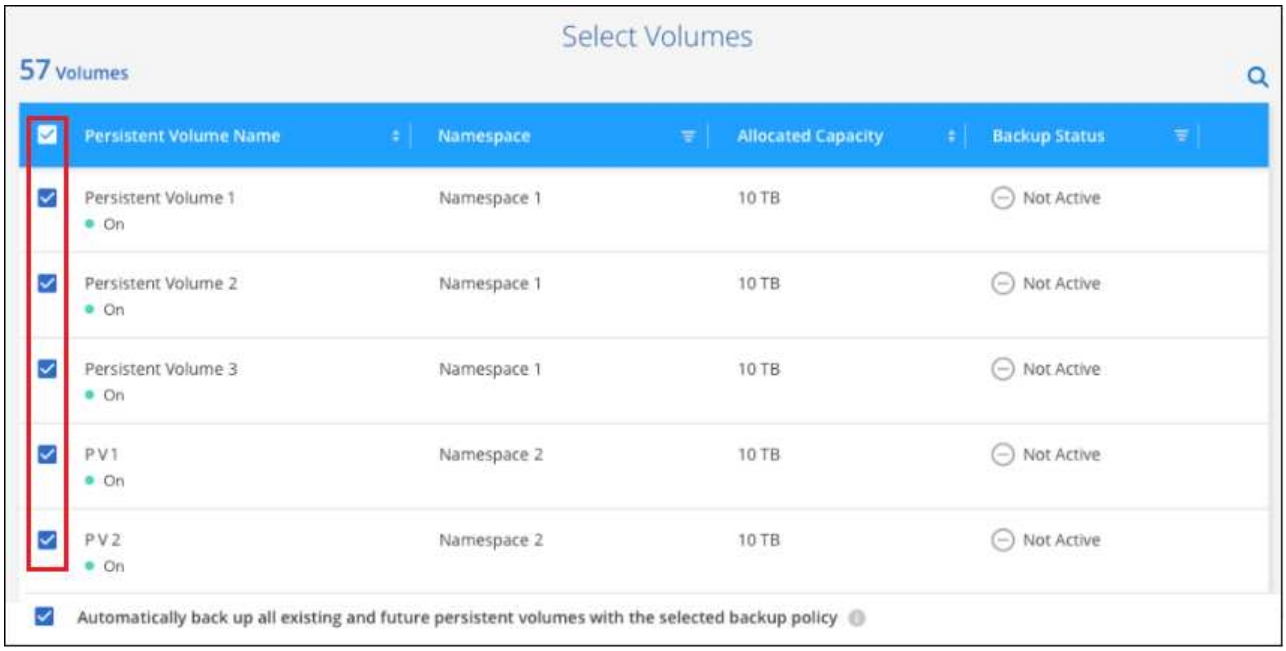
Steps

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

2. Enter the backup policy details and click **Next**.

   You can define the backup schedule and choose the number of backups to retain.

3. Select the persistent 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).



4. If you want all current and future volumes 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.
5. Click **Activate Backup** and Cloud Backup starts taking the initial backups of each selected volume.

Result

The backup files are stored in a Blob container using the same Azure subscription and Region as the Cloud Volumes ONTAP system.

The Kubernetes 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 as a new volume on the same or different Kubernetes cluster in Azure (in the same region).

Backing up Kubernetes persistent volume data to Google Cloud storage

Complete a few steps to get started backing up data from your persistent volumes on GKE Kubernetes clusters to Google Cloud storage.

Quick start

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

1 Review prerequisites

- You have discovered the Kubernetes cluster as a Cloud Manager working environment.
  - Trident must be installed on the cluster, and the Trident version must be 21.1 or greater.
  - All PVCs that will be used to create persistent volumes that you want to back up must have "snapshotPolicy" set to "default".
  - The cluster must be using Cloud Volumes ONTAP on GCP for its' backend storage.
  - The Cloud Volumes ONTAP system must be running ONTAP 9.7P5 or later.
- 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 existing Kubernetes cluster

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

3 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 you want to retain.

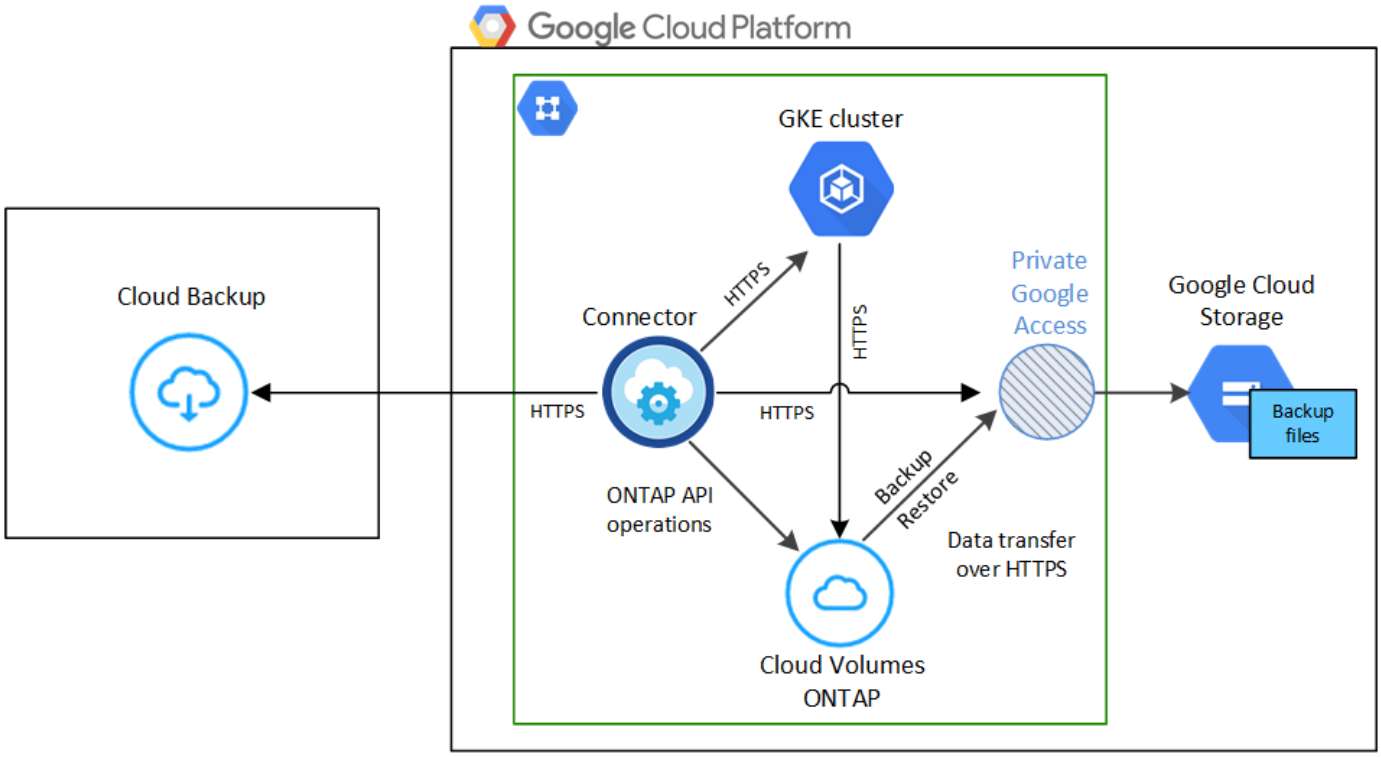
4 **Select the volumes that you want to back up**

Identify which volumes you want to back up in the Select Volumes page. The backup files are stored in a Google Cloud Storage bucket using the same GCP subscription and Region as the Cloud Volumes ONTAP system.

Requirements

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

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



Note that the Private Endpoint is optional.

Kubernetes cluster requirements

- You have discovered the Kubernetes cluster as a Cloud Manager working environment. See how to discover the Kubernetes cluster.
- Trident must be installed on the cluster, and the Trident version must be a minimum of 21.1. See how to install Trident or how to upgrade the Trident version.
- The cluster must be using Cloud Volumes ONTAP on GCP for its' backend storage.
- The Cloud Volumes ONTAP system must be in the same GCP region as the Kubernetes cluster, and it must be running ONTAP 9.7P5 or later (ONTAP 9.8P11 and later is recommended).

  Note that Kubernetes clusters in on-premises locations are not supported. Only Kubernetes clusters in cloud deployments that are using Cloud Volumes ONTAP systems are supported.

- All Persistent Volume Claim objects that will be used to create the persistent volumes that you want to back up must have "snapshotPolicy" set to "default".

  You can do this for individual PVCs by adding `snapshotPolicy` under annotations:

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: full
  annotations:
    trident.netapp.io/snapshotPolicy: "default"
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1000Mi
  storageClassName: silver
```

  You can do this for all PVCs associated with a particular backend storage by adding the `snapshotPolicy` field under defaults in the `backend.json` file:

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas-advanced
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  backendName: tbc-ontap-nas-advanced
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-nas-advanced-secret
  limitAggregateUsage: 80%
  limitVolumeSize: 50Gi
  nfsMountOptions: nfsvers=4
  defaults:
    spaceReserve: volume
    exportPolicy: myk8scluster
    snapshotPolicy: default
    snapshotReserve: '10'
  deletionPolicy: retain
```

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

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

Steps

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

2. Enter the backup policy details and click **Next**.

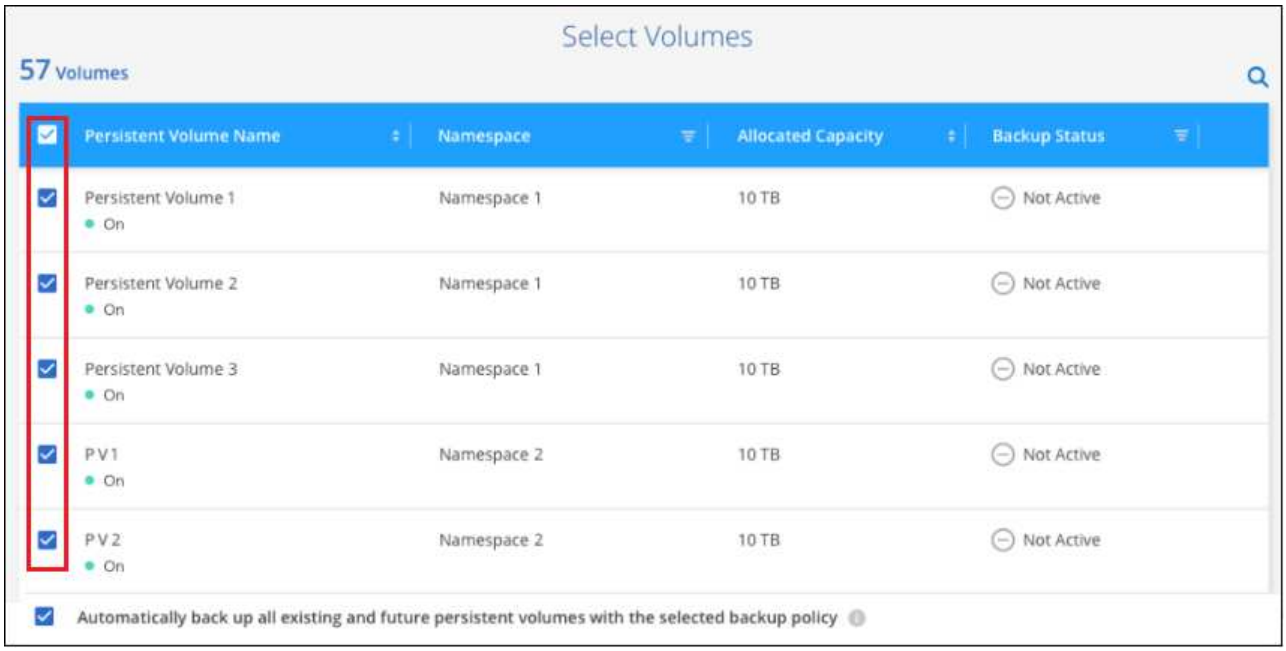
   You can define the backup schedule and choose the number of backups to retain.

3. Select the persistent volumes that you want to back up.

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

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

).



4. If you want all current and future volumes 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.
5. Click **Activate Backup** and Cloud Backup starts taking the initial backups of each selected volume.

Result

The backup files are stored in a Google Cloud Storage bucket using the same GCP subscription and Region as the Cloud Volumes ONTAP system.

The Kubernetes 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 as a new volume on the same or different Kubernetes cluster in GCP (in the same region).

Managing backups for your Kubernetes systems

You can manage backups for your Kubernetes systems by changing the backup schedule, enabling/disabling volume backups, deleting backups, and more.

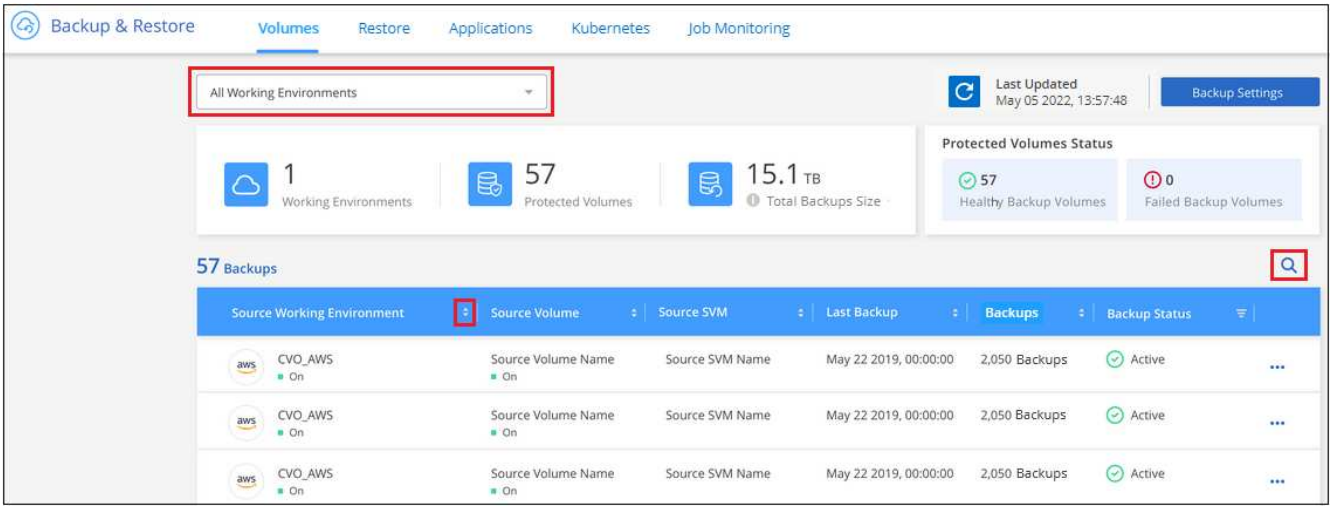
Do not manage or change backup files directly from your cloud provider environment. This may corrupt the files and will result in an unsupported configuration.

Viewing the volumes that are being backed up

You can view a list of all the volumes that are currently being backed up by Cloud Backup.

Steps

1. Click the **Backup & Restore** service.
2. Click the **Kubernetes** tab to view the list of persistent volumes for Kubernetes systems.



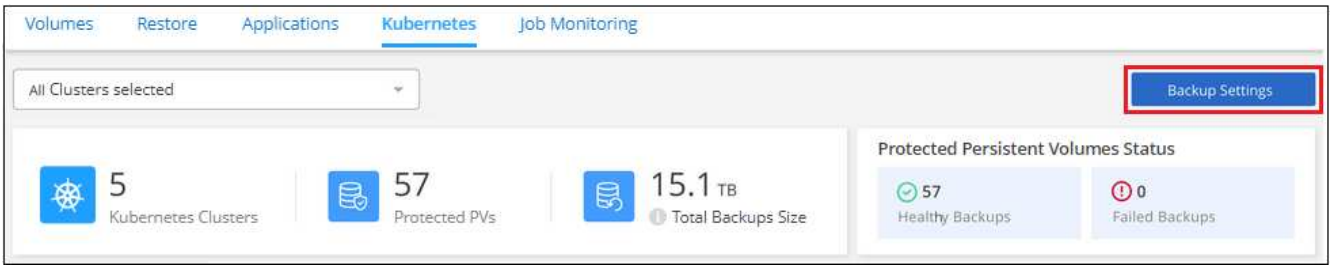
If you are looking for specific volumes in certain working environments, you can refine the list by working environment and volume, or you can use the search filter.

Enabling and disabling backups of volumes

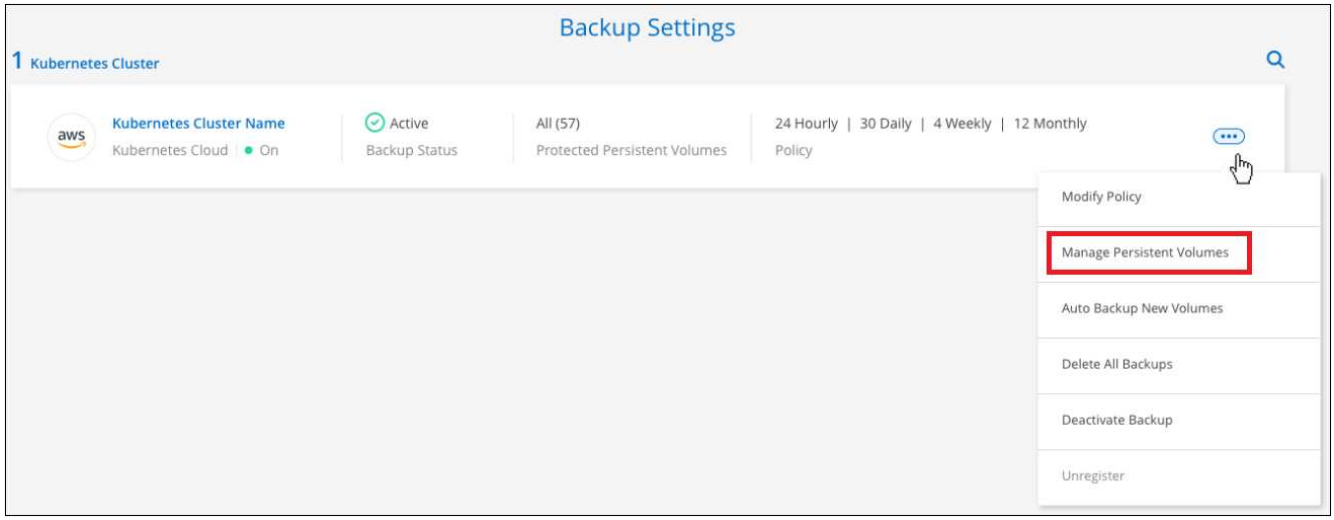
You can stop backing up a volume if you do not need backup copies of that volume and you do not want to pay for the cost to store the backups. You can also add a new volume to the backup list if it is not currently being backed up.

Steps

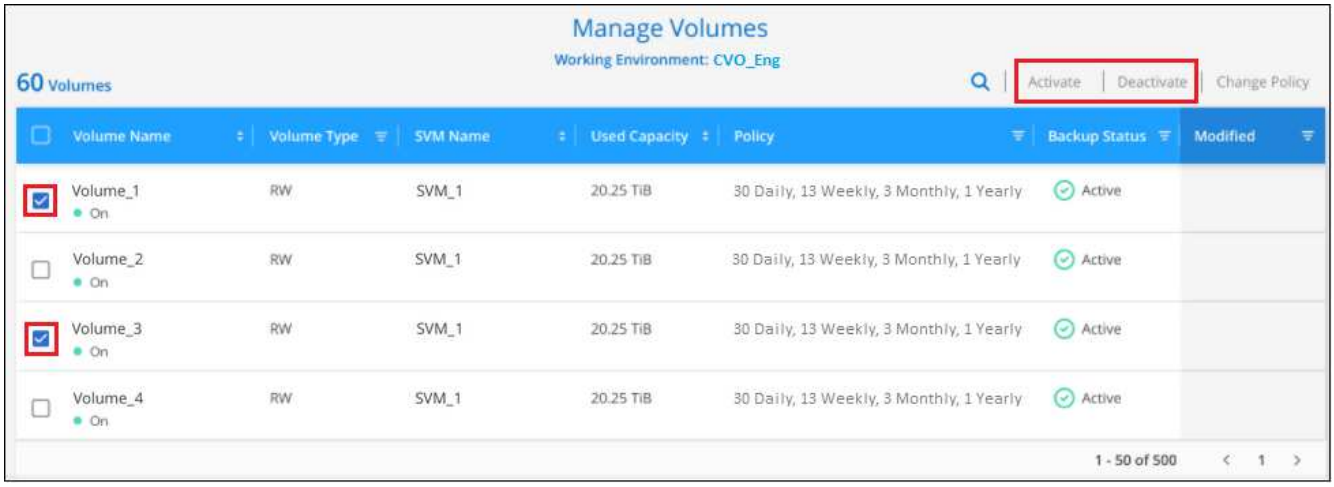
1. From the **Kubernetes** tab, select **Backup Settings**.



2. From the *Backup Settings page*, click ••• for the Kubernetes cluster and select **Manage Persistent Volumes**.



3. Select the checkbox for a volume, or volumes, that you want to change, and then click **Activate** or **Deactivate** depending on whether you want to start or stop backups for the volume.



4. Click **Save** to commit your changes.

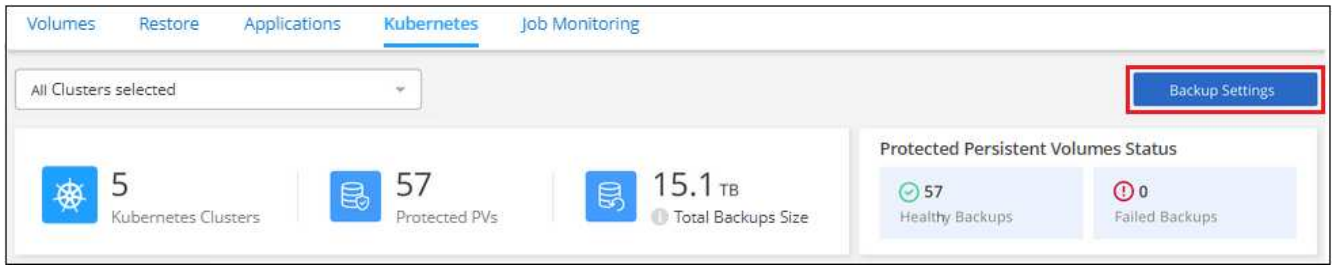
Note: When stopping a volume from being backed up you'll continue to be charged by your cloud provider for object storage costs for the capacity that the backups use unless you delete the backups.

Editing an existing backup policy

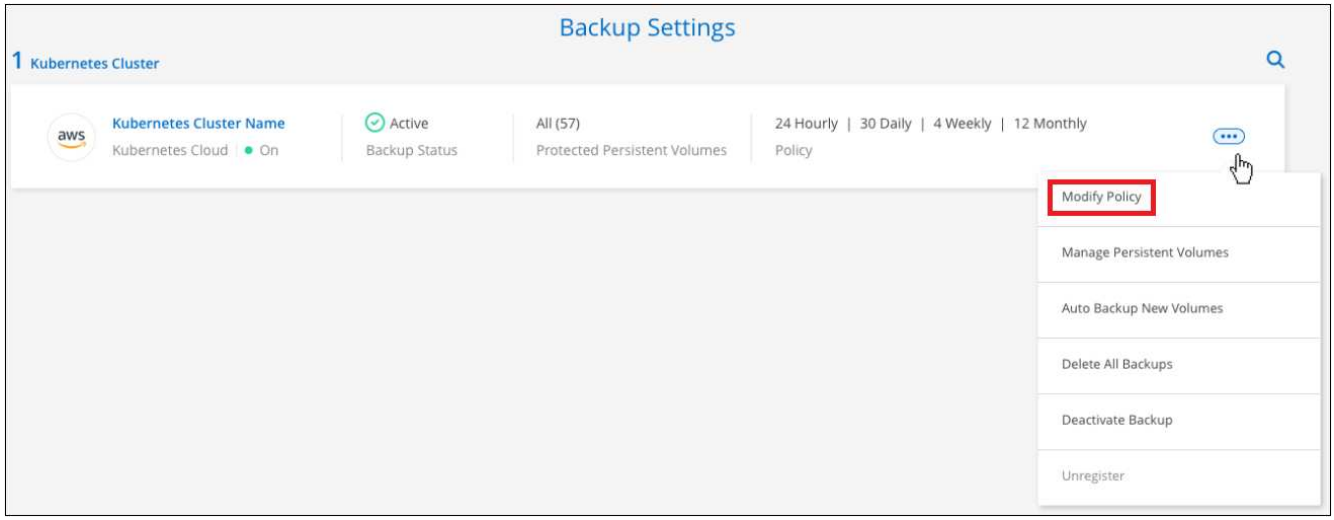
You can change the attributes for a backup policy that is currently applied to volumes in a working environment. Changing the backup policy affects all existing volumes that are using the policy.

Steps

1. From the **Kubernetes** tab, select **Backup Settings**.



2. From the *Backup Settings* page, click ••• for the working environment where you want to change the settings, and select **Manage Policies**.



3. From the *Manage Policies* page, click **Edit Policy** for the backup policy you want to change in that working environment.

4. From the *Edit Policy* page, change the schedule and backup retention and click **Save**.

Setting a backup policy to be assigned to new volumes

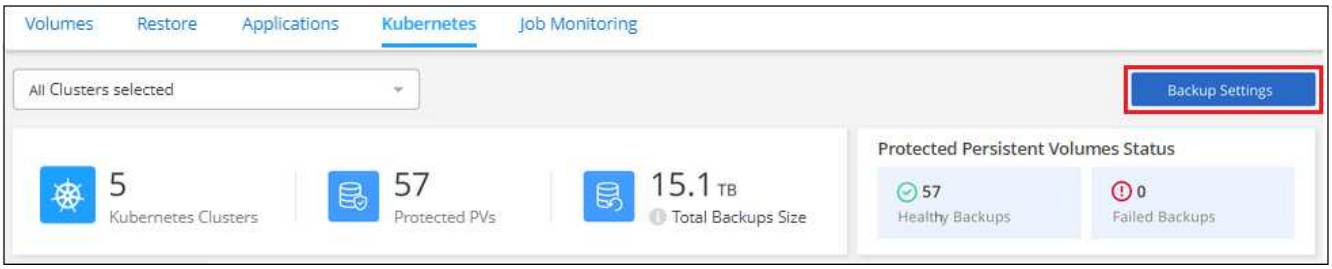
If you did not select the option to automatically assign a backup policy to newly created volumes when you first activated Cloud Backup on your Kubernetes cluster, you can choose this option in the *Backup Settings* page later. Having a backup policy assigned to newly created volumes ensures that all your data is protected.

Note that the policy that you want to apply to the volumes must already exist. See how to add a new backup policy for a working environment.

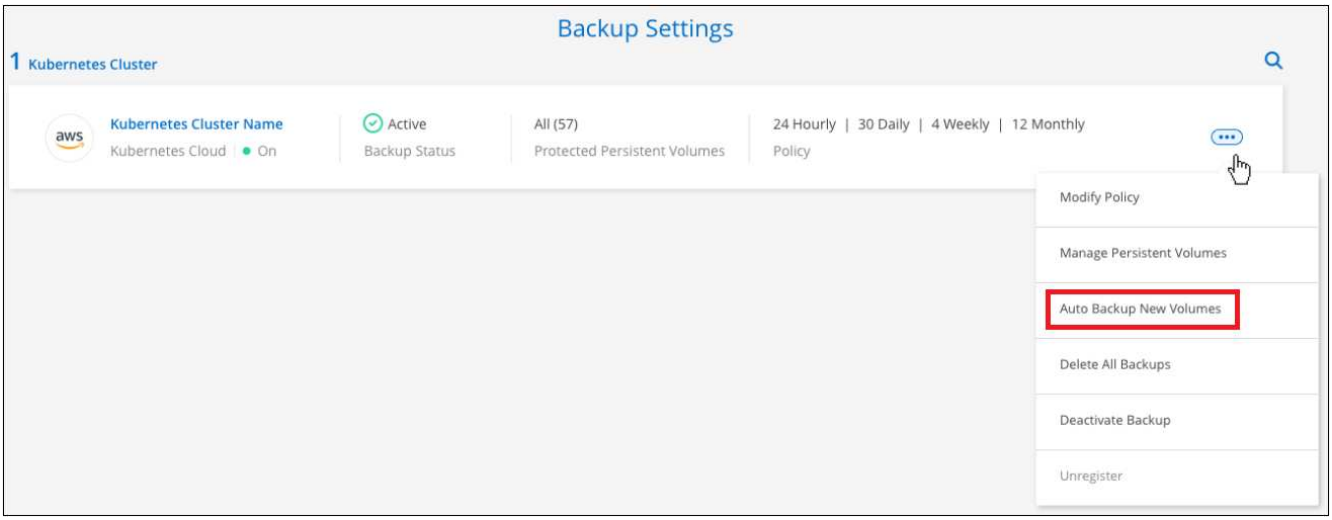
You can also disable this setting so that newly created volumes do not get backed up automatically. In that case you'll need to manually enable backups for any specific volumes that you do want to back up in the future.

Steps

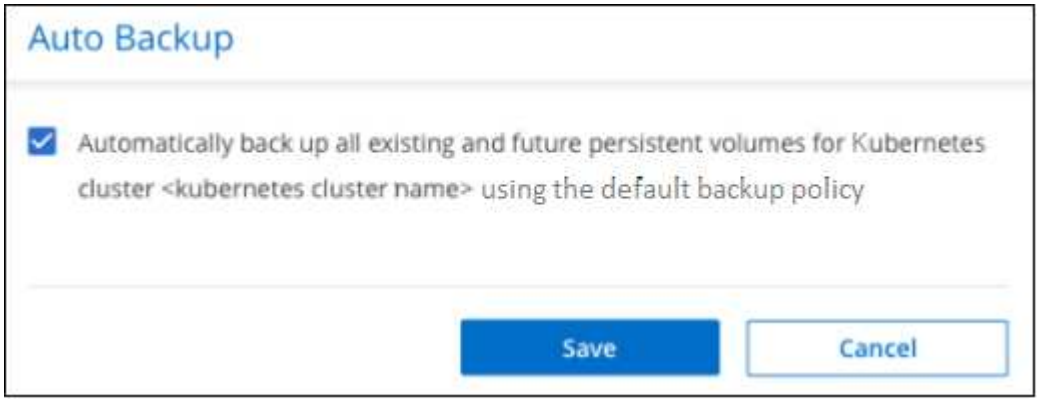
1. From the **Kubernetes** tab, select **Backup Settings**.



2. From the *Backup Settings page*, click ••• for the Kubernetes cluster where the volumes exist, and select **Auto Backup New Volumes**.



3. Select the checkbox "Automatically back up future persistent volumes…", choose the backup policy that you want to apply to new volumes, and click **Save**.



Result

Now this backup policy will be applied to any new volumes created in this Kubernetes cluster.

Viewing the list of backups for each volume

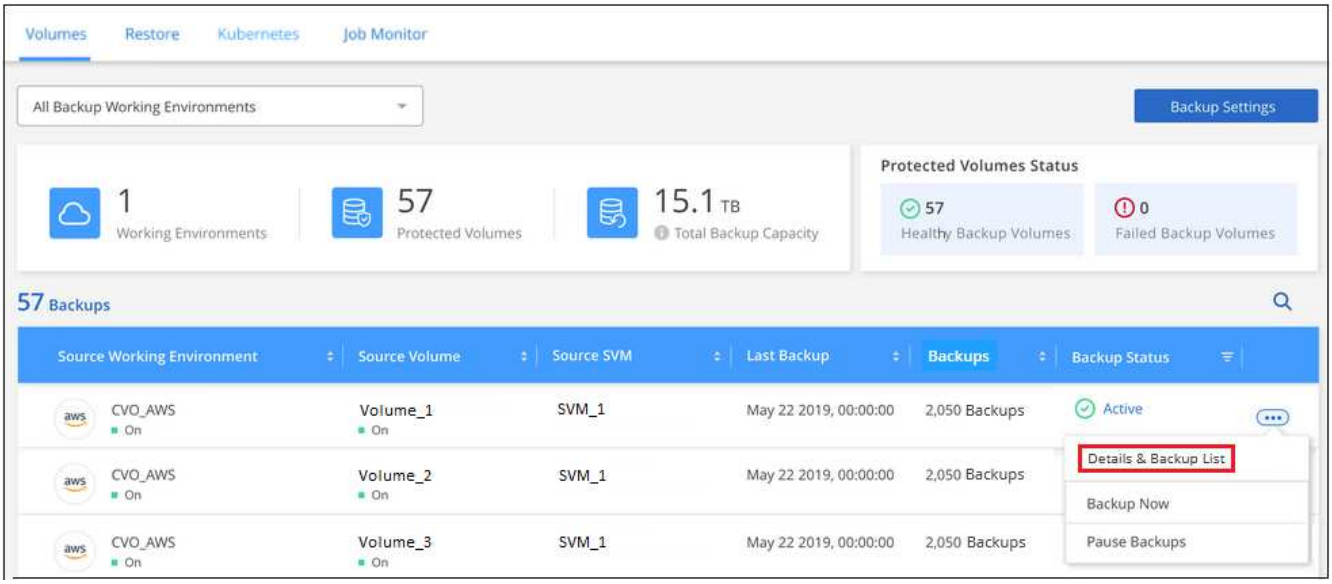
You can view the list of all backup files that exist for each volume. This page displays details about the source volume, destination location, and backup details such as last backup taken, the current backup policy, backup file size, and more.

This page also enables you perform the following tasks:

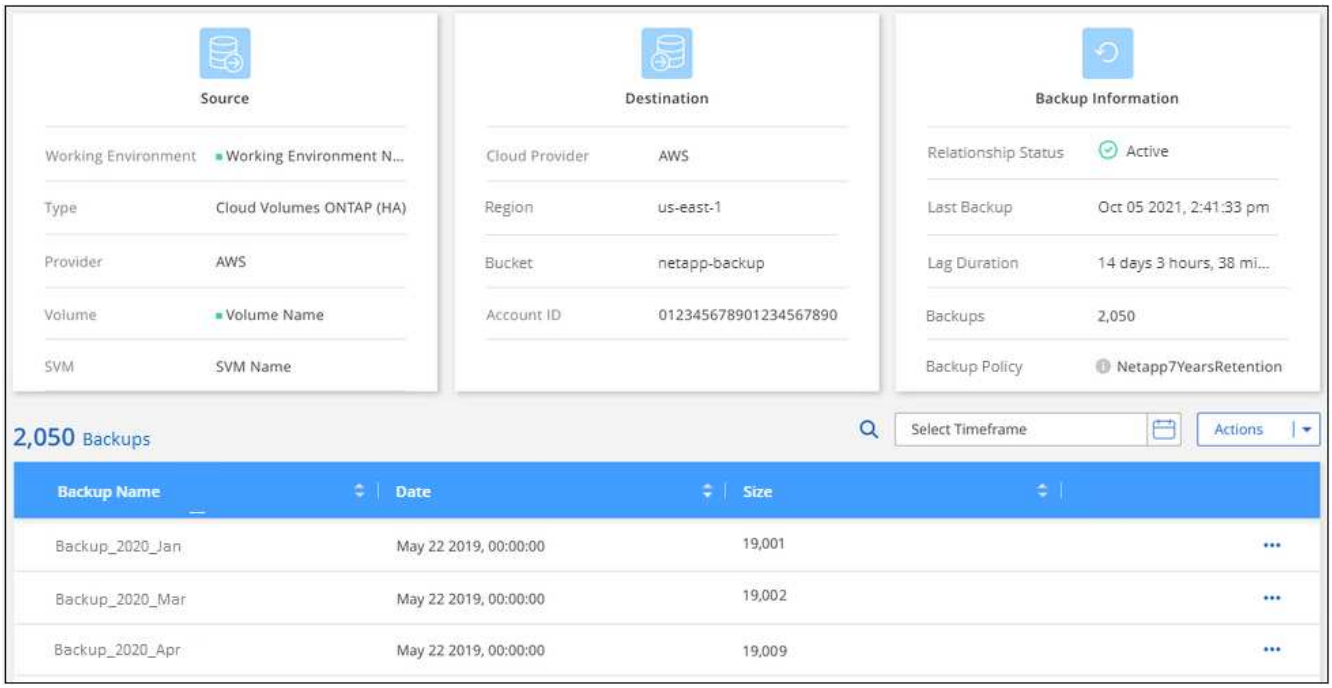
- Delete all backup files for the volume
- Delete individual backup files for the volume
- Download a backup report for the volume

Steps

1. From the **Kubernetes** tab, click ••• for the source volume and select **Details & Backup List**.



The list of all backup files is displayed along with details about the source volume, destination location, and backup details.



Deleting backups

Cloud Backup enables you to delete a single backup file, delete all backups for a volume, or delete all backups of all volumes in a Kubernetes cluster. You might want to delete all backups if you no longer need the backups or if you deleted the source volume and want to remove all backups.

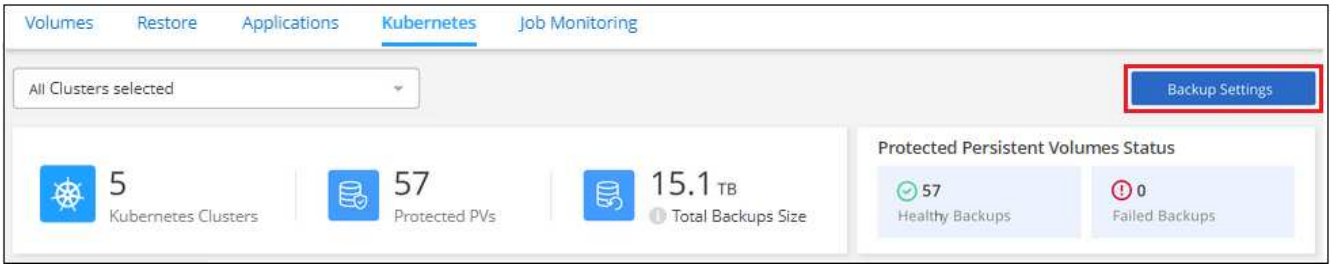
If you plan to delete a working environment or cluster that has backups, you must delete the backups **before** deleting the system. Cloud Backup doesn't automatically delete backups when you delete a system, and there is no current support in the UI to delete the backups after the system has been deleted. You'll continue to be charged for object storage costs for any remaining backups.

Deleting all backup files for a working environment

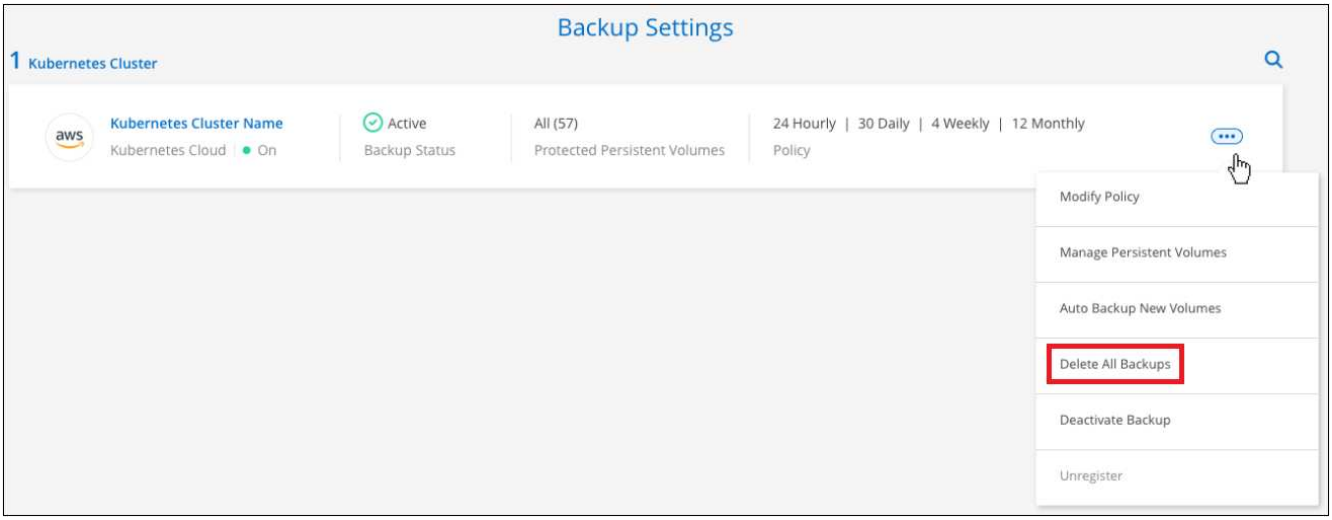
Deleting all backups for a working environment does not disable future backups of volumes in this working environment. If you want to stop creating backups of all volumes in a working environment, you can deactivate backups as described here.

Steps

1. From the **Kubernetes** tab, select **Backup Settings**.



2. Click ••• for the Kubernetes cluster where you want to delete all backups and select **Delete All Backups**.



3. In the confirmation dialog box, enter the name of the working environment and click **Delete**.

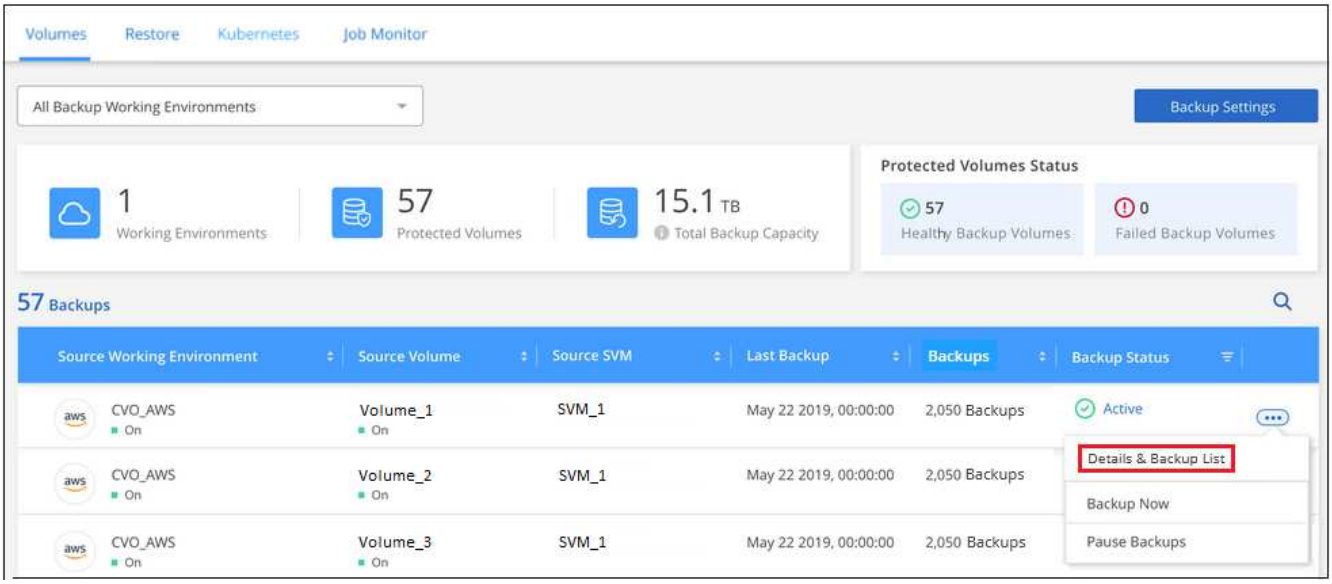
Deleting all backup files for a volume

Deleting all backups for a volume also disables future backups for that volume.

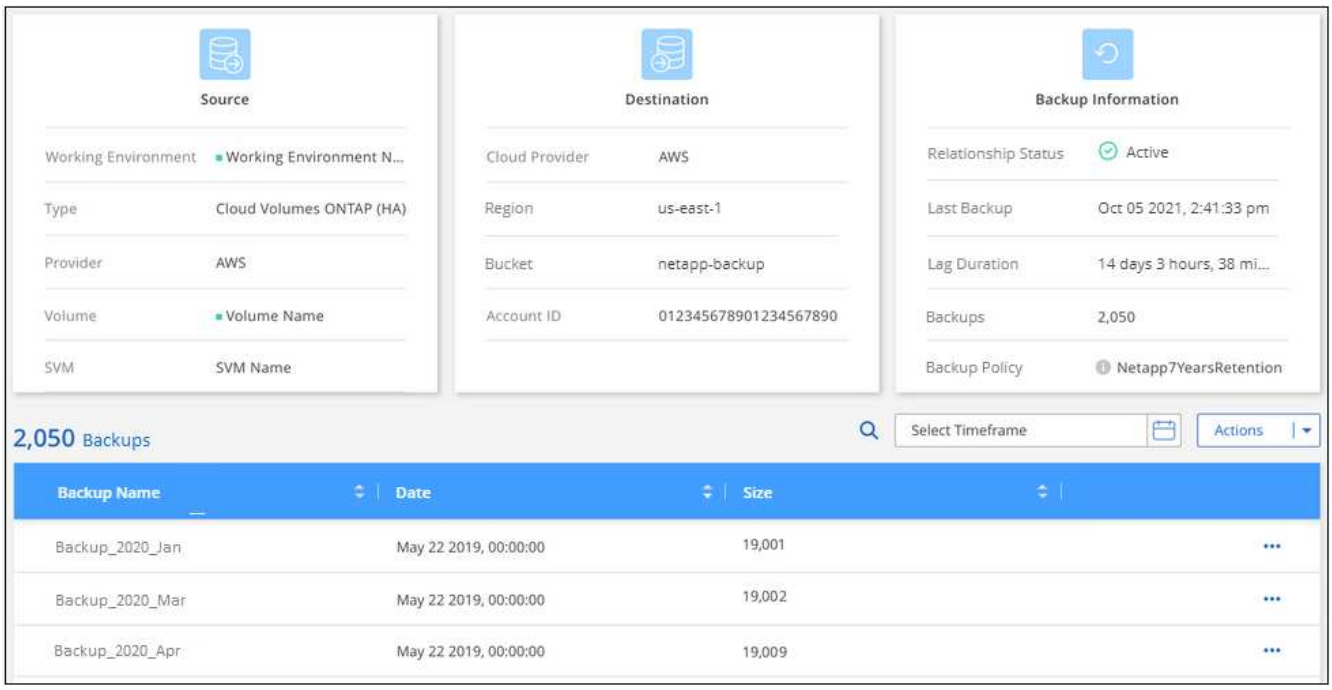
You can restart making backups for the volume at any time from the Manage Backups page.

Steps

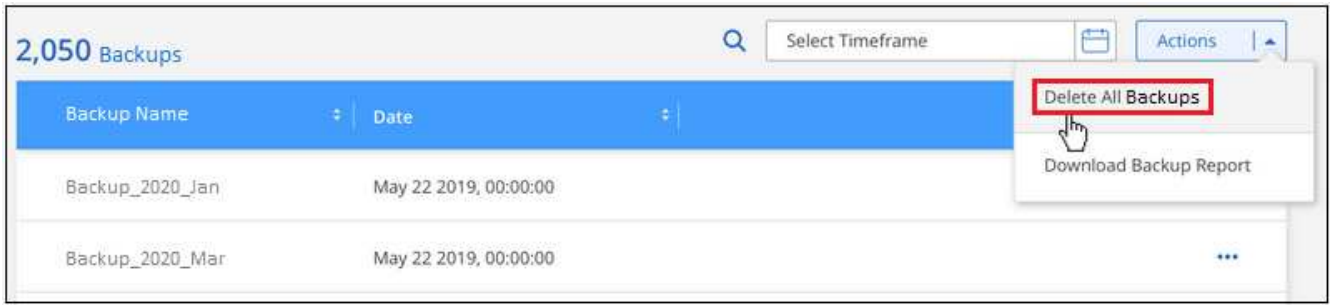
1. From the **Kubernetes** tab, click ••• for the source volume and select **Details & Backup List**.



The list of all backup files is displayed.



2. Click **Actions** > **Delete all Backups**.



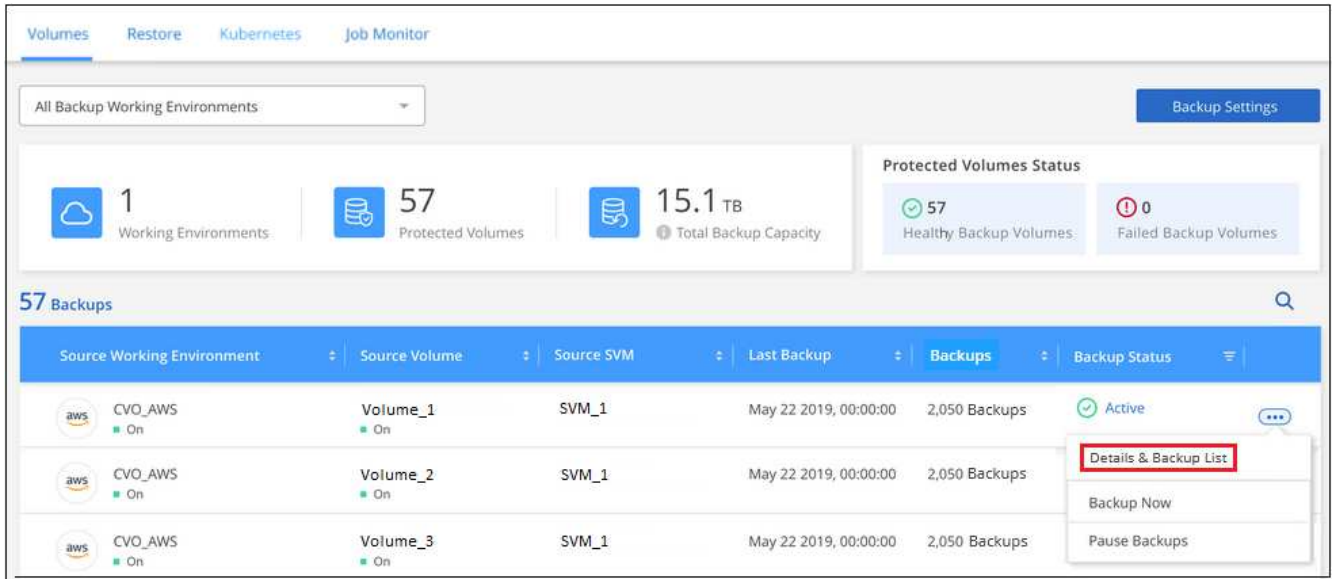
3. In the confirmation dialog box, enter the volume name and click **Delete**.

Deleting a single backup file for a volume

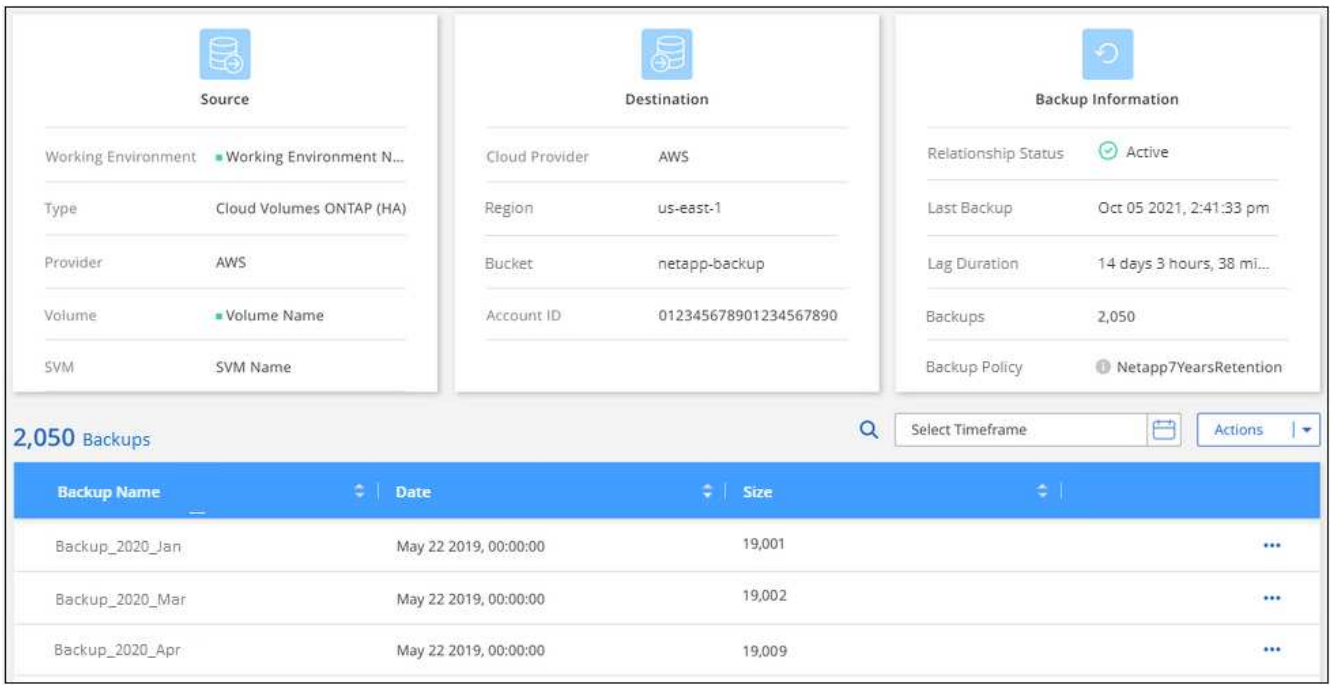
You can delete a single backup file. This feature is available only if the volume backup was created from a system with ONTAP 9.8 or greater.

Steps

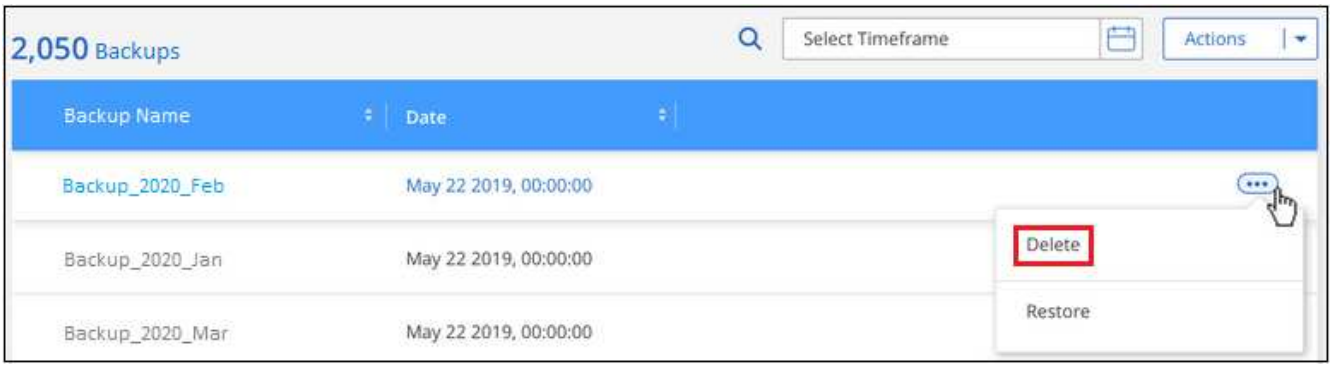
1. From the **Kubernetes** tab, click ••• for the source volume and select **Details & Backup List**.



The list of all backup files is displayed.



2. Click ••• for the volume backup file you want to delete and click **Delete**.



3. In the confirmation dialog box, click **Delete**.

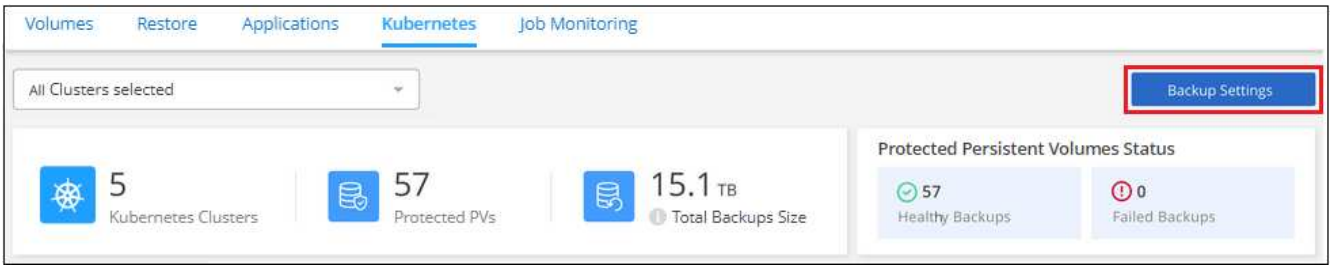
Disabling Cloud Backup for a working environment

Disabling Cloud Backup for a working environment disables backups of each volume on the system, and it also disables the ability to restore a volume. Any existing backups will not be deleted. This does not unregister the backup service from this working environment - it basically allows you to pause all backup and restore activity for a period of time.

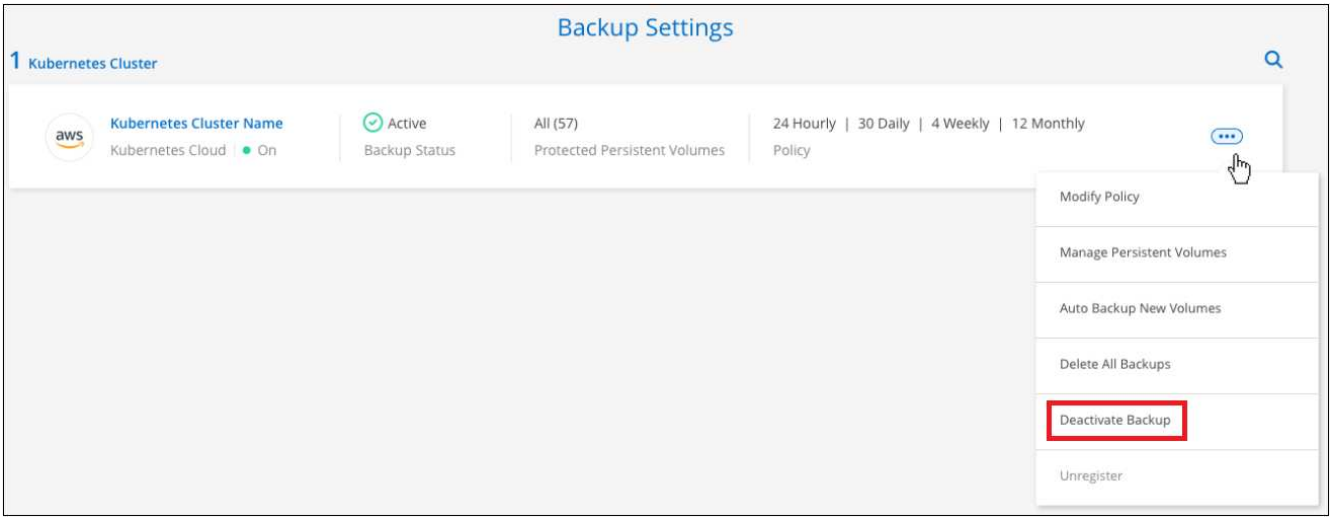
Note that you'll continue to be charged by your cloud provider for object storage costs for the capacity that your backups use unless you delete the backups.

Steps

1. From the **Kubernetes** tab, select **Backup Settings**.



2. From the *Backup Settings page*, click ••• for the working environment, or the Kubernetes cluster, where you want to disable backups and select **Deactivate Backup**.



3. In the confirmation dialog box, click **Deactivate**.

> An **Activate Backup** button appears for that working environment while backup is disabled. You can click this button when you want to re-enable backup functionality for that working environment.

Unregistering Cloud Backup for a working environment

You can unregister Cloud Backup for a working environment if you no longer want to use backup functionality and you want to stop being charged for backups in that working environment. Typically this feature is used when you're planning to delete a Kubernetes cluster, and you want to cancel the backup service.

You can also use this feature if you want to change the destination object store where your cluster backups are being stored. After you unregister Cloud Backup for the working environment, then you can enable Cloud Backup for that cluster using the new cloud provider information.

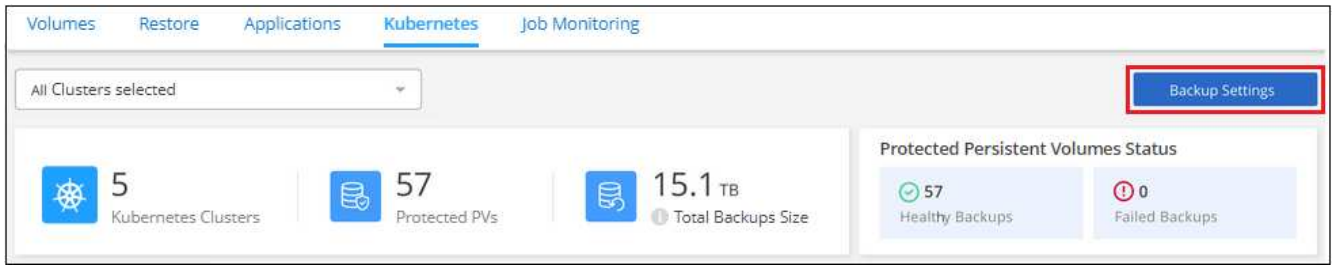
Before you can unregister Cloud Backup, you must perform the following steps, in this order:

- Deactivate Cloud Backup for the working environment
- Delete all backups for that working environment

The unregister option is not available until these two actions are complete.

Steps

1. From the **Kubernetes** tab, select **Backup Settings**.



2. From the *Backup Settings page*, click ••• for the Kubernetes cluster where you want to unregister the backup service and select **Unregister**.

3. In the confirmation dialog box, click **Unregister**.

Restoring Kubernetes data from backup files

Backups are stored in an object store in your cloud account so that you can restore data from a specific point in time. You can restore an entire Kubernetes persistent volume from a saved backup file.

You can restore a persistent volume (as a new volume) to the same working environment or to a different working environment that's using the same cloud account.

Supported working environments and object storage providers

You can restore a volume from a Kubernetes backup file to the following working environments:

Backup File Location	Destination Working Environment
Amazon S3	Kubernetes cluster in AWS
Azure Blob	Kubernetes cluster in Azure
Google Cloud Storage	Kubernetes cluster in Google

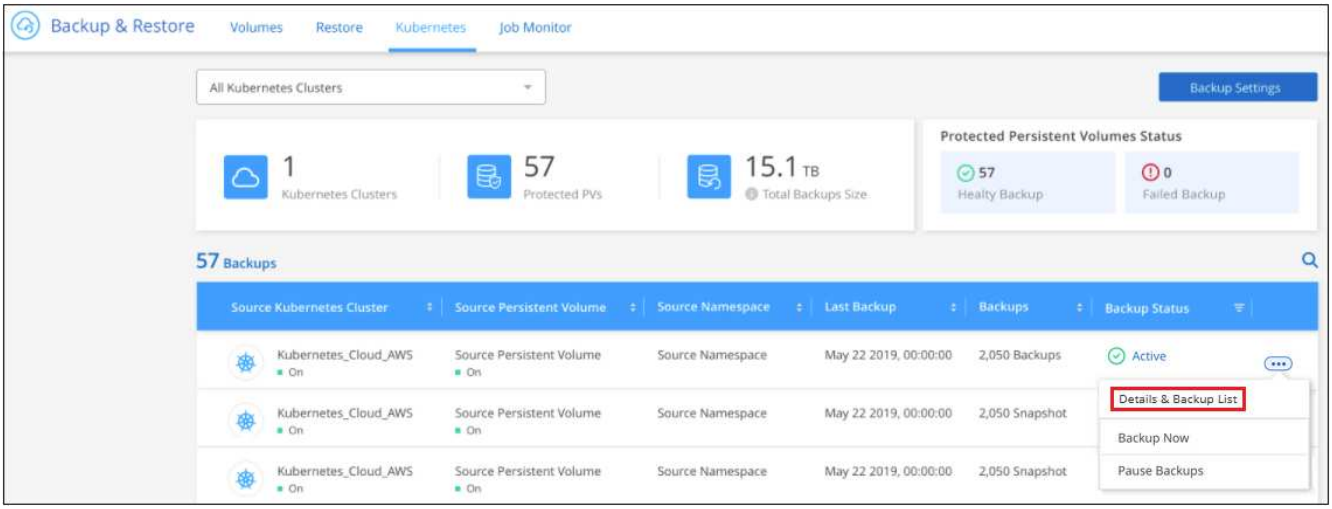
Restoring volumes from a Kubernetes backup file

When you restore a persistent volume from a backup file, Cloud Manager creates a *new* volume using the data from the backup. You can restore the data to a volume in the same Kubernetes cluster or to a different Kubernetes cluster that's located in the same cloud account as the source Kubernetes cluster.

Before you start, you should know the name of the volume you want to restore and the date of the backup file you want to use to create the newly restored volume.

Steps

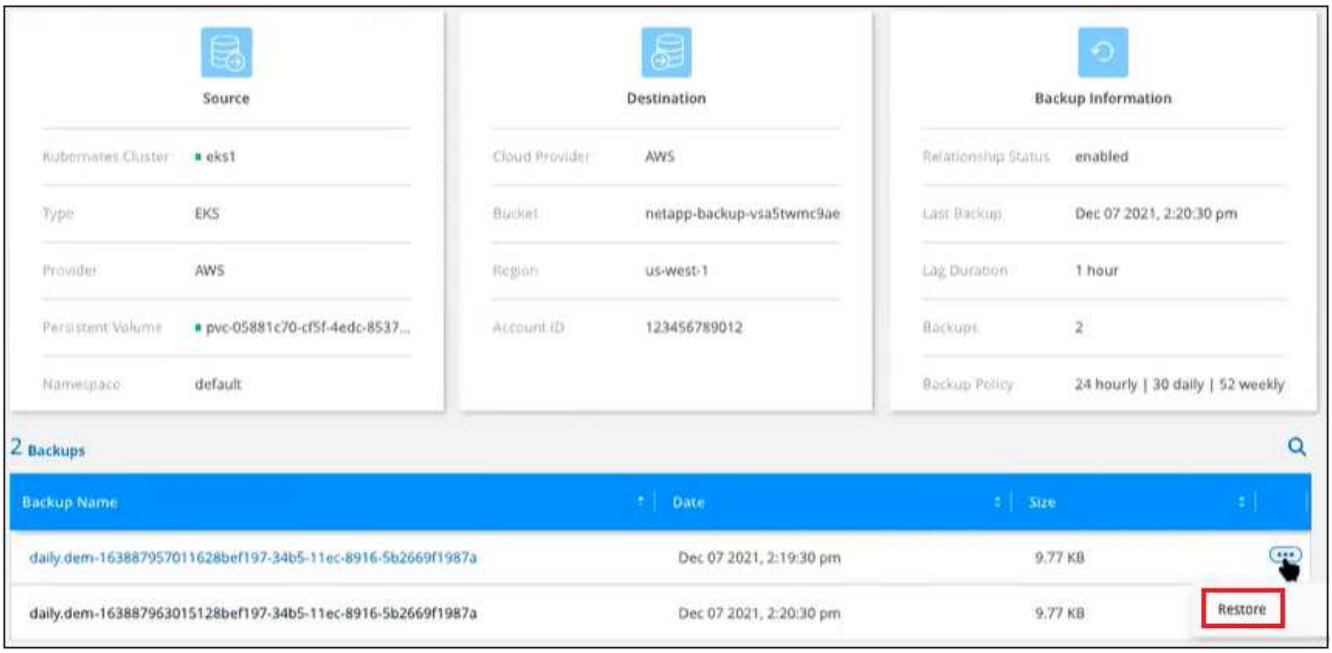
1. Select the **Backup & Restore** service.
2. Click the **Kubernetes** tab and the Kubernetes Dashboard is displayed.



3. Locate the volume you want to restore, click •••, and then click **Details & Backup List**.

   The list of all backup files for that volume is displayed along with details about the source volume,

destination location, and backup details.



4. Locate the specific backup file that you want to restore based on the date/time stamp, click •••, and then **Restore**.
5. In the *Select Destination* page, select the *Kubernetes cluster* where you want to restore the volume, the *Namespace*, the *Storage Class*, and the new *Persistent volume name*.

6. Click **Restore** and you are returned to the Kubernetes Dashboard so you can review the progress of the restore operation.

Result

Cloud Manager creates a new volume in the Kubernetes cluster based on the backup you selected. You can manage the backup settings for this new volume as required.