Back up Kubernetes cluster data

Cloud Manager

NetApp
March 08, 2022

This PDF was generated from https://docs.netapp.com/us-en/occm/task_backup_kubernetes_to_s3.html on March 08, 2022. Always check docs.netapp.com for the latest.

Table of Contents

Back up Kubernetes cluster data 1
Backing up Kubernetes persistent volume data to Amazon S3 1
Backing up Kubernetes persistent volume data to Azure Blob storage 7
Backing up Kubernetes persistent volume data to Google Cloud storage 12

Back up Kubernetes cluster data

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.

1 **Review prerequisites**

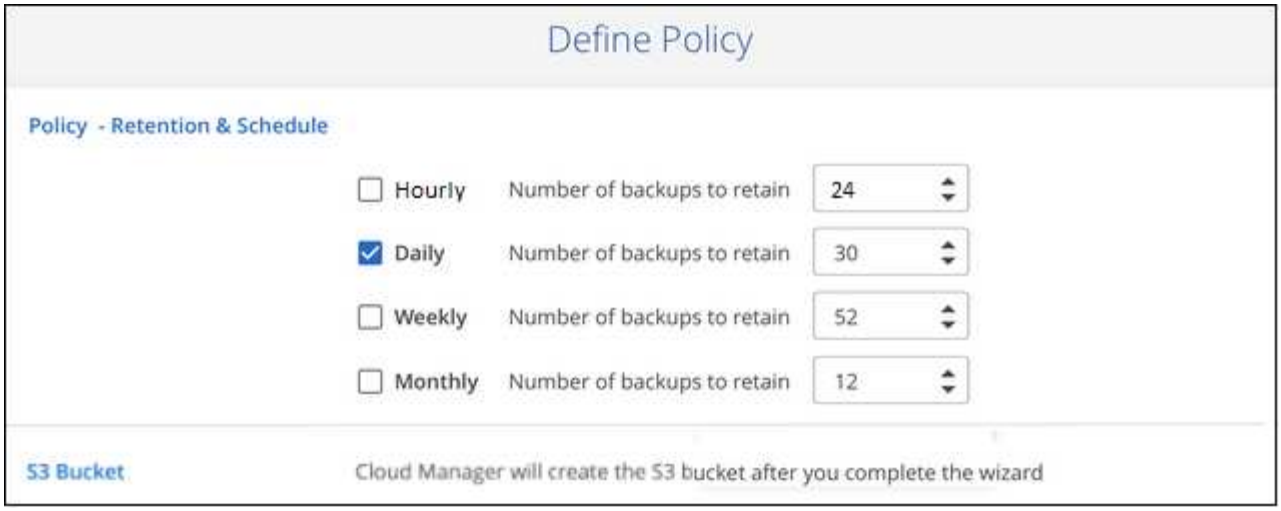
- You have discovered the Kubernetes cluster as a Cloud Manager working environment.
  - Trident must be installed on the cluster, and the Trident version must be 21.1 or greater.
  - All PVCs that will be used to create persistent volumes that you want to back up must have "snapshotPolicy" set to "default".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



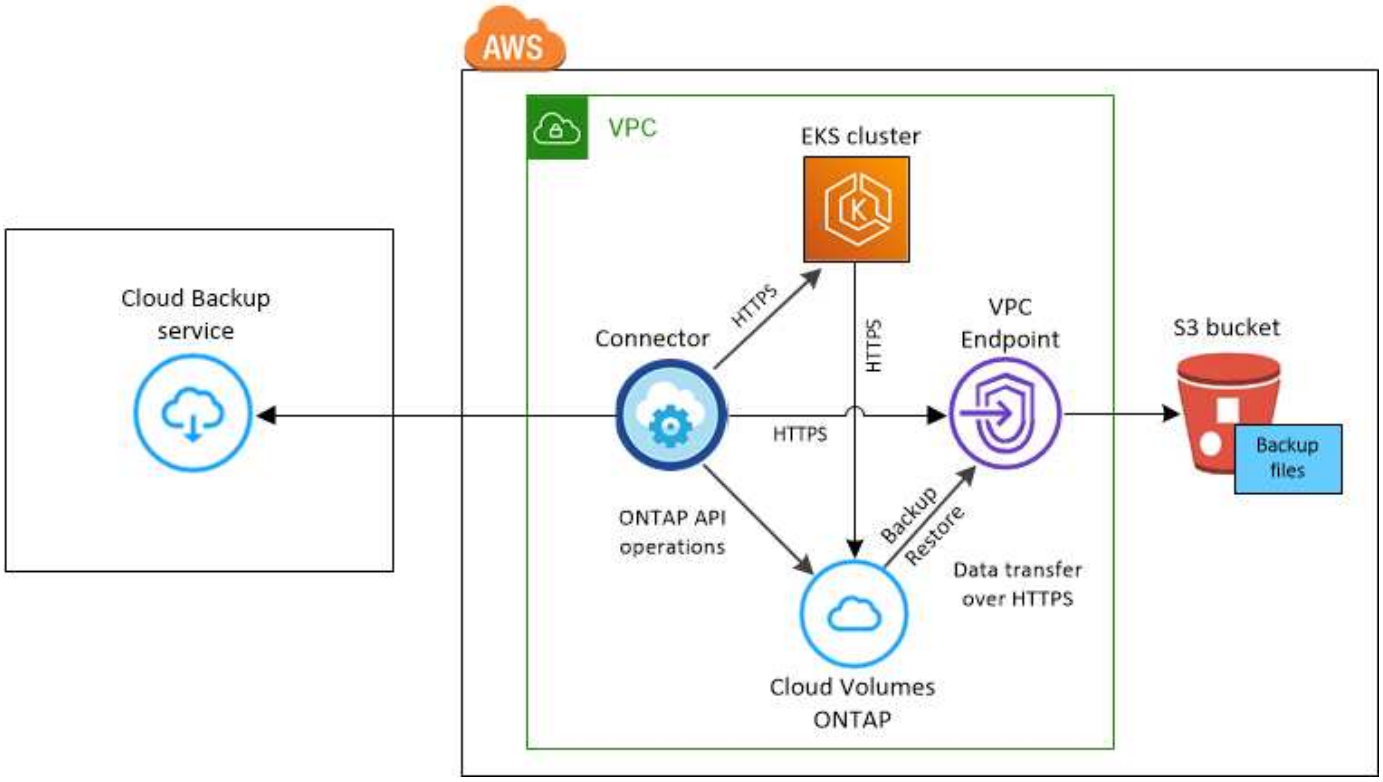
4 **Select the volumes that you want to back up**

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.

  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 on an existing system

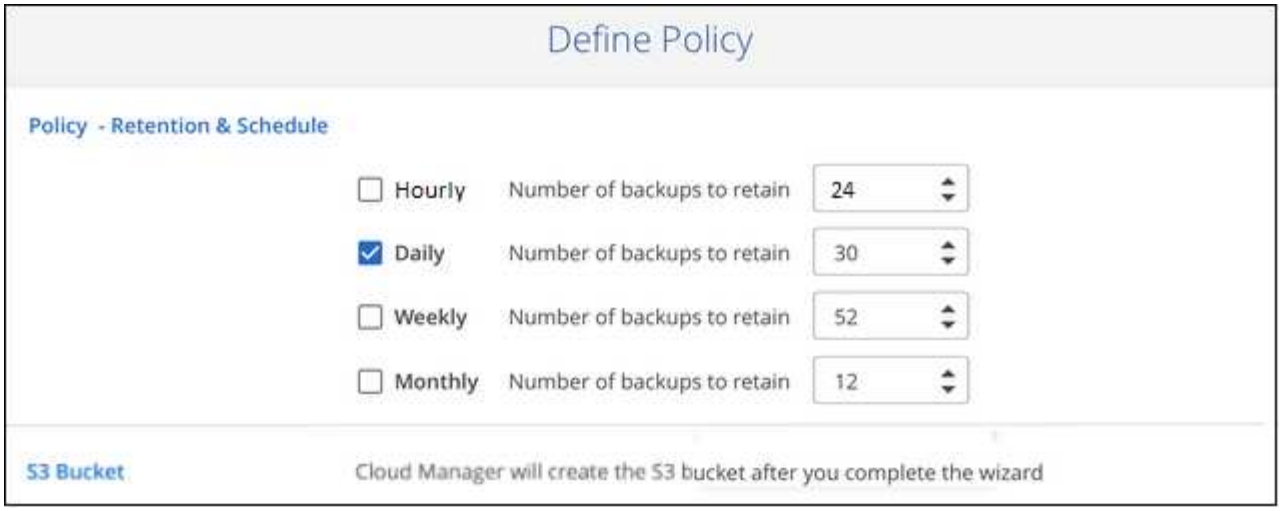
Enable Cloud Backup at any time directly from the working environment.

Steps

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

2. 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. 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.

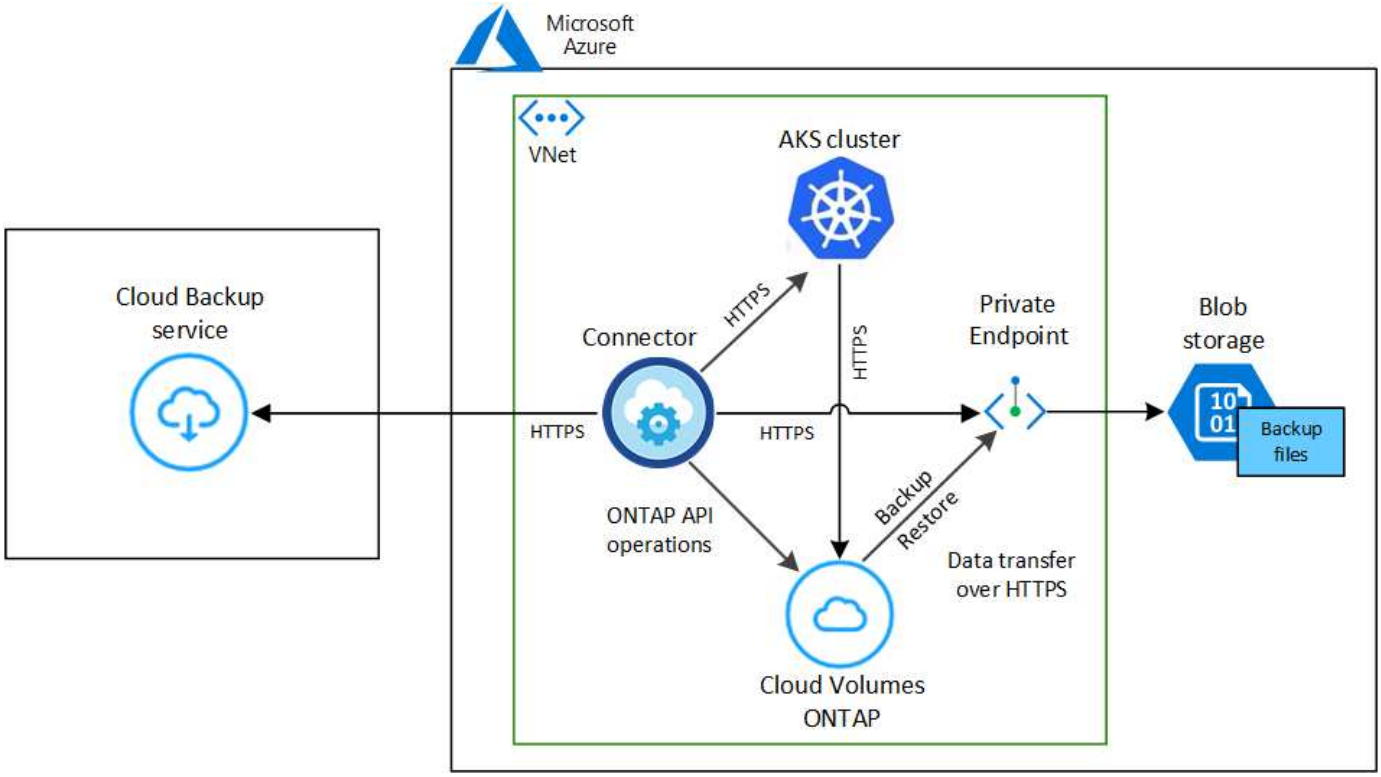
4 **Select the volumes that you want to back up**

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.

  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 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. 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. 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.

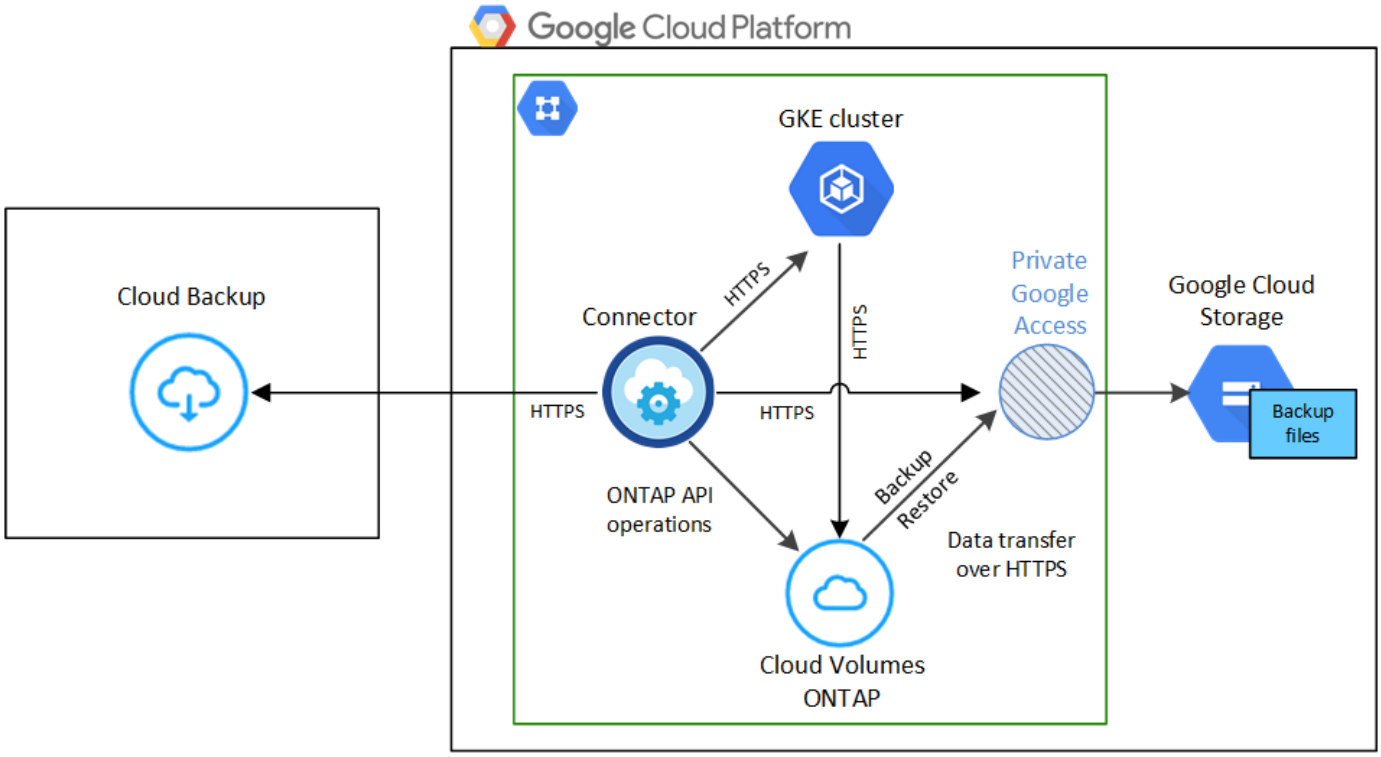
4 **Select the volumes that you want to back up**

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.

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

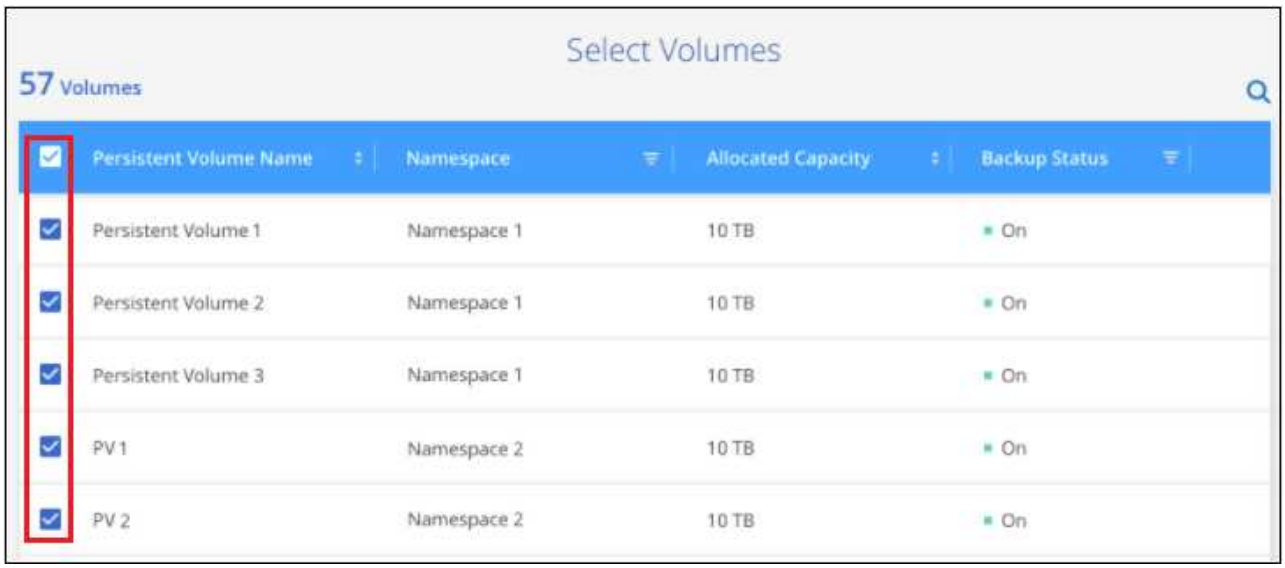
   You can define the backup schedule and choose the number of backups to retain.

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. 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).

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.