Cloud Backup documentation

Cloud Backup

NetApp
March 31, 2022

Table of Contents

Cloud Backup documentation

What's new with Cloud Backup

Learn what's new in Cloud Backup.

03 April 2022

Support for Cloud Backup for Applications 1.1.0

You can integrate Cloud Backup for Applications with Cloud Manager and on-premises SnapCenter to back up the application consistent Snapshots from on-premises ONTAP to cloud. When required you can restore from cloud to on-premises SnapCenter Server.

You can back up Oracle and Microsoft SQL applications data from on-premises ONTAP to either Amazon Web Services or Microsoft Azure.

Learn more about protecting on-premises applications data to cloud.

Support has been added to back up on-premises ONTAP cluster data in sites without internet access.

If your on-prem ONTAP cluster resides in a site with no internet access, also known as a dark site or offline site, now you can use Cloud Backup to back up volume data to NetApp StorageGRID systems that resides in the same site. This functionality requires that the Cloud Manager Connector (version 3.9.17 or greater) is deployed in the offline site. See how to back up data in an offline site.

New Search & Restore feature to search for volumes or files across all ONTAP backup files.

Now you can search for a volume or file across **all backup files** by partial or full volume name, partial or full file name, size range, and additional search filters. This is a great new way to find the data you want to restore if you are not sure which cluster or volume was the source for the data. Learn how to use Search & Restore.

03 March 2022

Ability to back up persistent volumes from your GKE Kubernetes clusters to Google Cloud storage.

If your GKE cluster has NetApp Astra Trident installed, and it's using Cloud Volumes ONTAP for GCP as backend storage for the cluster, then you can back up and restore your persistent volumes to and from Google Cloud storage. Go here for details.

The Beta capability to use Cloud Data Sense to scan your Cloud Backup files has been discontinued in this release.

14 February 2022

Now you can assign backup policies to individual volumes in a single cluster.

In the past you could assign only a single backup policy to all volumes in a cluster. Now you can create multiple backup policies for a single cluster and apply different policies to different volumes. See how to create

new backup policies for a cluster and assign them to selected volumes.

A new option enables you to automatically apply a default backup policy to newly created volumes.

In the past, new volumes created in a working environment after Cloud Backup was activated required that you manually apply a backup policy. Now, regardless of if the volume was created in Cloud Manager, System Manager, the CLI, or by using APIs, Cloud Backup will discover the volume and apply the backup policy you have chosen as the default policy.

This option is available when enabling backup in a new working environment, or from the *Manage Volumes* page for existing working environments.

New Job Monitor is available to see the in-process status of all backup and restore jobs.

The Job Monitor can be very helpful when you have initiated an operation against multiple volumes, like changing the backup policy, or deleting backups, so you can see when the operation has completed on all volumes. See how to use the Job Monitor.

2 January 2022

Ability to back up persistent volumes from your AKS Kubernetes clusters to Azure Blob storage.

If your AKS cluster has NetApp Astra Trident installed, and it's using Cloud Volumes ONTAP for Azure as backend storage for the cluster, then you can back up and restore volumes to and from Azure Blob storage. Go here for details.

Cloud Backup service charges have been changed in this release to align more closely with industry standards.

Instead of paying NetApp for capacity based on the size of your backup files, now you pay only for the data that you protect, calculated by the logical used capacity (before ONTAP efficiencies) of the source ONTAP volumes which are being backed up. This capacity is also known as Front-End Terabytes (FETB).

28 Nov 2021

Ability to back up persistent volumes from your EKS Kubernetes clusters to Amazon S3.

If your EKS cluster has NetApp Astra Trident installed, and it's using Cloud Volumes ONTAP for AWS as backend storage for the cluster, then you can back up and restore volumes to and from Amazon S3. Go here for details.

Enhanced functionality to back up DP volumes.

Cloud Backup now supports creating backups of DP volumes that exist on the target ONTAP system in an SVM-DR relationship. There are a few restrictions, so see the limitations for details.

5 Nov 2021

Ability to select a private endpoint when restoring a volume to an on-premises ONTAP system.

When restoring a volume to an on-premises ONTAP system from a backup file that resides on Amazon S3 or Azure Blob, now you can select a private endpoint that connects to your on-prem system privately and securely.

Now you can tier older backup files to archival storage after a number of days to save costs.

If your cluster is running ONTAP 9.10.1 or greater, and you're using AWS or Azure cloud storage, you can enable tiering of backups to archival storage. See more information about AWS S3 archival storage classes and Azure Blob archival access tiers.

Cloud Backup BYOL licenses have moved to the Data Services Licenses tab in the Digital Wallet.

BYOL licensing for Cloud Backup has moved from the Cloud Backup Licenses tab to the Data Services Licenses tab in the Cloud Manager Digital Wallet.

4 Oct 2021

Backup file size is now available in the Backup page when performing a volume or file restore.

This is useful if you want to delete large backup files that are unnecessary, or so you can compare backup file sizes to identify any abnormal backup files that could be the result of a malicious software attack.

TCO calculator is available to compare Cloud Backup costs.

The Total Cost of Ownership calculator helps you understand the total cost of ownership for Cloud Backup, and to compare these costs to traditional backup solutions and estimate potential savings. Check it out here.

Ability to unregister Cloud Backup for a working environment.

Now you can easily unregister Cloud Backup for a working environment if you no longer want to use backup functionality (or be charged) for that working environment.

2 September 2021

Ability to create an on-demand backup of a volume.

Now you can create an on-demand backup at any time to capture the current state of a volume. This is useful if important changes have been made to a volume and you don't want to wait for the next scheduled backup to protect that data.

See how to create an on-demand backup.

Ability to define a Private Interface connection for secure backups to Amazon S3.

When configuring backups to Amazon S3 from an on-premises ONTAP system, now you can define a connection to a Private Interface Endpoint in the activation wizard. This allows you to use a network interface that connects your on-prem system privately and securely to a service powered by AWS PrivateLink. See details about this option.

Now you can choose your own customer-managed keys for data encryption when backing up data to Amazon S3.

For additional security and control, you can choose your own customer-managed keys for data encryption in the activation wizard instead of using the default Amazon S3 encryption keys. This is available when configuring backups from an on-premises ONTAP system or from a Cloud Volumes ONTAP system in AWS.

Now you can restore files from directories that have more than 30,000 files.

1 Aug 2021

Ability to define a Private Endpoint connection for secure backups to Azure Blob.

When configuring backups to Azure Blob from an on-premises ONTAP system, you can define a connection to an Azure Private Endpoint in the activation wizard. This allows you to use a network interface that connects you privately and securely to a service powered by Azure Private Link.

An Hourly backup policy is now supported.

This new policy is in addition to the existing Daily, Weekly, and Monthly policies. The Hourly backup policy provides a minimal Recovery Point Objective (RPO).

7 July 2021

Now you can create backups using different accounts and in different regions.

Cloud Backup now allows you to create backups using a different account/subscription than the one you are using for your Cloud Volumes ONTAP system. You can also create backup files in a different region than the one in which your Cloud Volumes ONTAP system is deployed.

This capability is available when using when using AWS or Azure, and only when enabling backup on an existing working environment - it is not available when creating a new Cloud Volumes ONTAP working environment.

Now you can choose your own customer-managed keys for data encryption when backing up data to Azure Blob.

For additional security and control, you can choose your own customer-managed keys for data encryption in the activation wizard instead of using the default Microsoft-managed encryption keys. This is available when configuring backups from an on-premises ONTAP system or from a Cloud Volumes ONTAP system in Azure.

Now you can restore up to 100 files at a time when using single-file restore.

7 June 2021

Limitations lifted for DP volumes when using ONTAP 9.8 or greater.

Two known limitations for backing up data protection (DP) volumes have been resolved:

- Before, cascaded backup worked only if the SnapMirror relationship type was Mirror-Vault or Vault. Now you can make backups if the relationship type is MirrorAllSnapshots.
- Cloud Backup now can use any label for the backup as long as it is configured in the SnapMirror policy. The restriction of requiring labels with the names daily, weekly, or monthly is gone.

5 May 2021

Back up on-prem cluster data to Google Cloud Storage or NetApp StorageGRID systems.

Now you can create backups from your on-premises ONTAP systems to Google Cloud Storage or to your NetApp StorageGRID systems. See Backing up to Google Cloud Storage and Backing up to StorageGRID for details.

Now you can use System Manager to perform Cloud Backup operations.

A new feature in ONTAP 9.9.1 enables you to use System Manager to send backups of your on-premises ONTAP volumes to object storage you've set up through Cloud Backup. See how to use System Manager to back up your volumes to the cloud using Cloud Backup.

Backup policies have been improved with a few enhancements.

- Now you create a custom policy that includes a combination of daily, weekly, and monthly backups.
- When you change a backup policy, the change applies to all new backups **and** to all volumes using the original backup policy. In the past the change only applied to new volume backups.

Miscellaneous backup and restore improvements.

- When configuring the cloud destination for your backup files, now you can select a different region than the region in which the Cloud Volumes ONTAP system resides.
- The number of backup files you can create for a single volume has been increased from 1,019 to 4,000.
- In addition to the earlier ability to delete all backup files for a single volume, now you can delete just a single backup file for a volume, or you can delete all backup files for an entire working environment, if needed.

Get started

Learn about Cloud Backup

Cloud Backup is a service for Cloud Manager working environments that provides backup and restore capabilities for protection and long-term archive of your 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. When backing up ONTAP data, you can also choose to restore or one or more *files* from a backup to the same or different working environment.

Learn more about Cloud Backup.

Backup & Restore can be used to:

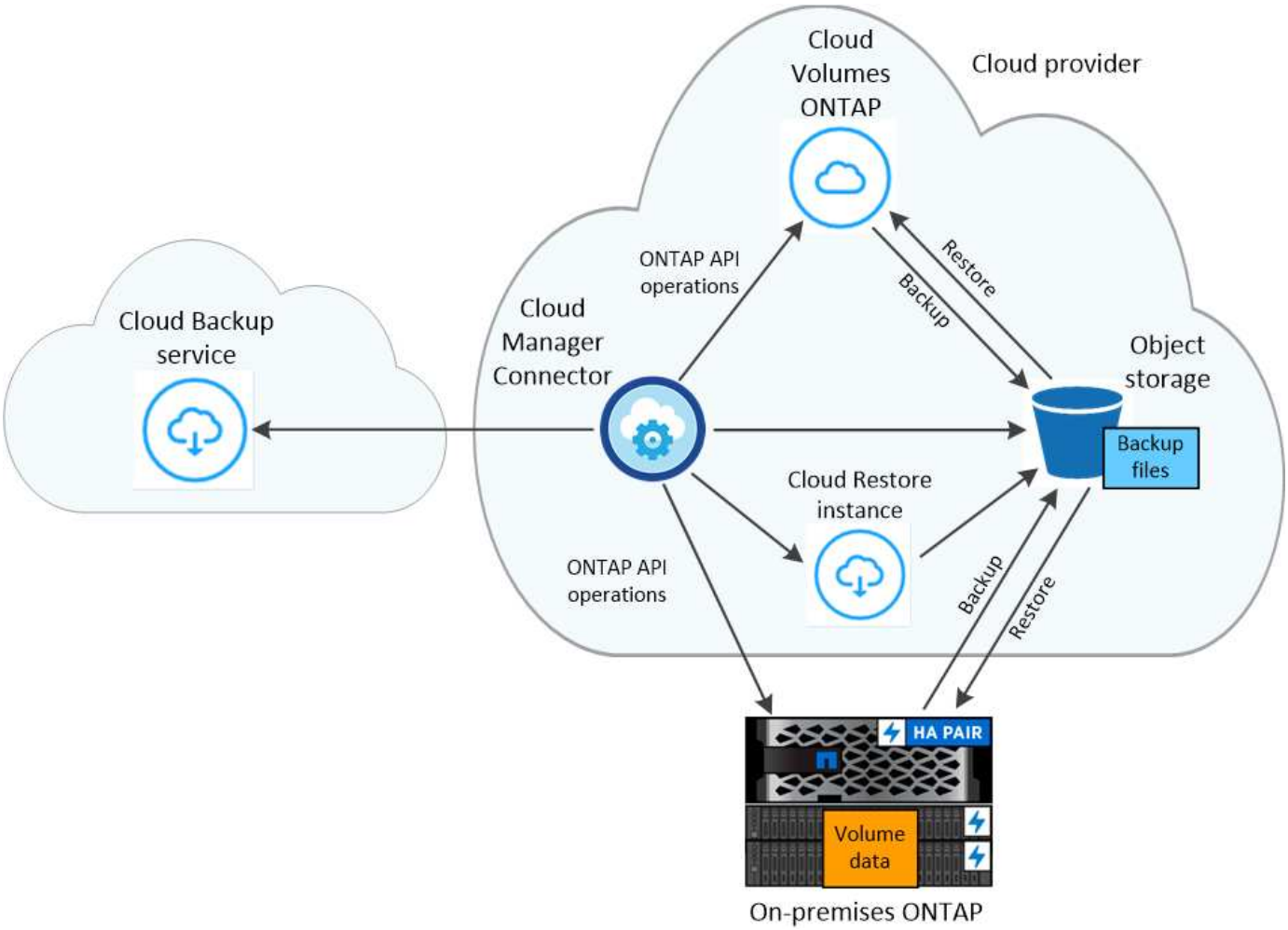
- Back up and Restore ONTAP volumes from Cloud Volumes ONTAP and on-premises ONTAP systems. See detailed features here.
- Back up and Restore Kubernetes persistent volumes. See detailed features here.
- Back up the application consistent Snapshots from on-premises ONTAP to cloud using Cloud Backup for Applications. See detailed features here.

How Cloud Backup works

When you enable Cloud Backup on a Cloud Volumes ONTAP or on-premises ONTAP system, the service performs a full backup of your data. Volume snapshots are not included in the backup image. 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.

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

The following image shows the relationship between each component:



Where backups reside

Backup copies are stored in an object store that Cloud Manager creates in your cloud account. There's one object store per cluster/working environment, and Cloud Manager names the object store as follows: "netapp-backup-clusteruuid". Be sure not to delete this object store.

- In AWS, Cloud Manager enables the Amazon S3 Block Public Access feature on the S3 bucket.
- In Azure, Cloud Manager uses a new or existing resource group with a storage account for the Blob container. Cloud Manager blocks public access to your blob data by default.
- In GCP, Cloud Manager uses a new or existing project with a storage account for the Google Cloud Storage bucket.
- In StorageGRID, Cloud Manager uses an existing storage account for the object store bucket.

Backups are taken at midnight

- Hourly backups start 5 minutes past the hour, every hour.
- Daily backups start just after midnight each day.
- Weekly backups start just after midnight on Sunday mornings.
- Monthly backups start just after midnight on the first day of each month.

The start time is based on the time zone set on each source ONTAP system. You can't schedule backup operations at a user-specified time from the UI. For more information, contact your System Engineer.

Backup copies are associated with your NetApp account

Backup copies are associated with the NetApp account in which the Connector resides.

If you have multiple Connectors in the same NetApp account, each Connector will display the same list of backups. That includes the backups associated with Cloud Volumes ONTAP and on-premises ONTAP instances from other Connectors.

Set up licensing for Cloud Backup

A 30-day free trial of Cloud Backup starts when you enable the Cloud Backup service. When the free trial ends, you'll need to pay for Cloud Backup using a pay-as-you-go (PAYGO) subscription through your cloud provider, or by purchasing a bring-your-own license (BYOL) from NetApp.

A few notes before you read any further:

- If you've already subscribed to the Cloud Manager pay-as-you-go (PAYGO) subscription in your cloud provider's marketplace, then you're automatically subscribed to Cloud Backup as well. You won't need to subscribe again.
- The Cloud Backup bring-your-own-license (BYOL) is a floating license that you can use across all systems associated with your Cloud Manager account.
- When backing up ONTAP data to StorageGRID, you need a BYOL license, but there's no cost for cloud provider storage space.

Learn more about the licensing and costs related to Cloud Backup.

Use a Cloud Backup PAYGO subscription

For pay-as-you-go you'll pay your cloud provider for object storage costs and for NetApp backup licensing costs. Use these links to subscribe to Cloud Backup from your cloud provider marketplace:

- AWS: Go to the Cloud Manager Marketplace offering for pricing details.
- Azure: Go to the Cloud Manager Marketplace offering for pricing details.
- GCP: Go to the Cloud Manager Marketplace offering for pricing details.

Subscribe to yearly contracts through AWS

There are two annual contracts available from the AWS Marketplace for Cloud Volumes ONTAP and on-premises ONTAP systems:

- An annual contract that enables you to back up Cloud Volumes ONTAP data and on-premises ONTAP data.

  Go to the AWS Marketplace page to view pricing details.

  If you want to use this option, set up your subscription from the Marketplace page and then associate the subscription with your AWS credentials. Note that you'll also need to pay for your Cloud Volumes ONTAP systems using this annual contract subscription since you can assign only one active subscription to your AWS credentials in Cloud Manager.

- A Professional Package that enables you to bundle Cloud Volumes ONTAP and Cloud Backup by using an annual contract for 1, 2, or 3 years. Payment is per TiB. This option doesn't enable you to back up on-premises ONTAP data.

  Go to the AWS Marketplace page to view pricing details and go to the Cloud Volumes ONTAP Release Notes to learn more about this licensing option.

  If you want to use this option, you can set up the annual contract when you create a Cloud Volumes ONTAP working environment and Cloud Manager prompts you to subscribe to the AWS Marketplace.

Use a Cloud Backup BYOL license

Bring-your-own licenses from NetApp provide 1-, 2-, or 3-year terms. You pay only for the data that you protect, calculated by the logical used capacity (*before* any efficiencies) of the source ONTAP volumes which are being backed up. This capacity is also known as Front-End Terabytes (FETB).

The BYOL Cloud Backup license is a floating license where the total capacity is shared across all systems associated with your Cloud Manager account. For ONTAP systems you can get a rough estimate of the capacity you'll need by running the ONTAP command `volume show-space -logical-used` for the volumes you plan to back up.

If you don't have a Cloud Backup BYOL license, click the chat icon in the lower-right of Cloud Manager to purchase one.

Optionally, if you have an unassigned node-based license for Cloud Volumes ONTAP that you won't be using, you can convert it to a Cloud Backup license with the same dollar-equivalence and the same expiration date. Go here for details.

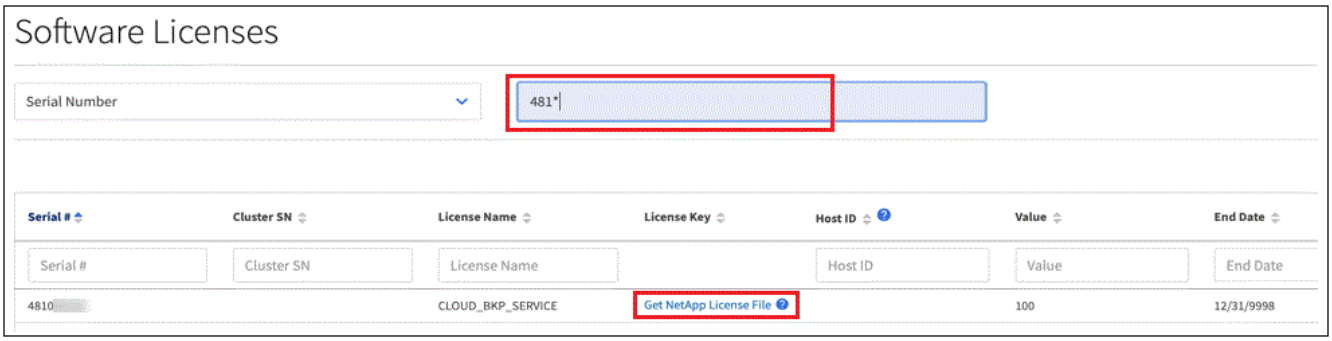
You use the Digital Wallet page in Cloud Manager to manage BYOL licenses for Cloud Backup. You can add new licenses and update existing licenses.

Obtain your Cloud Backup license file

After you've purchased your Cloud Backup license, you activate the license in Cloud Manager by entering the Cloud Backup serial number and NSS account, or by uploading the NLF license file. The steps below show how to get the NLF license file if you plan to use that method.

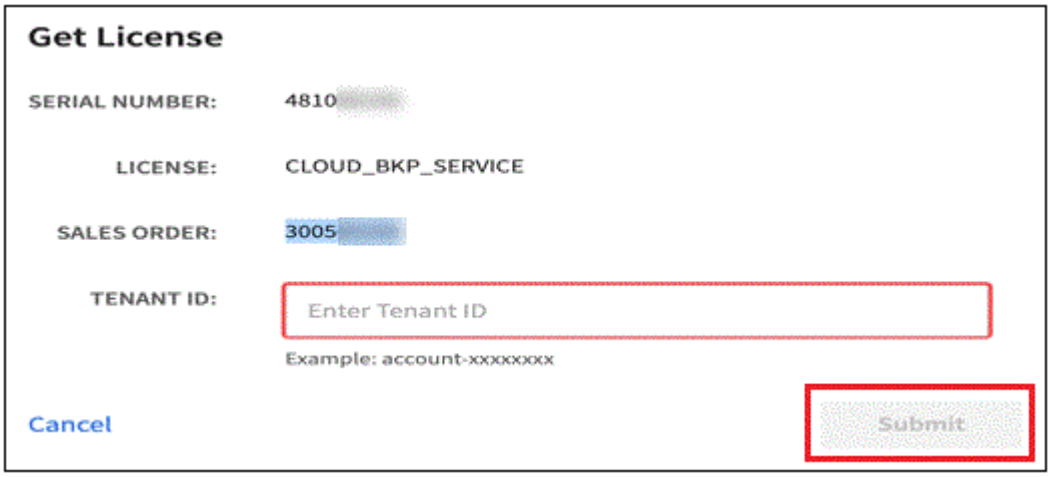
Steps

1. Sign in to the NetApp Support Site and click **Systems > Software Licenses**.
2. Enter your Cloud Backup license serial number.



3. In the **License Key** column, click **Get NetApp License File**.

4. Enter your Cloud Manager Account ID (this is called a Tenant ID on the support site) and click **Submit** to download the license file.



You can find your Cloud Manager Account ID by selecting the **Account** drop-down from the top of Cloud Manager, and then clicking **Manage Account** next to your account. Your Account ID is in the Overview tab.

Add Cloud Backup BYOL licenses to your account

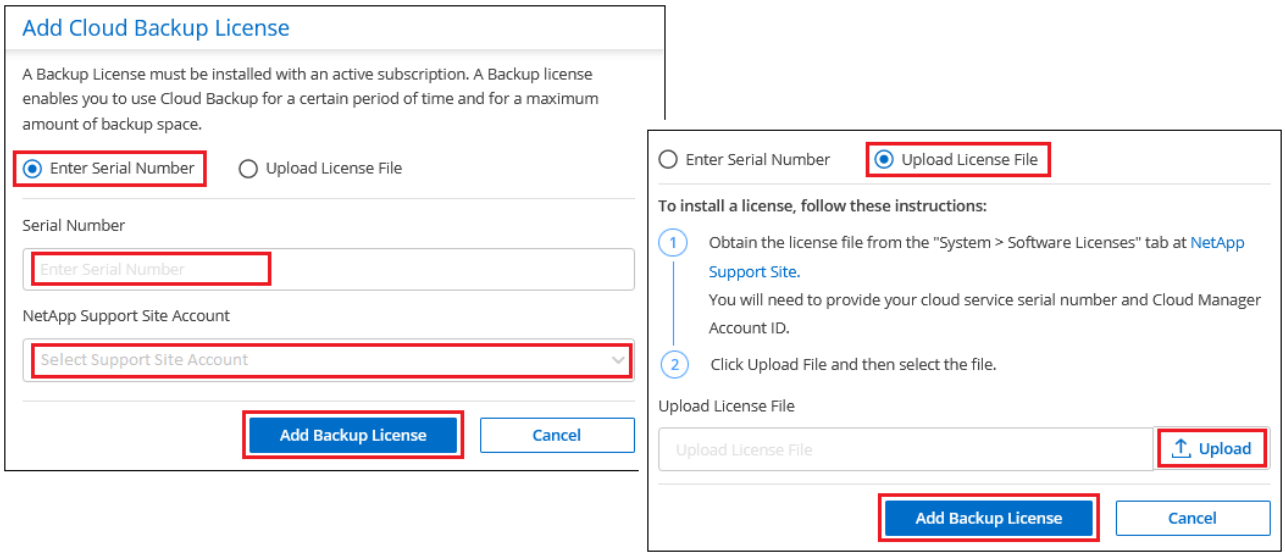
After you purchase a Cloud Backup license for your NetApp account, you need to add the license to Cloud Manager.

Steps

1. Click **All Services > Digital Wallet > Data Services Licenses**.
2. Click **Add License**.
3. In the *Add License* dialog, enter the license information and click **Add License**:
   - If you have the backup license serial number and know your NSS account, select the **Enter Serial Number** option and enter that information.

     If your NetApp Support Site account isn't available from the drop-down list, add the NSS account to Cloud Manager.

   - If you have the backup license file, select the **Upload License File** option and follow the prompts to attach the file.

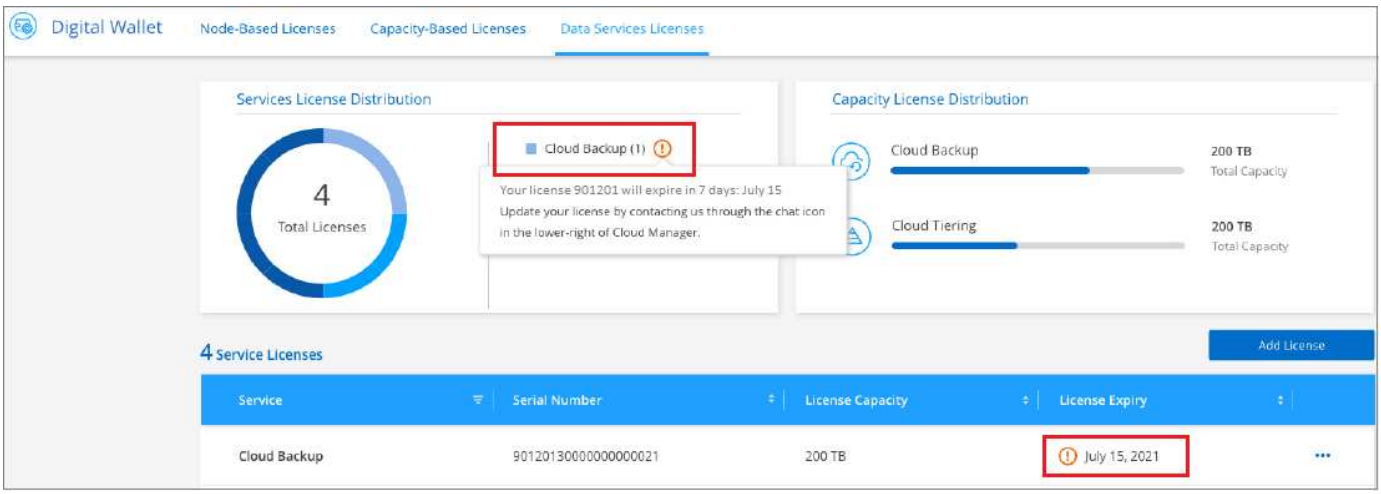


Result

Cloud Manager adds the license so that Cloud Backup is active.

Update a Cloud Backup BYOL license

If your licensed term is nearing the expiration date, or if your licensed capacity is reaching the limit, you'll be notified in the Backup UI. This status also appears in the Digital Wallet page and in Notifications.



You can update your Cloud Backup license before it expires so that there is no interruption in your ability to back up and restore your data.

Steps

1. Click the chat icon in the lower-right of Cloud Manager, or contact Support, to request an extension to your term or additional capacity to your Cloud Backup license for the particular serial number.

   After you pay for the license and it is registered with the NetApp Support Site, Cloud Manager automatically updates the license in the Digital Wallet and the Data Services Licenses page will reflect the change in 5 to 10 minutes.

2. If Cloud Manager can't automatically update the license, then you'll need to manually upload the license file.

a. You can obtain the license file from the NetApp Support Site.

b. On the Digital Wallet page *Data Services Licenses* tab, click ••• for the service serial number you are updating, and click **Update License**.

c. In the *Update License* page, upload the license file and click **Update License**.

Result

Cloud Manager updates the license so that Cloud Backup continues to be active.

BYOL license considerations

When using a Cloud Backup BYOL license, Cloud Manager displays a warning in the user interface when the size of all the data you are backing up is nearing the capacity limit or nearing the license expiration date. You receive these warnings:

- When backups have reached 80% of licensed capacity, and again when you have reached the limit
- 30 days before a license is due to expire, and again when the license expires

Use the chat icon in the lower right of the Cloud Manager interface to renew your license when you see these warnings.

Two things can happen when your license expires:

- If the account you are using has a marketplace account, the backup service continues to run, but you are shifted over to a PAYGO licensing model. You are charged for the capacity that your backups are using.
- If the account you are does not have a marketplace account, the backup service continues to run, but you will continue to see the warnings.

Once you renew your BYOL subscription, Cloud Manager automatically updates the license. If Cloud Manager can't access the license file over the secure internet connection, you can obtain the file yourself and manually upload it to Cloud Manager. For instructions, see how to update a Cloud Backup license.

Systems that were shifted over to a PAYGO license are returned to the BYOL license automatically. And systems that were running without a license will stop seeing the warnings and will be charged for backup activity that occurred while the license was expired.

Back up and restore ONTAP data

Protect your ONTAP cluster data using Cloud Backup

Cloud Backup provides backup and restore capabilities for protection and long-term archive of your ONTAP cluster data. Backups are automatically generated and stored in an object store in your public or private cloud account, independent of volume Snapshot copies used for near-term recovery or cloning.

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

Features

Backup features:

- Back up independent copies of your data 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.
- Tier older backup files to archival storage to save costs (supported with AWS and Azure when using ONTAP 9.10.1+)
- Back up from cloud to cloud, and from on-premises systems to public or private cloud.
- For Cloud Volumes ONTAP systems, your backups can reside on a different subscription/account or different region.
- Backup data is secured with AES-256 bit encryption at-rest and TLS 1.2 HTTPS connections in-flight.
- Use your own customer-managed keys for data encryption instead of using the default encryption keys from your cloud provider.
- Support for up to 4,000 backups of a single volume.

Restore features:

- Restore data from a specific point in time.
- Restore a volume, or individual files, to the source system or to a different system.
- Restore data to a working environment using a different subscription/account or that is in a different region.
- Restores data on a block level, placing the data directly in the location you specify, all while preserving the original ACLs.
- Browsable file catalog for selecting individual files for single file restore.

Supported ONTAP working environments and object storage providers

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

Source Working Environment	Backup File Destination
Cloud Volumes ONTAP in AWS	Amazon S3

Source Working Environment	Backup File Destination
Cloud Volumes ONTAP in Azure	Azure Blob
Cloud Volumes ONTAP in Google	Google Cloud Storage
On-premises ONTAP system	Amazon S3 Azure Blob Google Cloud Storage NetApp StorageGRID

You can restore a volume, or individual files, from an ONTAP backup file to the following working environments:

Backup File	Destination Working Environment	
Location	**Volume Restore**	**File Restore**
Amazon S3	Cloud Volumes ONTAP in AWS On-premises ONTAP system	Cloud Volumes ONTAP in AWS On-premises ONTAP system
Azure Blob	Cloud Volumes ONTAP in Azure On-premises ONTAP system	Cloud Volumes ONTAP in Azure On-premises ONTAP system
Google Cloud Storage	Cloud Volumes ONTAP in Google On-premises ONTAP system	
NetApp StorageGRID	On-premises ONTAP system	

Note that references to "on-premises ONTAP systems" includes FAS, AFF, and ONTAP Select systems.

Cost

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

Resource charges

Resource charges are paid to the cloud provider for object storage capacity and for running a virtual machine/instance in the cloud.

- For Backup, you pay your cloud provider for object storage costs.

  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).

- For File Restore using Browse & Restore, you pay your cloud provider for compute costs only when the Restore instance is running.

  The instance resides in the same subnet as the Connector, and it runs only when browsing a backup file to locate the individual files you want to restore. The instance is turned off when not in use to save costs.

  - In AWS, the Restore instance runs on an m5n.xlarge instance with 4 CPUs, 16 GB memory, and EBS Only instance storage. The operating system image is Amazon Linux 2.

    In regions where m5n.xlarge instance isn't available, Restore runs on an m5.xlarge instance instead.

    - In Azure, the Restore virtual machine runs on a Standard_D4s_v3 VM with 4 CPUs, 16 GB memory, and a 32 GiB disk. The operating system image is CentOS 7.5).

      The instance is named *Cloud-Restore-Instance* with your Account ID concatenated to it. For example: *Cloud-Restore-Instance-MyAccount*.

- For Volume Restore using Browse & Restore, there is no cost because no separate instance or virtual machine is required.
- For Volume or File Restore using Search & Restore, the Amazon Athena and AWS Glue resources are required. A cost is associated with these resources when restoring volumes and files. Search & Restore is supported using AWS A3 only at this time.
- If you need to restore volume data from a backup file that has been moved to archival storage (supported with AWS and Azure when using ONTAP 9.10.1+), then there is an additional per-GiB retrieval fee and per-request fee from the cloud provider.

Service charges

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

There are three 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 get an annual contract - this is only available through AWS. The third option is to purchase licenses directly from NetApp. Read the Licensing section for details.

Licensing

Cloud Backup is available in three licensing options: Pay As You Go (PAYGO), an annual contract from the AWS Marketplace, 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 GiB 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 TiB BYOL license, all capacity beyond the 10 TiB 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.

Annual contract (AWS only)

Two annual contracts are available from the AWS Marketplace:

- An annual contract that enables you to back up Cloud Volumes ONTAP data and on-premises ONTAP data.

  You'll also need to pay for your Cloud Volumes ONTAP systems using this annual contract subscription since you can assign only one active subscription to your AWS credentials in Cloud Manager.

- A Professional Package that enables you to bundle Cloud Volumes ONTAP and Cloud Backup by using an annual contract for 12, 24, or 36 months. This option doesn't enable you to back up on-prem data.

  You can set up the annual contract when you create a Cloud Volumes ONTAP working environment and Cloud Manager will prompt you to subscribe to the AWS Marketplace.

Learn how to set up yearly AWS contracts.

Bring your own license

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

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.

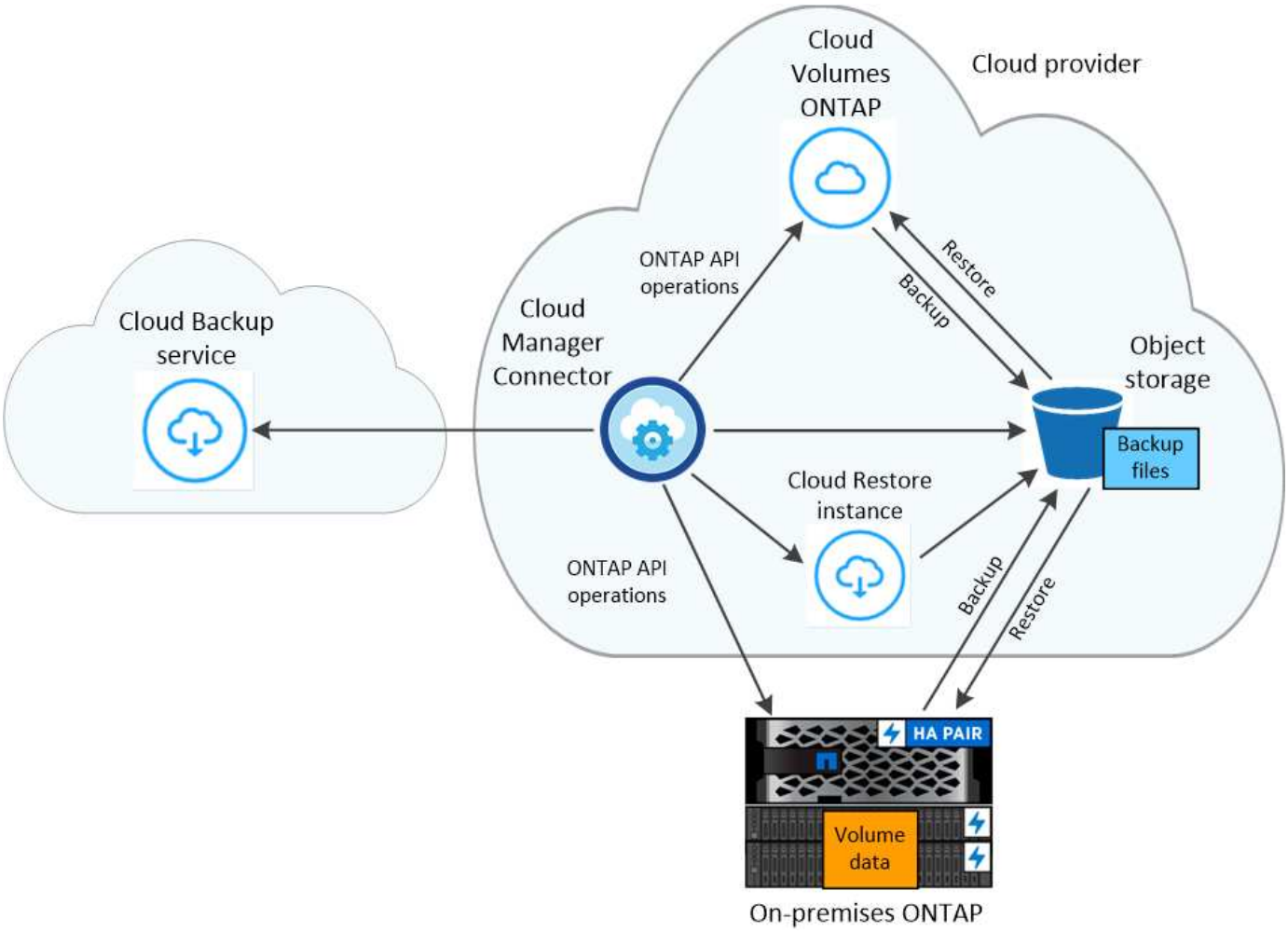
How Cloud Backup works

When you enable Cloud Backup on a Cloud Volumes ONTAP or on-premises ONTAP system, the service performs a full backup of your data. Volume snapshots are not included in the backup image. 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.

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

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:



Where backups reside

Backup copies are stored in an object store that Cloud Manager creates in your cloud account. There's one object store per cluster/working environment, and Cloud Manager names the object store as follows: "netapp-backup-clusteruuid". Be sure not to delete this object store.

- In AWS, Cloud Manager enables the Amazon S3 Block Public Access feature on the S3 bucket.
- In Azure, Cloud Manager uses a new or existing resource group with a storage account for the Blob container. Cloud Manager blocks public access to your blob data by default.
- In GCP, Cloud Manager uses a new or existing project with a storage account for the Google Cloud Storage bucket.
- In StorageGRID, Cloud Manager uses an existing storage account for the object store bucket.

If you want to change the destination object store for a cluster in the future, you'll need to unregister Cloud Backup for the working environment, and then enable Cloud Backup using the new cloud provider information.

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.

If your cluster is using ONTAP 9.10.1 or greater, you can choose to tier older backups to either *S3 Glacier* or *S3 Glacier Deep Archive* storage after a certain number of days for further cost optimization. Learn more about AWS archival storage.

- In Azure, backups are associated with the *Cool* access tier.

  If your cluster is using ONTAP 9.10.1 or greater, you can choose to tier older backups to *Azure Archive* storage after a certain number of days for further cost optimization. Learn more about Azure archival storage.

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

  You can also use the lower cost *Nearline* storage class, or the *Coldline* or *Archive* storage classes. See the Google topic Storage classes for information about changing the storage class.

- In StorageGRID, backups are associated with the *Standard* storage class.

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. You can also select one of the system-defined policies that provide backups and retention for 3 months, 1 year, and 7 years. These policies are:

Backup Policy Name	Backups per interval…			Max. Backups
	Daily	Weekly	Monthly	
Netapp3MonthsRetention	30	13	3	46
Netapp1YearRetention	30	13	12	55
Netapp7YearsRetention	30	53	84	167

Backup protection policies that you have created on the cluster using ONTAP System Manager or the ONTAP CLI will also appear as selections.

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.

Note that you can create an on-demand backup of a volume from the Backup Dashboard at any time, in addition to those backup files created from the scheduled backups.

The retention period for backups of data protection volumes is the same as defined in the source SnapMirror relationship. You can change this if you want by using the API.

FabricPool tiering policy considerations

There are certain things you need to be aware of when the volume you are backing up resides on a FabricPool aggregate and it has an assigned policy other than `none`:

- The first backup of a FabricPool-tiered volume requires reading all local and all tiered data (from the object store). A backup operation does not "reheat" the cold data tiered in object storage.

  This operation could cause a one-time increase in cost to read the data from your cloud provider.

  - Subsequent backups are incremental and do not have this effect.
  - If the tiering policy is assigned to the volume when it is initially created you will not see this issue.
- Consider the impact of backups before assigning the `all` tiering policy to volumes. Because data is tiered immediately, Cloud Backup will read data from the cloud tier rather than from the local tier. Because concurrent backup operations share the network link to the cloud object store, performance degradation might occur if network resources become saturated. In this case, you may want to proactively configure multiple network interfaces (LIFs) to decrease this type of network saturation.

Supported volumes

Cloud Backup supports FlexVol read-write volumes and SnapMirror data protection (DP) destination volumes.

FlexGroup volumes and SnapLock volumes aren’t currently supported.

Limitations

- The ability to tier older backup files to archival storage requires that the cluster is running ONTAP 9.10.1 or greater (supported currently with AWS and Azure). Restoring volumes from backup files that reside in archival storage also requires that the destination cluster is running ONTAP 9.10.1+.
- 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.
- When backing up data protection (DP) volumes, relationships with the following SnapMirror labels won’t be backed up to cloud:
  - app_consistent
  - all_source_snapshot
- SVM-DR volume backup is supported with the following restrictions:
  - Backups are supported from the ONTAP secondary only.
  - The Snapshot policy applied to the volume must be one of the policies recognized by Cloud Backup, including daily, weekly, monthly, etc. The default "sm_created" policy (used for **Mirror All Snapshots**) is not recognized and the DP volume will not be shown in the list of volumes that can be backed up.
- Ad-hoc volume backups using the **Backup Now** button aren’t supported on data protection volumes.
- SM-BC configurations are not supported.
- MetroCluster (MCC) backup is supported from ONTAP secondary only: MCC > SnapMirror > ONTAP > Cloud Backup > object storage.
- ONTAP doesn’t support fan-out of SnapMirror relationships from a single volume to multiple object stores; therefore, this configuration is not supported by Cloud Backup.
- WORM/Compliance mode on an object store is not supported.

Single File Restore limitations

- Single file restore can restore up to 100 individual files at a time. There is currently no support for restoring folders/directories.
- The file being restored must be using the same language as the language on the destination volume. You will receive an error message if the languages are not the same.
- File level restore is not supported when using the same account with different Cloud Managers in different subnets.

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.

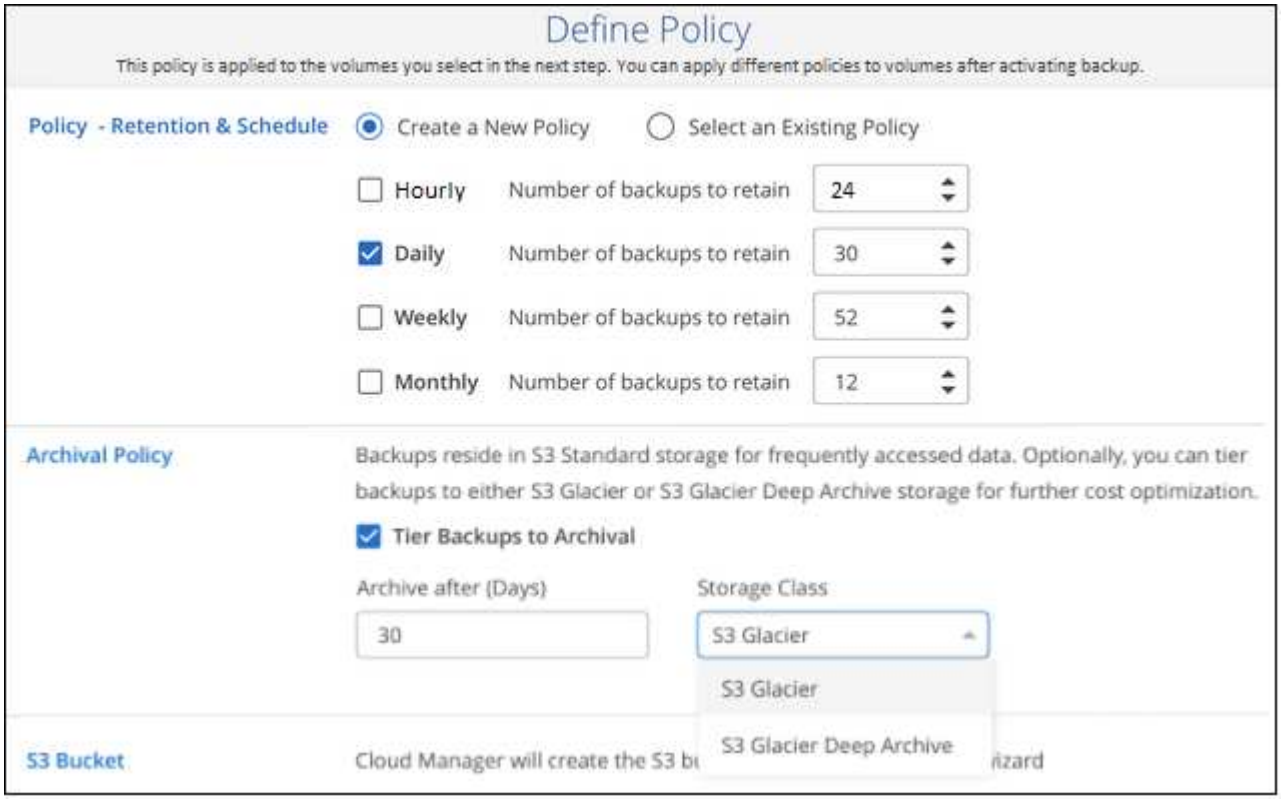
3 Enter the provider details

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

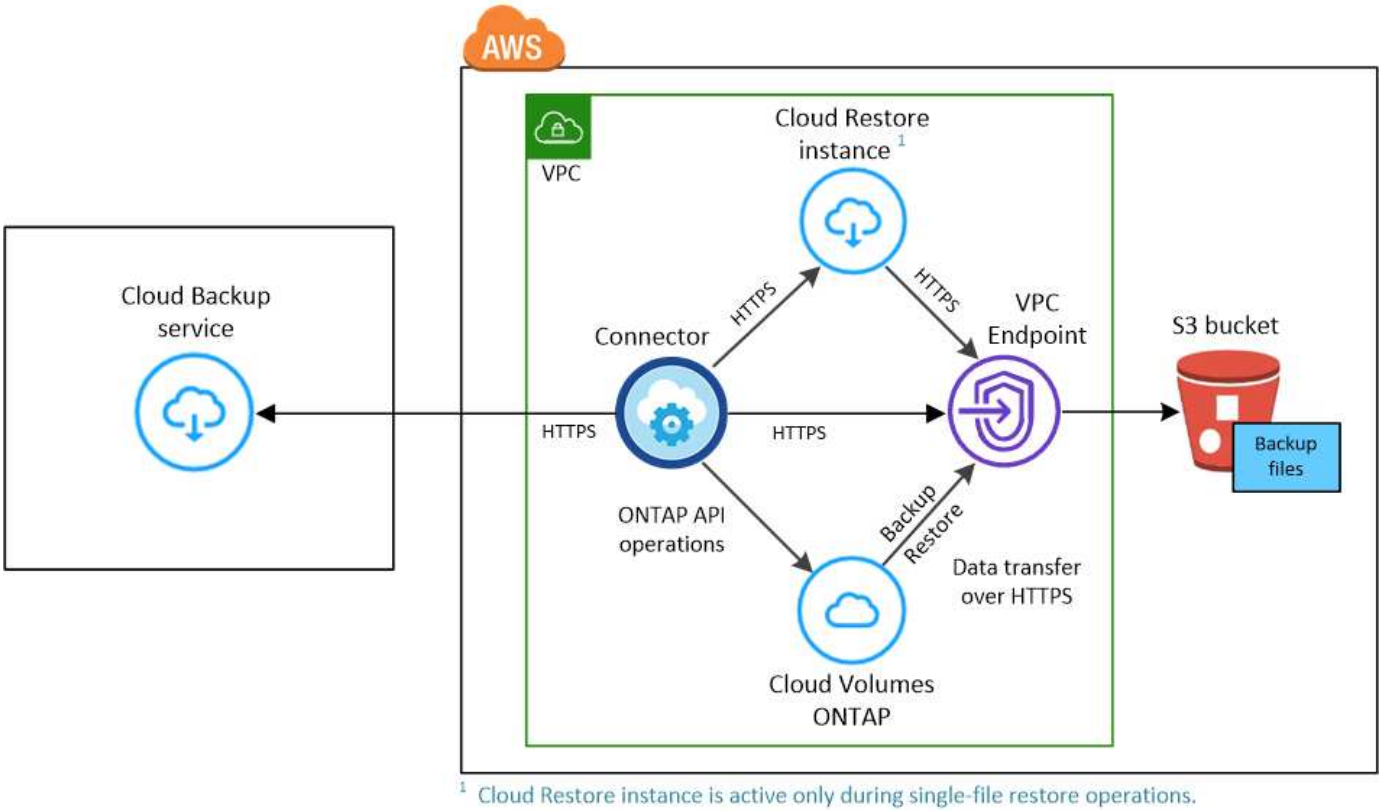
Identify which volumes you want to back up using the default backup policy in the Select Volumes page. If you want to assign different backup policies to certain volumes, you can create additional policies and apply them

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:PutObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock",
                "s3:PutEncryptionConfiguration",
                "athena:StartQueryExecution",
                "athena:GetQueryResults",
                "athena:GetQueryExecution",
                "glue:GetDatabase",
                "glue:GetTable",
                "glue:CreateTable",
                "glue:CreateDatabase",
                "glue:GetPartitions",
                "glue:BatchCreatePartition",
                "glue:BatchDeletePartition"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
            ]
        },
```

If you deployed the Connector using version 3.9.15 or greater, these permissions should be part of the IAM role already. Otherwise you'll need to add the missing permissions.

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

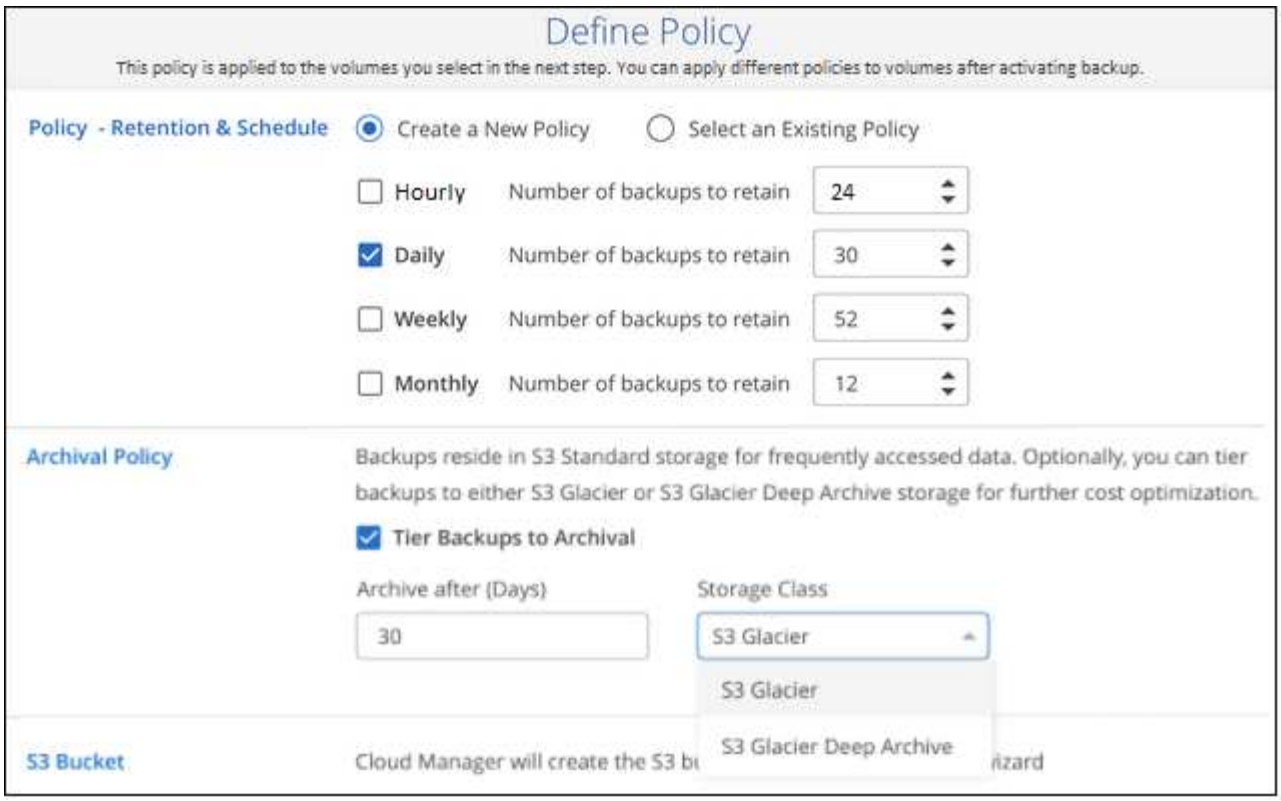
1. Select the working environment and click **Enable** next to the Backup & Restore service in the right-panel.

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.

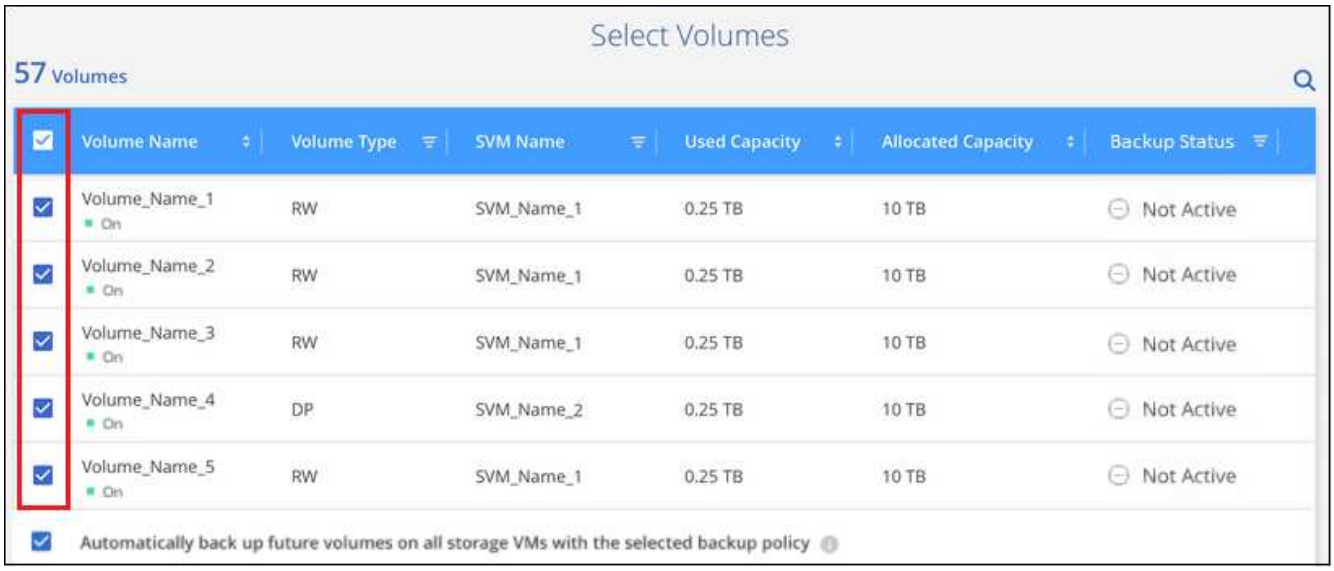
      If you want to use a different AWS account for your backups, you must log in to the AWS portal and link the two accounts.

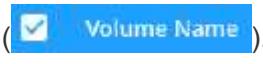
   b. The region where the backups will be stored. This can be a different region than where the Cloud Volumes ONTAP system resides.
   c. Whether you'll use the default Amazon S3 encryption keys or choose your own customer-managed keys from your AWS account to manage encryption of your data. (See how to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

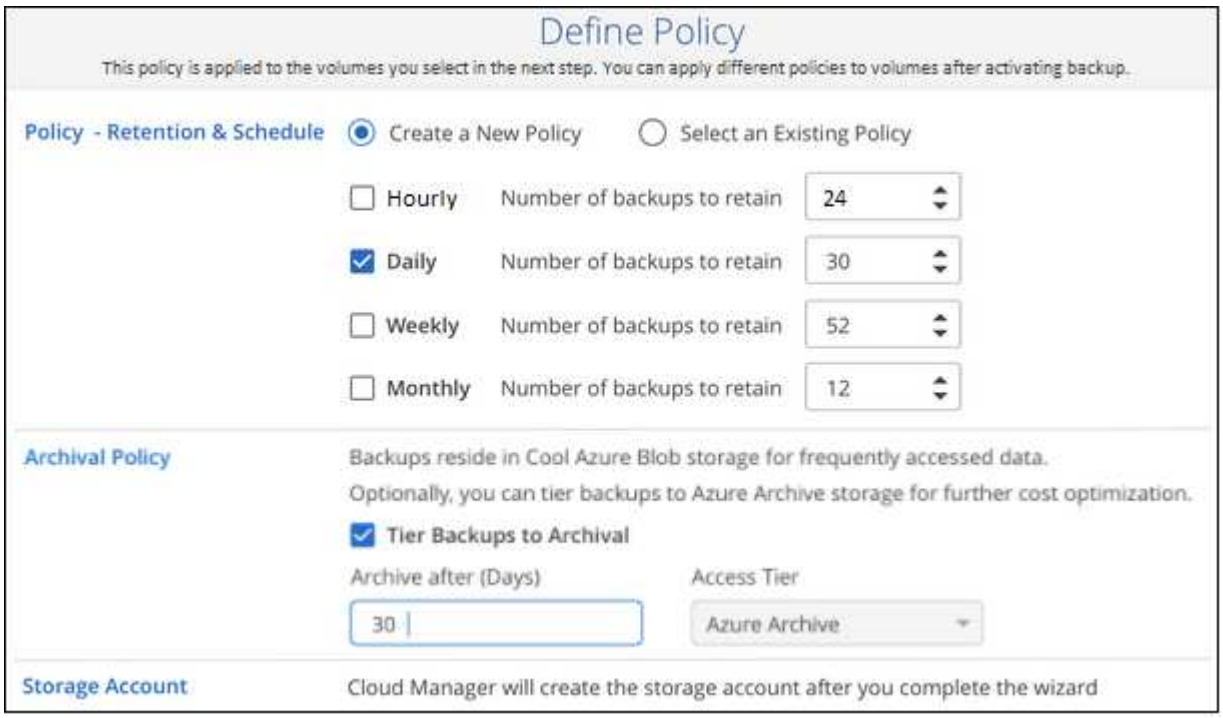
3 Enter the provider details

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.



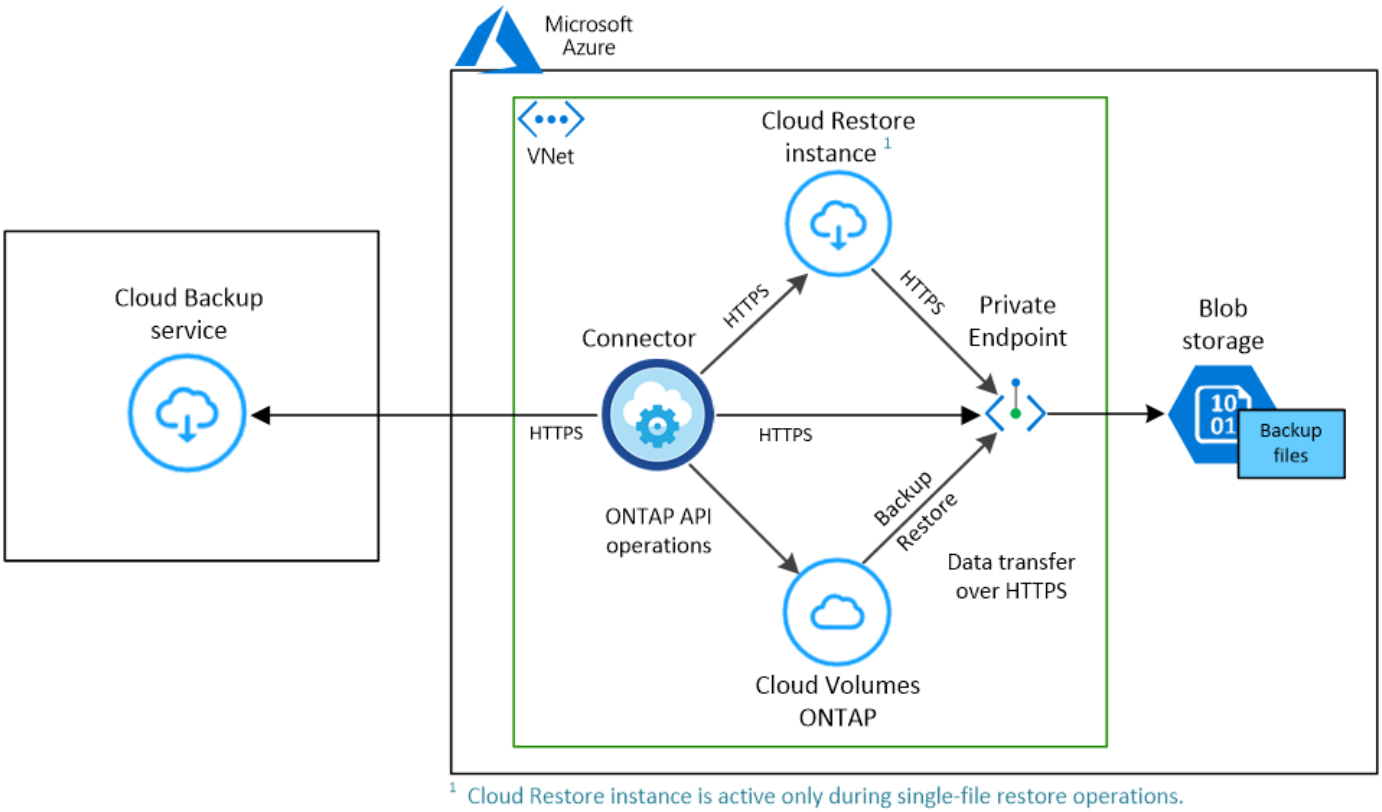
5 Select the volumes that you want to back up

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.

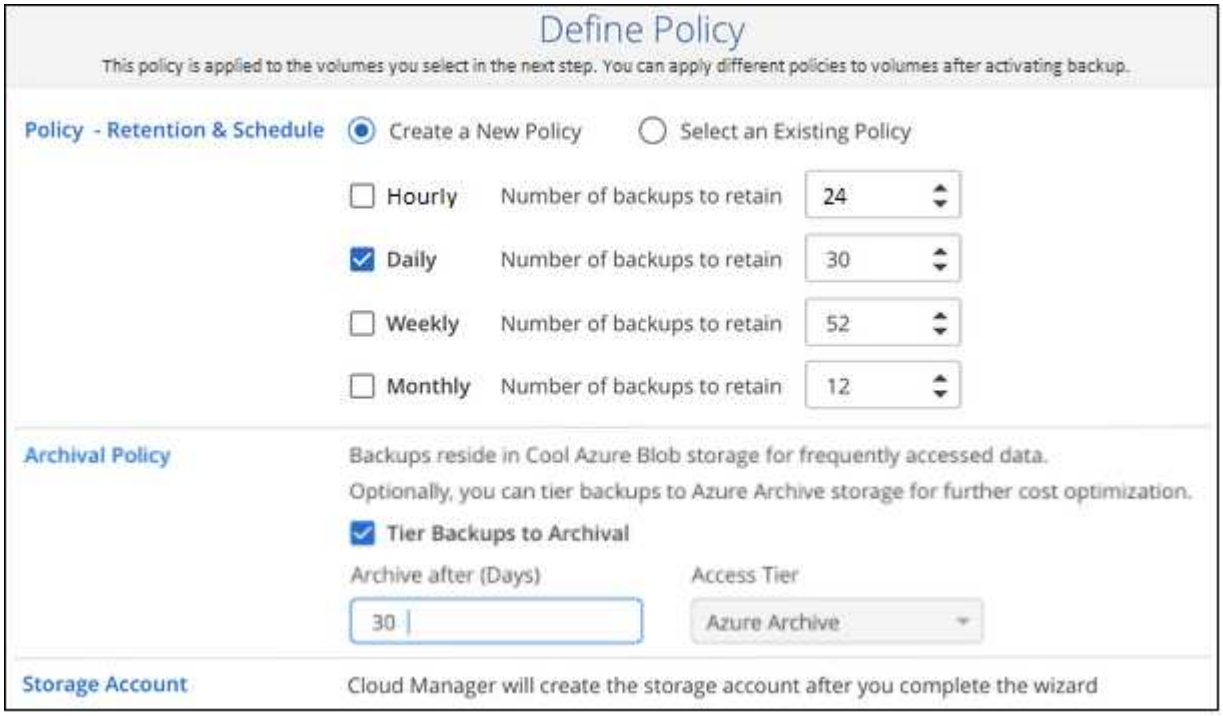
      If you want to use a different Azure subscription for your backups, you must log in to the Azure portal and link the two subscriptions.

   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).

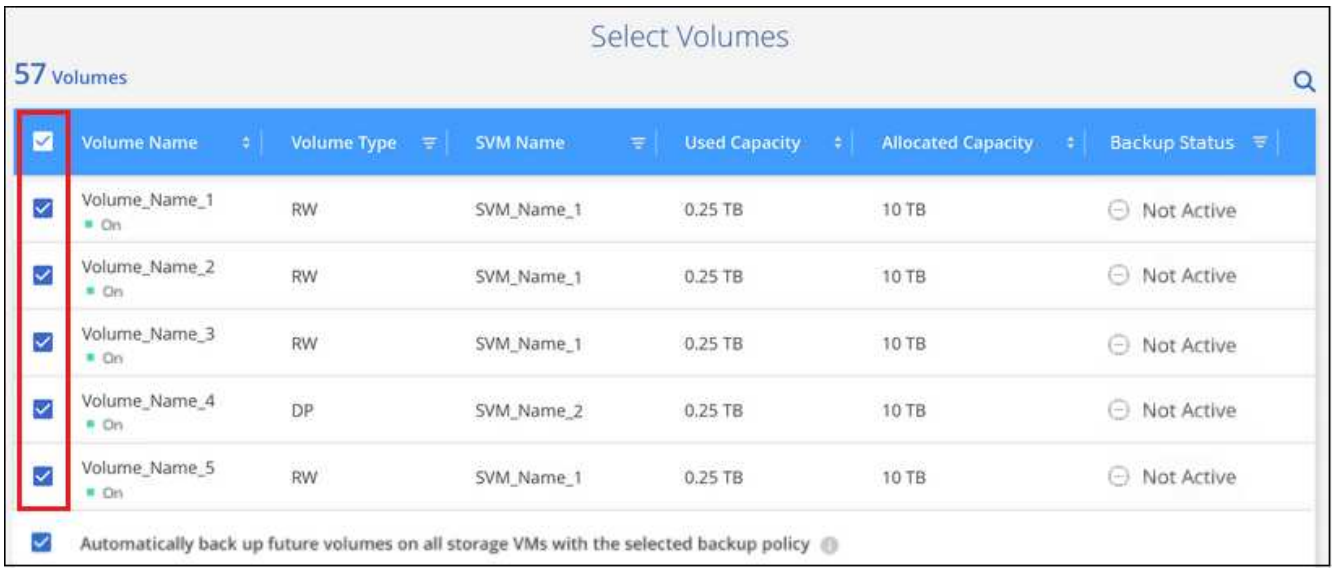
3. Enter the default backup policy details and click **Next**.

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

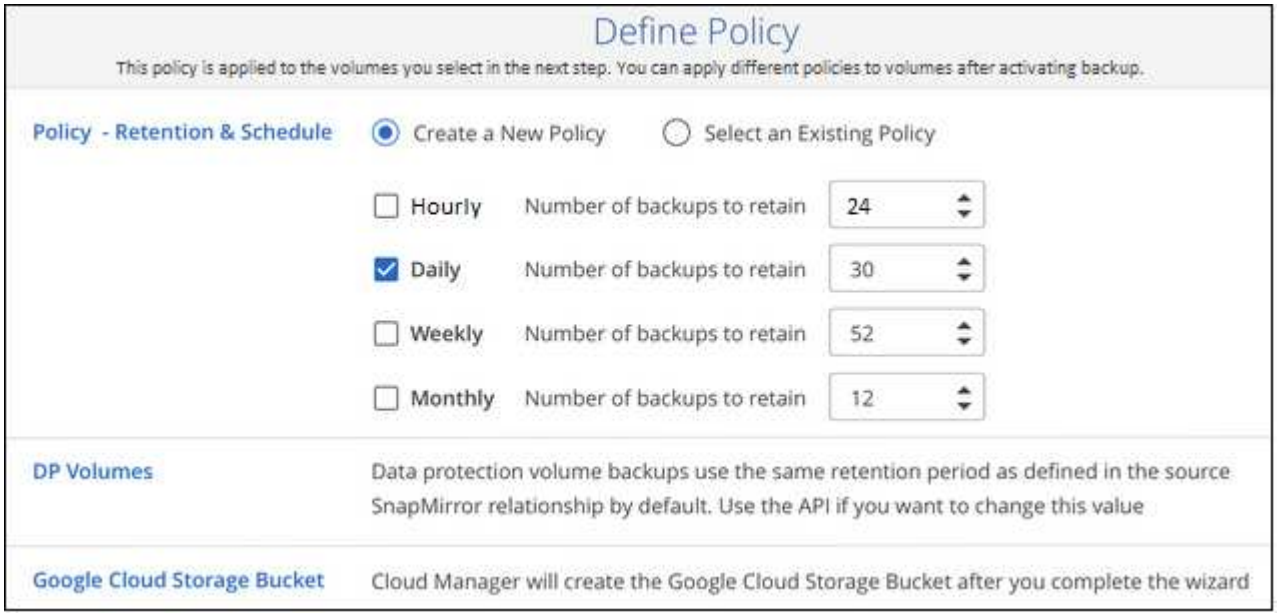
- New systems: Cloud Backup can be enabled when you complete the new working environment wizard.
- Existing systems: Select the working environment and click **Enable** next to the Backup & Restore service in the right-panel, and then follow the setup wizard.

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.



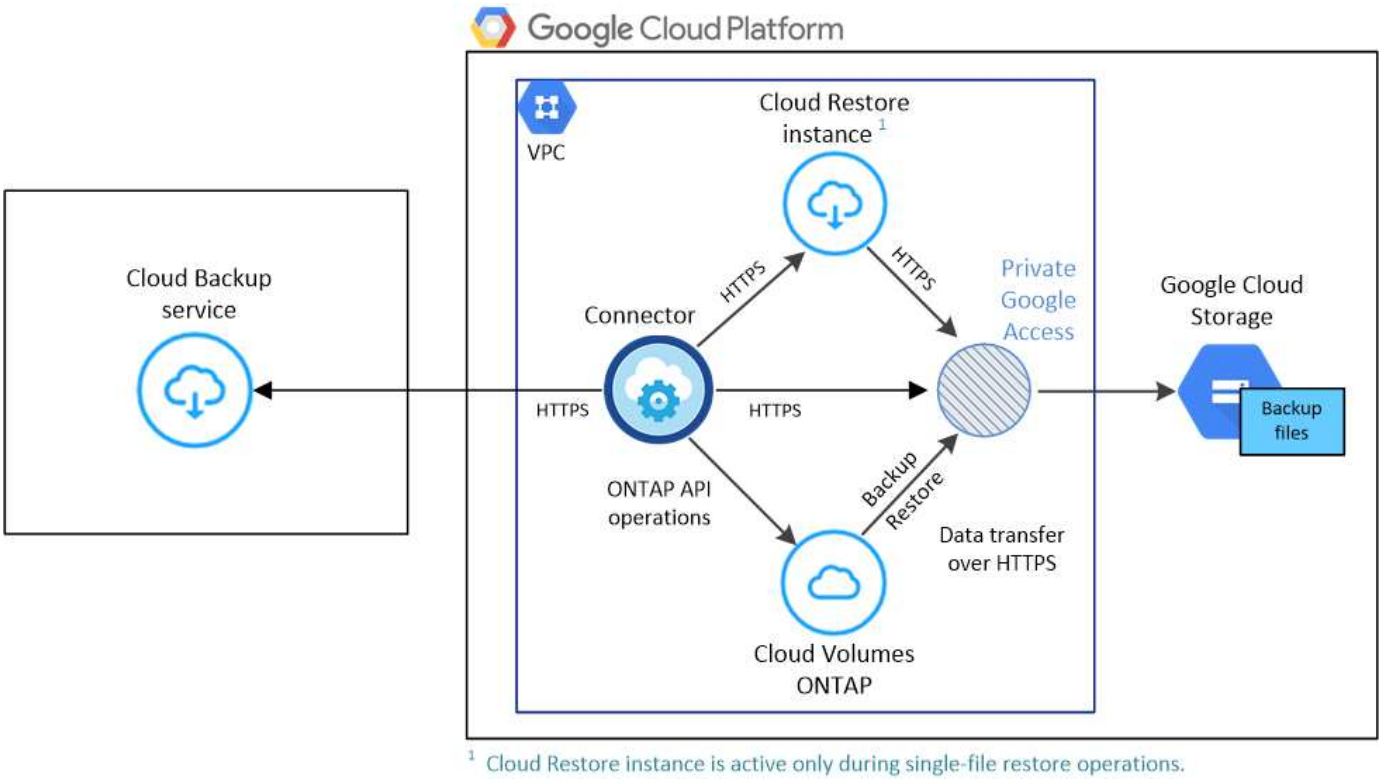
5 **Select the volumes that you want to back up**

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.

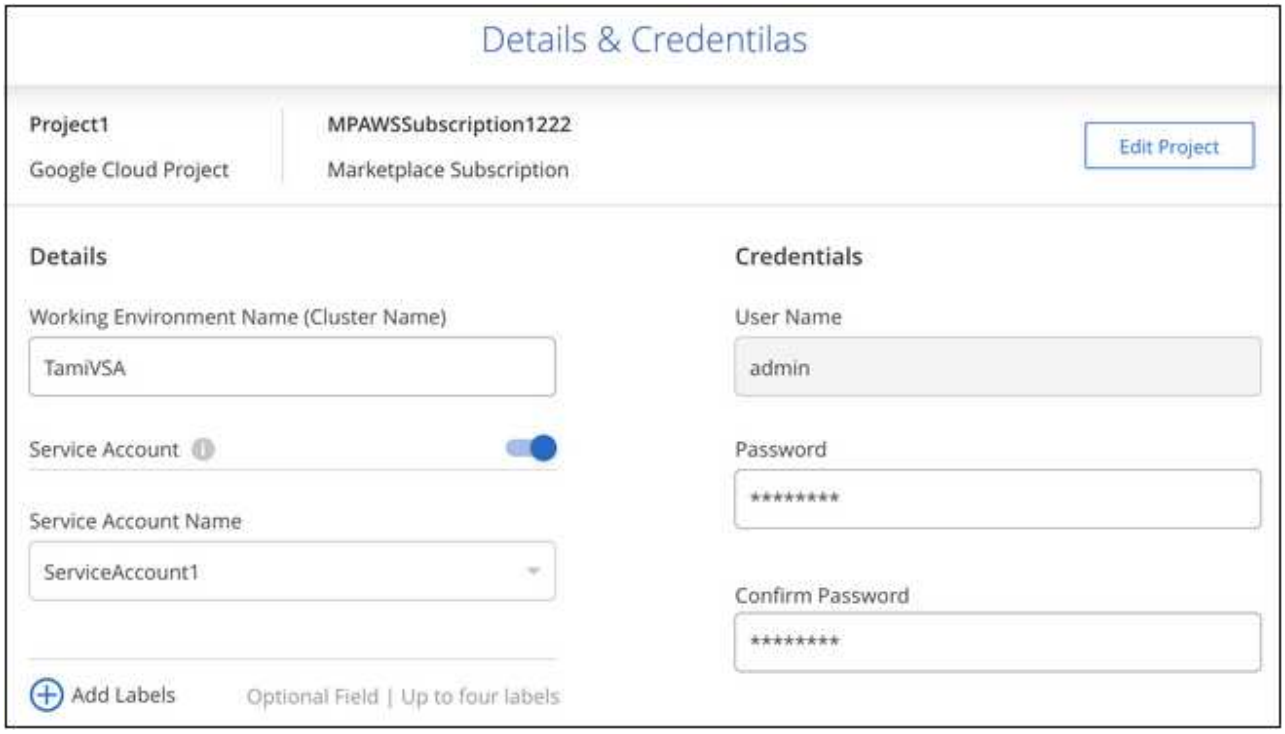
See Launching Cloud Volumes ONTAP in GCP for requirements and details for creating your Cloud Volumes

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.

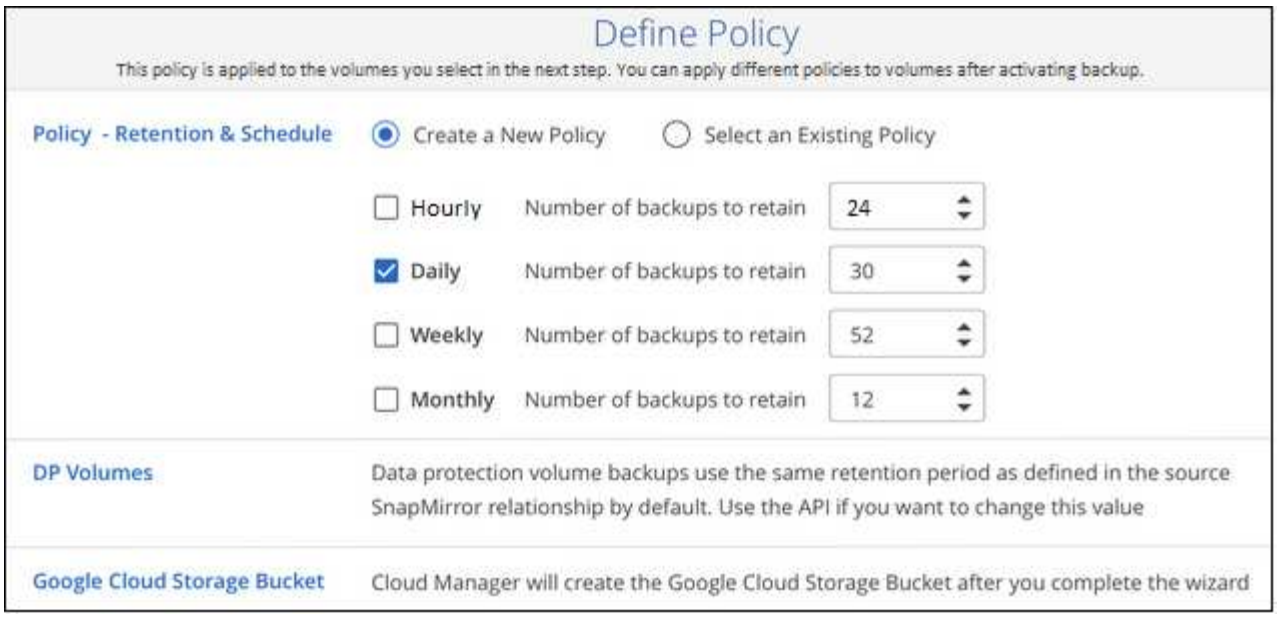
Steps

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**.

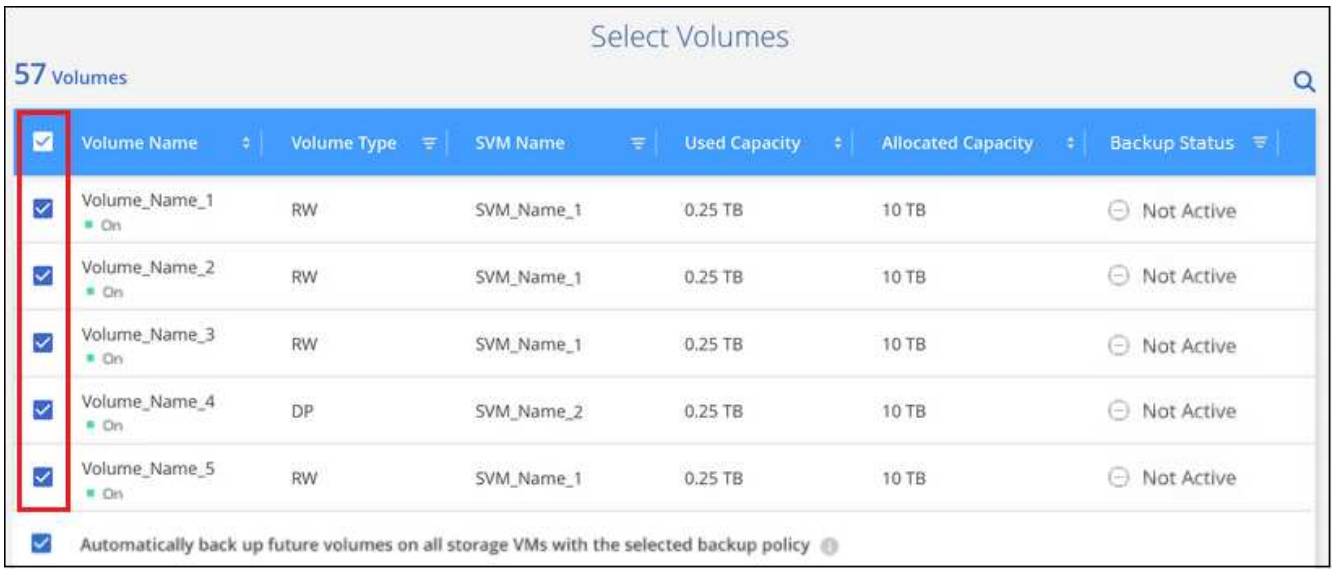
   Note that the Project must have a Service Account that has the predefined Storage Admin role.

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.

Backing up on-premises ONTAP data to Amazon S3

Complete a few steps to get started backing up data from your on-premises ONTAP systems to Amazon S3 storage.

Note that "on-premises ONTAP systems" includes FAS, AFF, and ONTAP Select systems.

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

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 have discovered the on-premises cluster and added it to a working environment in Cloud Manager. See Discovering ONTAP clusters for details.
  - The cluster is running ONTAP 9.7P5 or later.
  - The cluster has a SnapMirror license — it is included as part of the Premium Bundle or Data Protection Bundle.
  - The cluster must have the required network connections to S3 storage and to the Connector.
- The Connector must have the required network connections to S3 storage and to the cluster, and the required permissions.
- You have a valid AWS subscription for the object storage space where your backups will be located.
- You have an AWS Account with an access key and secret key, and the required permissions so the ONTAP cluster can back up and restore data.

2 Enable Cloud Backup on the system

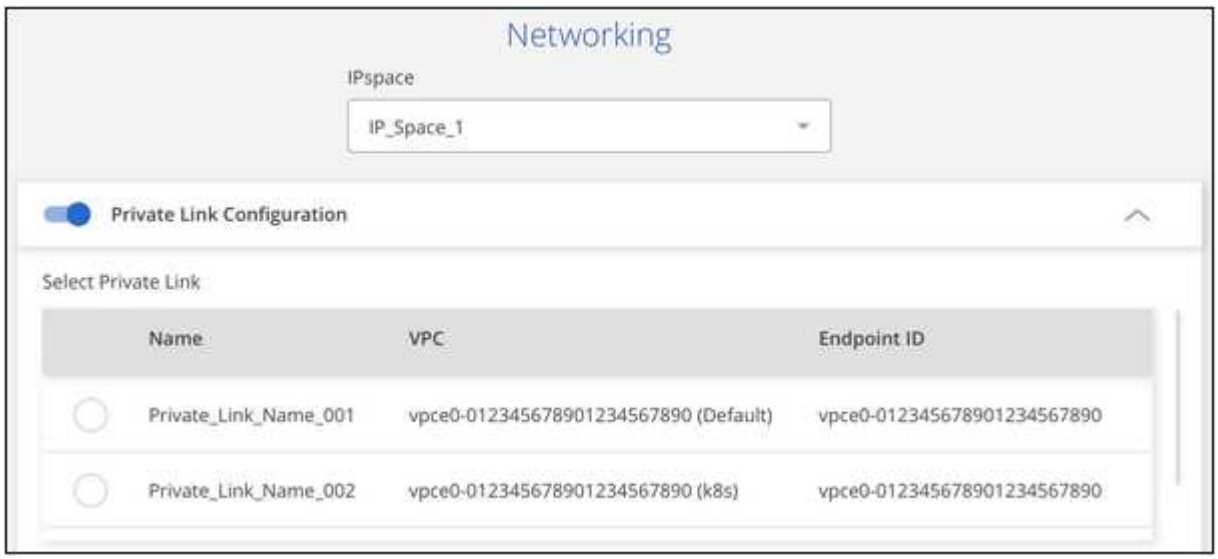
Select the working environment and click **Enable > Backup Volumes** next to the Backup & Restore service in the right-panel, and then follow the setup wizard.

3 Select the cloud provider and enter the provider details

Select Amazon Web Services as your provider and then enter the provider details. You'll need to 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 Select the cluster IPspace and optionally select an AWS PrivateLink connection

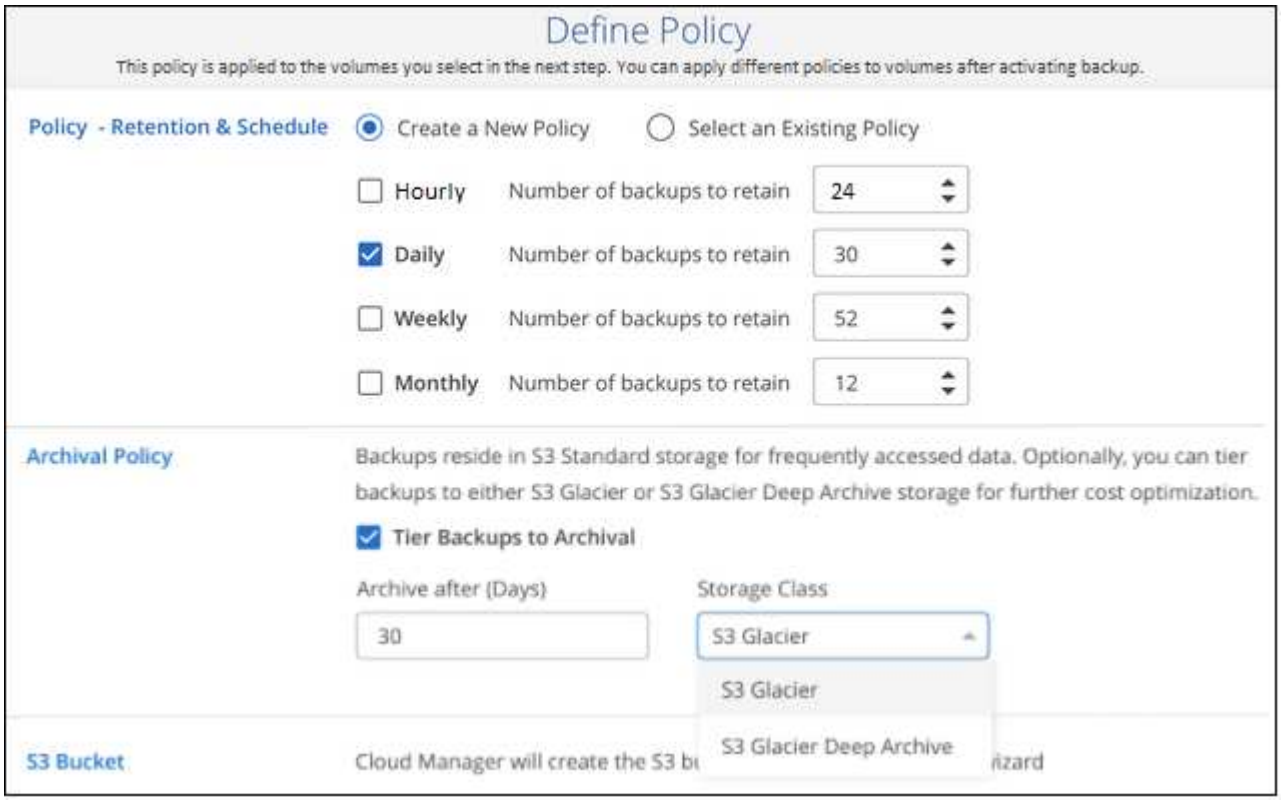
Select the IPspace in the ONTAP cluster where the volumes reside. You can also choose to use an existing AWS PrivateLink configuration for a more secure connection to the VPC from your on-prem data center.



5 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 S3 Standard storage. 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.



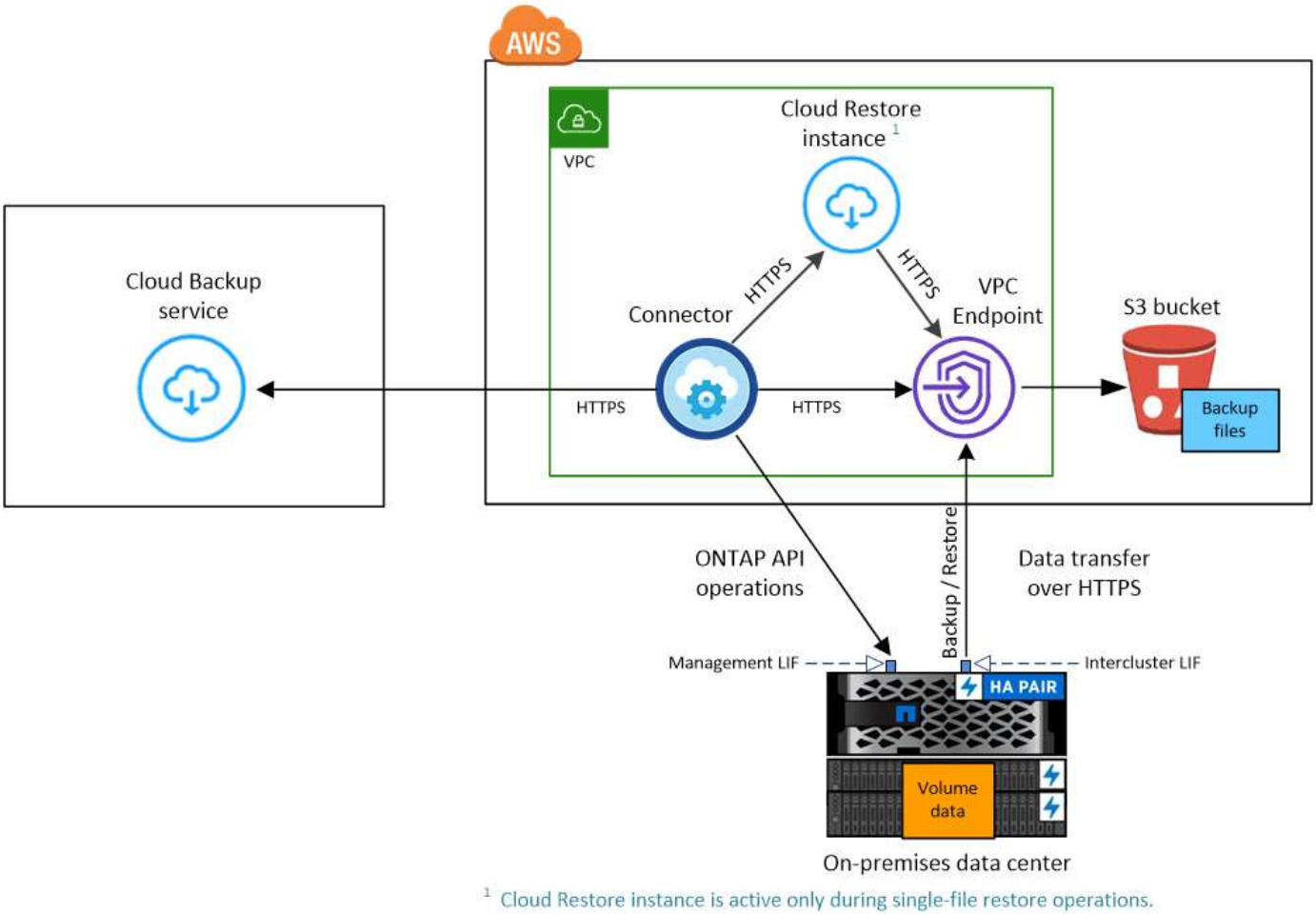
6 **Select the volumes that you want to back up**

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 you have a supported configuration before you start backing up on-premises volumes to S3 storage.

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



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

Preparing your ONTAP clusters

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

Learn how to discover a cluster.

ONTAP requirements

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

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

  See how to manage your cluster licenses.

- Time and time zone are set correctly.

  See how to configure your cluster time.

Cluster networking requirements

- The ONTAP cluster initiates an HTTPS connection over port 443 from the intercluster LIF to Amazon S3 storage for backup and restore operations.

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

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

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

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

Creating or switching Connectors

A Connector is required to back up data to the cloud, and the Connector must be in an AWS VPC when backing up data to AWS S3 storage. You can't use a Connector that's deployed on-premises. You'll either need to create a new Connector or make sure that the currently selected Connector resides in the correct provider.

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

Preparing networking for the Connector

Ensure that the Connector has the required networking connections.

Steps

1. Ensure that the network where the Connector is installed enables the following connections:
   - An outbound internet connection to the Cloud Backup service over port 443 (HTTPS)
   - An HTTPS connection over port 443 to your S3 object storage
   - An HTTPS connection over port 443 to your ONTAP cluster management LIF
2. Enable a VPC Endpoint to S3. This is needed if you have a Direct Connect or VPN connection from your ONTAP cluster to the VPC and you want communication between the Connector and S3 to stay in your AWS internal network.

Supported regions

You can create backups from on-premises systems to Amazon S3 in all regions where Cloud Volumes ONTAP is supported; including AWS GovCloud regions. You specify the region where the backups will be stored when you set up the service.

License requirements

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

- For Cloud Backup PAYGO licensing, you'll need a subscription to the AWS Cloud Manager Marketplace offering to continue using Cloud Backup. Billing for Cloud Backup is done through this subscription.
- For Cloud Backup BYOL licensing, you'll need the serial number from NetApp that enables you to use the service for the duration and capacity of the license. Learn how to manage your BYOL licenses.

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

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

Preparing Amazon S3 for backups

When you are using Amazon S3, you must configure permissions for the Connector to create and manage the S3 bucket, and you must configure permissions so the on-premises ONTAP cluster can read and write to the S3 bucket.

Steps

1. Confirm that the following S3 permissions (from the latest Cloud Manager policy) are part of the IAM role that provides the Connector with permissions.

```
{
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:PutObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock",
                "s3:PutEncryptionConfiguration",
                "athena:StartQueryExecution",
                "athena:GetQueryResults",
                "athena:GetQueryExecution",
                "glue:GetDatabase",
                "glue:GetTable",
                "glue:CreateTable",
                "glue:CreateDatabase",
                "glue:GetPartitions",
                "glue:BatchCreatePartition",
                "glue:BatchDeletePartition"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
            ]
        },
```

```
If you deployed the Connector using version 3.9.15 or greater, these
permissions should be part of the IAM role already. Otherwise you'll
need to add the missing permissions.
```

2. Add the following EC2 permissions to the IAM role that provides the Connector with permissions so that it can start, stop, and terminate the Cloud Restore instance:

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

3. When activating the service, the Backup wizard will prompt you to enter an access key and secret key. For that, you'll need to create an IAM user with the following permissions. Cloud Backup passes these credentials on to the ONTAP cluster so that ONTAP can backup and restore data to the S3 bucket.

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetBucketLocation",
"s3:GetObject",
"s3:PutObject",
"s3:PutBucketencryption",
"s3:DeleteObject"
```

   See the AWS Documentation: Creating a Role to Delegate Permissions to an IAM User for details.

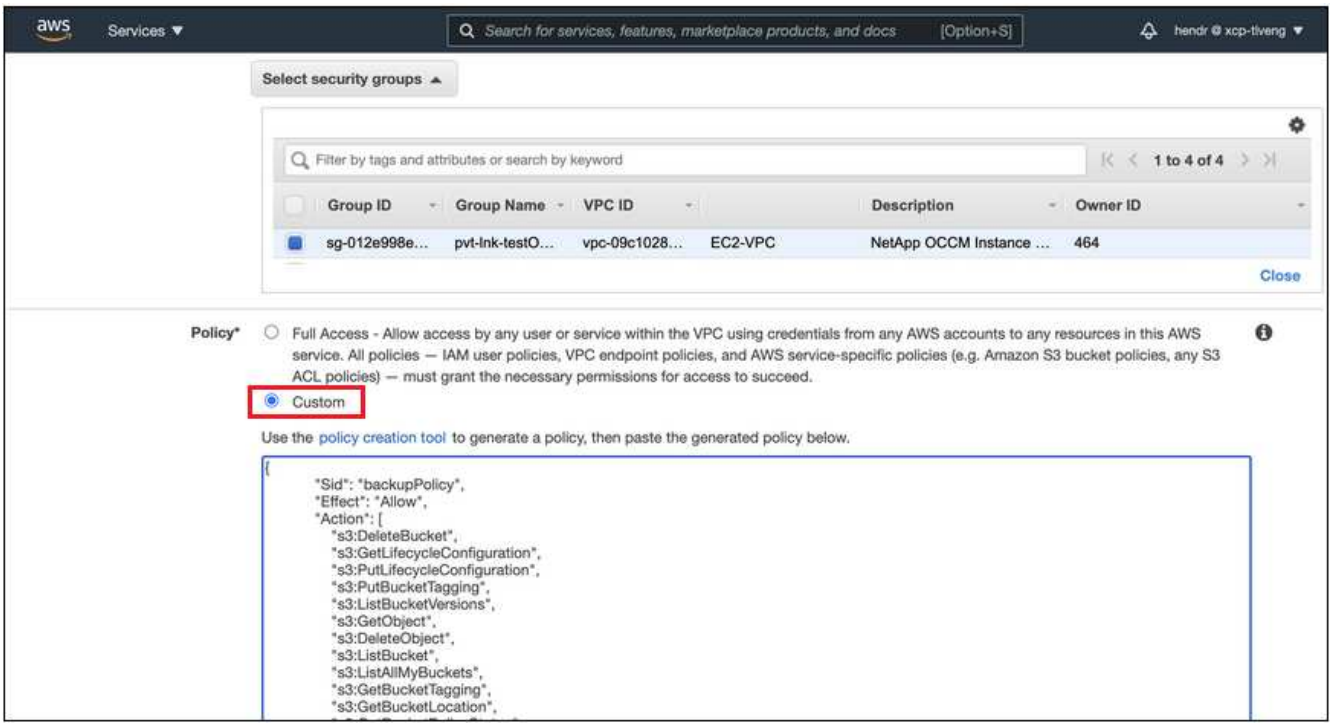
4. If your virtual or physical network uses a proxy server for internet access, ensure that the Cloud Restore instance has outbound internet access to contact the following endpoints.

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.

5. You can choose your own custom-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.

6. If you want to have a more secure connection over the public internet from your on-prem data center to the VPC, there is an option to select an AWS PrivateLink connection in the activation wizard. It is required if you are connecting your on-premises system via VPN/DirectConnect. In this case you'll need to have created an Interface endpoint configuration using the Amazon VPC console or the command line. See details about using AWS PrivateLink for Amazon S3.

   Note that you'll also need to modify the security group configuration that is associated with the Cloud Manager Connector. You must change the policy to "Custom" (from "Full Access"), and you must add the permissions from the backup policy as shown earlier (above).



Enabling Cloud Backup

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

Steps

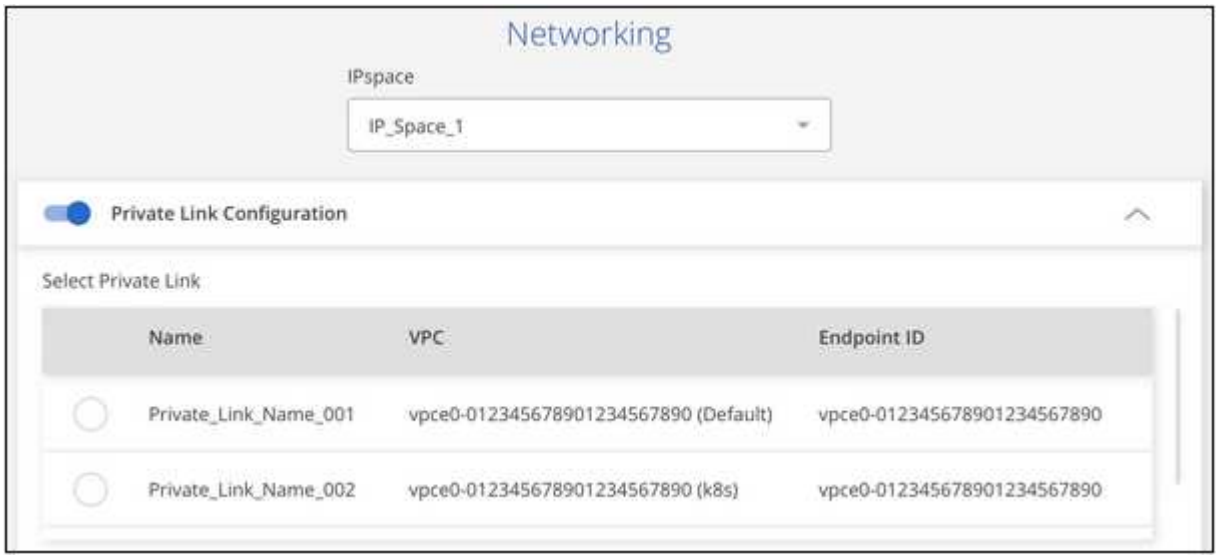
1. From the Canvas, select the working environment and click **Enable > Backup Volumes** next to the Backup & Restore service in the right-panel.

2. Select Amazon Web Services as your provider and click **Next**.
3. Enter the provider details and click **Next**.
   a. The AWS Account, the AWS Access Key, and the Secret Key used to store the backups.

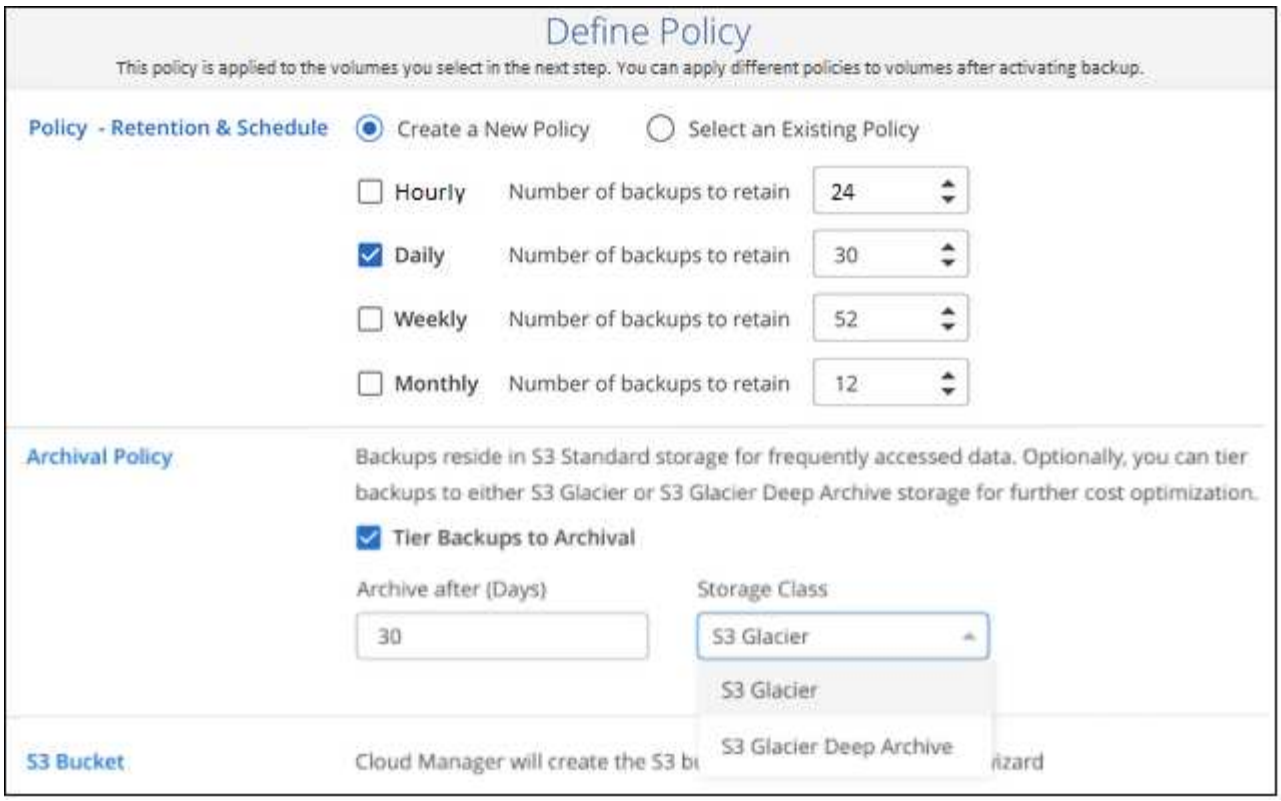
      The access key and secret key are for the user you created to give the ONTAP cluster access to the S3 bucket.

   b. The AWS region where the backups will be stored.
   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 keys).

4. Enter the networking details and click **Next**.
   a. The IPspace in the ONTAP cluster where the volumes you want to back up reside. The intercluster LIFs for this IPspace must have outbound internet access.
   b. Optionally, choose whether you'll use an AWS PrivateLink that you have previously configured. See details about using AWS PrivateLink for Amazon S3.

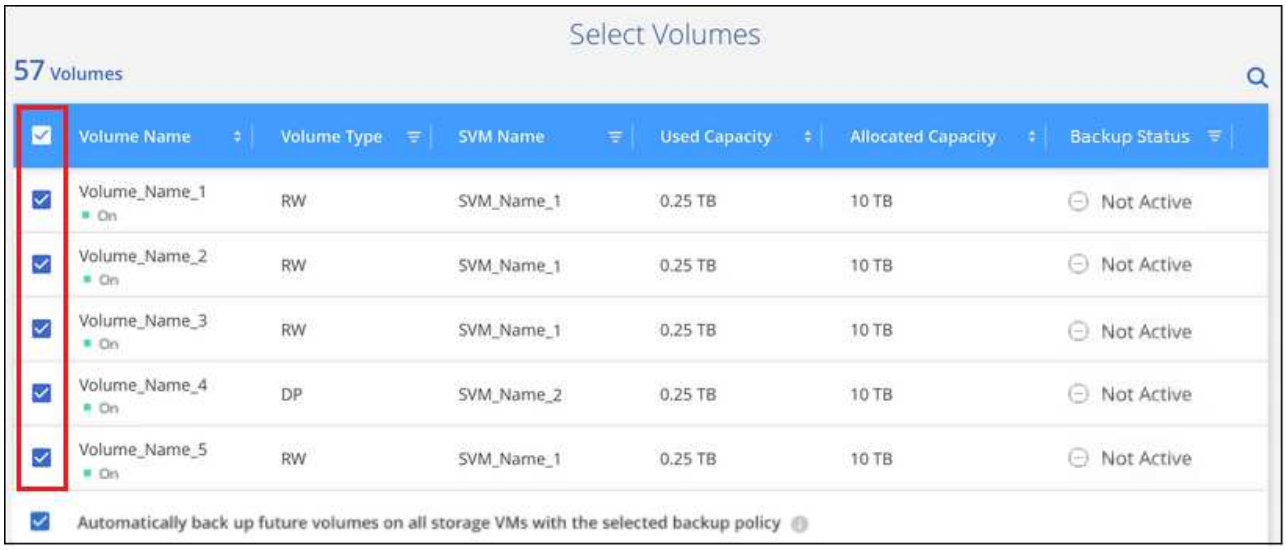


5. Enter the default backup policy details and click **Next**.
   a. Define the backup schedule and choose the number of backups to retain. See the list of existing policies you can choose.
   b. When using ONTAP 9.10.1 and greater, you can choose to tier backups to either S3 Glacier or S3 Glacier Deep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



6. 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).



   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.

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

Result

Cloud Backup starts taking the initial backups of each selected volume and the 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 on-premises ONTAP data to Azure Blob storage

Complete a few steps to get started backing up data from your on-premises ONTAP systems to Azure Blob storage.

Note that "on-premises ONTAP systems" includes FAS, AFF, and ONTAP Select systems.

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

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

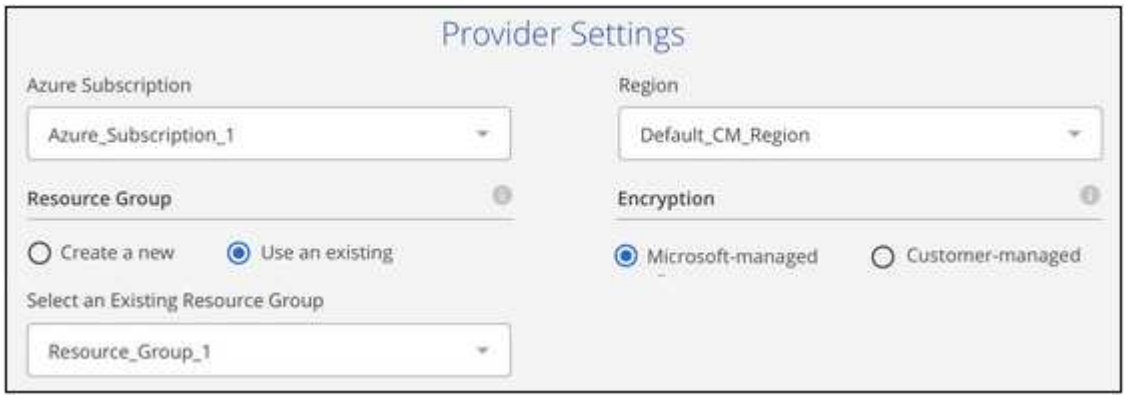
- You have discovered the on-premises cluster and added it to a working environment in Cloud Manager. See Discovering ONTAP clusters for details.
  - The cluster is running ONTAP 9.7P5 or later.
  - The cluster has a SnapMirror license — it is included as part of the Premium Bundle or Data Protection Bundle.
  - The cluster must have the required network connections to Blob storage and to the Connector.
- The Connector must have the required network connections to Blob storage and to the cluster, and the required permissions.
- You have a valid Azure subscription for the object storage space where your backups will be located.

2 Enable Cloud Backup on the system

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

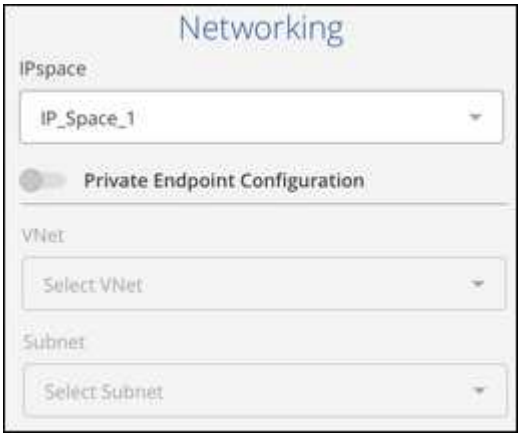
3 Select the cloud provider and enter the provider details

Select Microsoft Azure as your provider and then enter the provider details. You'll need to select the Azure Subscription 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 Microsoft-managed encryption key.



4 Select the cluster IPspace and optional use of a private VNet endpoint

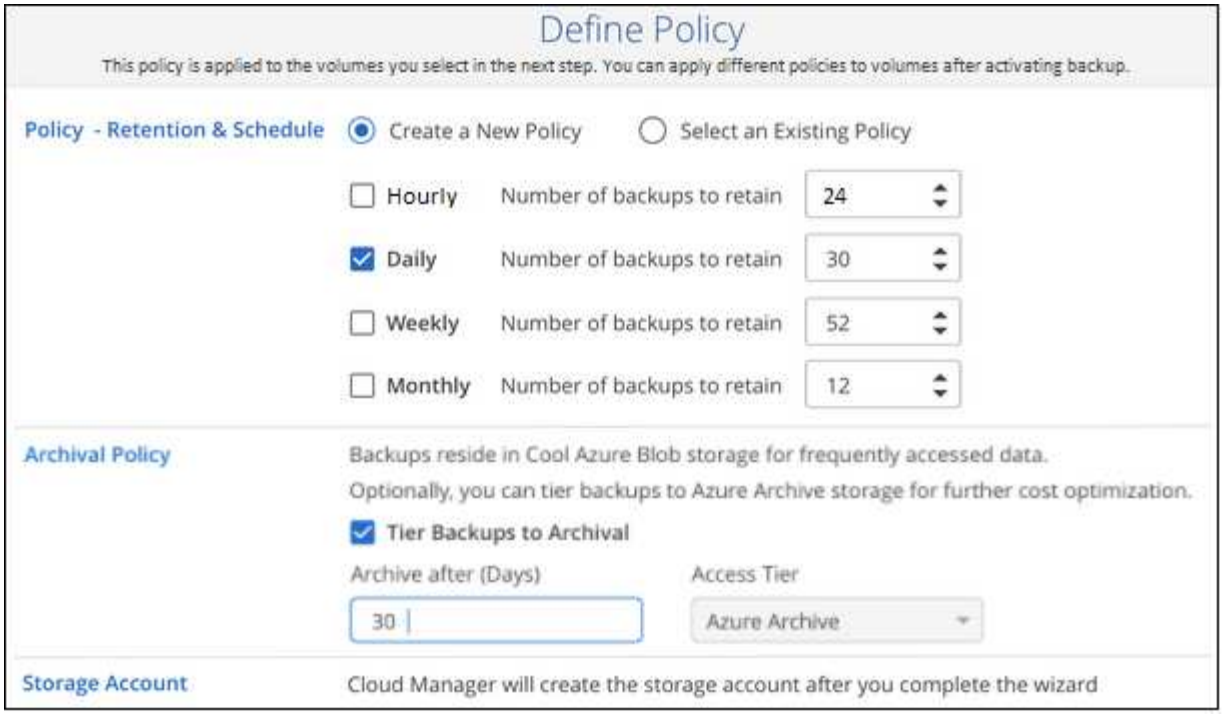
Select the IPspace in the ONTAP cluster where the volumes reside. You can also choose to use an existing Azure Private Endpoint for a more secure connection to the VNet from your on-prem data center.



5 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.



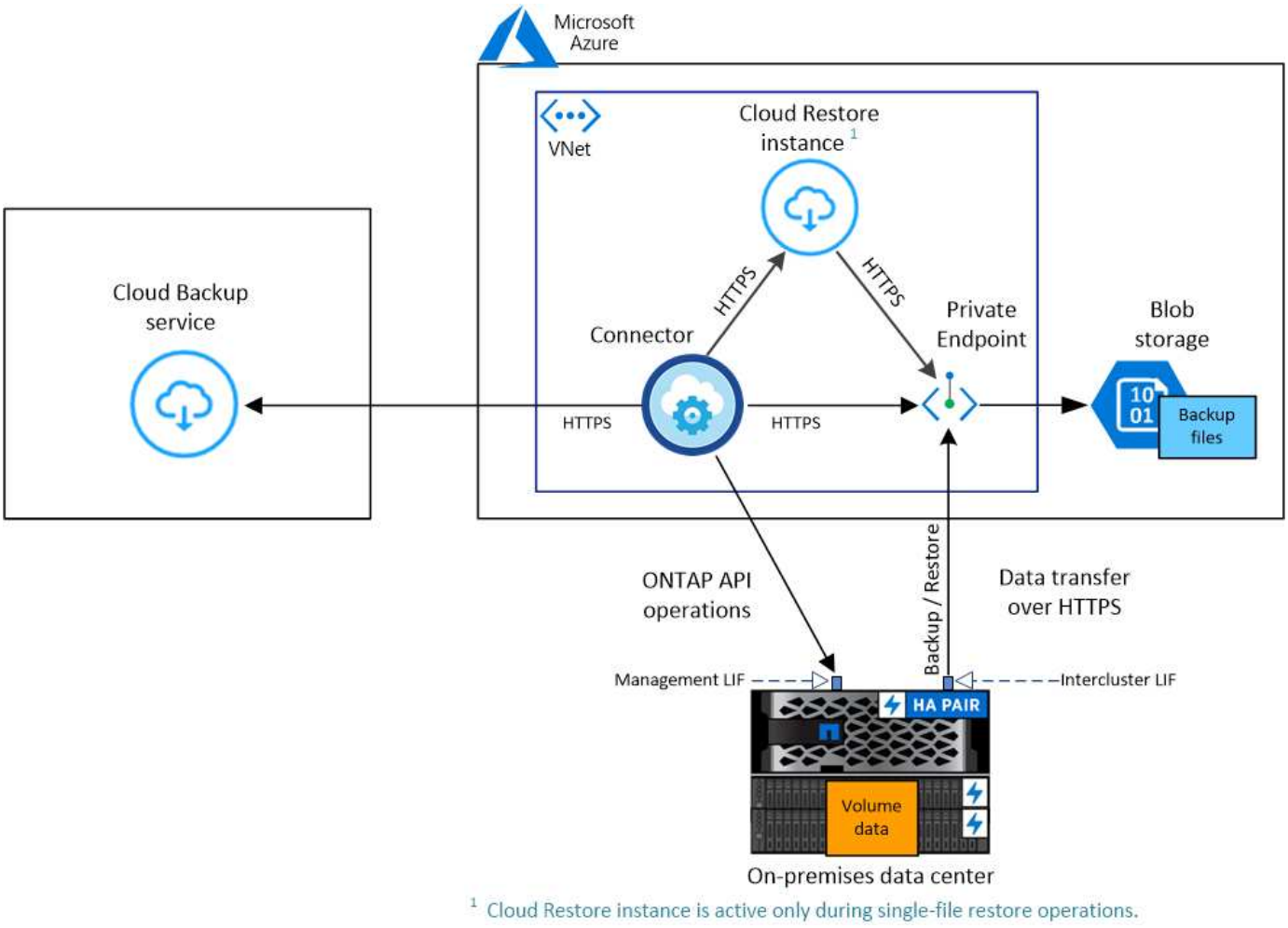
6 **Select the volumes that you want to back up**

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 you have a supported configuration before you start backing up on-premises volumes to Azure Blob storage.

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



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

Preparing your ONTAP clusters

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

Learn how to discover a cluster.

ONTAP requirements

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

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

  See how to manage your cluster licenses.

- Time and time zone are set correctly.

  See how to configure your cluster time.

Cluster networking requirements

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

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

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

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

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

Creating or switching Connectors

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

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

Preparing networking for the Connector

Ensure that the Connector has the required networking connections.

Steps

1. Ensure that the network where the Connector is installed enables the following connections:
   - An outbound internet connection to the Cloud Backup service over port 443 (HTTPS)
   - An HTTPS connection over port 443 to your Blob object storage
   - An HTTPS connection over port 443 to your ONTAP cluster management LIF
2. Enable a VNet Private Endpoint to Azure storage. This is needed if you have an ExpressRoute or VPN connection from your ONTAP cluster to the VNet and you want communication between the Connector and Blob storage to stay in your virtual private network.

Supported regions

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

License requirements

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

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

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

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

Preparing Azure Blob storage for backups

1. If your virtual or physical network uses a proxy server for internet access, ensure that the Cloud Restore virtual machine 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.

2. You use choose your own custom-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.
3. If you want to have a more secure connection over the public internet from your on-prem data center to the VNet, there is an option to configure an Azure Private Endpoint in the activation wizard. In this case you will need to know the VNet and Subnet for this connection. See details about using a Private Endpoint.

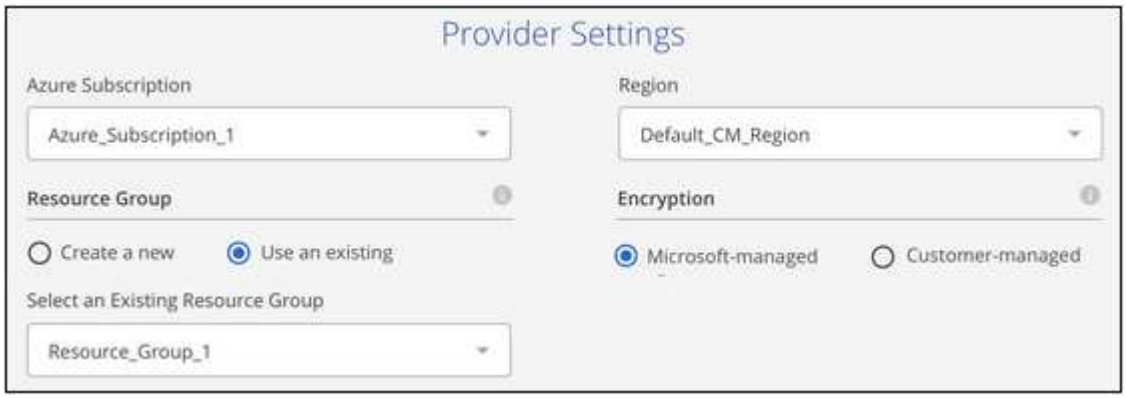
Enabling Cloud Backup

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

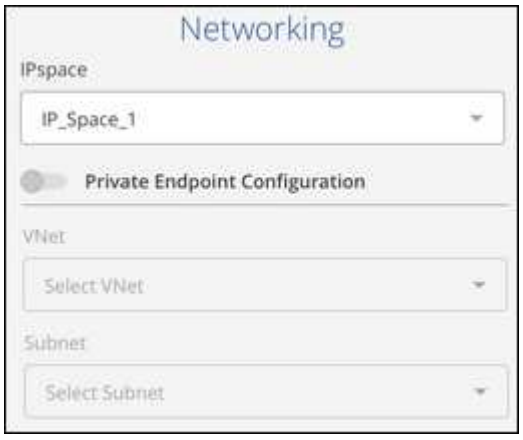
Steps

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

2. Select Microsoft Azure as your provider and click **Next**.
3. Enter the provider details and click **Next**.
   a. The Azure subscription used for backups and the Azure region where the backups will be stored.
   b. The resource group that manages the Blob container - you can create a new resource group or select an existing resource group.
   c. Whether you will 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).

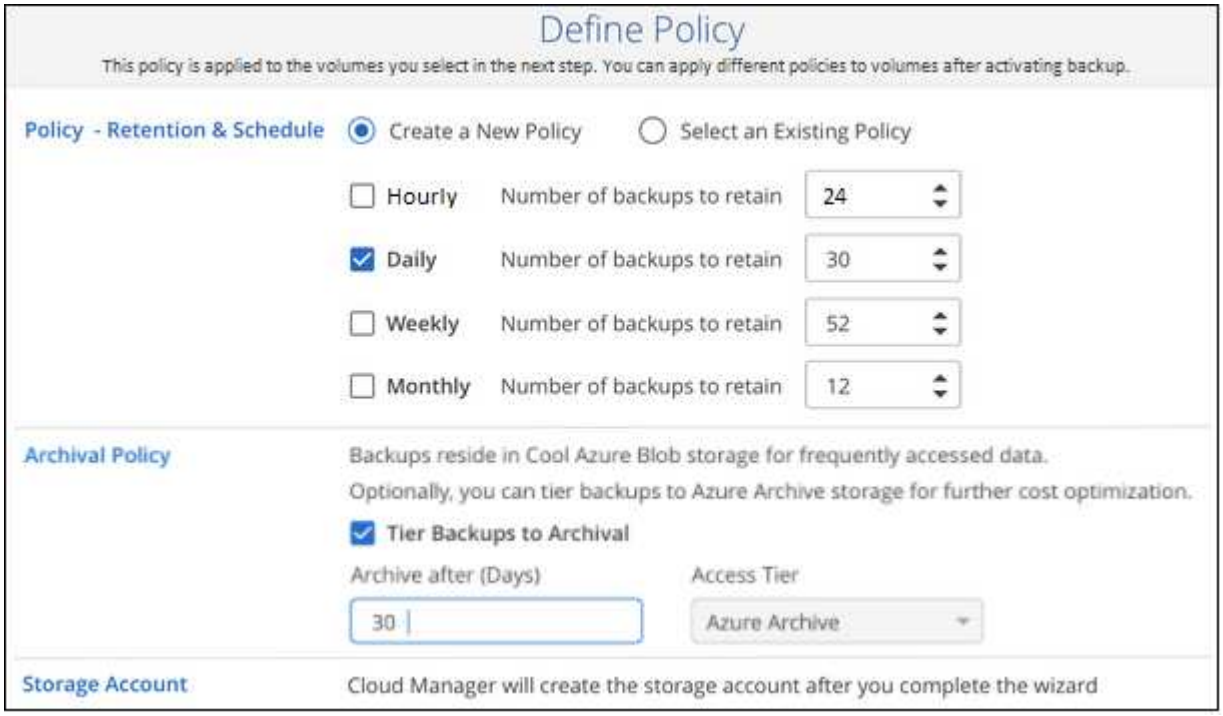


4. Enter the networking details and click **Next**.
   a. The IPspace in the ONTAP cluster where the volumes you want to back up reside. The intercluster LIFs for this IPspace must have outbound internet access.
   b. Optionally, choose whether you will configure an Azure Private Endpoint. See details about using a Private Endpoint.



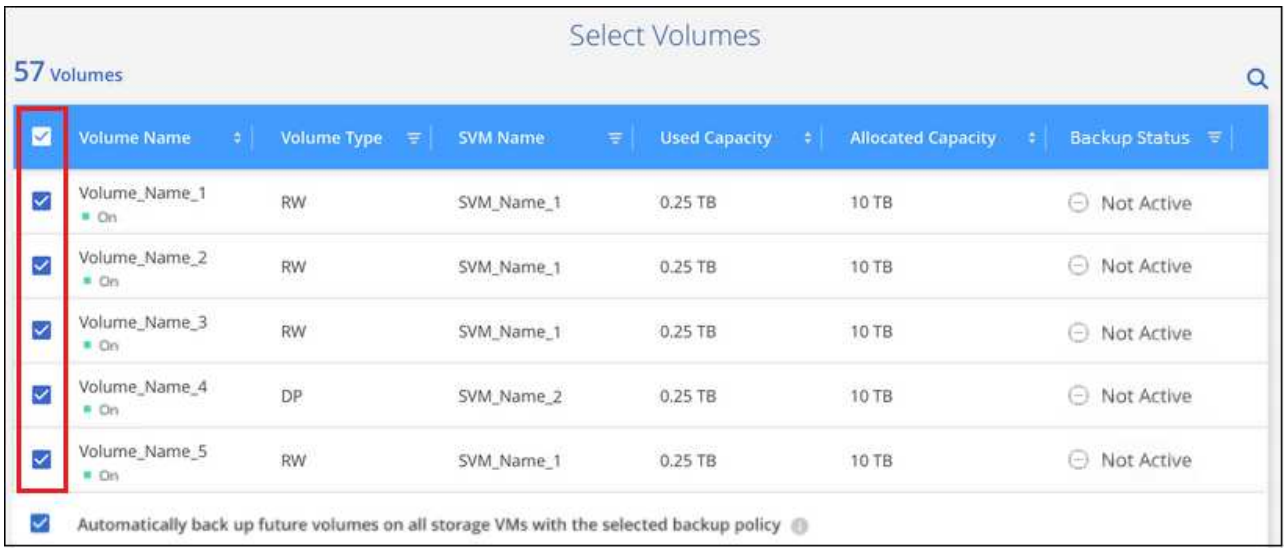
5. Enter the default backup policy details and click **Next**.
   a. Define the backup schedule and choose the number of backups to retain. See the list of existing policies you can choose.
   b. When using ONTAP 9.10.1 and greater, you can choose to tier backups to Azure Archive storage after

a certain number of days for further cost optimization. Learn more about using archival tiers.



6. 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).



   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.

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

Result

Cloud Backup starts taking the initial backups of each selected volume and the 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 on-premises ONTAP data to Google Cloud Storage

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

Note that "on-premises ONTAP systems" includes FAS, AFF, and ONTAP Select systems.

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

Quick start

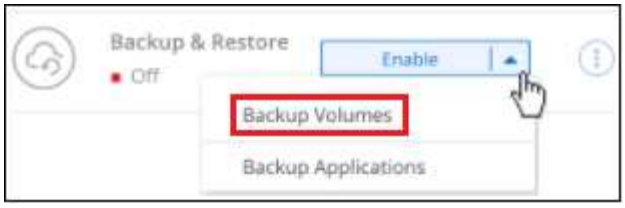
Get started quickly by following these steps, or scroll down to the remaining sections for full details.

Verify support for your configuration

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

Enable Cloud Backup on the system

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

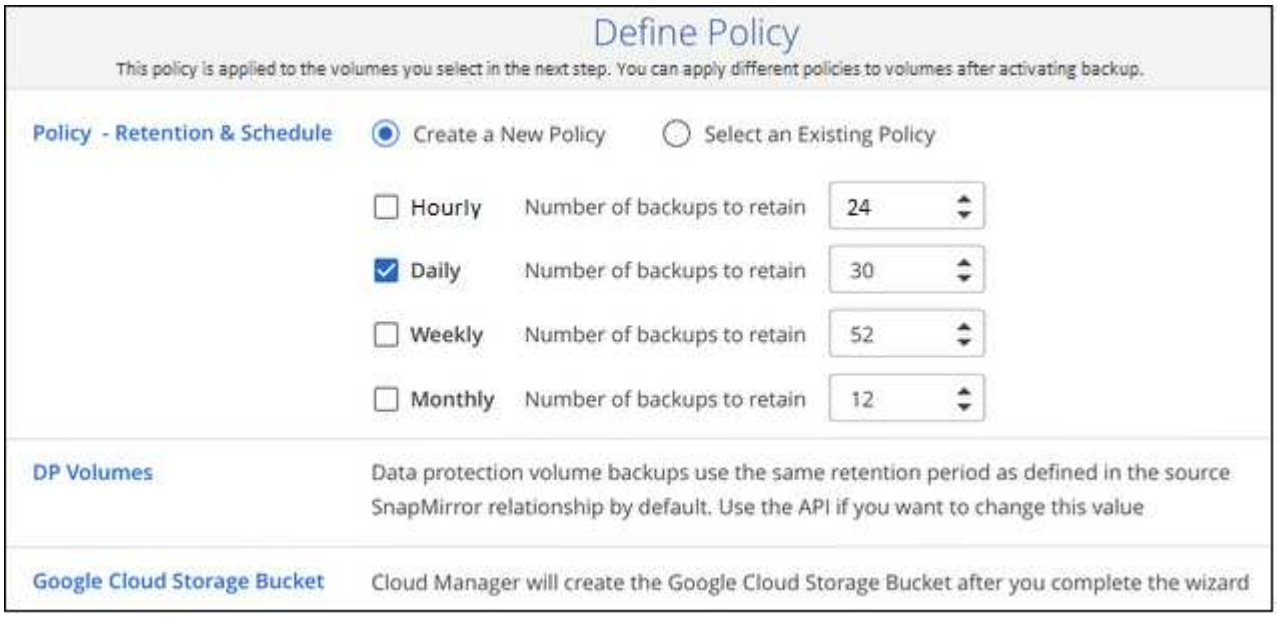


3 Select the cloud provider and enter the provider details

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

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.



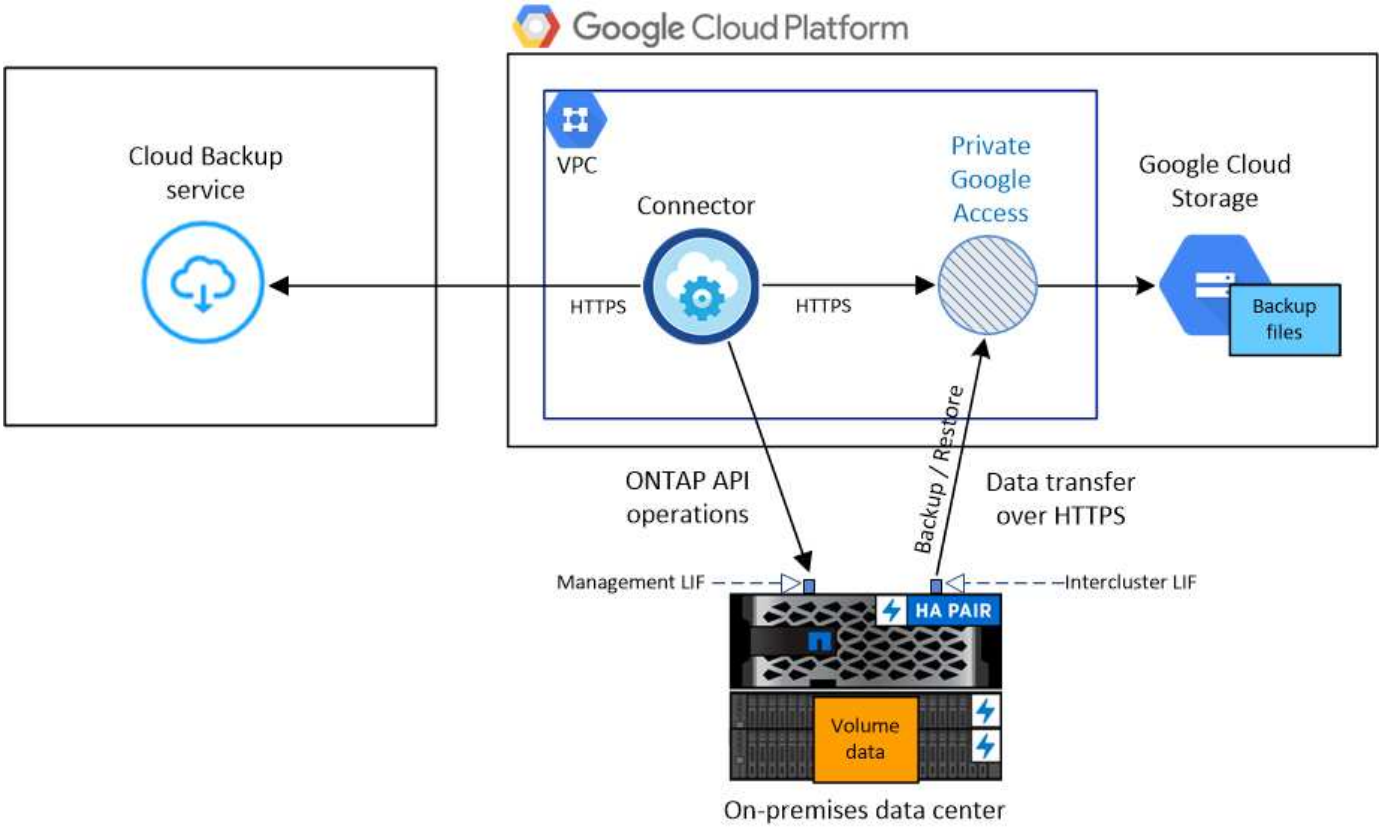
5 Select the volumes that you want to back up

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 you have a supported configuration before you start backing up on-premises volumes to Google Cloud storage.

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



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

Preparing your ONTAP clusters

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

Learn how to discover a cluster.

ONTAP requirements

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

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

  See how to manage your cluster licenses.

- Time and time zone are set correctly.

  See how to configure your cluster time.

Cluster networking requirements

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

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

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

  When you set up Cloud Backup, you are prompted for the IPspace to use. You should choose the IPspace that each LIF is associated with. That might be the "Default" IPspace or a custom IPspace that you created.
- The nodes' intercluster LIFs are able to access the object store.
- DNS servers have been configured for the storage VM where the volumes are located. See how to configure DNS services for the SVM.
- Note that if you use are using a different IPspace than the Default, then you might need to create a static route to get access to the object storage.
- Update firewall rules, if necessary, to allow Cloud Backup service connections from ONTAP to object storage through port 443 and name resolution traffic from the storage VM to the DNS server over port 53 (TCP/UDP).

Creating or switching Connectors

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

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

Preparing networking for the Connector

Ensure that the Connector has the required networking connections.

Steps

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

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

Supported regions

You can create backups from on-premises systems to Google Cloud storage in all regions where Cloud

Volumes ONTAP is supported. You specify the region where the backups will be stored when you set up the service.

License requirements

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

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

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

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

Preparing Google Cloud Storage for backups

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

Steps

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

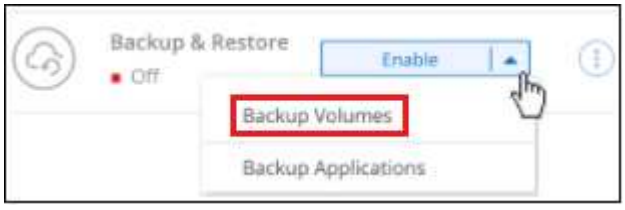
      You'll need to enter the keys in Cloud Backup later when you configure the backup service.

Enabling Cloud Backup

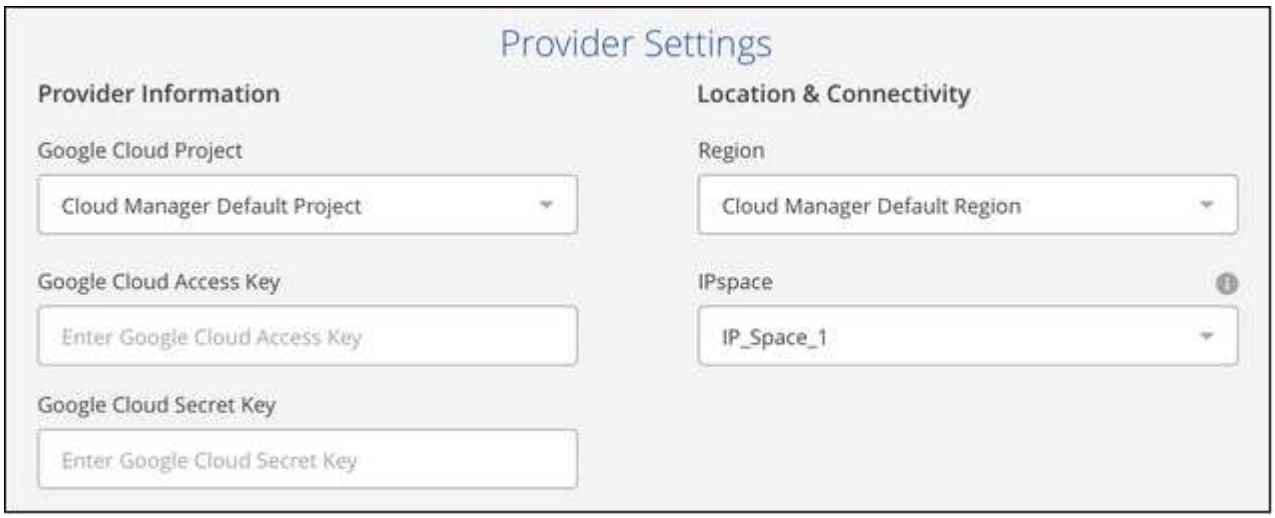
Enable Cloud Backup at any time directly from the on-premises working environment.

Steps

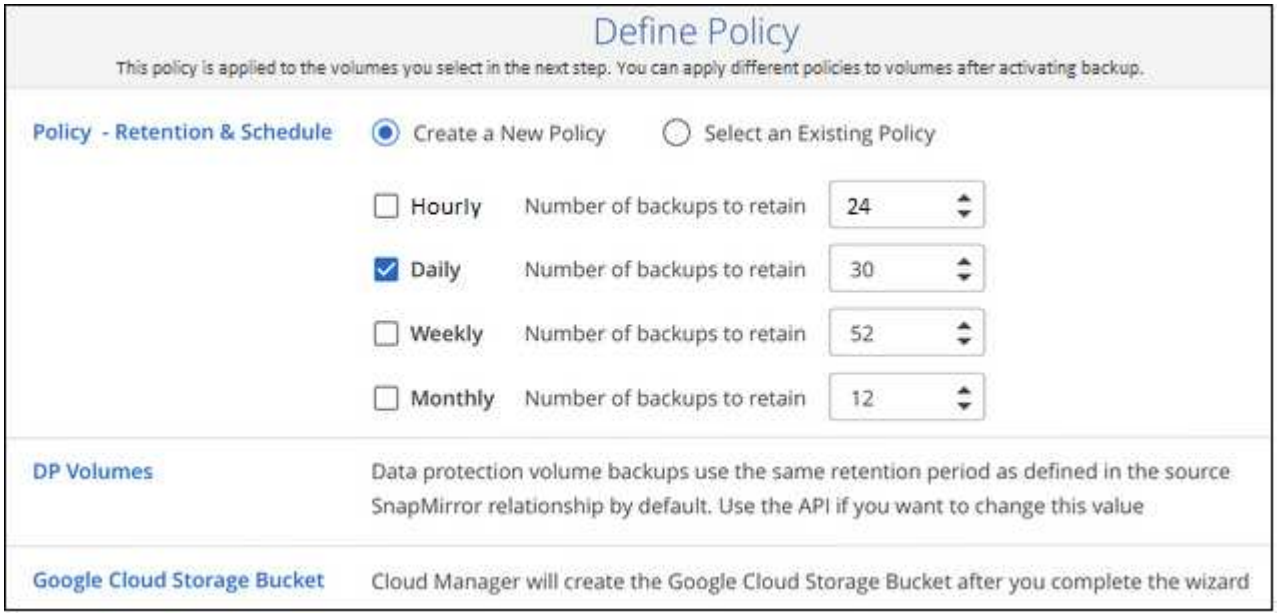
1. From the Canvas, select the working environment and click **Enable > Backup Volumes** next to the Backup & Restore service in the right-panel.



2. Select Google Cloud as your provider and click **Next**.
3. Enter the provider details and click **Next**.
   a. The Google Cloud Project where you want the Google Cloud Storage bucket to be created for backups. (The Project must have a Service Account that has the predefined Storage Admin role.)
   b. The Google Access Key and Secret Key used to store the backups.
   c. The Google region where the backups will be stored.
   d. The IPspace in the ONTAP cluster where the volumes you want to back up reside. The intercluster LIFs for this IPspace must have outbound internet access.



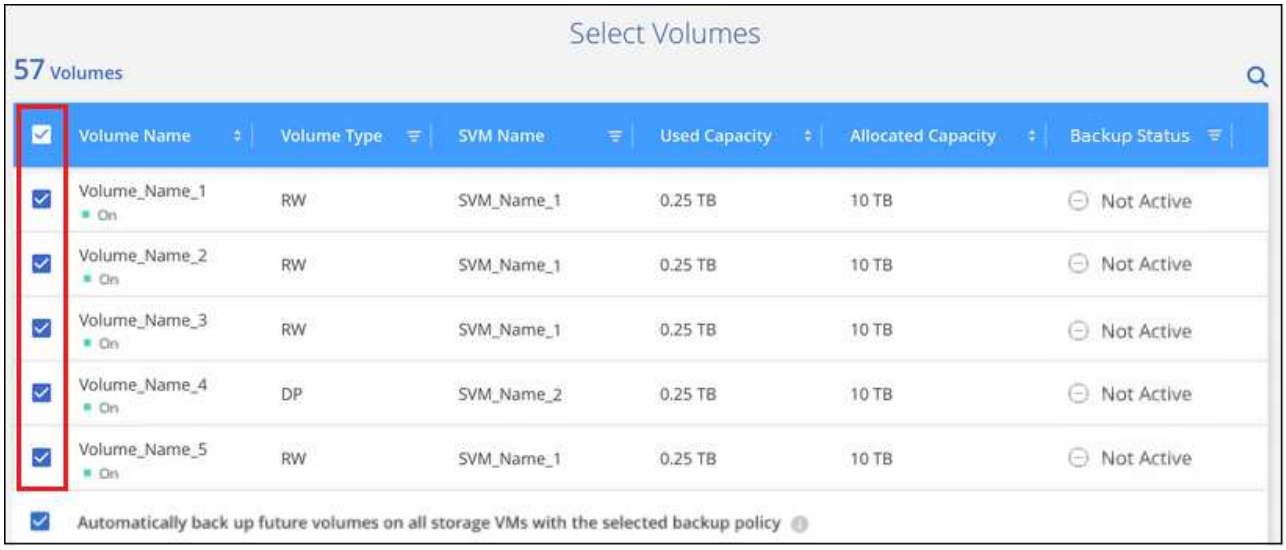
4. In the *Define Policy* page, select an existing backup schedule and retention value, or define a new default backup policy, and click **Next**.



   See the list of existing policies.

5. 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).



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 your volumes.

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.

Backing up on-premises ONTAP data to StorageGRID

Complete a few steps to get started backing up data from your on-premises ONTAP systems to object storage in your NetApp StorageGRID systems.

Note that "on-premises ONTAP systems" includes FAS, AFF, and ONTAP Select systems.

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

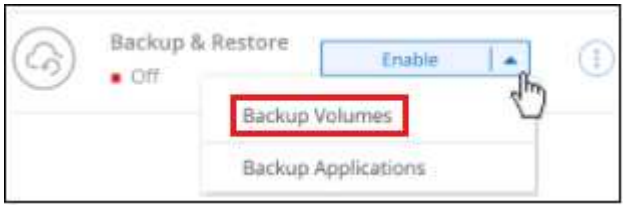
- You have discovered the on-premises cluster and added it to a working environment in Cloud Manager. See Discovering ONTAP clusters for details.

- The cluster is running ONTAP 9.7P5 or later.
- The cluster has a SnapMirror license — it is included as part of the Premium Bundle or Data Protection Bundle.
- The cluster must have the required network connections to StorageGRID and to the Connector.

- You have a Connector installed on your premises.
  - Networking for the Connector enables an outbound HTTPS connection to the ONTAP cluster and to StorageGRID.
- You have purchased and activated a Cloud Backup BYOL license from NetApp.
- Your StorageGRID has version 10.3 or later with access keys that have S3 permissions.

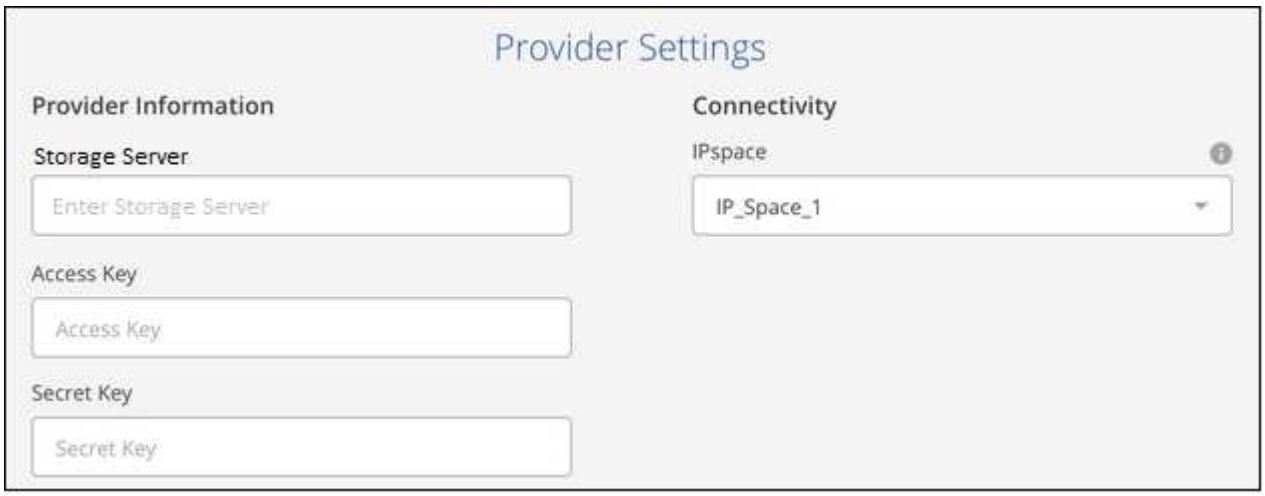
2 Enable Cloud Backup on the system

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



3 Enter the StorageGRID details

Select StorageGRID as the provider, and then enter the StorageGRID server and service account details. You also need to specify the IPspace in the ONTAP cluster where the volumes reside.



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**

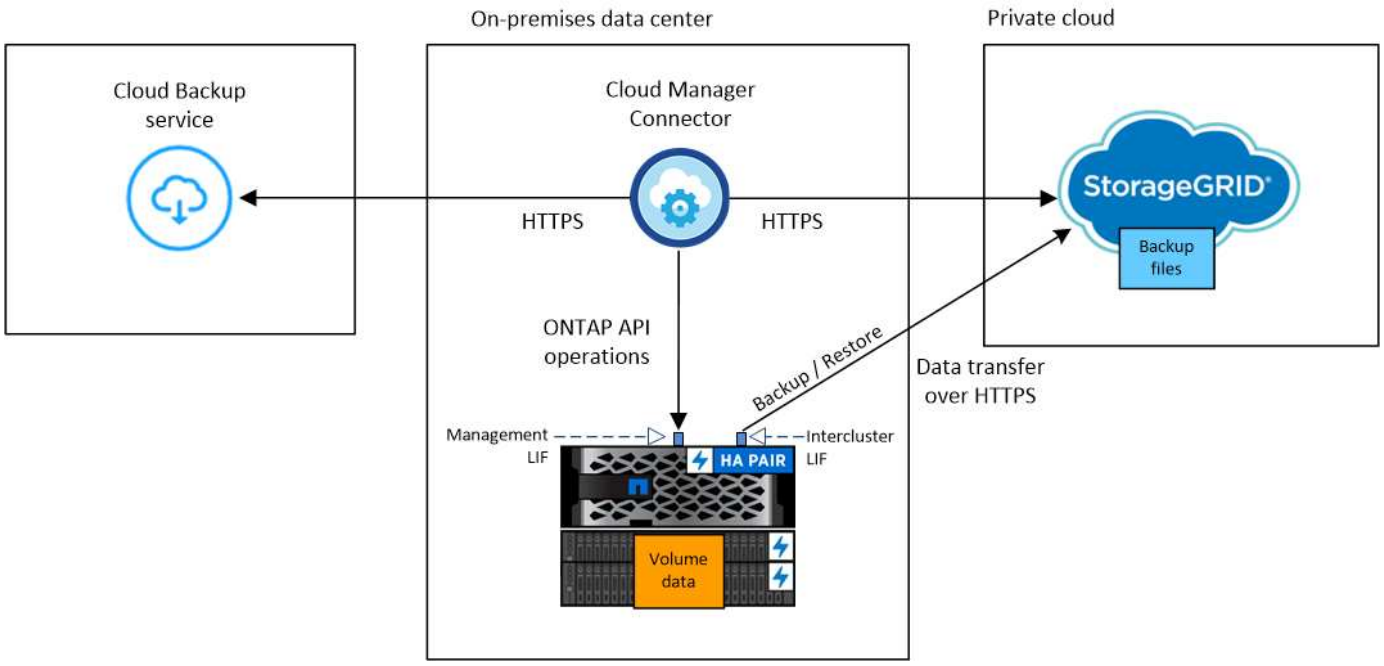
Identify which volumes you want to back up using the default backup policy in the Select Volumes page. If you want to assign different backup policies to certain volumes, you can create additional policies and apply them to volumes later.

An S3 bucket is created automatically in the service account indicated by the S3 access key and secret key you entered, and the backup files are stored there.

Requirements

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

The following image shows each component when backing up an on-prem ONTAP system to StorageGRID and the connections that you need to prepare between them:



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

Preparing your ONTAP clusters

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

Learn how to discover a cluster.

ONTAP requirements

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

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

  See how to manage your cluster licenses.

- Time and time zone are set correctly.

  See how to configure your cluster time.

Cluster networking requirements

- The ONTAP cluster initiates an HTTPS connection over a user-specified port from the intercluster LIF to StorageGRID for backup and restore operations. The port is configurable during backup setup.

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

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

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

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

Preparing StorageGRID

StorageGRID must meet the following requirements. See the StorageGRID documentation for more information.

Supported StorageGRID versions

StorageGRID 10.3 and later is supported.

S3 credentials

When you set up backup to StorageGRID, the backup wizard prompts you for an S3 access key and secret key for a service account. A service account enables Cloud Backup to authenticate and access the StorageGRID buckets used to store backups. The keys are required so that StorageGRID knows who is making the request.

These access keys must be associated with a user who has the following permissions:

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject",
"s3:CreateBucket"
```

Object versioning

You must not enable StorageGRID object versioning on the object store bucket.

Creating or switching Connectors

When backing up data to StorageGRID, a Connector must be available on your premises. You'll either need to install a new Connector or make sure that the currently selected Connector resides on-prem.

- Learn about Connectors
- Installing the Connector on a Linux host with internet access
- Switching between Connectors

Preparing networking for the Connector

Ensure that the Connector has the required networking connections.

Steps

1. Ensure that the network where the Connector is installed enables the following connections:
    - An HTTPS connection over port 443 to StorageGRID
    - An HTTPS connection over port 443 to your ONTAP cluster management LIF
    - An outbound internet connection over port 443 to Cloud Backup

License requirements

Before your 30-day free trial of Cloud Backup expires, you need to purchase and activate a Cloud Backup BYOL license from NetApp. This license is for the account and can be used across multiple systems.

You'll 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.

PAYGO licensing is not supported when backing up files to StorageGRID.

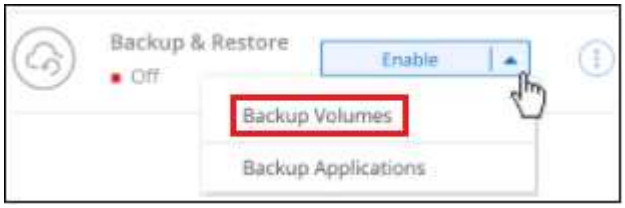
A SnapMirror license is required on the cluster. Note that the "Hybrid Cloud Bundle" is not required when using Cloud Backup.

Enabling Cloud Backup to StorageGRID

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

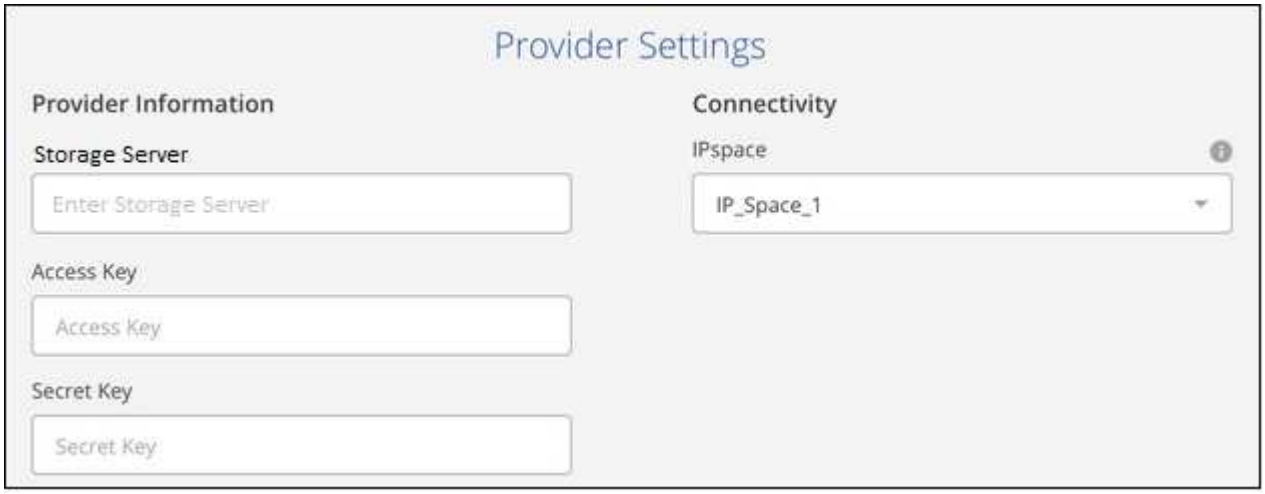
Steps

1. From the Canvas, select the on-premises working environment and click **Enable > Backup Volumes** next to the Backup & Restore service in the right-panel.



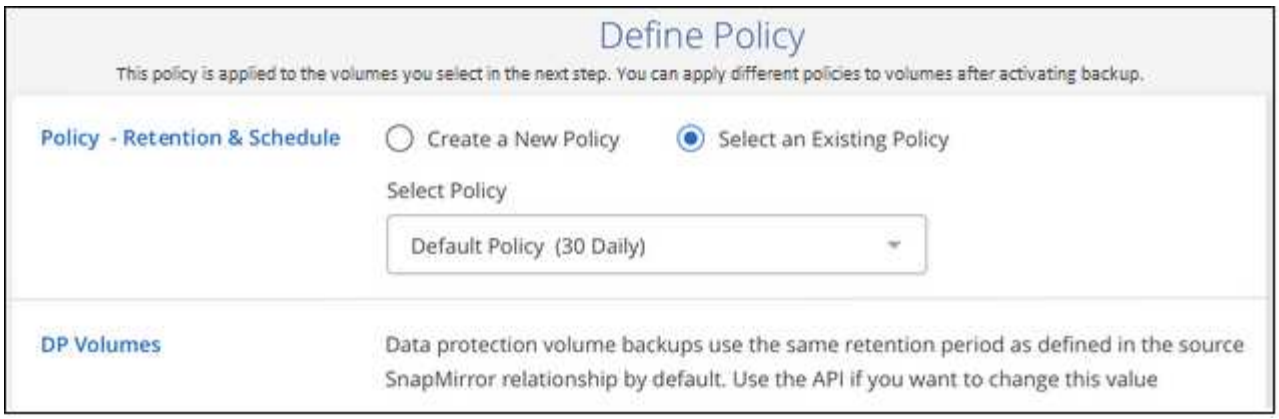
2. Select **StorageGRID** as the provider, click **Next**, and then enter the provider details:
   a. The FQDN of the StorageGRID server and the port that ONTAP should use for HTTPS communication with StorageGRID; for example: `s3.eng.company.com:8082`
   b. The Access Key and the Secret Key used to access the bucket to store backups.
   c. The IPspace in the ONTAP cluster where the volumes you want to back up reside. The intercluster LIFs for this IPspace must have outbound internet access.

      Selecting the correct IPspace ensures that Cloud Backup can set up a connection from ONTAP to your StorageGRID object storage.



      Note that you cannot change this information after the service has started.

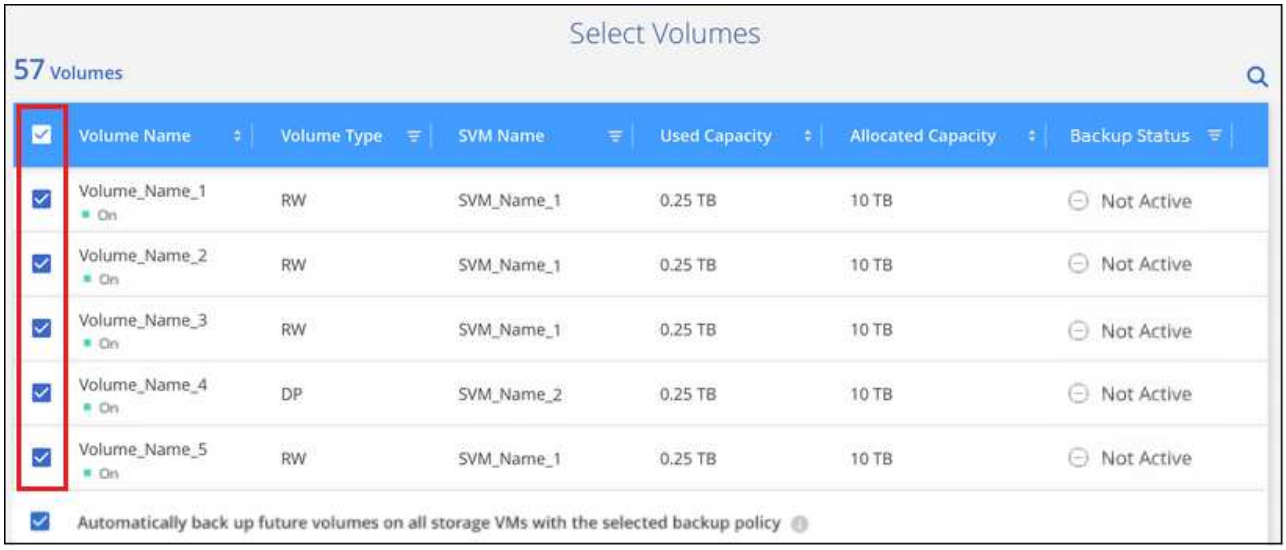
3. In the *Define Policy* page, select the default backup schedule and retention value and click **Next**.



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).



   If you want all volumes added in the future to this cluster 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 service account indicated by the S3 access key and secret key you entered, and the backup files are stored there. 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 new volume on an on-premises ONTAP system.

Managing backups for your ONTAP systems

You can manage backups for your Cloud Volumes ONTAP and on-premises ONTAP systems by changing the backup schedule, enabling/disabling volume backups, deleting backups, and more.

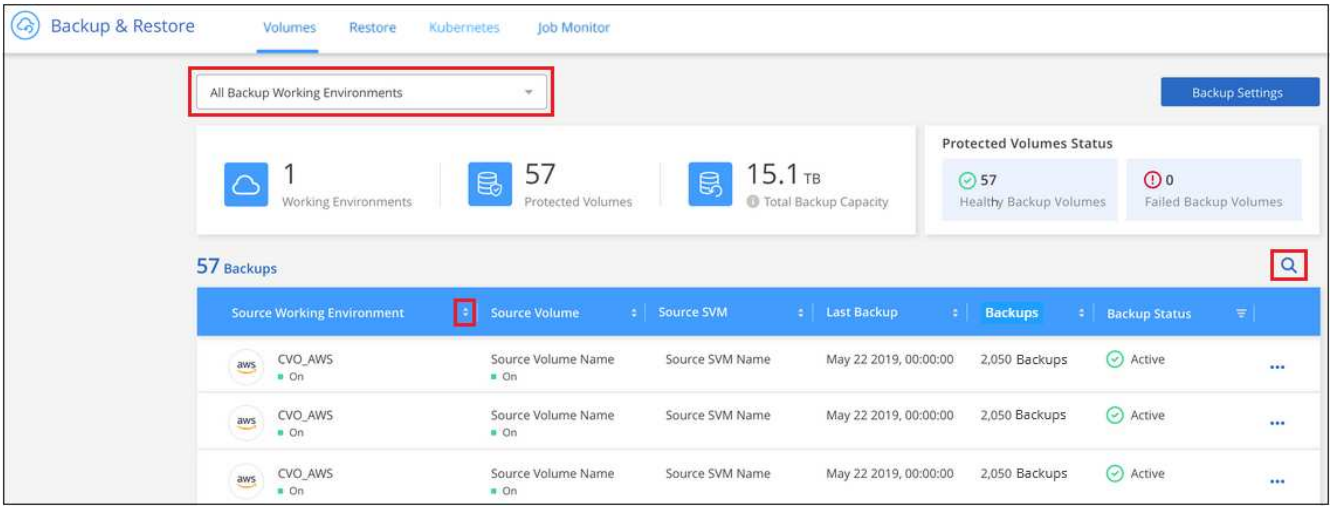
Do not manage or change backup files directly from your cloud provider environment. This may corrupt the files and will result in an unsupported configuration.

Viewing the volumes that are being backed up

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

Steps

1. Click the **Backup & Restore** tab.
2. Click the **Volumes** tab to view the list of volumes for Cloud Volumes ONTAP and on-premises ONTAP systems.



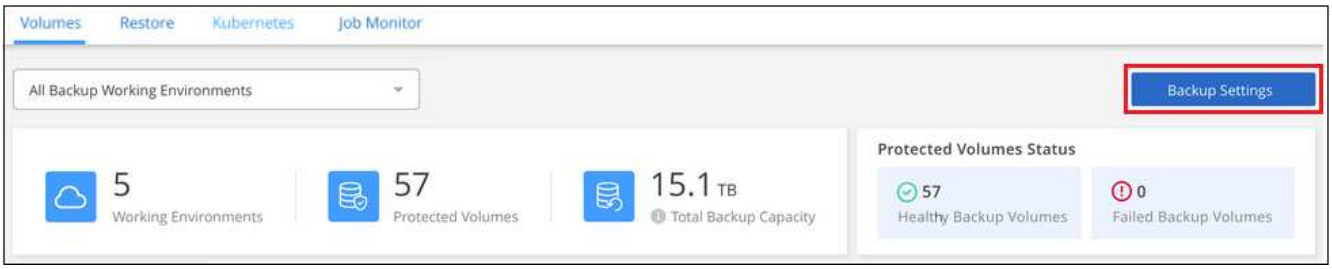
If you are looking for specific volumes in certain working environments, you can refine the list by working environment and volume, or you can use the search filter.

Editing an existing backup policy

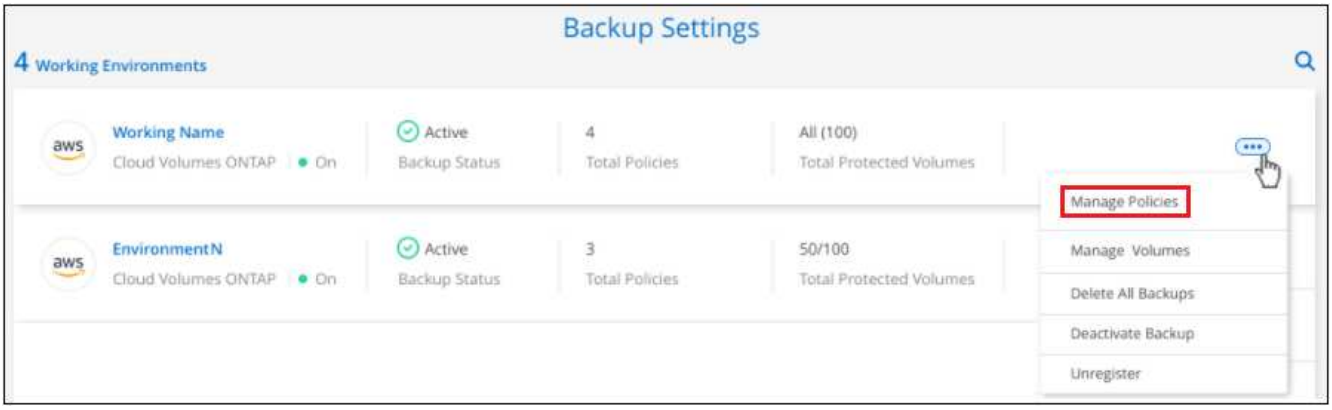
You can change the attributes for a backup policy that is currently applied to volumes in a working environment. Changing the backup policy affects all existing volumes that are using the policy.

Steps

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



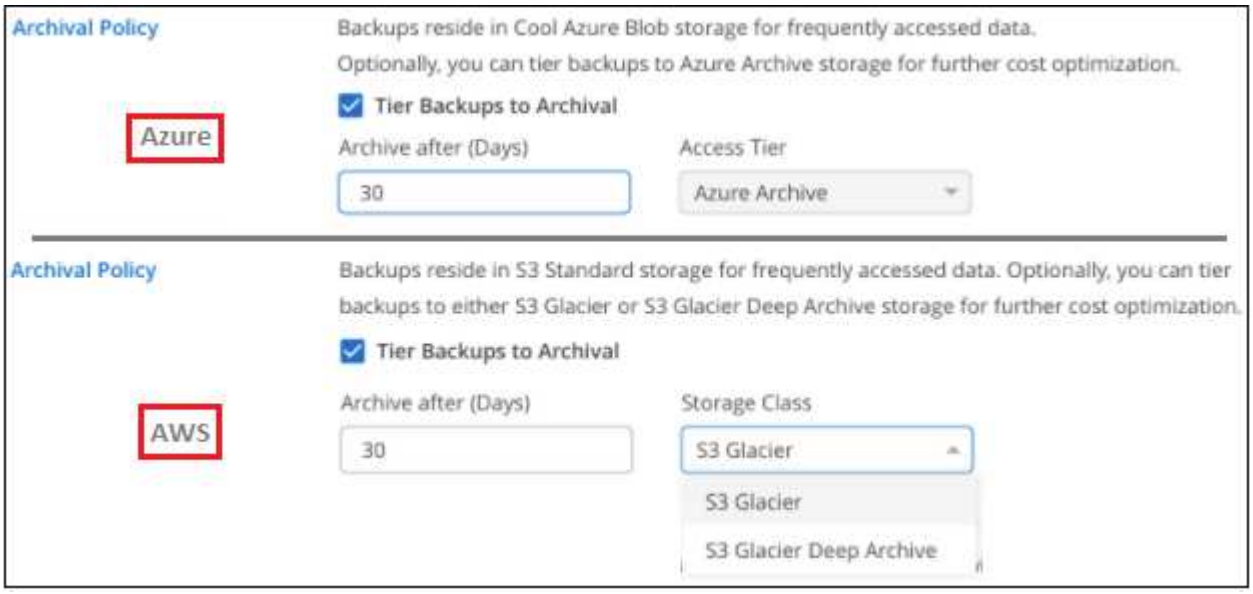
2. From the *Backup Settings* page, click ••• for the working environment where you want to change the settings, and select **Manage Policies**.



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**.

If your cluster is running ONTAP 9.10.1 or greater, and you are using AWS or Azure for your cloud storage, you also have the option to enable or disable tiering of backups to archival storage after a certain number of days.
Learn more about using Azure archival storage.
Learn more about using AWS archival storage.



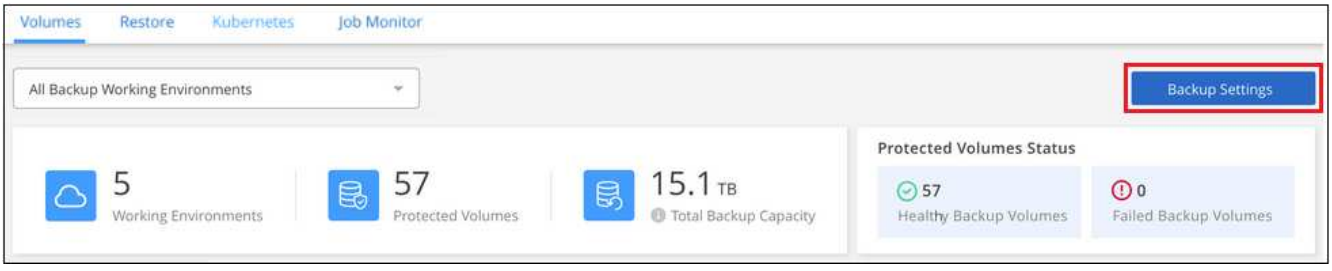
Note that any backup files that have been tiered to archival storage are left in that tier if you stop tiering backups to archive - they are not automatically moved back to the standard tier.

Enabling and disabling backups of volumes

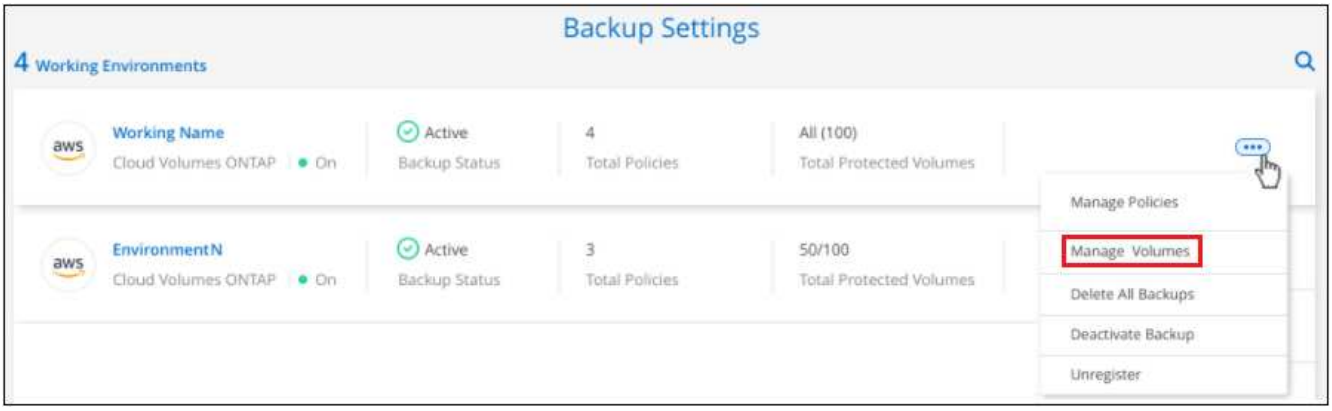
You can stop backing up a volume if you do not need backup copies of that volume and you do not want to pay for the cost to store the backups. You can also add a new volume to the backup list if it is not currently being backed up.

Steps

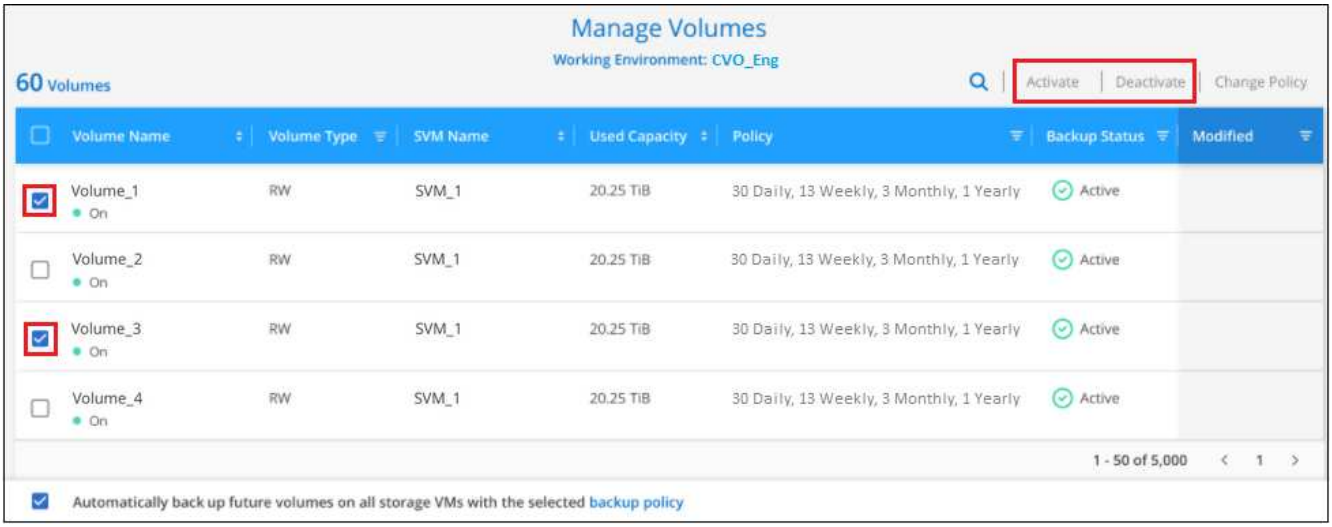
1. From the **Volumes** tab, select **Backup Settings**.



2. From the *Backup Settings page*, click ••• for the working environment and select **Manage 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.



You can choose to have all volumes added in the future to have backup enabled, or not, by using the checkbox for "Automatically back up future volumes…". If you disable this setting, you'll need to manually enable backups for volumes added in the future.

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.

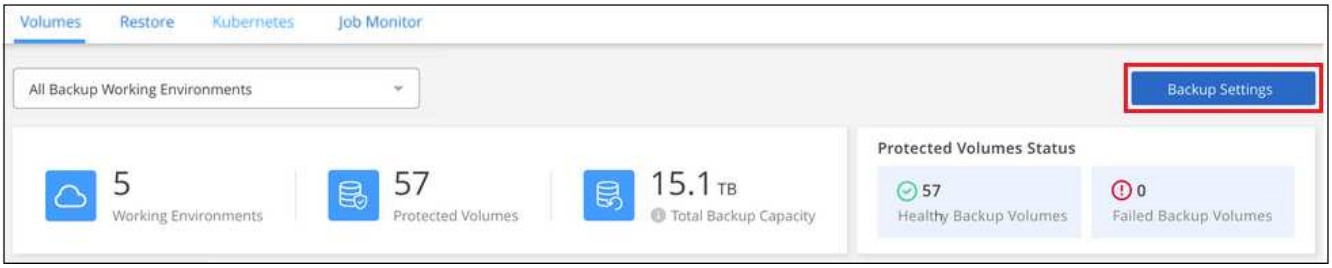
Adding a new backup policy

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 defined. 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.

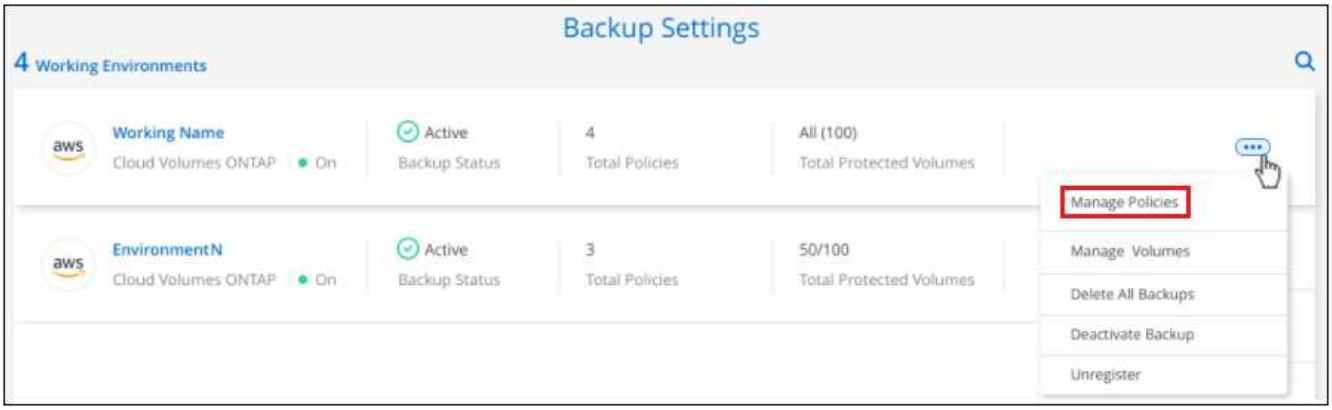
If you want to apply a new backup policy to certain volumes in a working environment, you first need to add the backup policy to the working environment. Then you can apply the policy to volumes in that working environment.

Steps

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

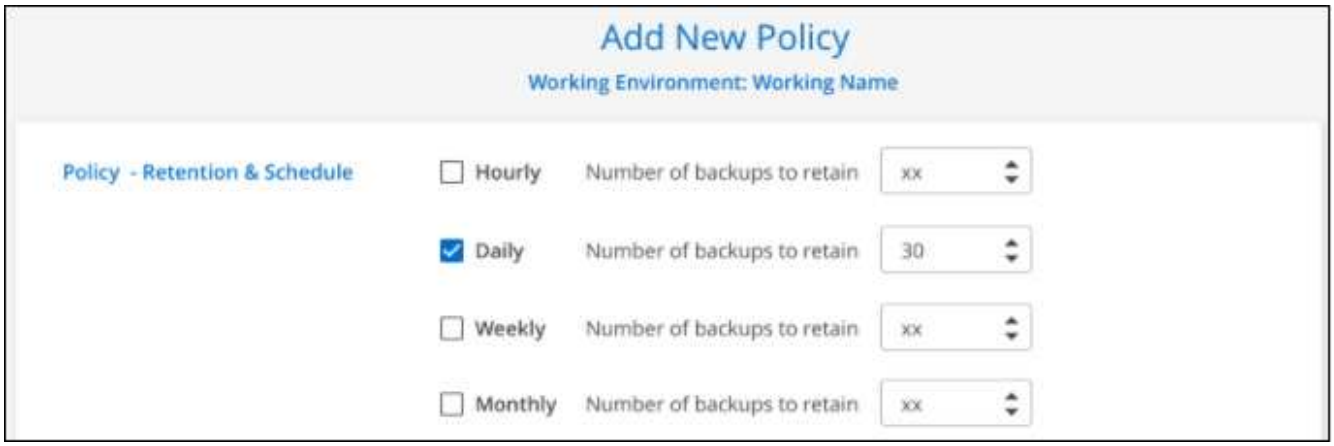


2. From the *Backup Settings* page, click ••• for the working environment where you want to add the new policy, and select **Manage Policies**.



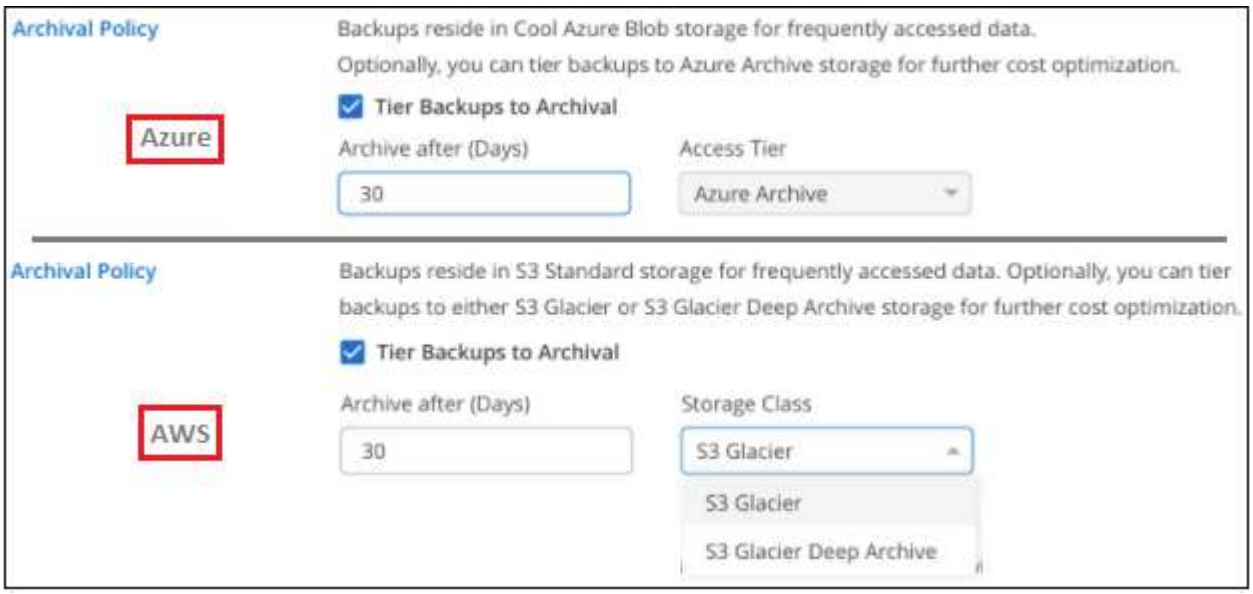
3. From the *Manage Policies* page, click **Add New Policy**.

4. From the *Add New Policy* page, define the schedule and backup retention and click **Save**.



If your cluster is running ONTAP 9.10.1 or greater, and you are using AWS or Azure for your cloud storage,

you also have the option to enable or disable tiering of backups to archival storage after a certain number of days.
Learn more about using Azure archival storage.
Learn more about using AWS archival storage.



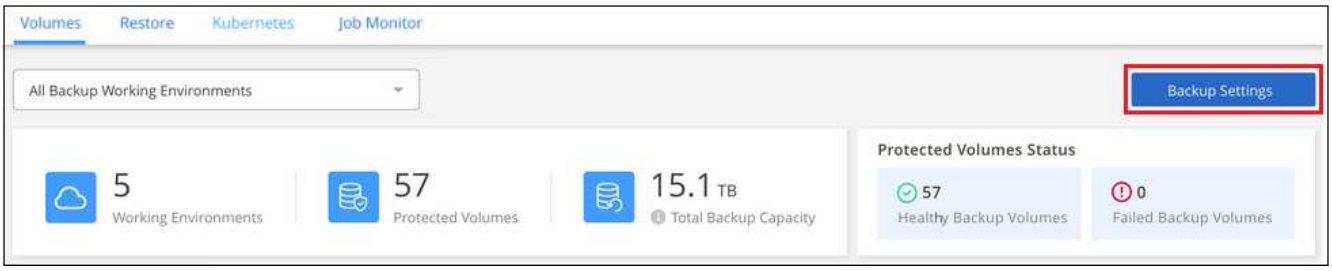
Changing the policy assigned to existing volumes

You can change the backup policy assigned to your existing volumes if you want to change the frequency of taking backups, or if you want to change the retention value.

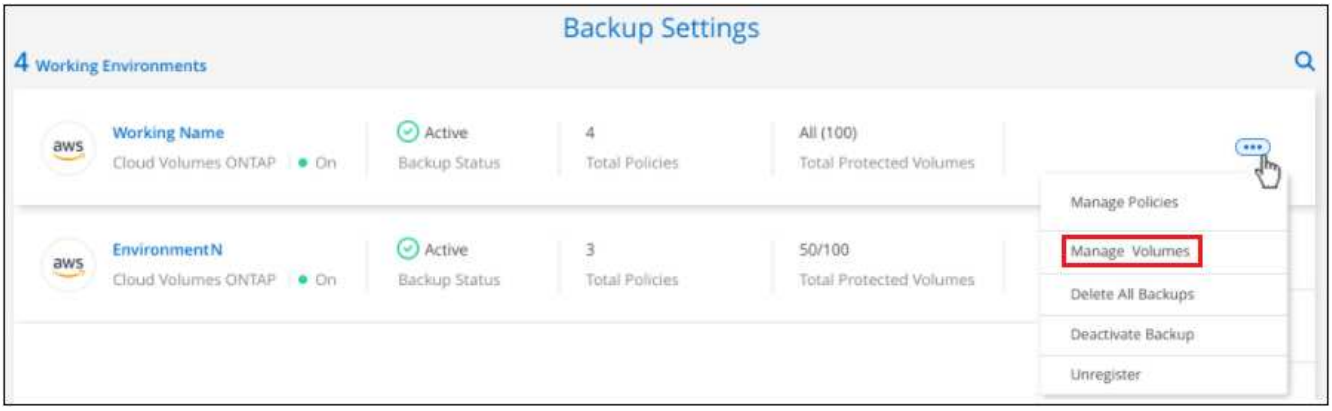
Note that the policy that you want to apply to the volumes must already exist. See how to add a new backup policy for a working environment.

Steps

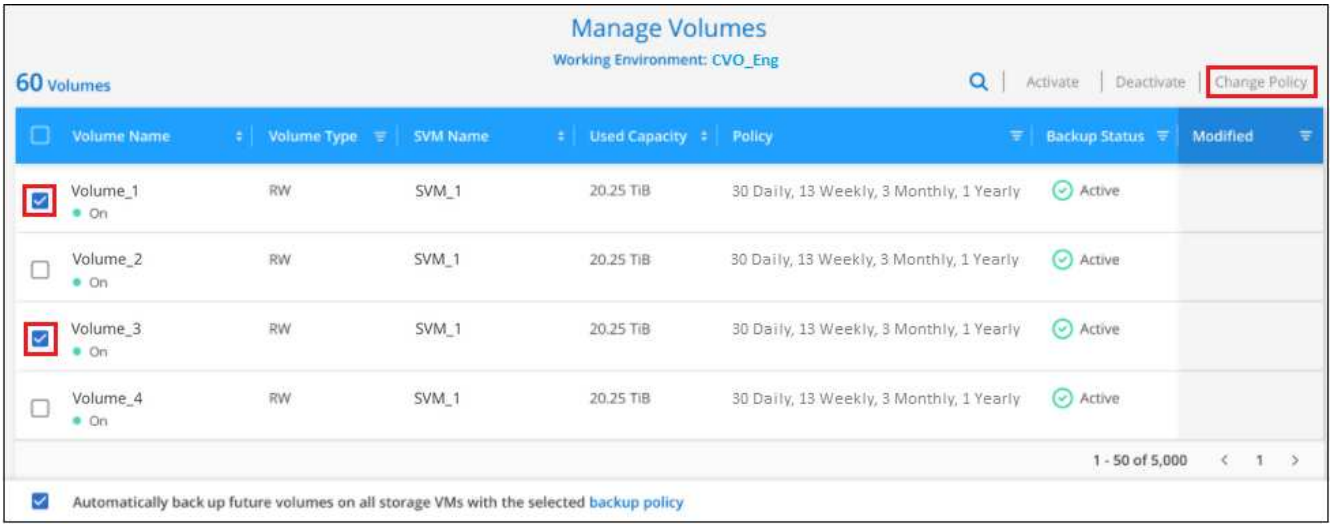
1. From the **Volumes** tab, select **Backup Settings**.



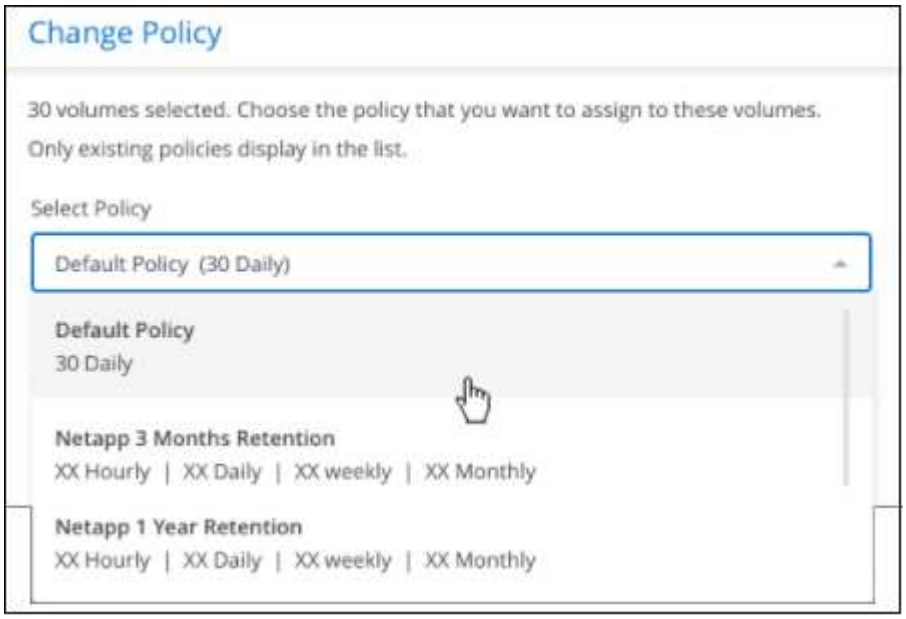
2. From the *Backup Settings page*, click ••• for the working environment where the volumes exist, and select **Manage Volumes**.



3. Select the checkbox for a volume, or volumes, that you want to change the policy for, and then click **Change Policy**.



4. In the *Change Policy* page, select the policy that you want to apply to the volumes, and click **Change Policy**.



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

Creating a manual volume backup at any time

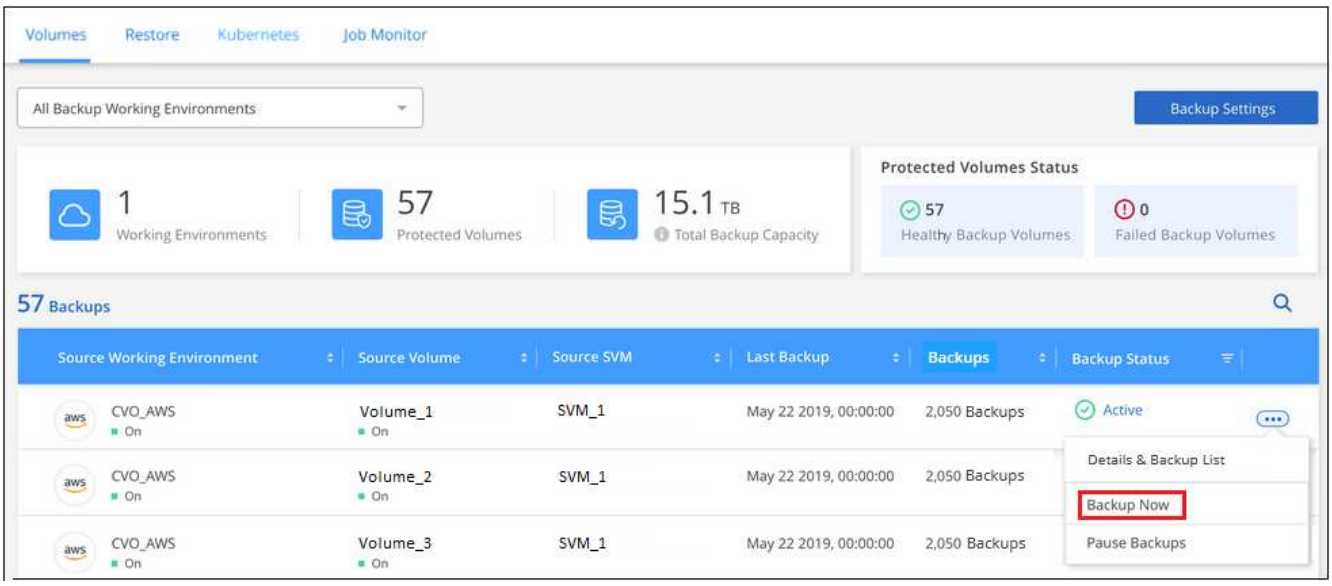
You can create an on-demand backup at any time to capture the current state of the volume. This can be useful if very important changes have been made to a volume and you don't want to wait for the next scheduled backup to protect that data, or if the volume is not currently being backed up and you want to capture its current state.

The backup name includes the timestamp so you can identify your on-demand backup from other scheduled backups.

On-demand volume backup isn't supported on data protection volumes.

Steps

1. From the **Volumes** tab, click ••• for the volume and select **Backup Now**.



The Backup Status column for that volume displays "In Progress" until the backup is created.

Viewing the list of backups for each volume

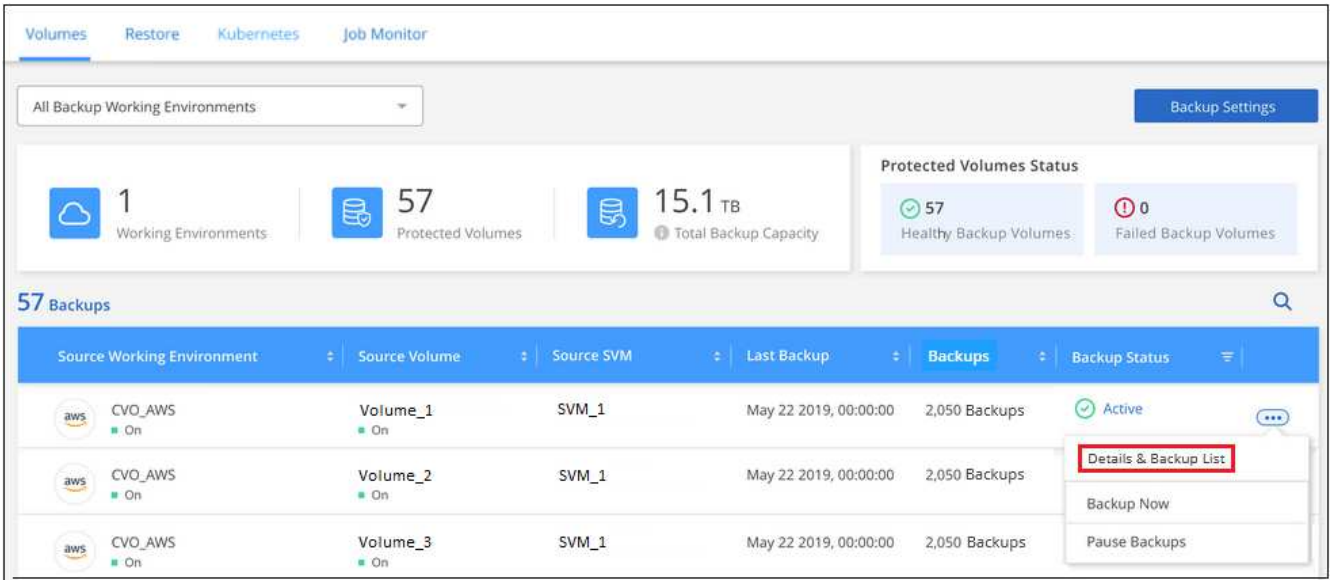
You can view the list of all backup files that exist for each volume. This page displays details about the source volume, destination location, and backup details such as last backup taken, the current backup policy, backup file size, and more.

This page also enables you perform the following tasks:

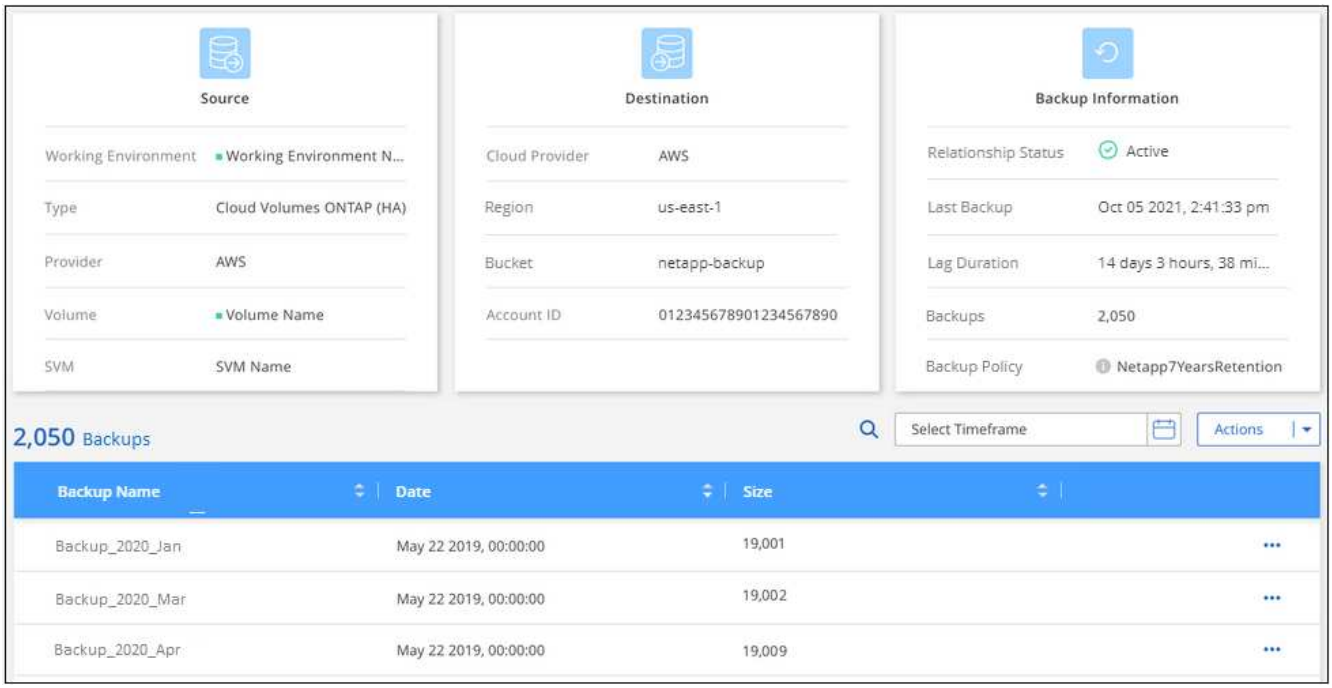
- Delete all backup files for the volume
- Delete individual backup files for the volume
- Download a backup report for the volume

Steps

1. From the **Volumes** 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 working environment or 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.

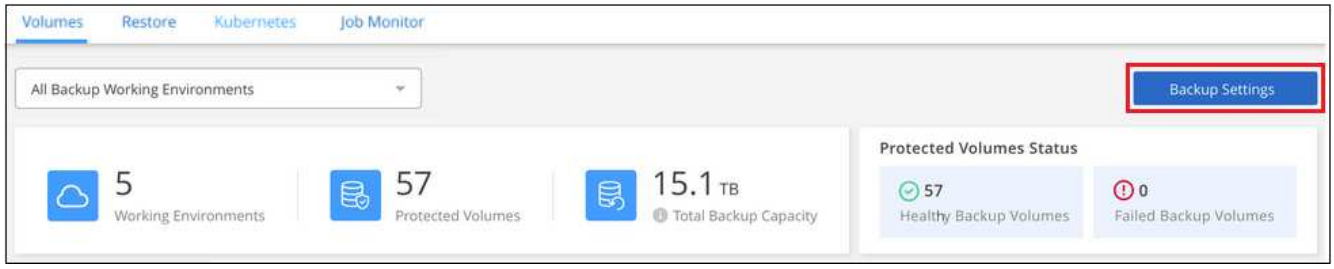
If you plan to delete a working environment or cluster that has backups, you must delete the backups **before** deleting the system. Cloud Backup doesn't automatically delete backups when you delete a system, and there is no current support in the UI to delete the backups after the system has been deleted.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

Deleting all backup files for a working environment

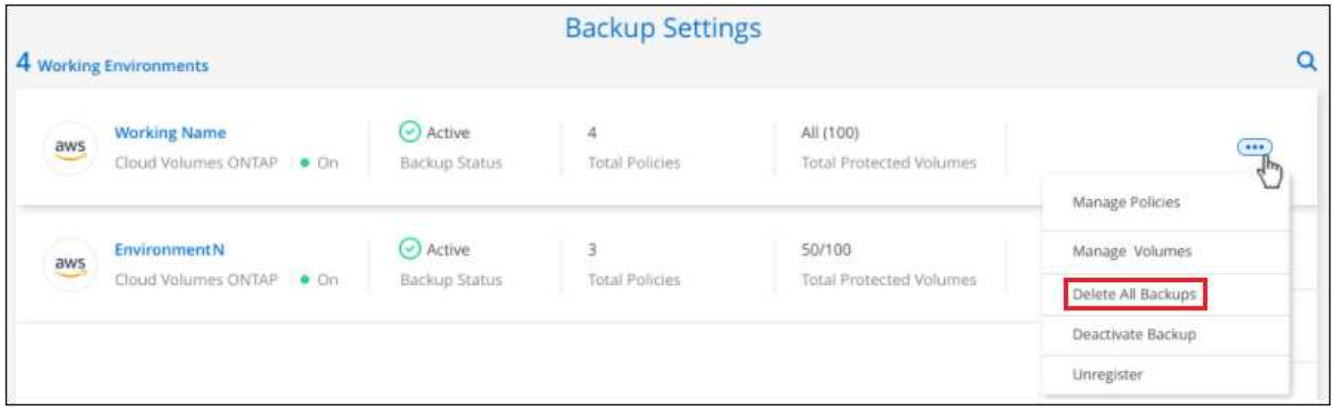
Deleting all backups for a working environment does not disable future backups of volumes in this working environment. If you want to stop creating backups of all volumes in a working environment, you can deactivate backups as described here.

Steps

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



2. Click ••• for the working environment, or 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**.

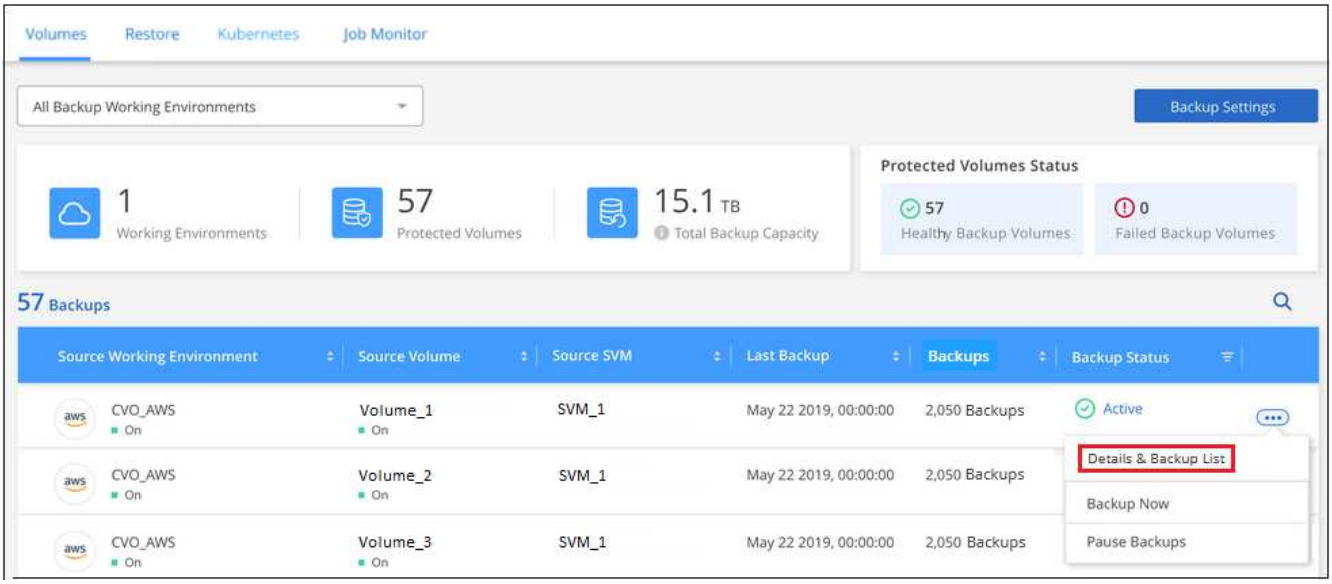
Deleting all backup files for a volume

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

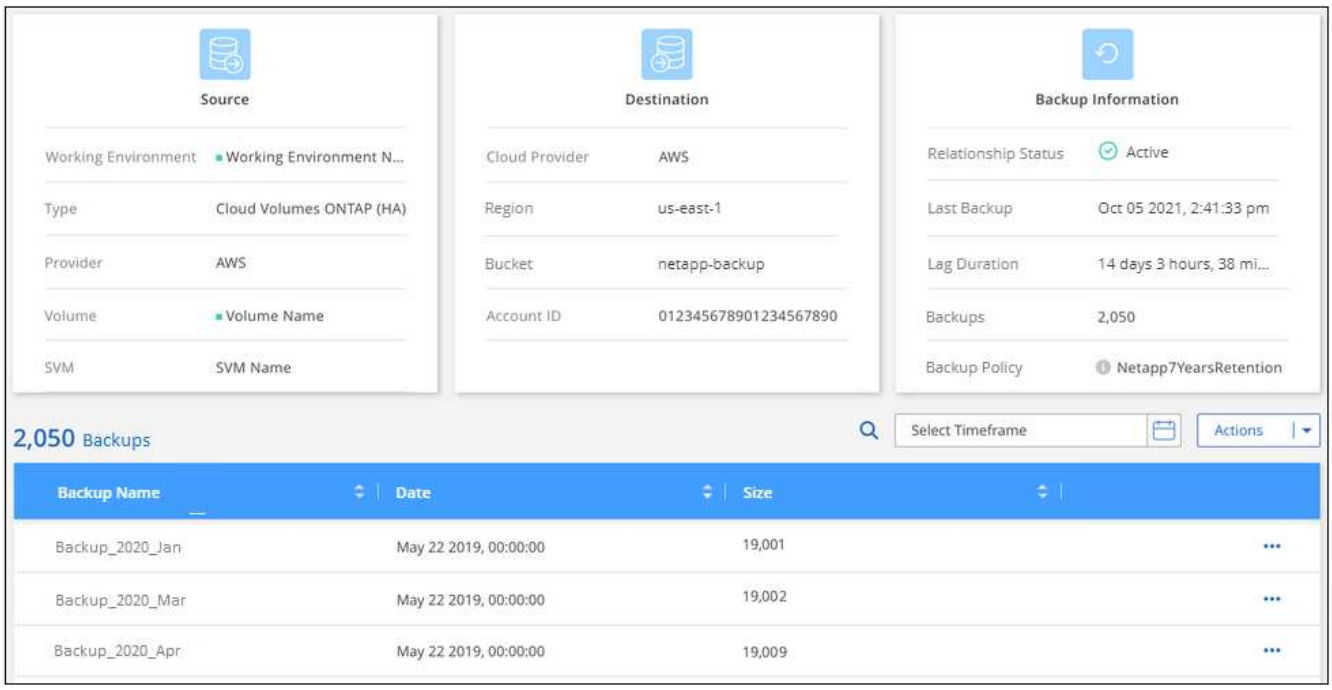
You can restart making backups for the volume at any time from the Manage Backups page.

Steps

1. From the **Volumes** 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**.

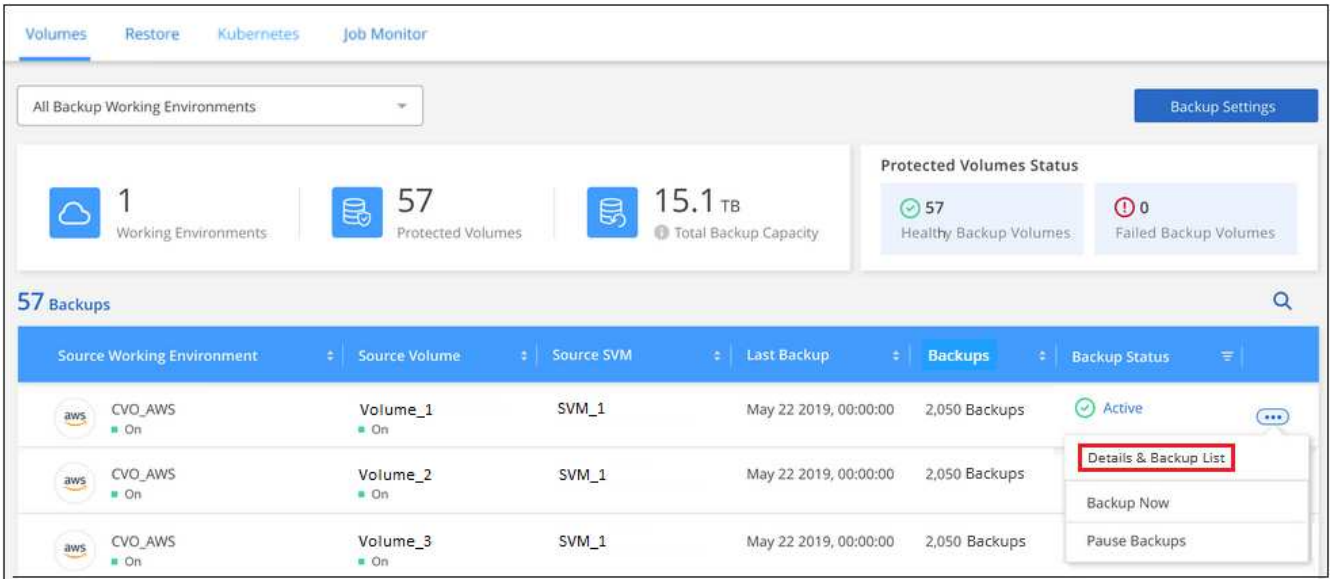
3. In the confirmation dialog box, enter the volume name and click **Delete**.

Deleting a single backup file for a volume

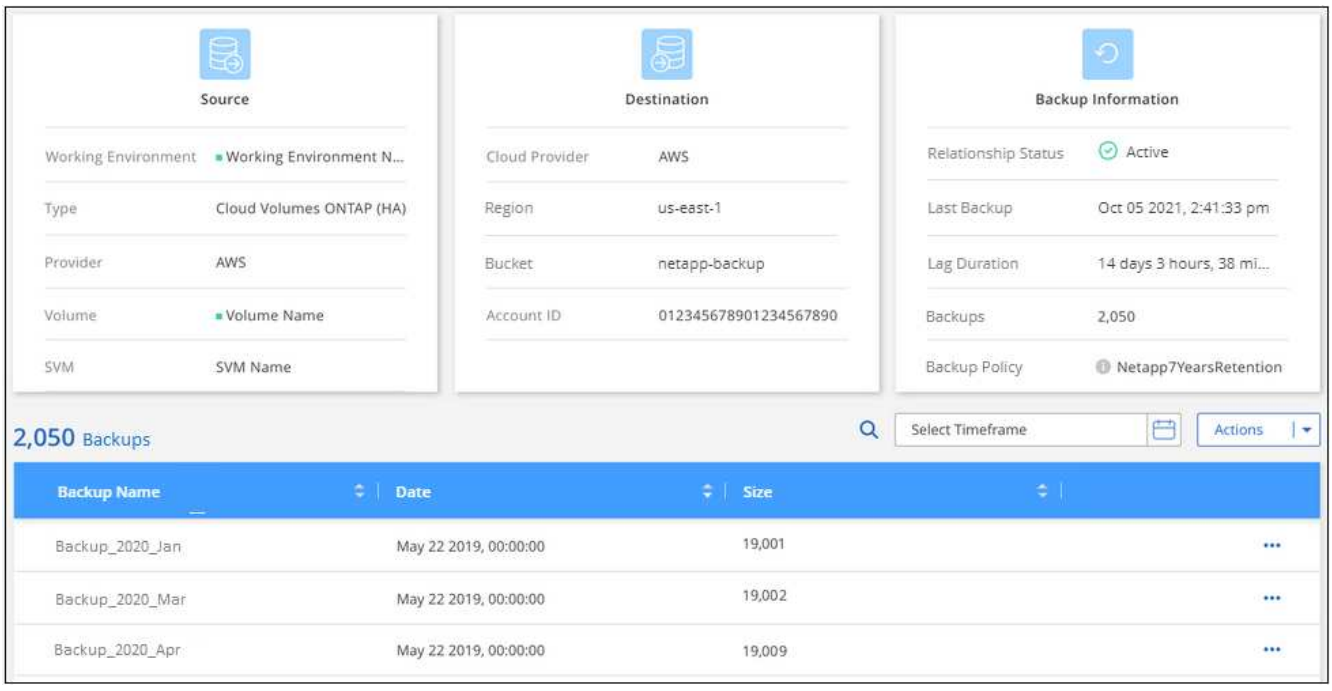
You can delete a single backup file. This feature is available only if the volume backup was created from a system with ONTAP 9.8 or greater.

Steps

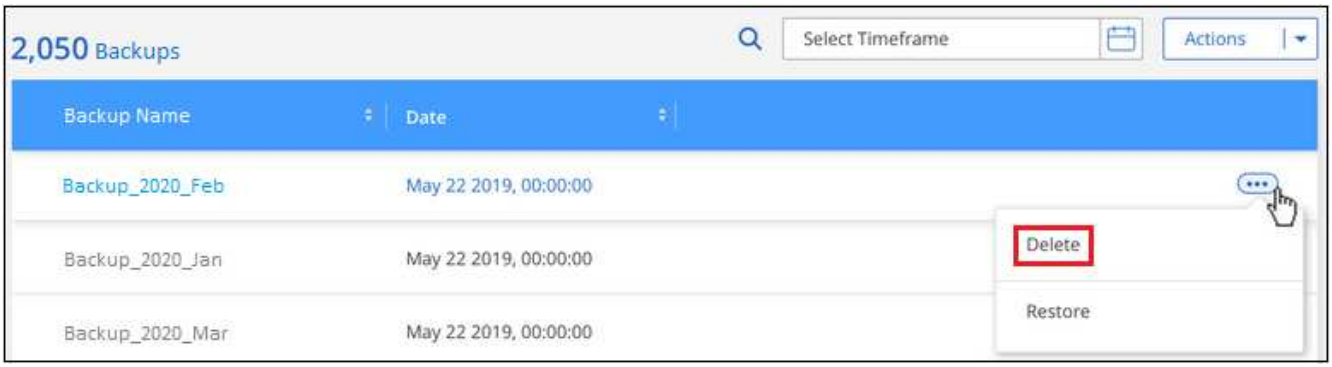
1. From the **Volumes** tab, click ••• for the source volume and select **Details & Backup List**.



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**.

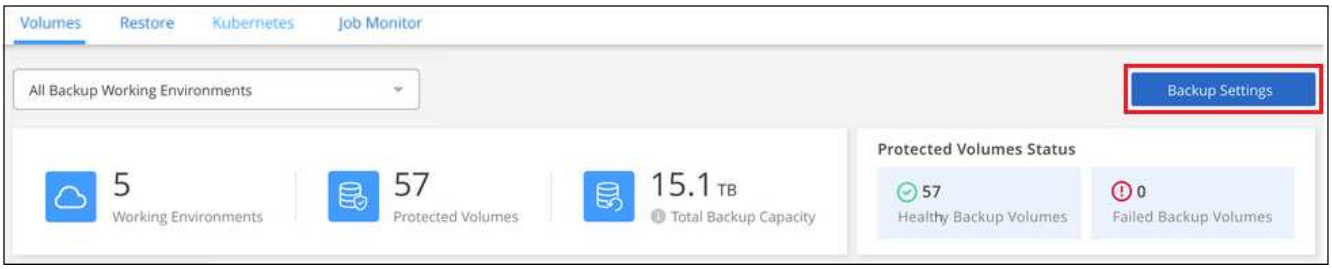
Disabling Cloud Backup for a working environment

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.

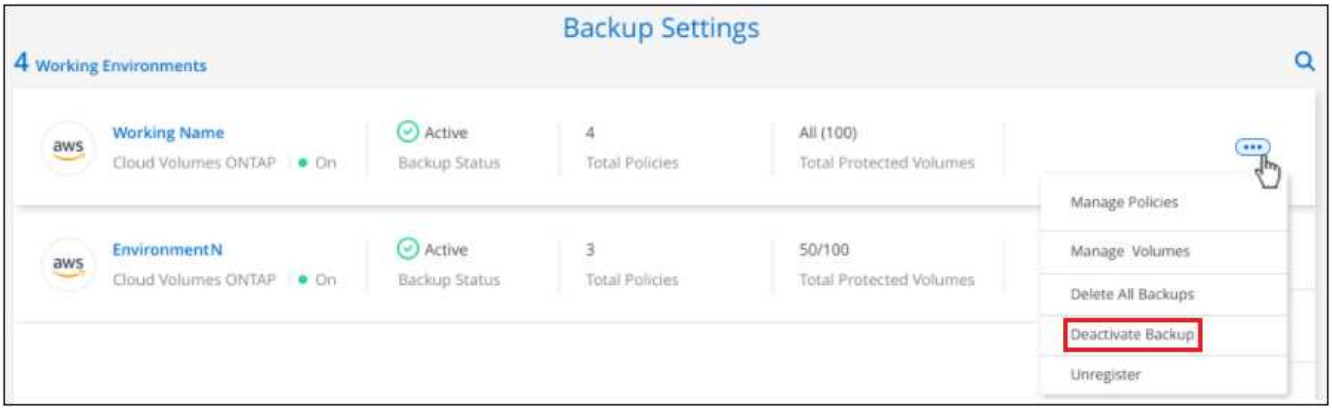
Note that you'll continue to be charged by your cloud provider for object storage costs for the capacity that your backups use unless you delete the backups.

Steps

1. From the **Volumes** 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 working environment, 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.

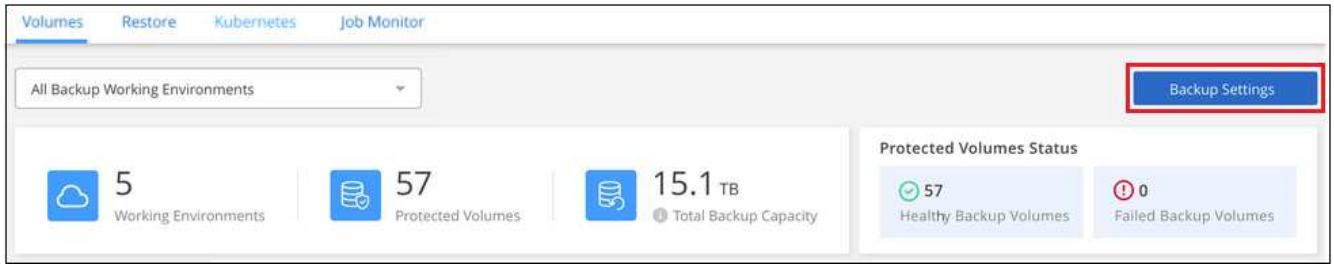
Before you can unregister Cloud Backup, you must perform the following steps, in this order:

- 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 **Volumes** tab, select **Backup Settings**.



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

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

Restoring ONTAP 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 volume from a backup file, or if you

only need to restore a few files, you can restore individual files from a backup file.

You can restore a **volume** (as a new volume) to the same working environment, to a different working environment that's using the same cloud account, or to an on-premises ONTAP system.

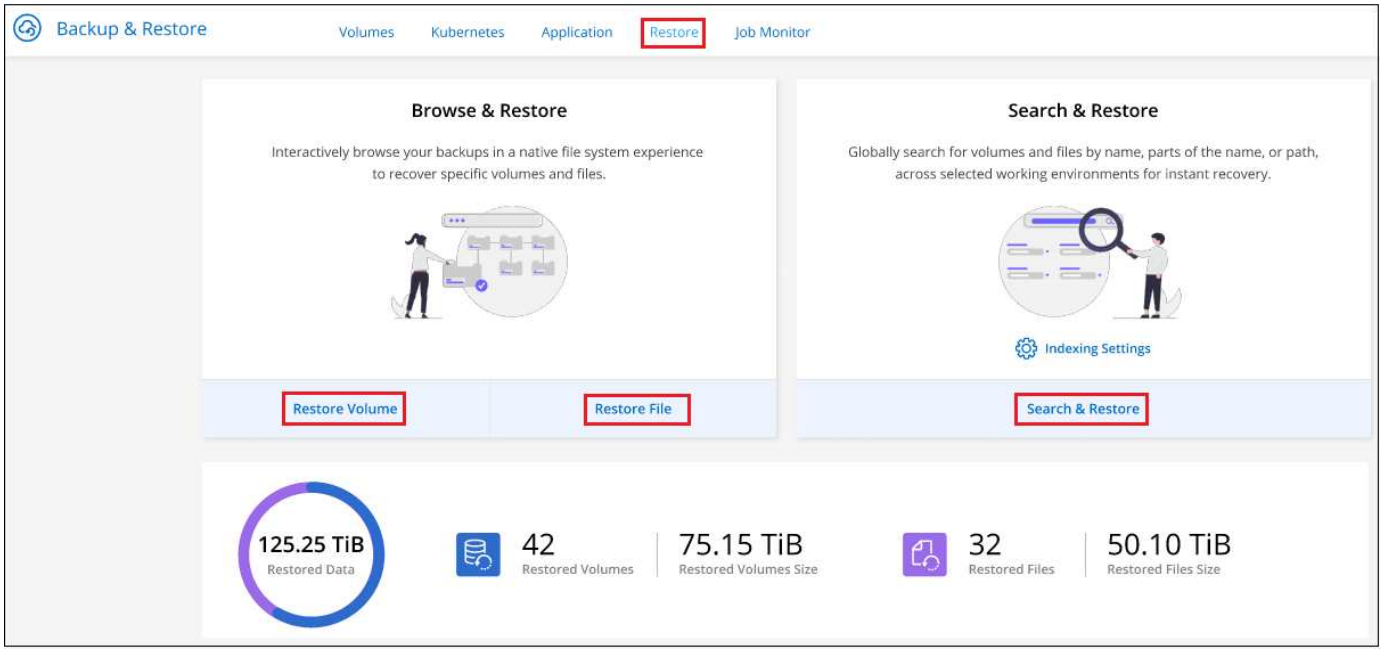
You can restore **files** to a volume in the same working environment, to a volume in a different working environment that's using the same cloud account, or to a volume on an on-premises ONTAP system.

The Restore Dashboard

You use the Restore Dashboard to perform volume and file restore operations. You access the Restore Dashboard by clicking **Backup & Restore** from the top of Cloud Manager, and then clicking the **Restore** tab.

You can also click > **View Restore Dashboard** from the Backup & Restore service from the Services panel.

Cloud Backup must already be activated for at least one working environment and initial backup files must exist.



As you can see, the Restore Dashboard provides 2 different ways to restore data from backup files: **Browse & Restore** and **Search & Restore**.

Comparing Browse & Restore and Search & Restore

In broad terms, *Browse & Restore* is typically better when you need a specific volume or file from the last week, month, or year — and you know the name and location of the file, and the date when it was last in good shape. *Search & Restore* is typically better when you need a volume or file, but you don't remember the exact name, or the volume in which it resides, or the date when it was last in good shape.

This table provides a comparison of the 2 methods.

Browse & Restore	Search & Restore
Browse through a folder-style structure to find the volume or file within a single backup file	Search for a volume or file across **all backup files** by partial or full volume name, partial or full file name, size range, and additional search filters
Volume restore works with backup files stored in Amazon S3, Azure Blob, Google Cloud Storage, and NetApp StorageGRID. File restore works with backup files stored in Amazon S3 and Azure Blob	Volume and file restore works with backup files stored in Amazon S3
Does not handle files that have been renamed or deleted	Handles newly created/deleted/renamed directories and newly created/deleted/renamed files
Browse for results across public or private clouds	Browse for results across public clouds, and in the future, across private clouds and local Snapshots copies
Separate Cloud Restore instance is required for file restore	No Cloud Restore instance required
No extra Amazon resources required	New bucket and Amazon Athena and AWS Glue resources required per account
Cost associated with Cloud Restore instance when restoring files	Cost associated with Amazon Athena and AWS Glue resources when restoring volumes and files
Volume restore from standard and archival tiers. File restore only from standard tiers	Volume and file restore from standard and archival tiers

Before you can use either restore method, make sure you have configured your environment for the unique resource requirements. Those requirements are described in the sections below.

See the requirements and restore steps for the type of restore operation you want to use:

- Restore volumes using Browse & Restore
- Restore files using Browse & Restore
- Restore volumes and files using Search & Restore

Restoring ONTAP data using Browse & Restore

Before you start restoring a volume or files, you should know the name of the volume or file you want to restore, and the approximate date of the backup file where the volume resides.

Note: If the backup file for the volume that you want to restore resides in archival storage (available for AWS and Azure starting with ONTAP 9.10.1), the restore operation will take a longer amount of time and will incur a cost. Additionally, the destination cluster must also be running ONTAP 9.10.1 or greater.

Learn more about restoring from Azure archival storage.
Learn more about restoring from AWS archival storage.

Browse & Restore supported working environments and object storage providers

You can restore a volume, or individual files, from an ONTAP backup file to the following working environments:

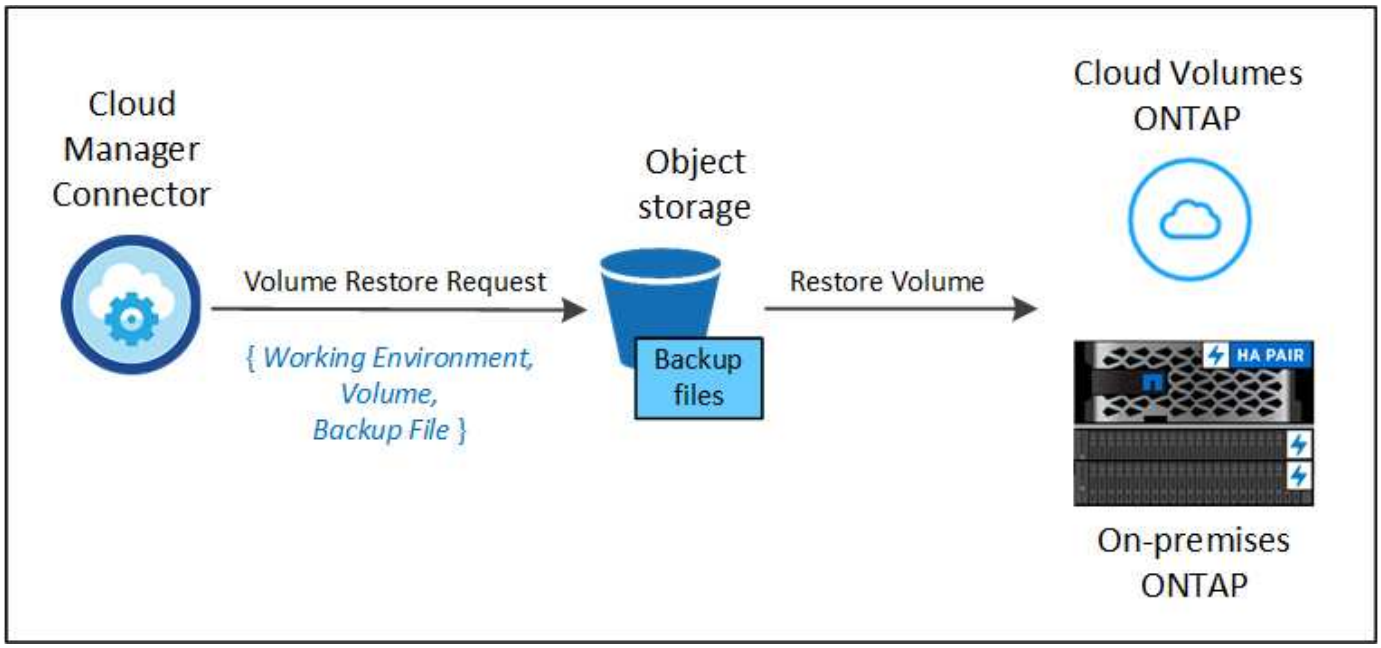
Backup File Location	Destination Working Environment	
	Volume Restore	**File Restore**
Amazon S3	Cloud Volumes ONTAP in AWS On-premises ONTAP system	Cloud Volumes ONTAP in AWS On-premises ONTAP system
Azure Blob	Cloud Volumes ONTAP in Azure On-premises ONTAP system	Cloud Volumes ONTAP in Azure On-premises ONTAP system
Google Cloud Storage	Cloud Volumes ONTAP in Google On-premises ONTAP system	
NetApp StorageGRID	On-premises ONTAP system	

Note that references to "on-premises ONTAP systems" includes FAS, AFF, and ONTAP Select systems.

If the backup file resides in archival storage, only volume restore is supported. File restore is not currently supported from archival storage when using Browse & Restore.

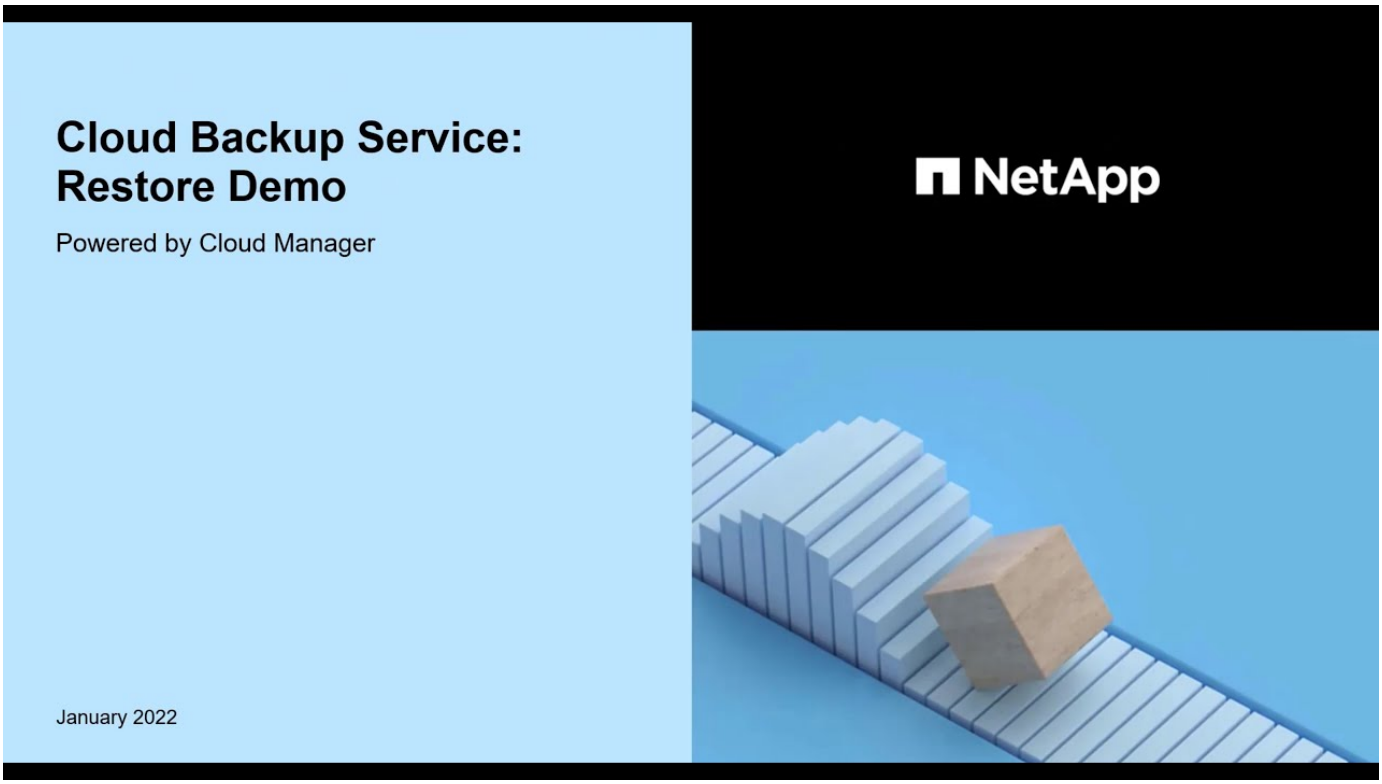
Restoring volumes using Browse & Restore

When you restore a 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 working environment or to a different working environment that's located in the same cloud account as the source working environment. You can also restore volumes to an on-premises ONTAP system.



As you can see, you need to know the working environment name, volume name, and backup file date to perform a volume restore.

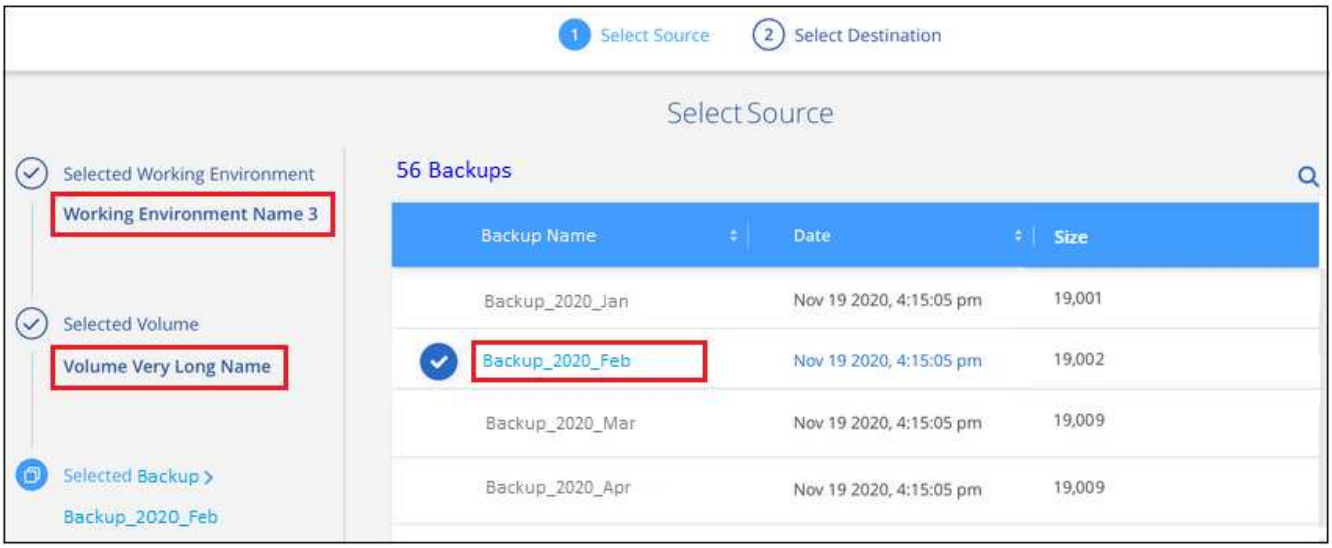
The following video shows a quick walkthrough of restoring a volume:



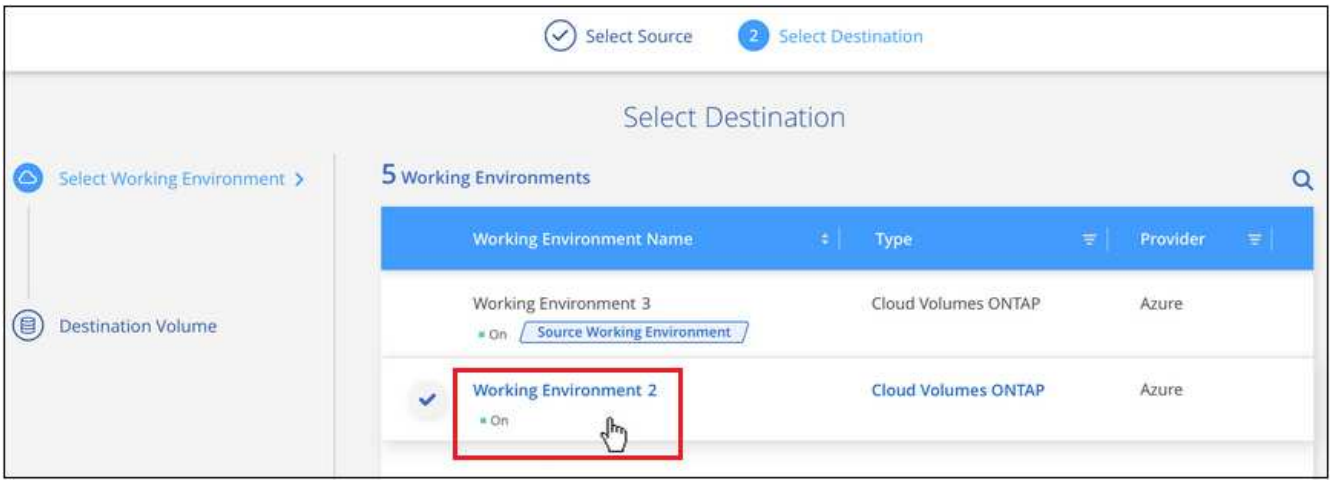
Steps

1. Select the **Backup & Restore** service.
2. Click the **Restore** tab and the Restore Dashboard is displayed.
3. From the *Browse & Restore* section, click **Restore Volume**.

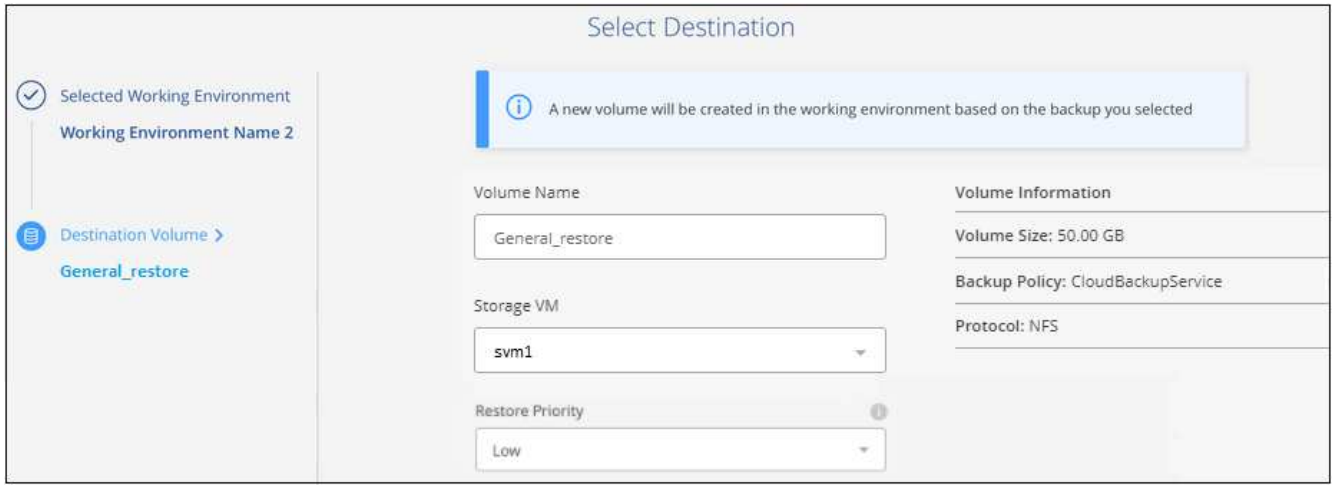
4. In the *Select Source* page, navigate to the backup file for the volume you want to restore. Select the **Working Environment**, the **Volume**, and the **Backup** file that has the date/time stamp from which you want to restore.



5. Click **Continue**.
6. In the *Select Destination* page, select the **Working Environment** where you want to restore the volume.



7. If you select an on-premises ONTAP system and you haven't already configured the cluster connection to the object storage, you are prompted for additional information:
   - When restoring from Amazon S3, select the IPspace in the ONTAP cluster where the destination volume will reside, enter the access key and secret key for the user you created to give the ONTAP cluster access to the S3 bucket, and optionally choose a private VPC endpoint for secure data transfer.
   - When restoring from Azure Blob, select the IPspace in the ONTAP cluster where the destination volume will reside, select the Azure Subscription to access the object storage, and optionally choose a private endpoint for secure data transfer by selecting the VNet and Subnet.
   - When restoring from Google Cloud Storage, select the Google Cloud Project and the Access Key and Secret Key to access the object storage, the region where the backups are stored, and the IPspace in the ONTAP cluster where the destination volume will reside.
   - When restoring from StorageGRID, select the Access Key and Secret Key needed to access the object storage, and the IPspace in the ONTAP cluster where the destination volume will reside.
8. Enter the name you want to use for the restored volume, and select the Storage VM where the volume will reside. By default, **<source_volume_name>_restore** is used as the volume name.



You can select the Aggregate that the volume will use for its' capacity only when restoring a volume to an on-premises ONTAP system.

And if you are restoring the volume from a backup file that resides in an archival storage tier (available starting with ONTAP 9.10.1), then you can select the Restore Priority.

Learn more about restoring from Azure archival storage.
Learn more about restoring from AWS archival storage.

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

Result

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

Note that restoring a volume from a backup file that resides in archival storage can take many minutes or hours depending on the archive tier and the restore priority. You can click the **Job Monitor** tab to see the restore progress.

Restoring ONTAP files using Browse & Restore

If you only need to restore a few files from a volume, you can choose to restore individual files instead of restoring the entire volume. You can restore files to a existing volume in the same working environment, or to a different working environment that's using the same cloud account. You can also restore files to a volume on an on-premises ONTAP system.

If you select multiple files, all the files are restored to the same destination volume that you choose. If you want to restore files to different volumes, you'll need to run the restore process multiple time.

You can't restore individual files if the backup file resides in archival storage. In this case, you can restore files from a newer backup file that has not been archived, you can restore files using Search & Restore, or you can restore the entire volume from the archived backup and then access the files you need.

Prerequisites

- The ONTAP version must be 9.6 or greater in your Cloud Volumes ONTAP or on-premises ONTAP systems to perform file restore operations.

- Restoring individual files from a backup file uses a separate Restore instance/virtual machine. See the AWS Requirements or Azure Requirements to make sure your environment is ready.
- Restoring files also requires that specific AWS EC2 permissions are added to the user role that provides Cloud Manager with permissions. Make sure all the permissions are configured correctly.
- AWS cross-account restore requires manual action in the AWS console. See the AWS topic granting cross-account bucket permissions for details.

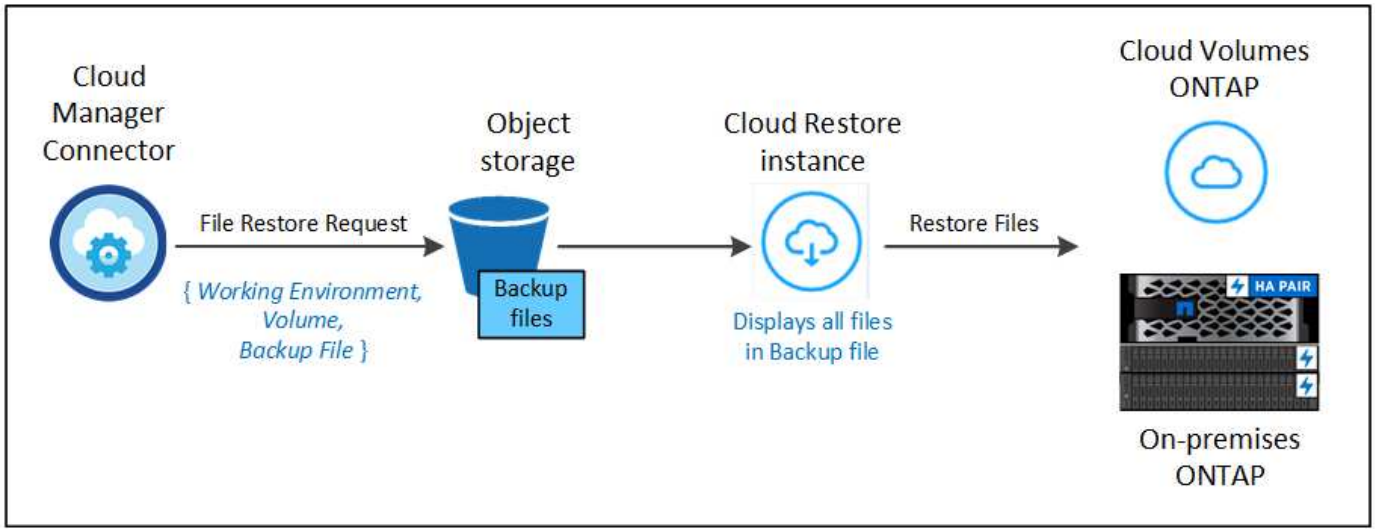
File Restore process

The process goes like this:

1. When you want to restore one or more files from a volume backup, click the **Restore** tab, click **Restore Files** under *Browse & Restore*, and select the backup file in which the file (or files) reside.
2. The Restore instance starts up and displays the folders and files that exist within the selected backup file.

   Note: The Restore instance is deployed in your cloud providers' environment the first time you restore a file.

3. Choose the file (or files) that you want to restore from that backup.
4. Select the location where you want the file(s) to be restored (the working environment, volume, and folder), and click **Restore**.
5. The file(s) are restored, and then the Restore instance is shut down to save costs after a period of inactivity.

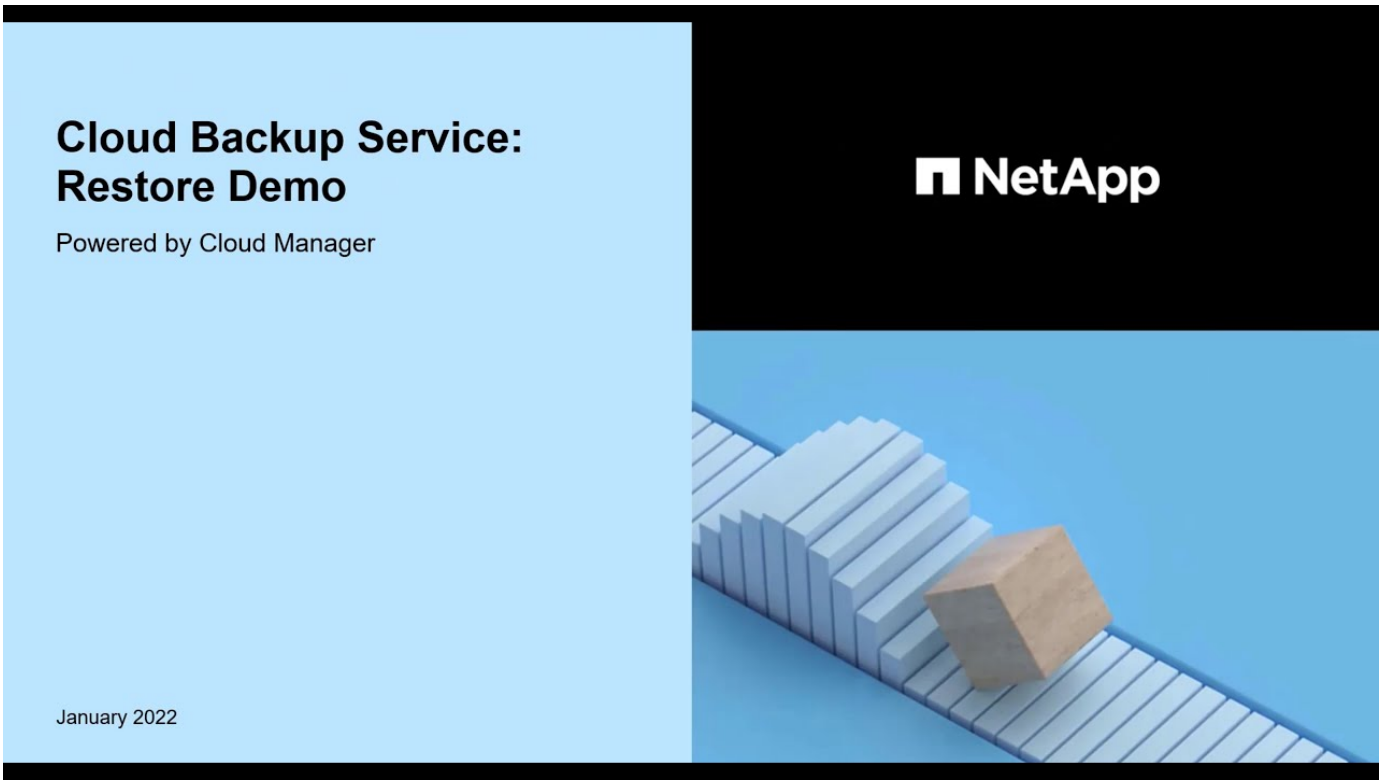


As you can see, you need to know the working environment name, volume name, backup file date, and file name to perform a file restore.

Restoring files using Browse & Restore

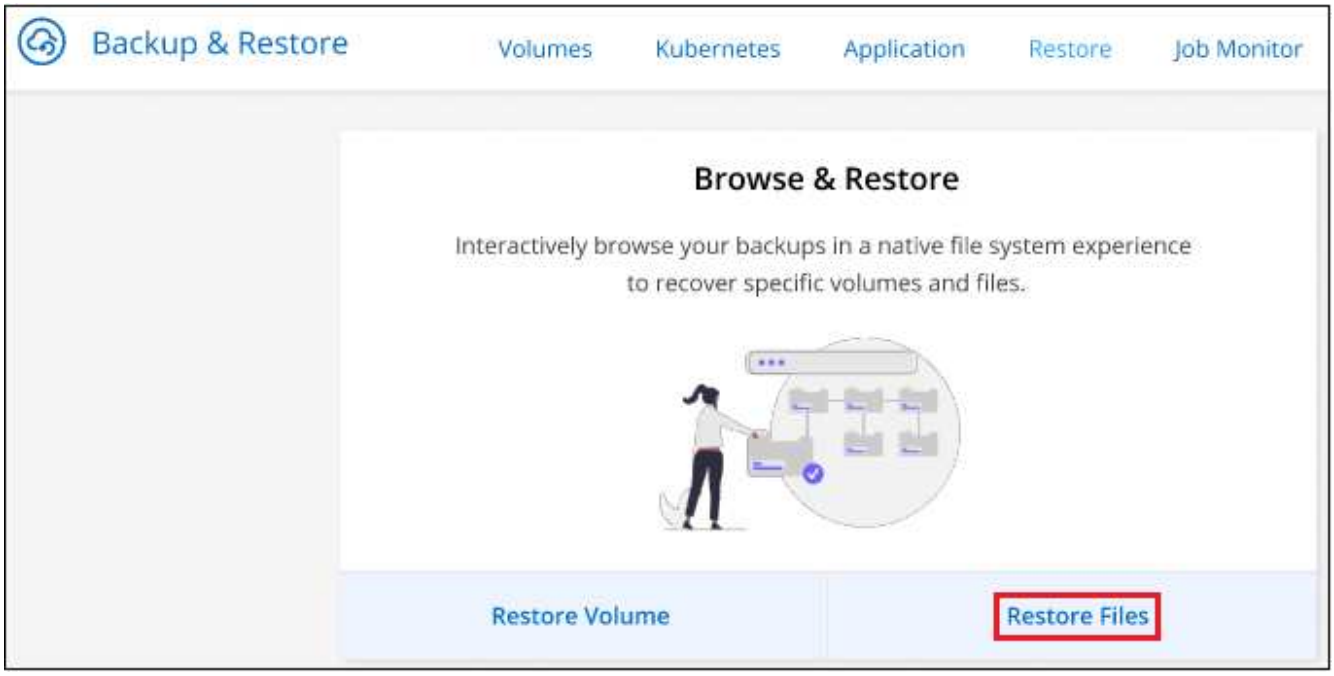
Follow these steps to restore files to a volume from a volume backup. You should know the name of the volume and the date of the backup file that you want to use to restore the file, or files. This functionality uses Live Browsing so that you can view the list of directories and files within each backup file.

The following video shows a quick walkthrough of restoring a single file:

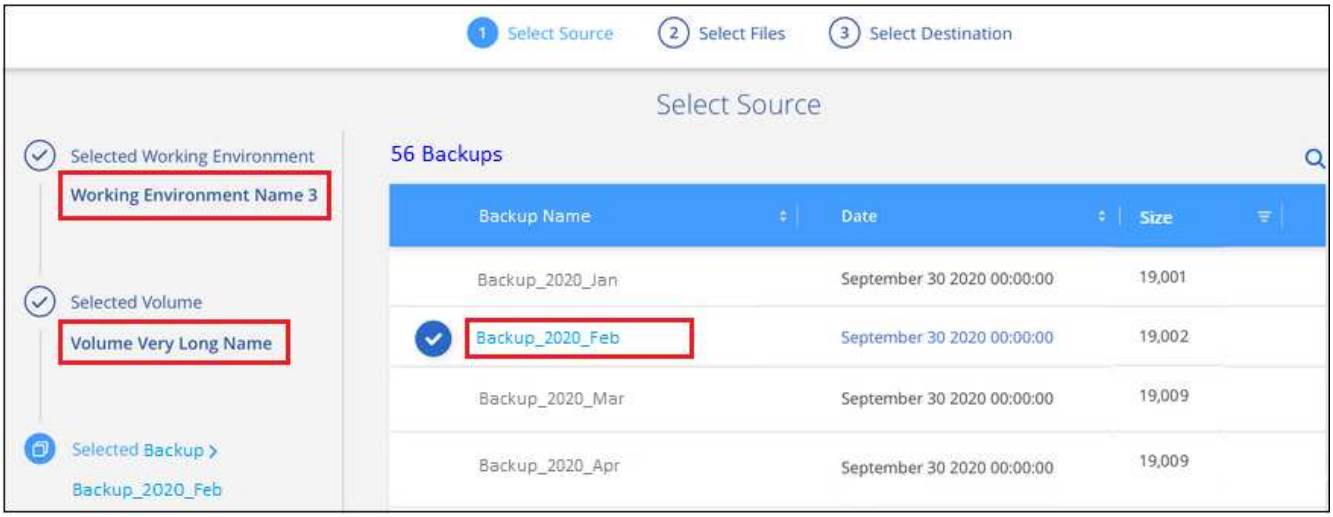


Steps

1. Select the **Backup & Restore** service.
2. Click the **Restore** tab and the Restore Dashboard is displayed.
3. From the *Browse & Restore* section, click **Restore Files**.

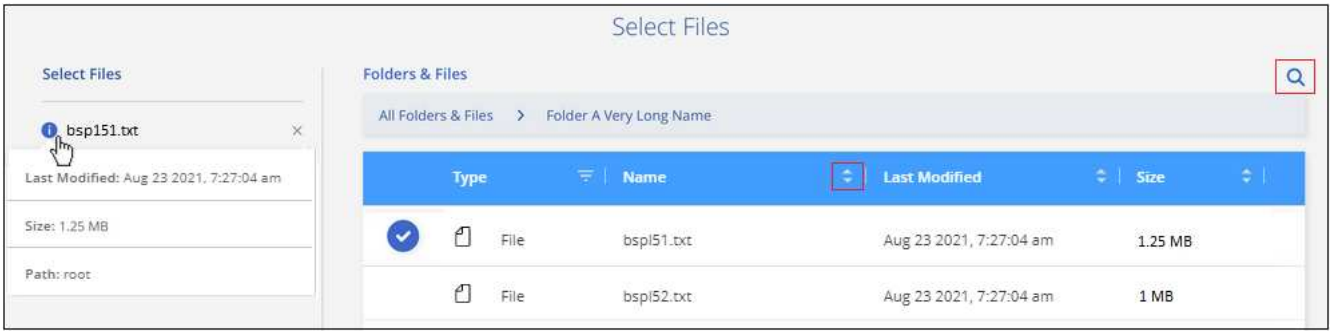


4. In the *Select Source* page, navigate to the backup file for the volume that contains the files you want to restore. Select the **Working Environment**, the **Volume**, and the **Backup** that has the date/time stamp from which you want to restore files.



5. Click **Continue** and the Restore instance is started. After a few minutes the Restore instance displays the list of folders and files from the volume backup.

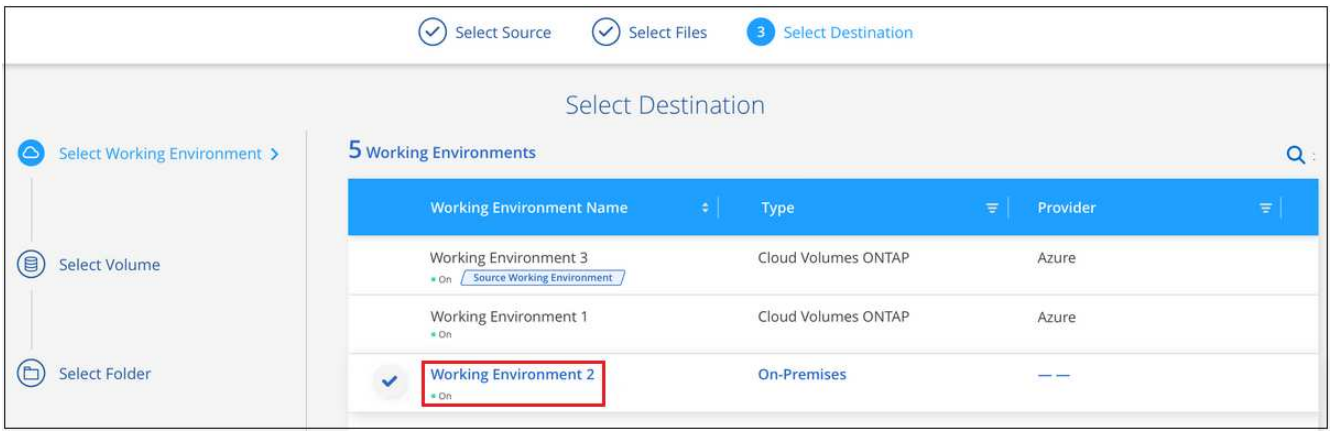
   Note: The Restore instance is deployed in your cloud providers' environment the first time you restore a file, so this step could take a few minutes longer the first time.



6. In the *Select Files* page, select the file or files that you want to restore and click **Continue**. To assist you in finding the file:
   - You can click the file name if you see it.
   - You can click the search icon and enter the name of the file to navigate directly to the file.
   - You can navigate down levels in folders using the › button at the end of the row to find the file.

     As you select files they are added to the left side of the page so you can see the files that you have already chosen. You can remove a file from this list if needed by clicking the **x** next to the file name.

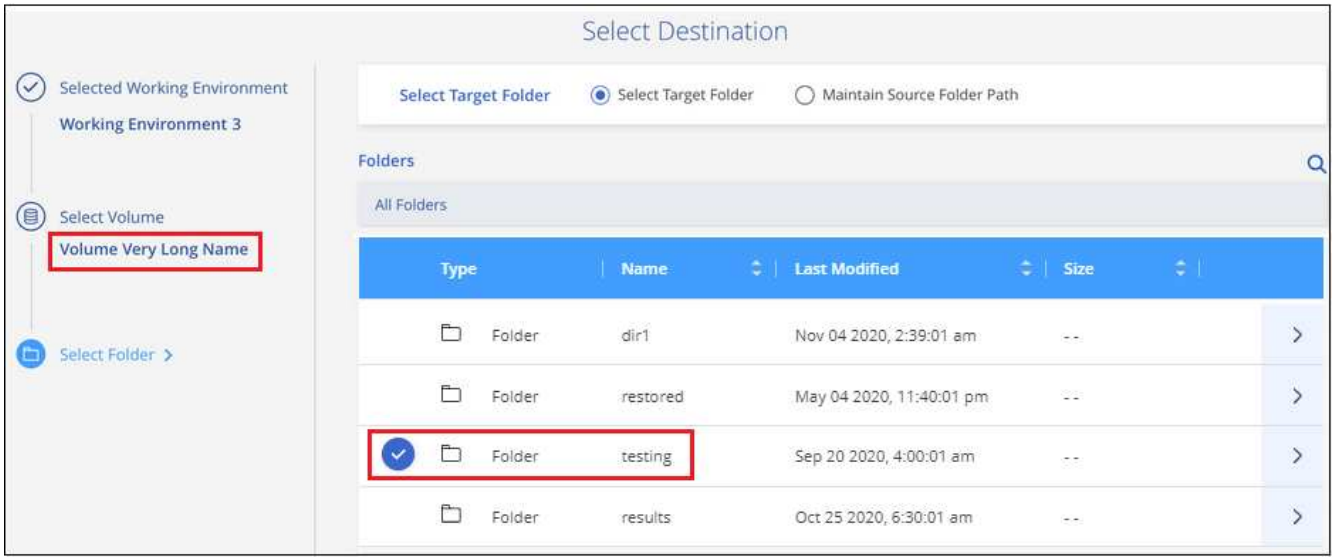
7. In the *Select Destination* page, select the **Working Environment** where you want to restore the files.



If you select an on-premises cluster and you haven't already configured the cluster connection to the object storage, you are prompted for additional information:

- When restoring from Amazon S3, enter the IPspace in the ONTAP cluster where the destination volume resides, and the AWS Access Key and Secret Key needed to access the object storage.
- When restoring from Azure Blob, enter the IPspace in the ONTAP cluster where the destination volume resides.

8. Then select the **Volume** and the **Folder** where you want to restore the files.



You have a few options for the location when restoring files.

- When you have chosen **Select Target Folder**, as shown above:
  - You can select any folder.
  - You can hover over a folder and click ❯ at the end of the row to drill down into subfolders, and then select a folder.
- If you have selected the same destination Working Environment and Volume as where the source file was located, you can select **Maintain Source Folder Path** to restore the file, or all files, to the same folder where they existed in the source structure. All the same folders and sub-folders must already exist; folders are not created.

9. Click **Restore** and you are returned to the Restore Dashboard so you can review the progress of the restore operation. You can also click the **Job Monitor** tab to see the restore progress.

The Restore instance is shut down after a certain period of inactivity to save you money so that you incur costs only when it is active.

Restoring ONTAP data using Search & Restore

You can restore a volume or individual files from a backup file using Search & Restore. Search & Restore enables you to search for a specific volume or file from all backups stored on cloud storage for a particular provider, and then perform a restore. You don't need to know the exact working environment name or volume name - the search looks through all volume backup files.

When you restore a volume from a backup file, Cloud Manager creates a *new* volume using the data from the backup. You can restore the data as a volume in the same working environment, or to a different working environment that's located in the same cloud account as the source working environment. You can also restore volumes to an on-premises ONTAP system.

You can restore files to the original volume location, to a different volume in the same working environment, or to a different working environment that's using the same cloud account. You can also restore files to a volume on an on-premises ONTAP system.

If the backup file for the volume that you want to restore resides in archival storage (available for AWS starting with ONTAP 9.10.1), the restore operation will take a longer amount of time and will incur additional cost. Note that the destination cluster must also be running ONTAP 9.10.1 or greater.

Learn more about restoring from AWS archival storage.

Before you start, you should have some idea of the name or location of the volume or file you want to restore.

The following video shows a quick walkthrough of restoring a single file:

Search & Restore supported working environments and object storage providers

You can restore a volume, or individual files, from an ONTAP backup file to the following working environments:

Backup File Location	Destination Working Environment	
	Volume Restore	**File Restore**
Amazon S3	Cloud Volumes ONTAP in AWS On-premises ONTAP system	Cloud Volumes ONTAP in AWS On-premises ONTAP system

More cloud providers will be supported in future releases.

Note that references to "on-premises ONTAP systems" includes FAS, AFF, and ONTAP Select systems.

Prerequisites

- Cluster requirements:
  - The ONTAP version must be 9.8 or greater.
  - The storage VM (SVM) on which the volume resides must have a configured data LIF.
  - NFS must be enabled on the volume.
  - The SnapDiff RPC Server must be activated on the SVM. Cloud Manager does this automatically when you enable Indexing on the working environment.
- AWS requirements:
  - Specific Amazon Athena, AWS Glue, and AWS S3 permissions must be added to the user role that provides Cloud Manager with permissions. Make sure all the permissions are configured correctly.

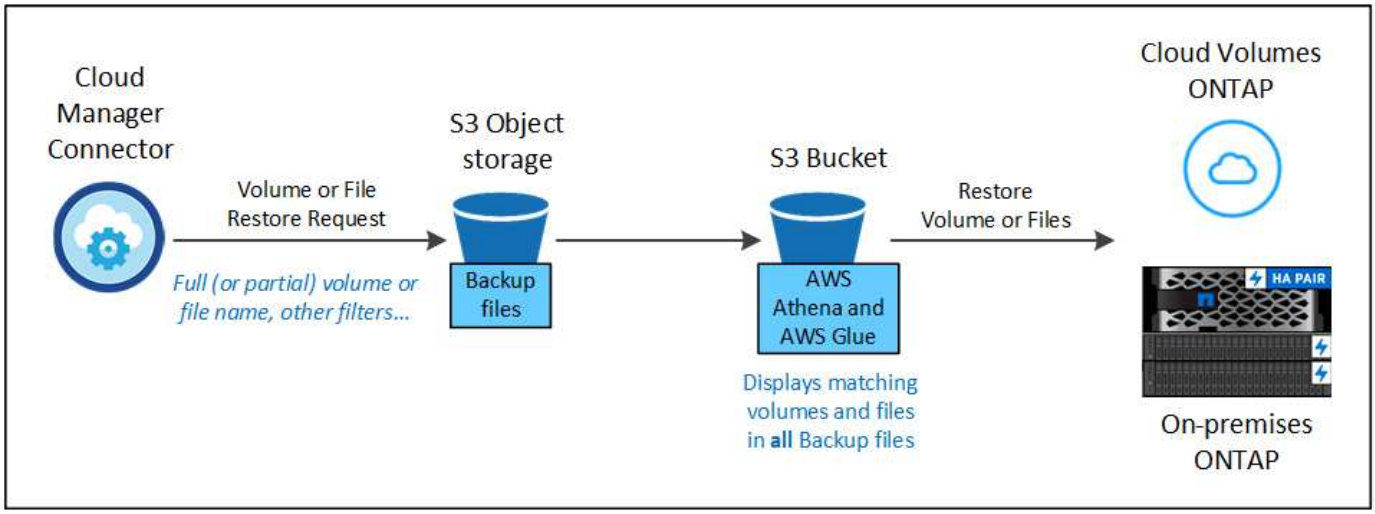
Search & Restore process

The process goes like this:

1. Before you can use Search & Restore, you need to enable "Indexing" on each source working environment from which you'll want to restore volumes or files. This allows the Indexed Catalog to track the backup files for every volume. It enables SnapDiff v3 on data-serving SVMs, and provisions a new S3 bucket and the Amazon Athena interactive query service and AWS Glue serverless data integration service.
2. When you want to restore a volume or files from a volume backup, under *Search & Restore*, click **Search & Restore**.
3. Enter the search criteria for a volume or file by partial or full volume name, partial or full file name, size range, creation date range, other search filters, and click **Search**.

   The Search Results page displays all the backup files that have a file or volume that matches your search criteria.

4. Click **View All Backups** for the backup file you want to use to restore the volume or file, and then click **Restore** on the actual backup file you want to use.
5. Select the location where you want the volume or file(s) to be restored and click **Restore**.
6. The volume or file(s) are restored.



As you can see, you really only need to know a partial volume or file name and Cloud backup searches through all backup files that match your search.

Enabling the Indexed Catalog for each working environment

Before you can use Search & Restore, you need to enable "Indexing" on each source working environment from which you're planning to restore volumes or files. This allows the Indexed Catalog to track every volume and every backup file - making your searches very quick and efficient.

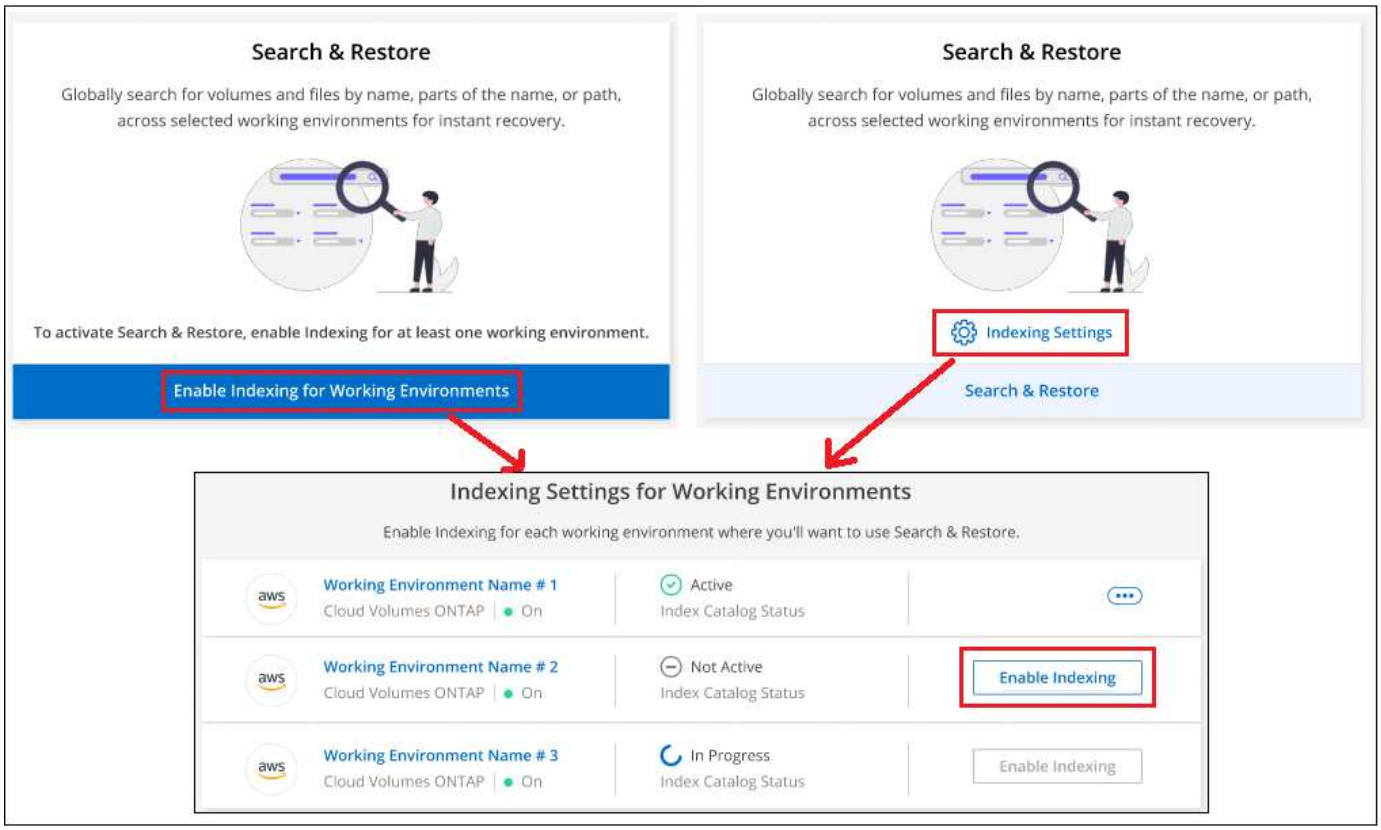
When you enable this functionality, Cloud Backup enables SnapDiff v3 on the SVM for your volumes, and it creates a new bucket in which it provisions the Amazon Athena interactive query service and AWS Glue serverless data integration service.

If Indexing has been enabled already for your working environment, go to the next section to restore your data.

To enable Indexing for a working environment:

- If no working environments have been indexed, on the Restore Dashboard under *Search & Restore*, click **Enable Indexing for Working Environments**, and click **Enable Indexing** for the working environment.
- If at least one working environment has already been indexed, on the Restore Dashboard under *Search & Restore*, click **Indexing Settings**, and click **Enable Indexing** for the working environment.

After all the services are provisioned and the Indexed Catalog has been activated, the working environment is shown as "Active".



Depending on the size of the volumes in the working environment, and the number of backup files in the cloud, the initial indexing process could take up to an hour. After that it is updated hourly with incremental changes to stay current.

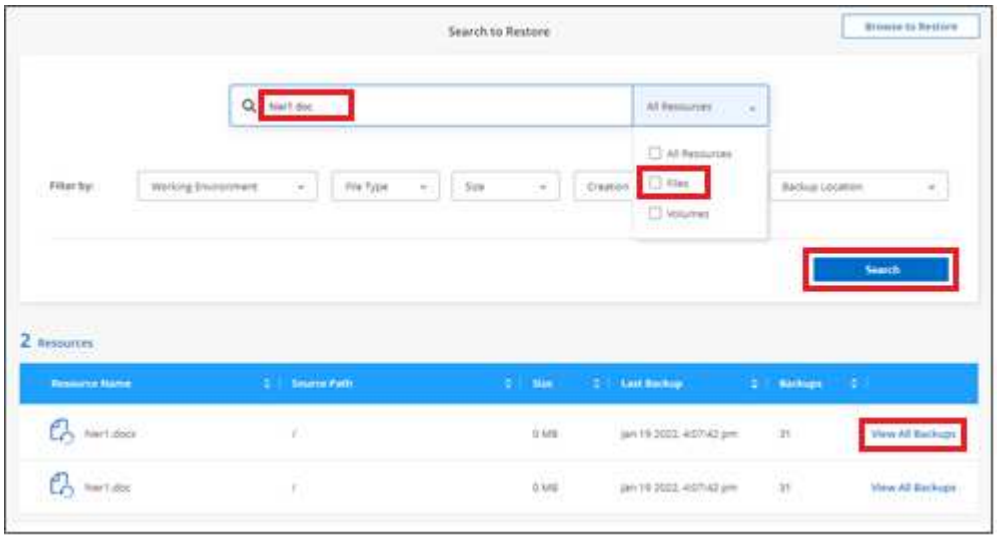
Restoring volumes and files using Search & Restore

After you have enabled Indexing for your working environment, you can restore volumes or files using Search & Restore. This allows you to use a broad range of filters to find the exact file or volume that you want to restore from all backup files.

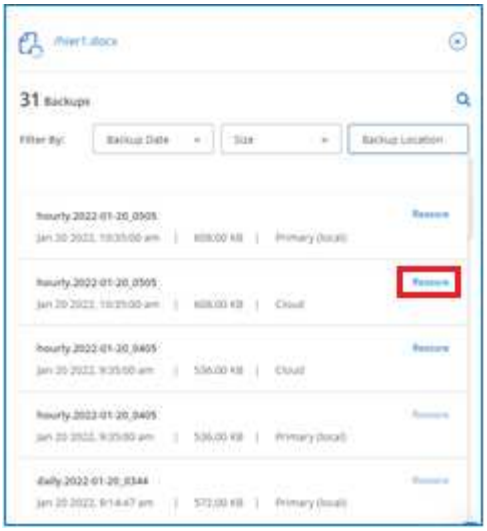
Steps

1. Select the **Backup & Restore** service.
2. Click the **Restore** tab and the Restore Dashboard is displayed.
3. From the *Search & Restore* section, click **Search & Restore**.

4. From the Search & Restore page:
   a. In the Search bar, enter a full or partial volume name or file name.
   b. In the Filter area, select the filter criteria. For example, you can select the working environment where the data resides and the file type, for example a .doc file.
5. Click **Search** and the Search Results area displays all the locations that have a file or volume that matches your search.



6. Click **View All Backups** for the location that has the data you want to restore to display all the backup files that contain the volume or file.



7. Click **Restore** for the backup file you want to use to restore the volume or file.
8. Select the location where you want the volume or file(s) to be restored and click **Restore**.
   - For files, you can restore to the original location or you can select an alternate location
   - For volumes you can select the location.

Results

The volume or file(s) are restored and you are returned to the Restore Dashboard so you can review the progress of the restore operation. You can also click the **Job Monitor** tab to see the restore progress.

For restored volumes, you can manage the backup settings for this new volume as required.

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.

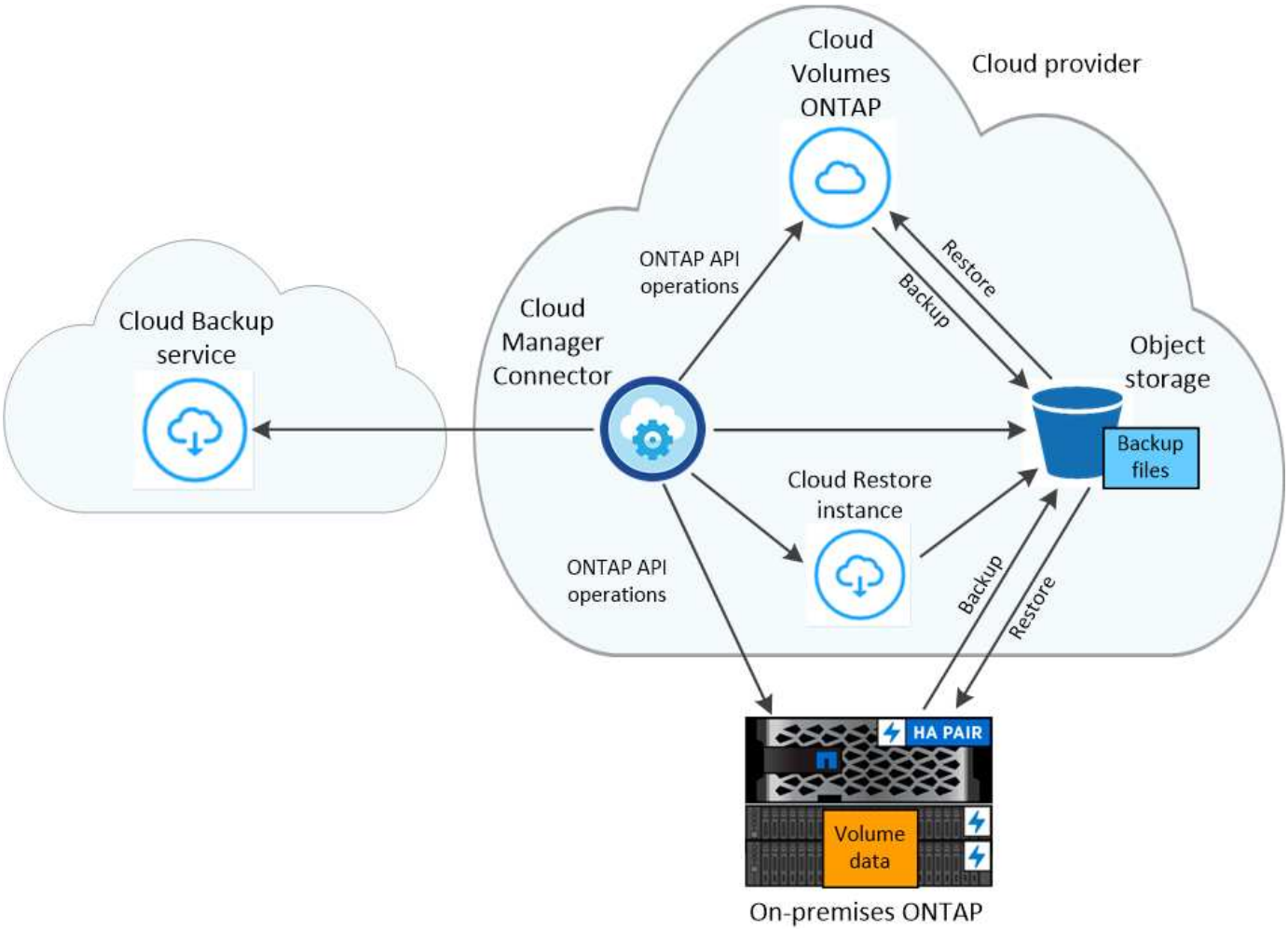
Learn how to manage your BYOL licenses.

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.

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.

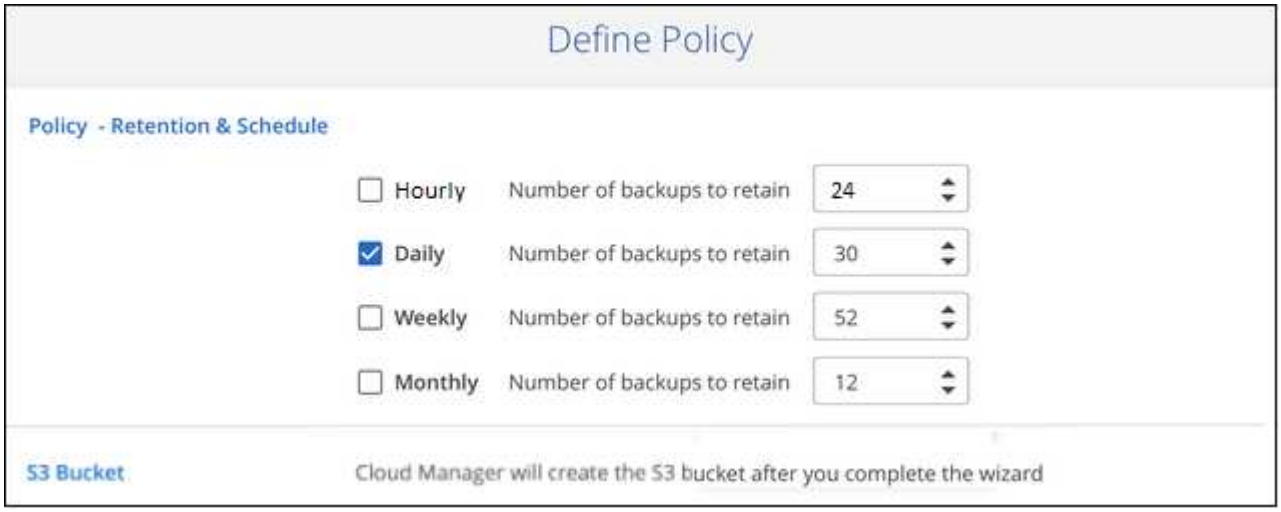
2 Enable Cloud Backup on your existing Kubernetes cluster

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.



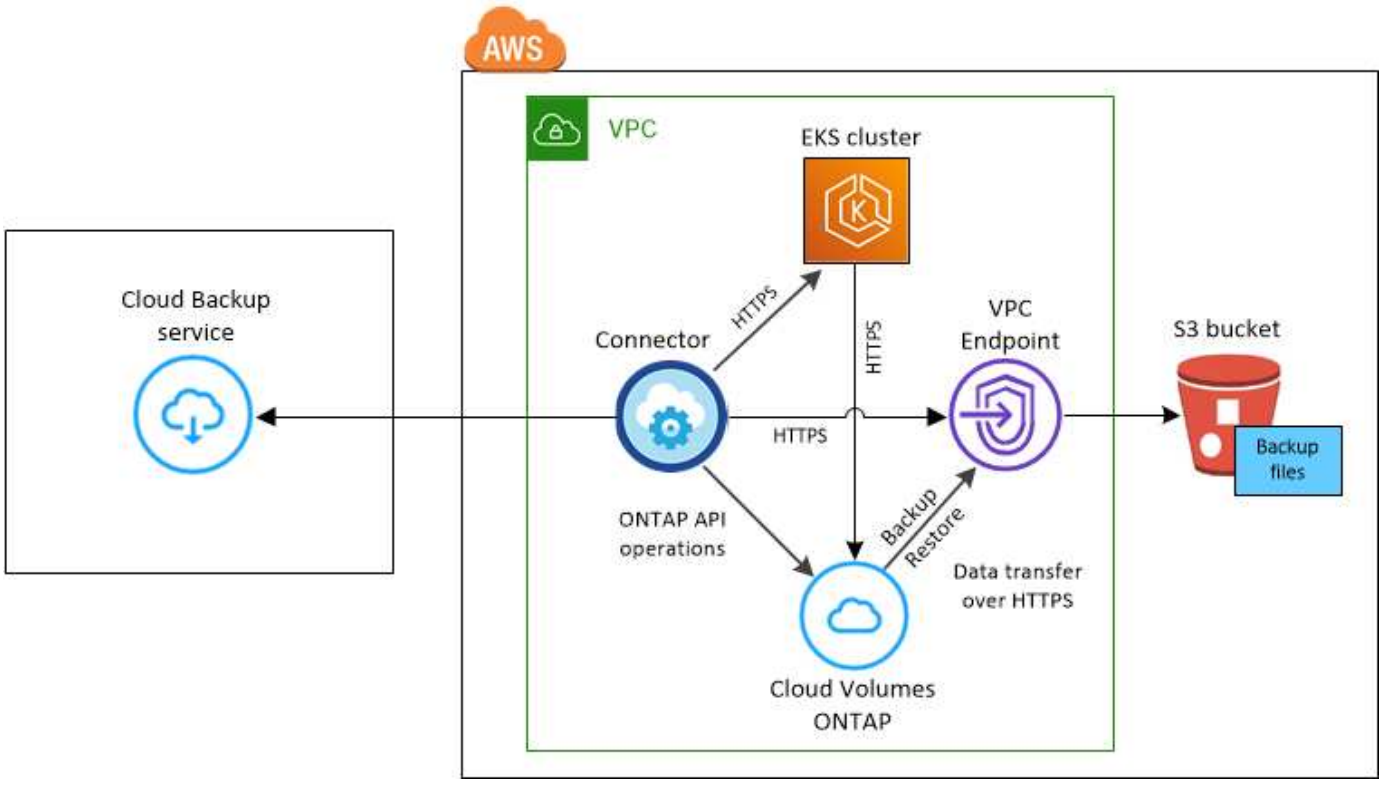
4 **Select the volumes that you want to back up**

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

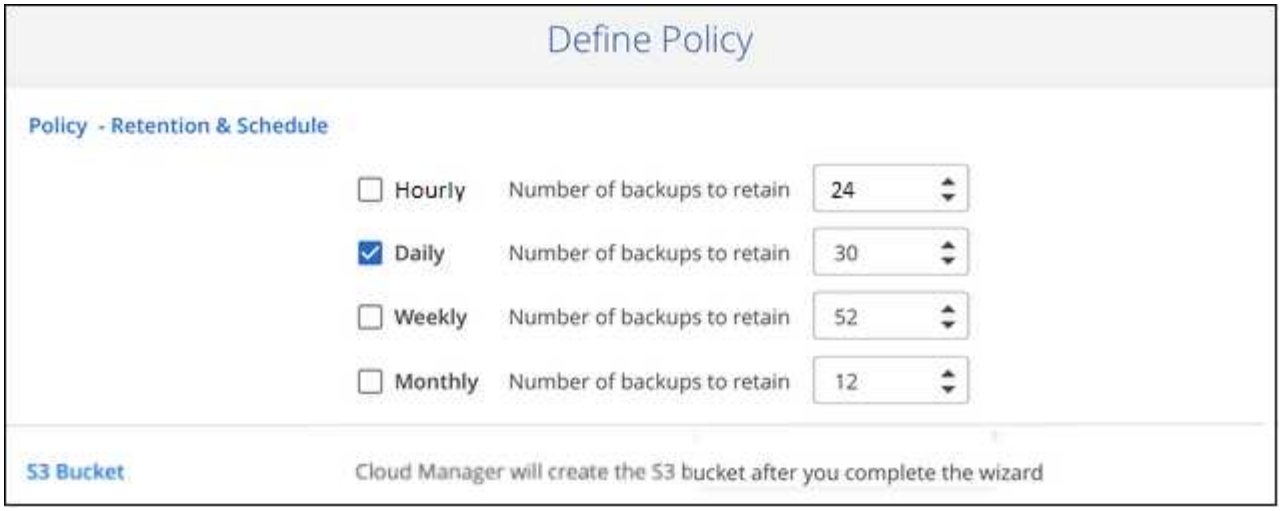
Enable Cloud Backup at any time directly from the working environment.

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.

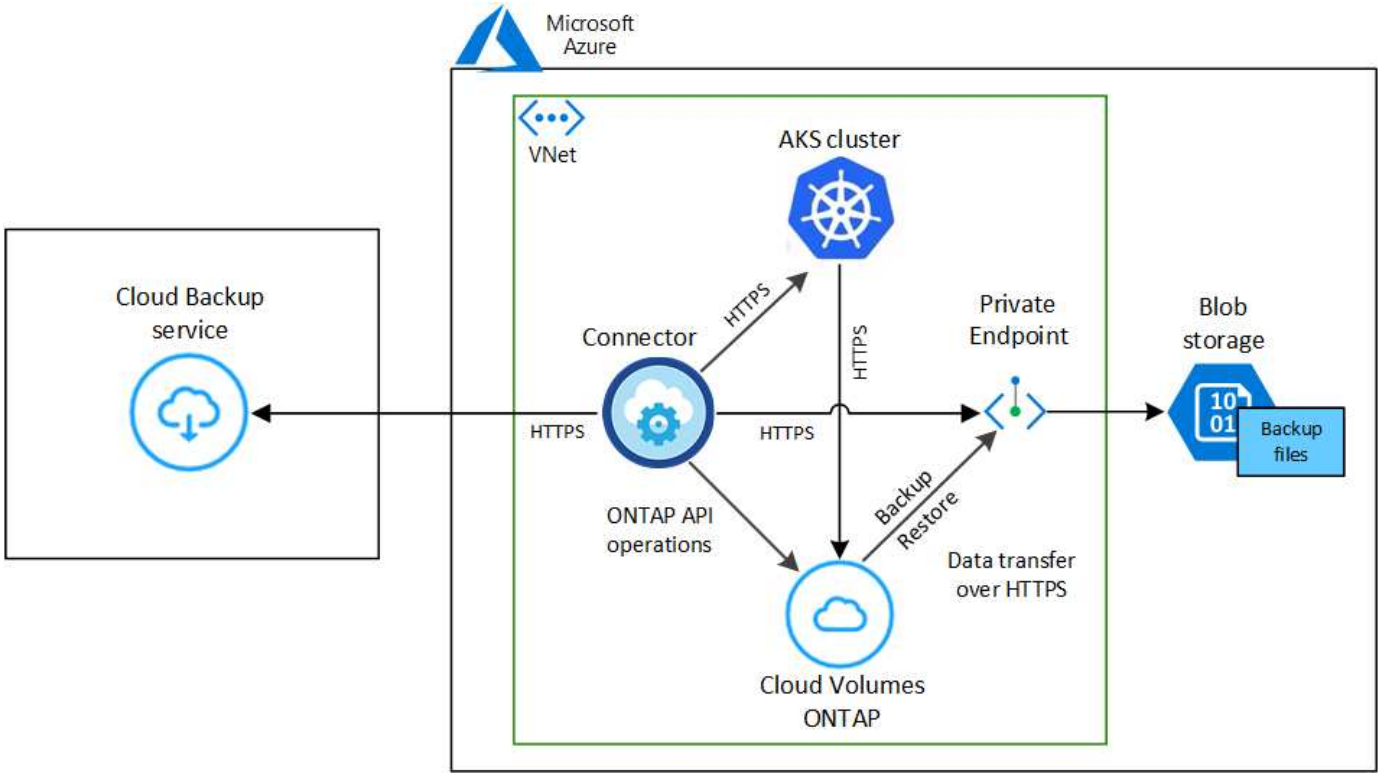
4 **Select the volumes that you want to back up**

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.

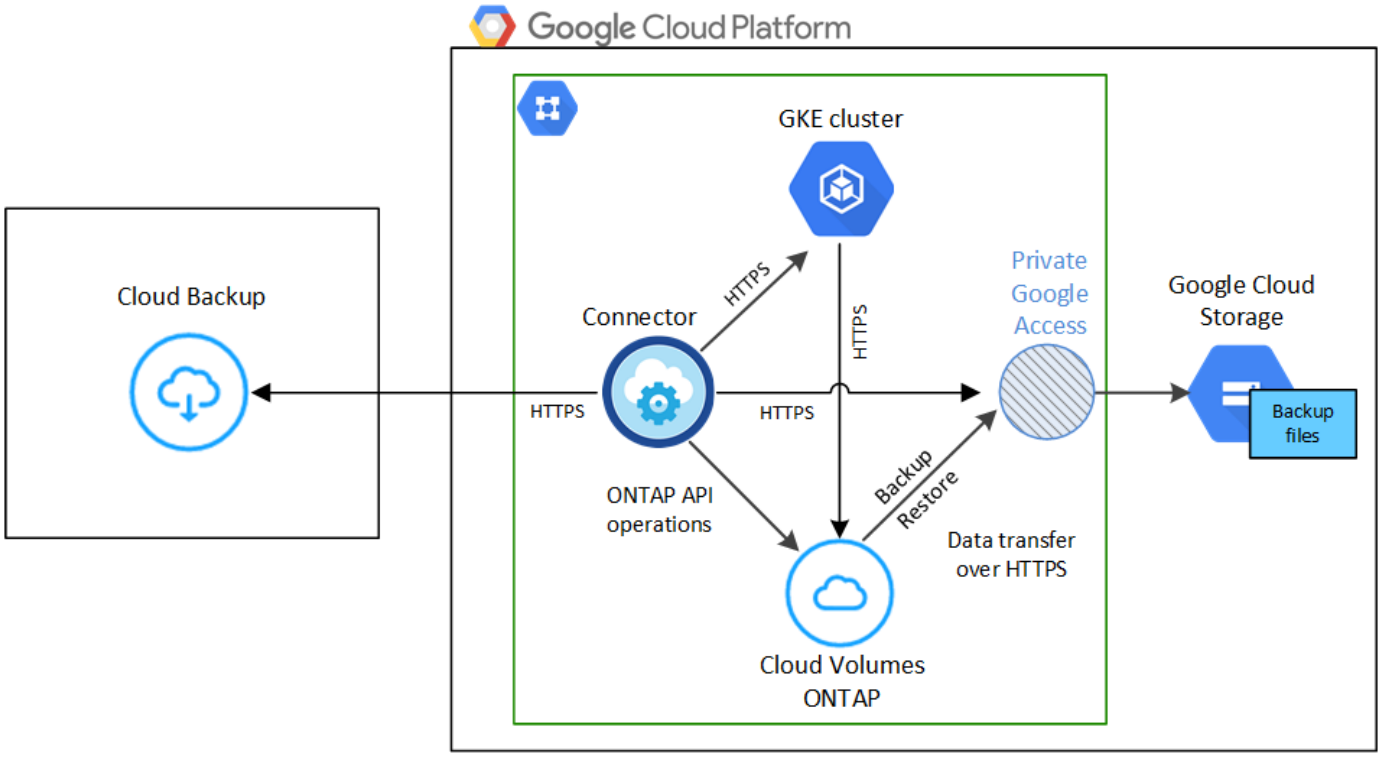
4 **Select the volumes that you want to back up**

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

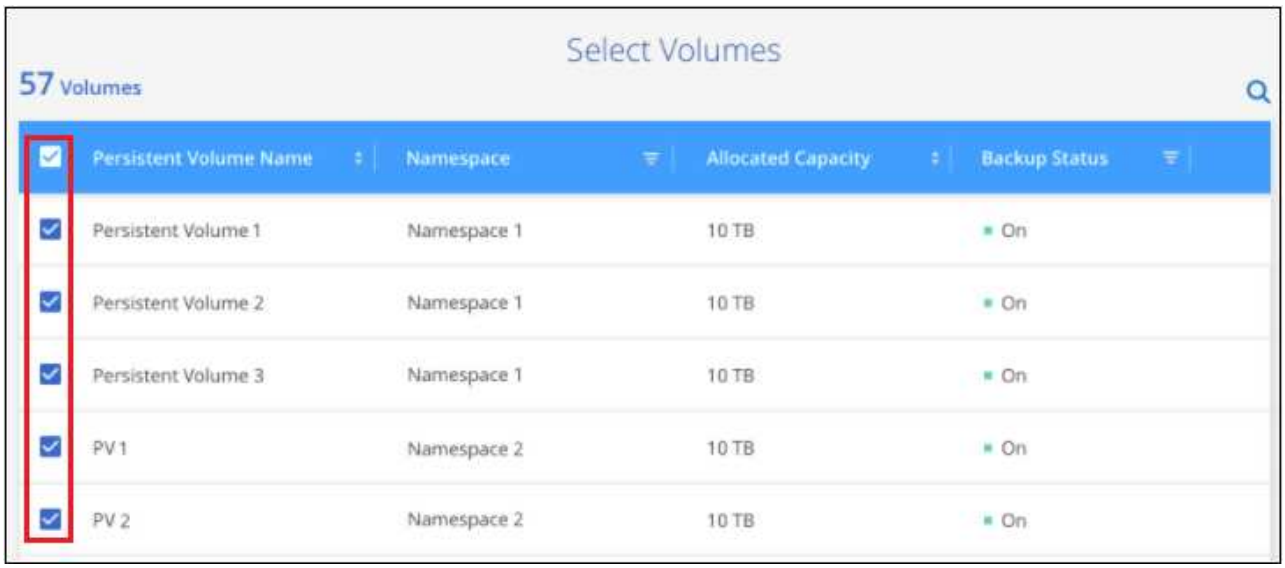
1. Select the working environment and click **Enable** next to the Backup & Restore service in the right-panel.

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 (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 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.

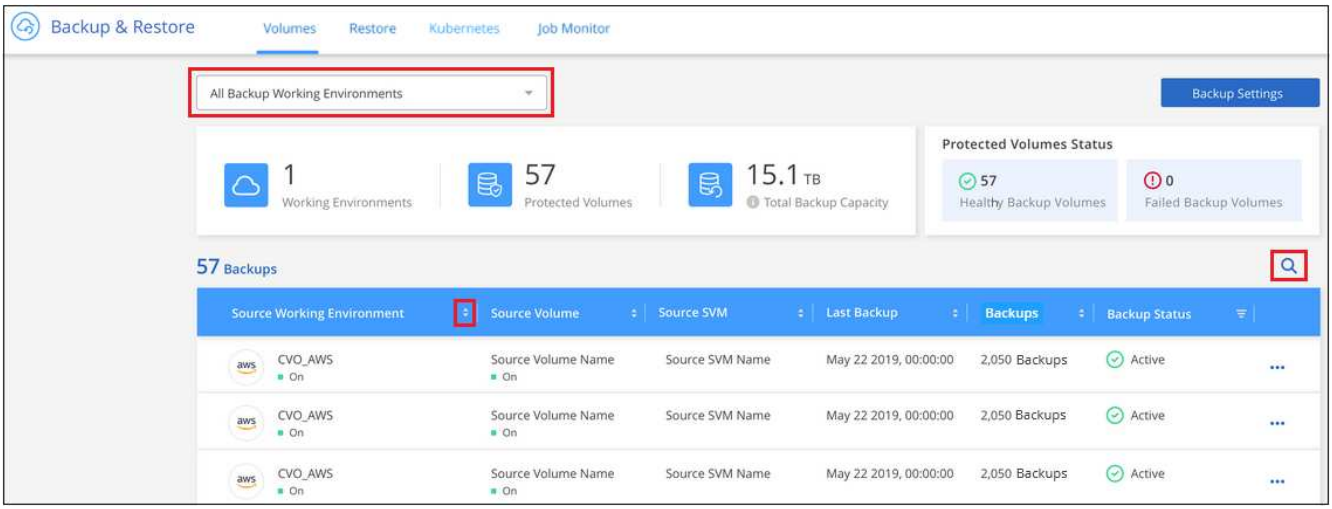
Do not manage or change backup files directly from your cloud provider environment. This may corrupt the files and will result in an unsupported configuration.

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.



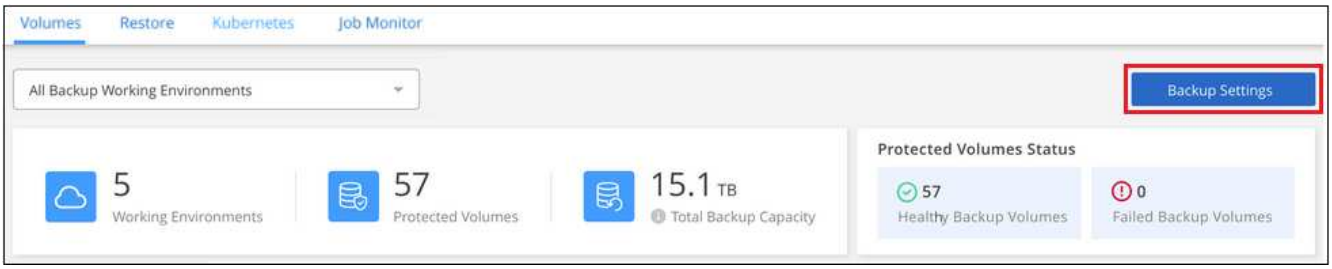
If you are looking for specific volumes in certain working environments, you can refine the list by working environment and volume, or you can use the search filter.

Editing an existing backup policy

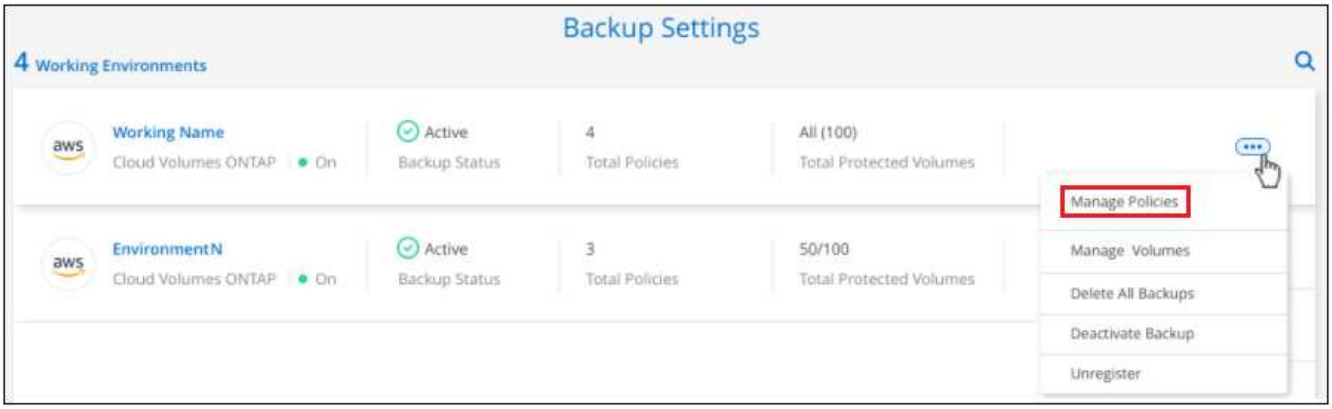
You can change the attributes for a backup policy that is currently applied to volumes in a working environment. Changing the backup policy affects all existing volumes that are using the policy.

Steps

1. From the **Volumes** 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.

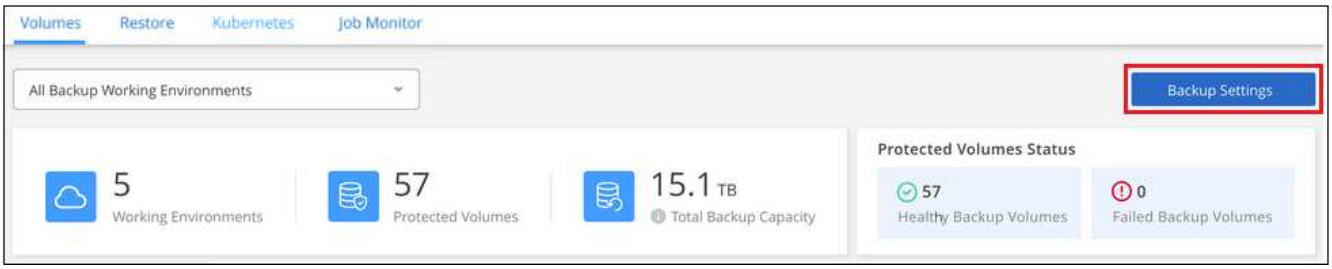
4. From the *Edit Policy* page, change the schedule and backup retention and click **Save**.

Enabling and disabling backups of volumes

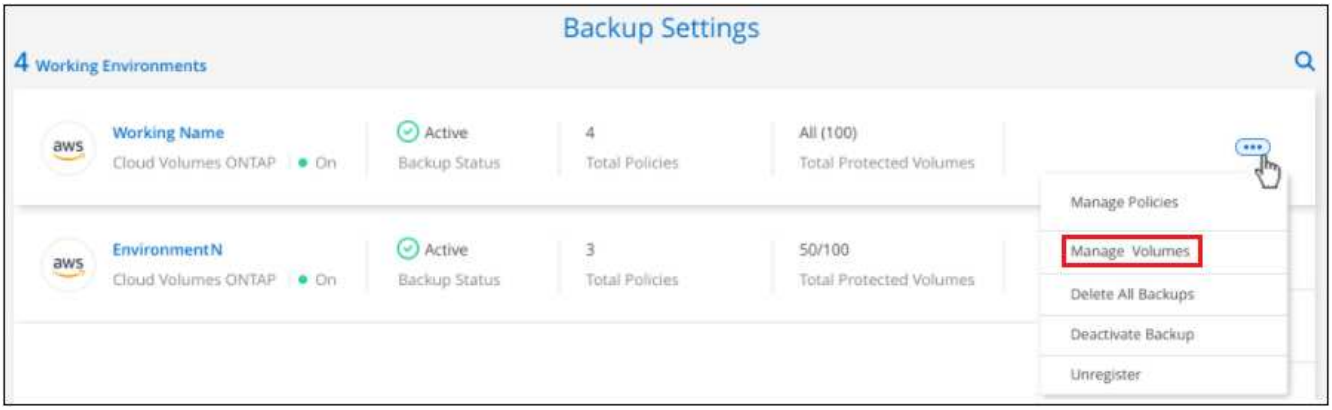
You can stop backing up a volume if you do not need backup copies of that volume and you do not want to pay for the cost to store the backups. You can also add a new volume to the backup list if it is not currently being backed up.

Steps

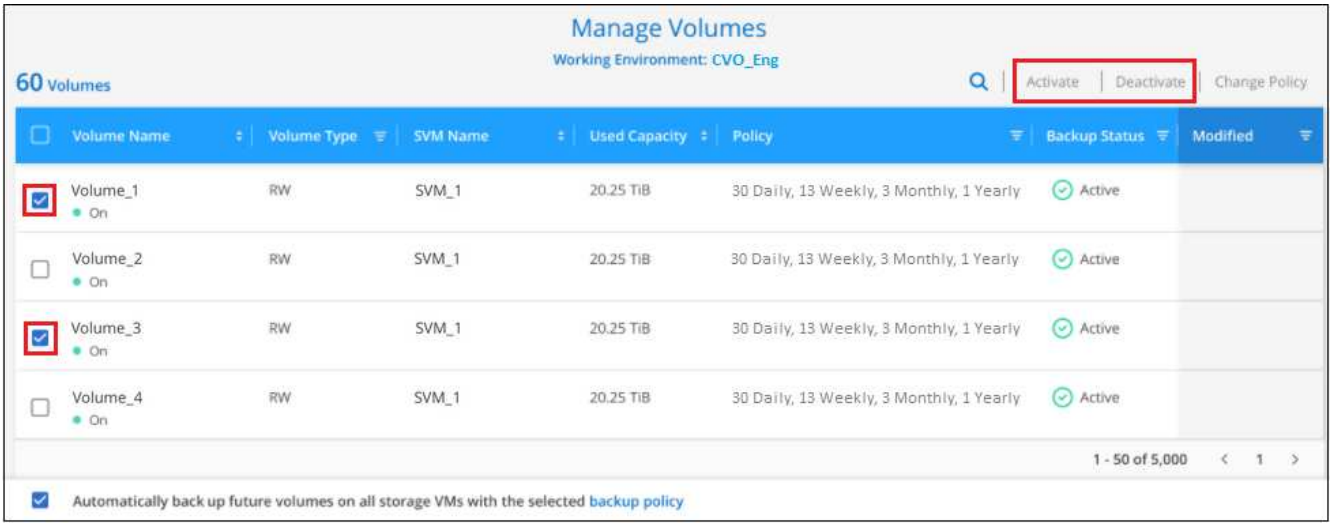
1. From the **Kubernetes** tab, select **Backup Settings**.



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



You can choose to have all volumes added in the future to have backup enabled, or not, by using the checkbox for "Automatically back up future volumes…". If you disable this setting, you'll need to manually enable backups for volumes added in the future.

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.

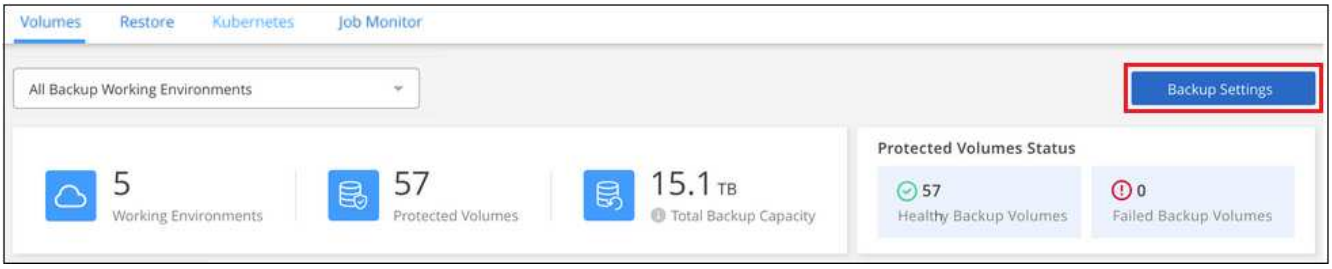
Adding a new backup policy

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 defined. 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.

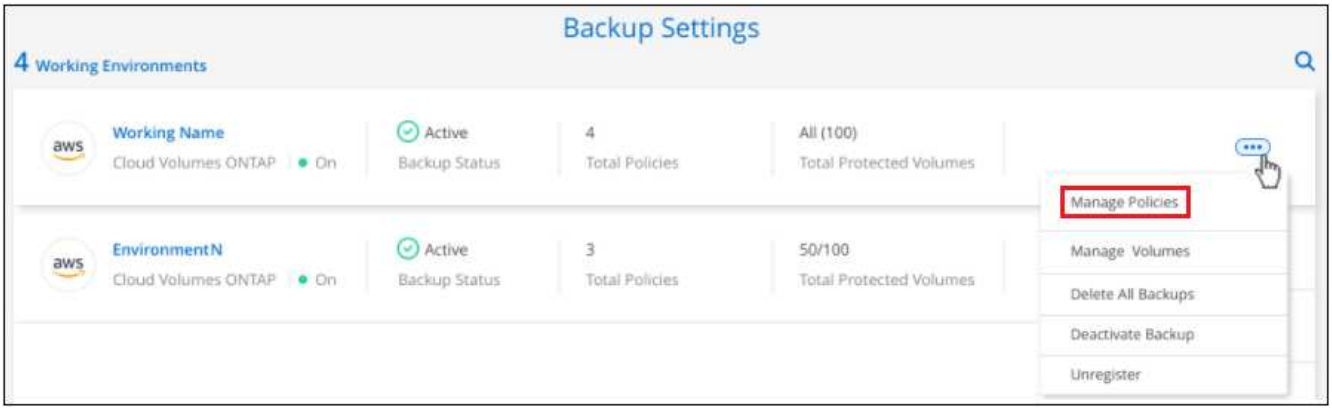
If you want to apply a new backup policy to certain volumes in a working environment, you first need to add the backup policy to the working environment. Then you can apply the policy to volumes in that working environment.

Steps

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

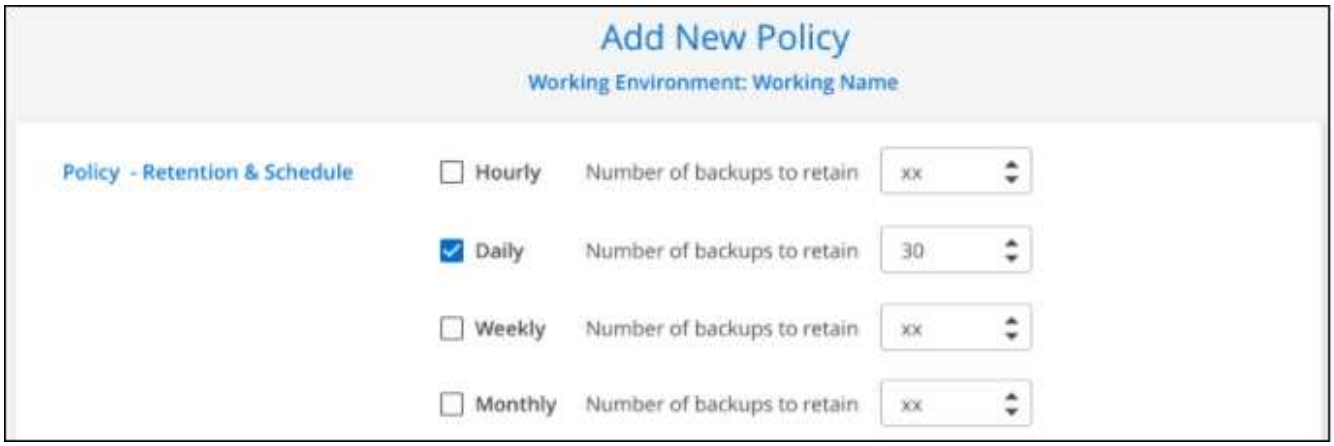


2. From the *Backup Settings* page, click ••• for the working environment where you want to add the new policy, and select **Manage Policies**.



3. From the *Manage Policies* page, click **Add New Policy**.

4. From the *Add New Policy* page, define the schedule and backup retention and click **Save**.



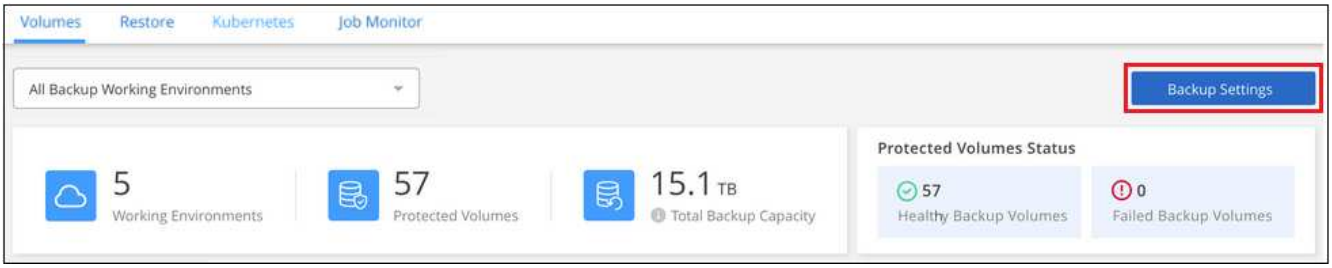
Changing the policy assigned to existing volumes

You can change the backup policy assigned to your existing volumes if you want to change the frequency of taking backups, or if you want to change the retention value.

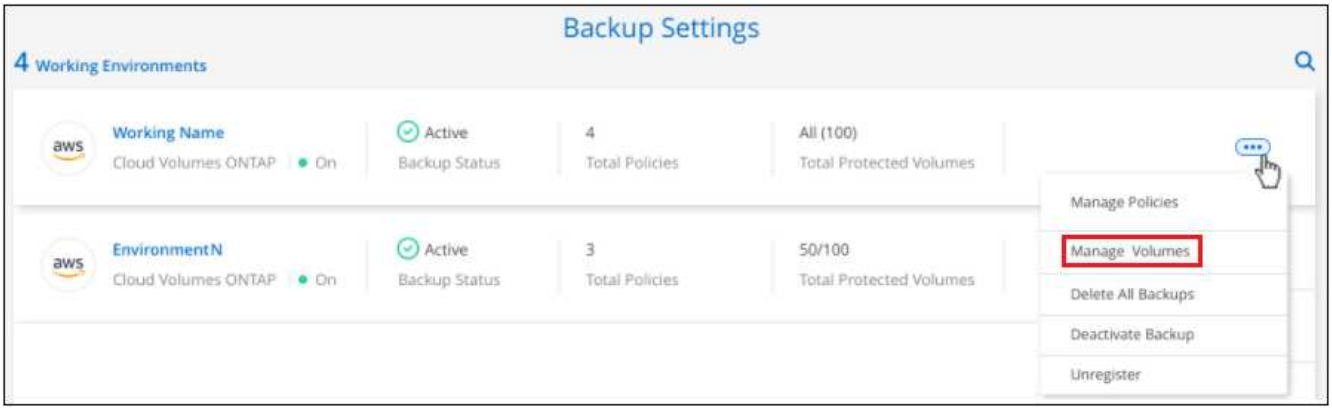
Note that the policy that you want to apply to the volumes must already exist. See how to add a new backup policy for a working environment.

Steps

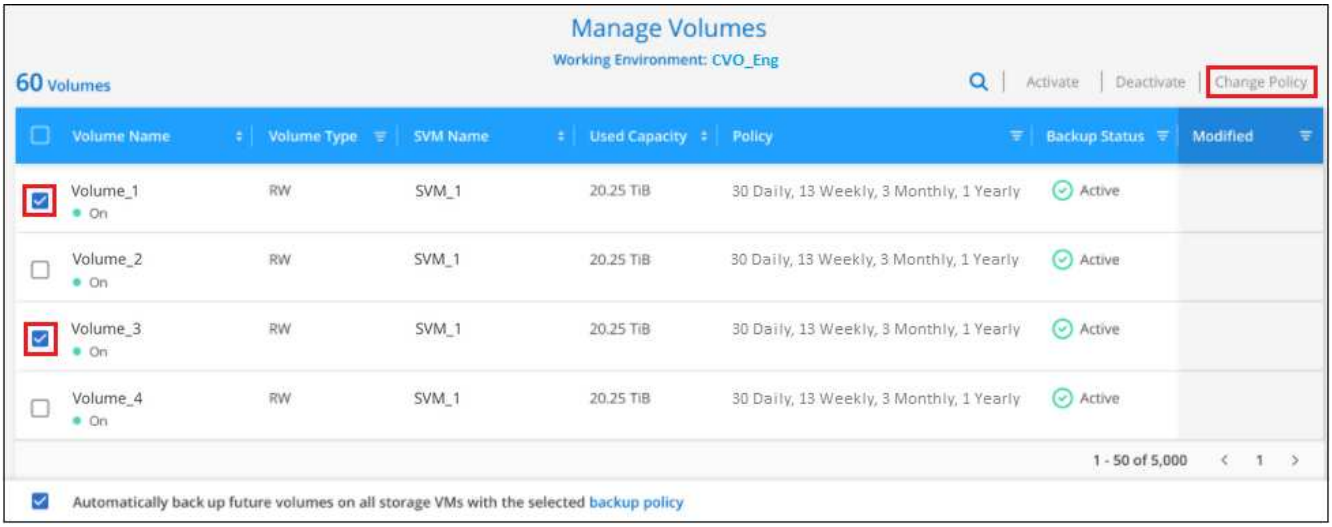
1. From the **Volumes** tab, select **Backup Settings**.



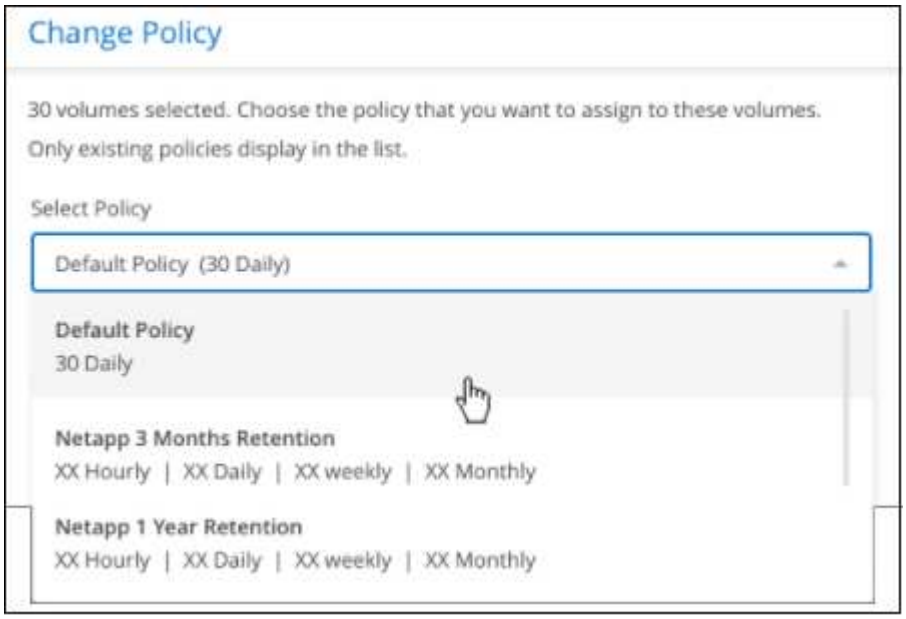
2. From the *Backup Settings page*, click ••• for the working environment where the volumes exist, and select **Manage Volumes**.



3. Select the checkbox for a volume, or volumes, that you want to change the policy for, and then click **Change Policy**.



4. In the *Change Policy* page, select the policy that you want to apply to the volumes, and click **Change Policy**.



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

Viewing the list of backups for each volume

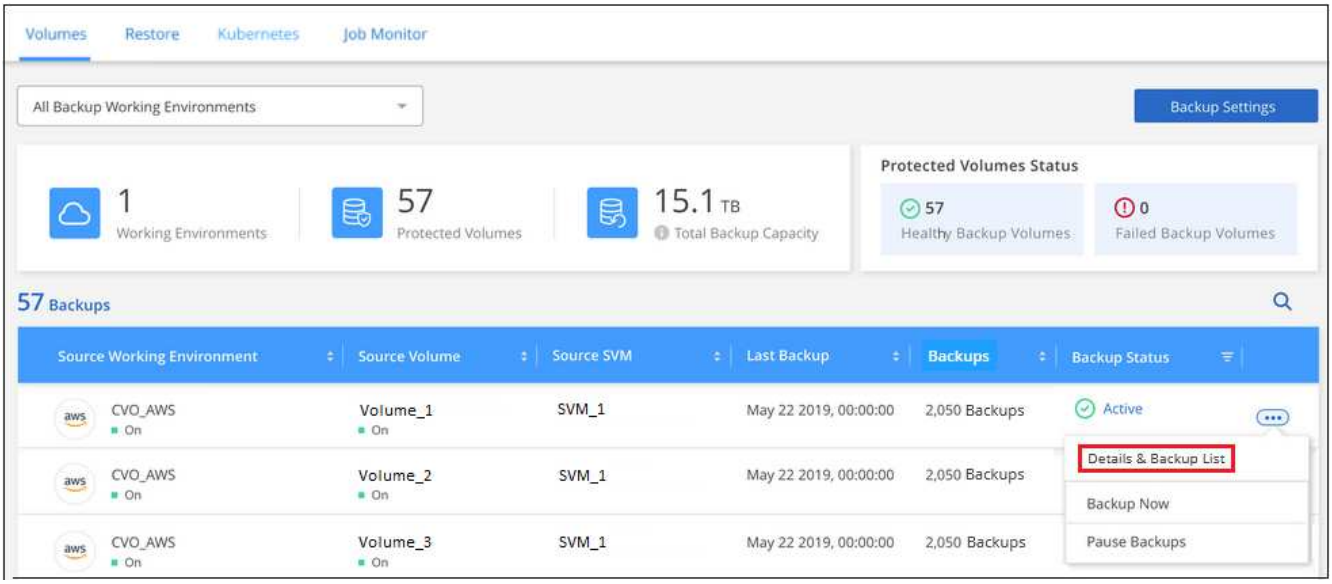
You can view the list of all backup files that exist for each volume. This page displays details about the source volume, destination location, and backup details such as last backup taken, the current backup policy, backup file size, and more.

This page also enables you perform the following tasks:

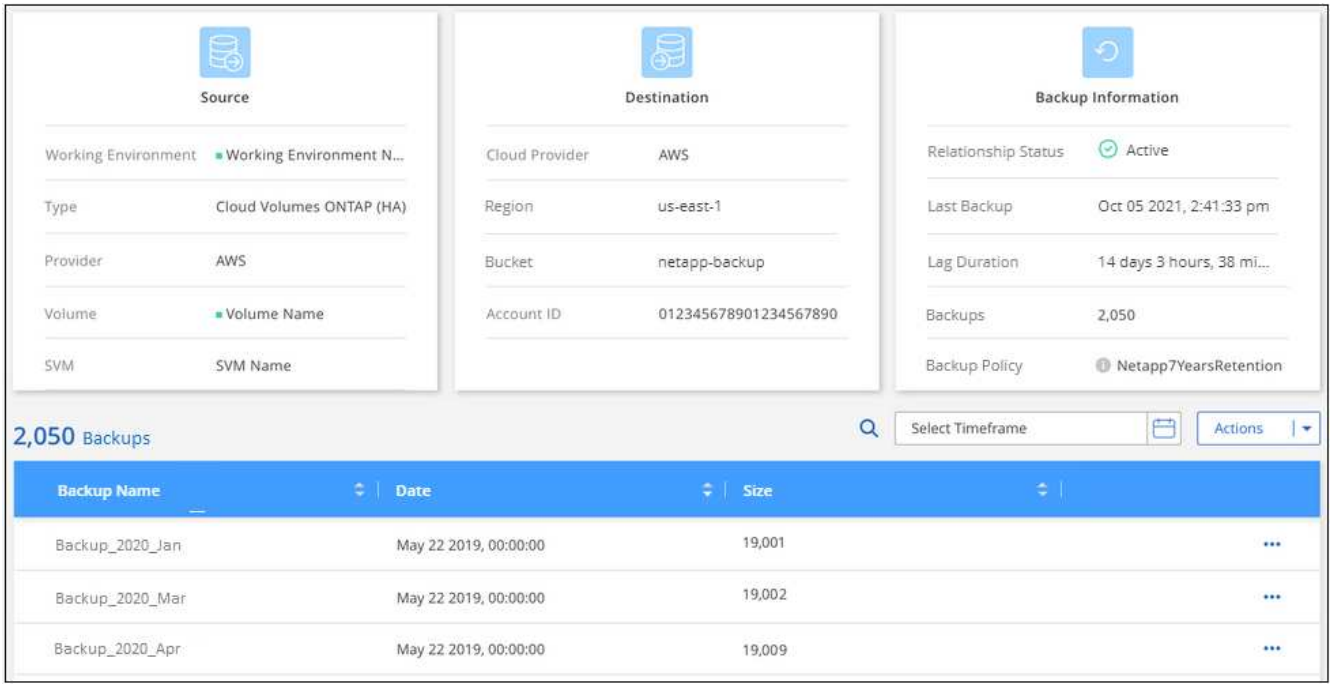
- Delete all backup files for the volume
- Delete individual backup files for the volume
- Download a backup report for the volume

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.

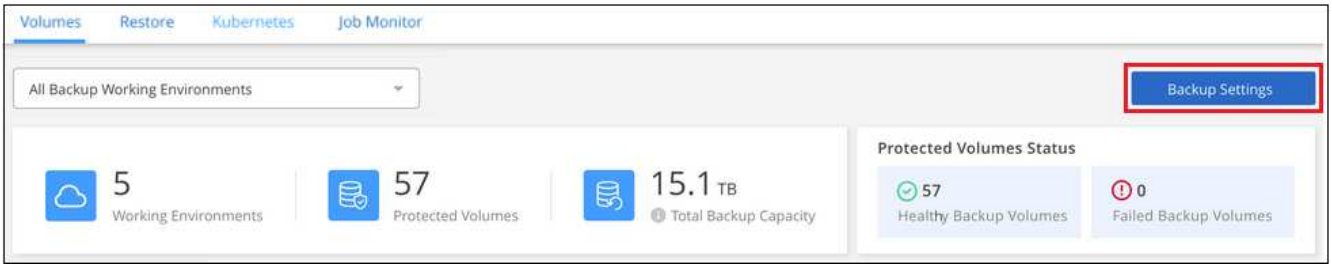
If you plan to delete a working environment or cluster that has backups, you must delete the backups **before** deleting the system. Cloud Backup doesn't automatically delete backups when you delete a system, and there is no current support in the UI to delete the backups after the system has been deleted.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

Deleting all backup files for a working environment

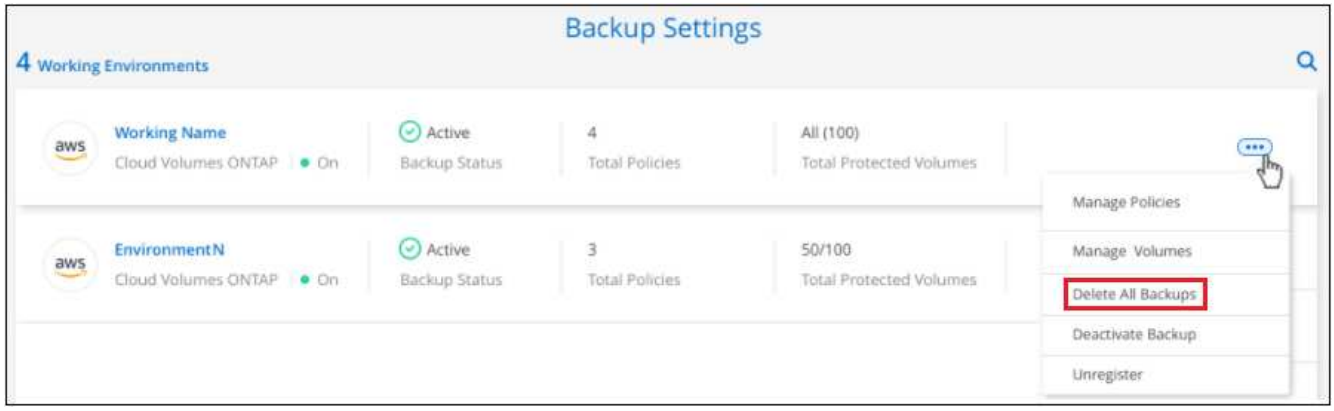
Deleting all backups for a working environment does not disable future backups of volumes in this working environment. If you want to stop creating backups of all volumes in a working environment, you can deactivate backups as described here.

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**.

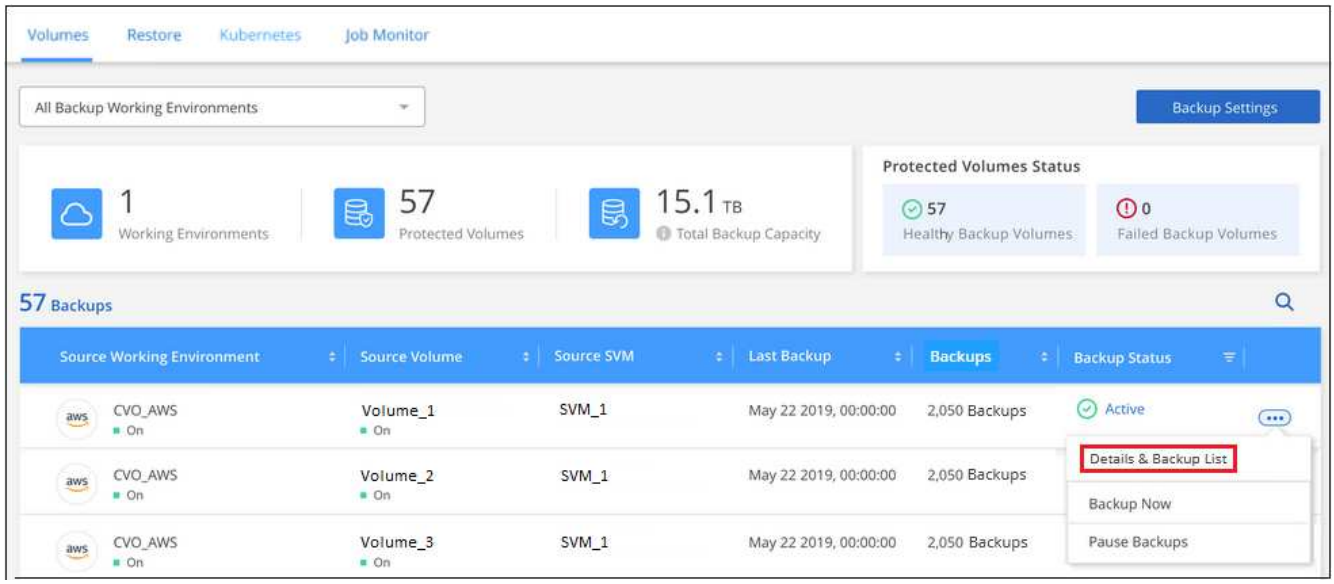
Deleting all backup files for a volume

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

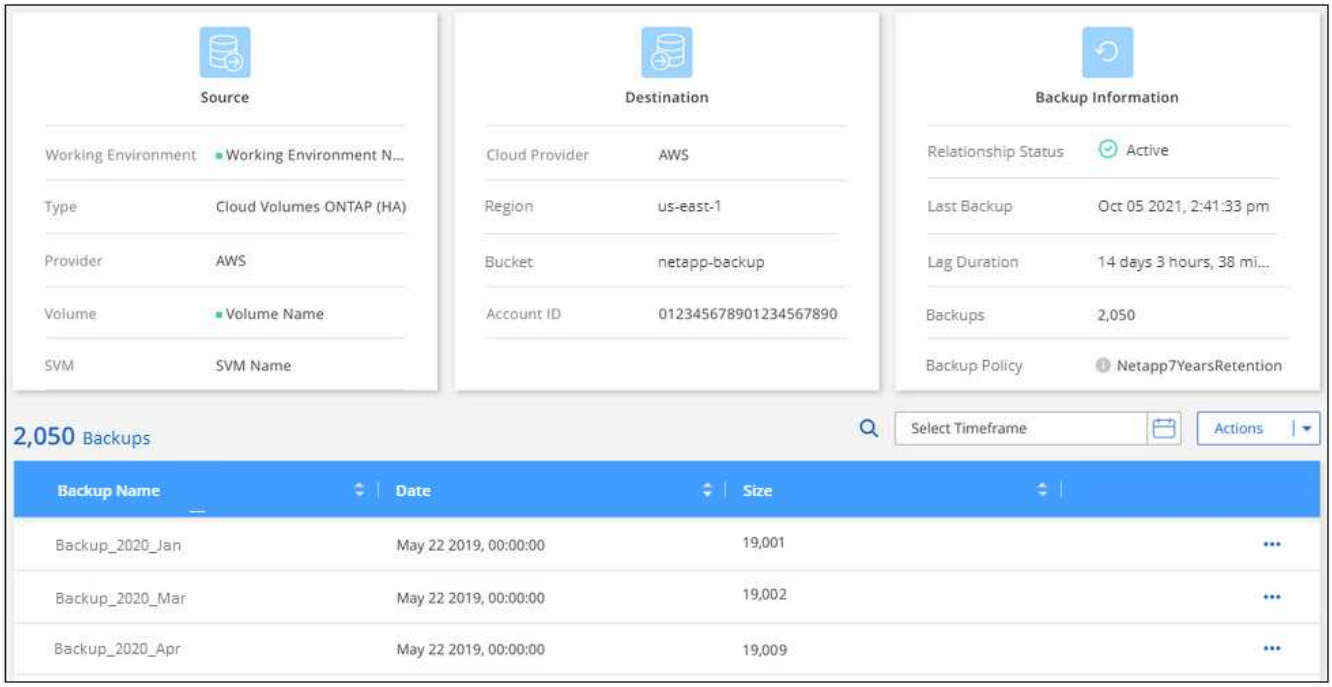
You can restart making backups for the volume at any time from the Manage Backups page.

Steps

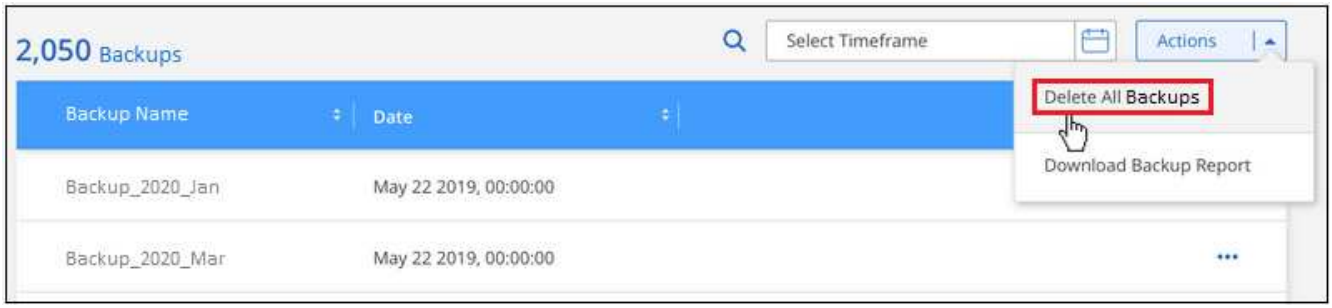
1. From the **Kubernetes** tab, click ••• for the source volume and select **Details & Backup List**.



The list of all backup files is displayed.



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



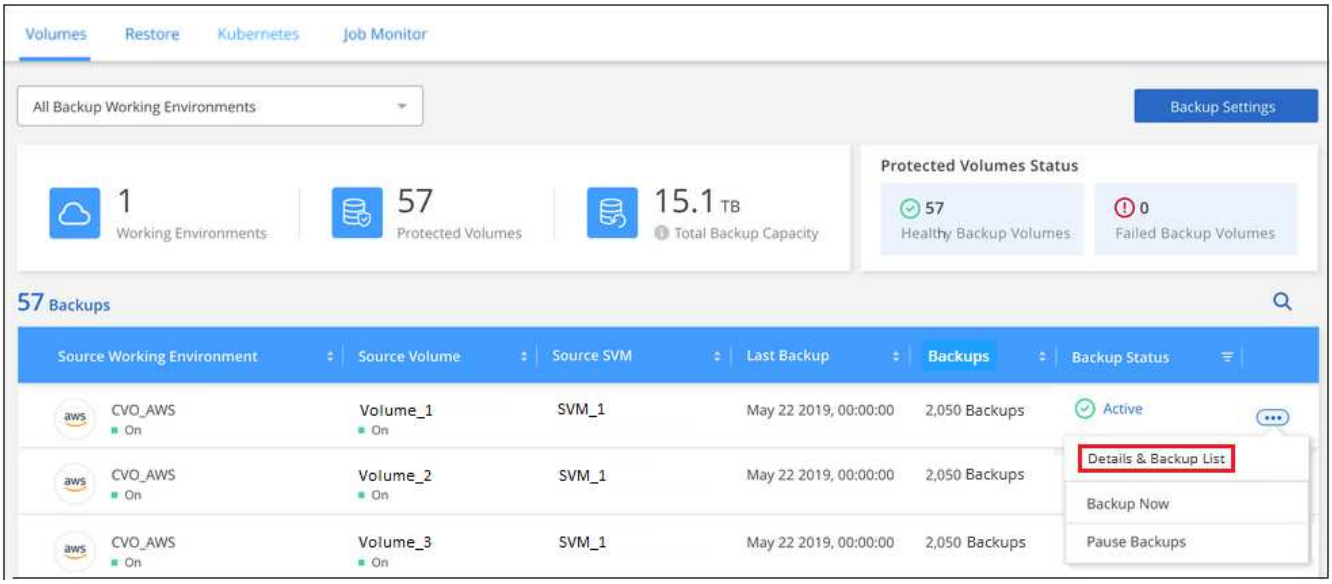
3. In the confirmation dialog box, enter the volume name and click **Delete**.

Deleting a single backup file for a volume

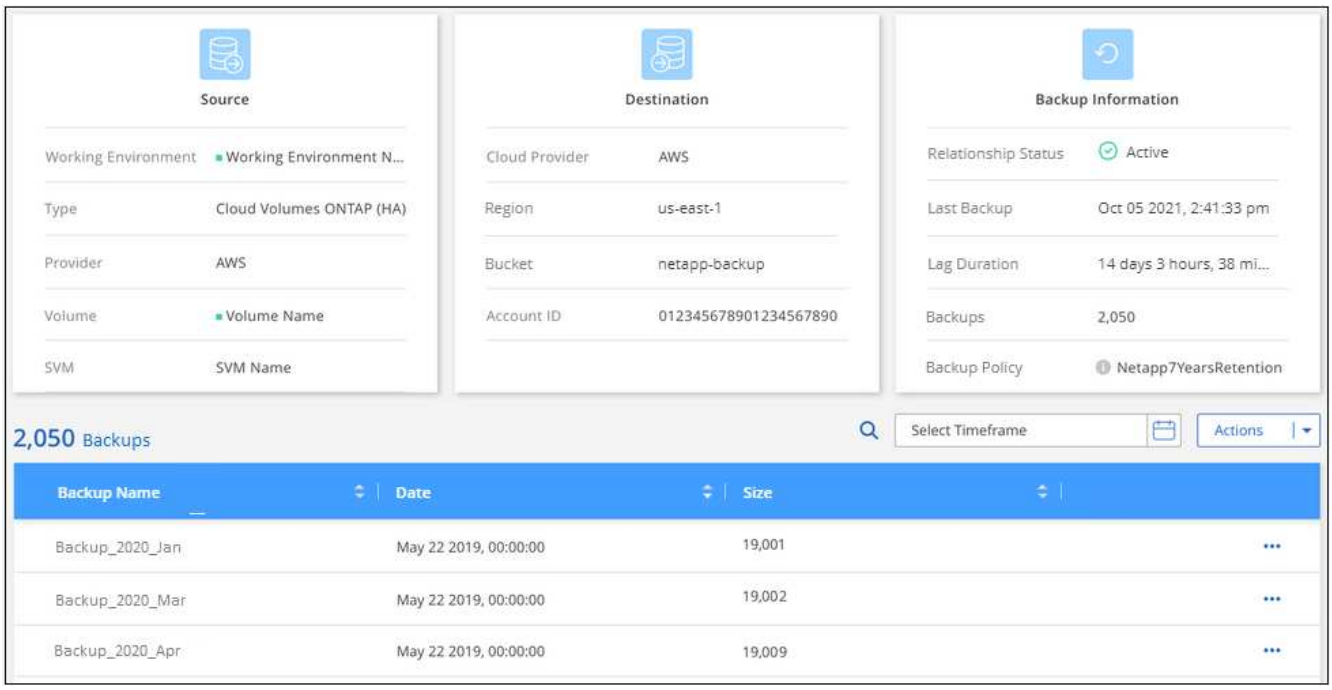
You can delete a single backup file. This feature is available only if the volume backup was created from a system with ONTAP 9.8 or greater.

Steps

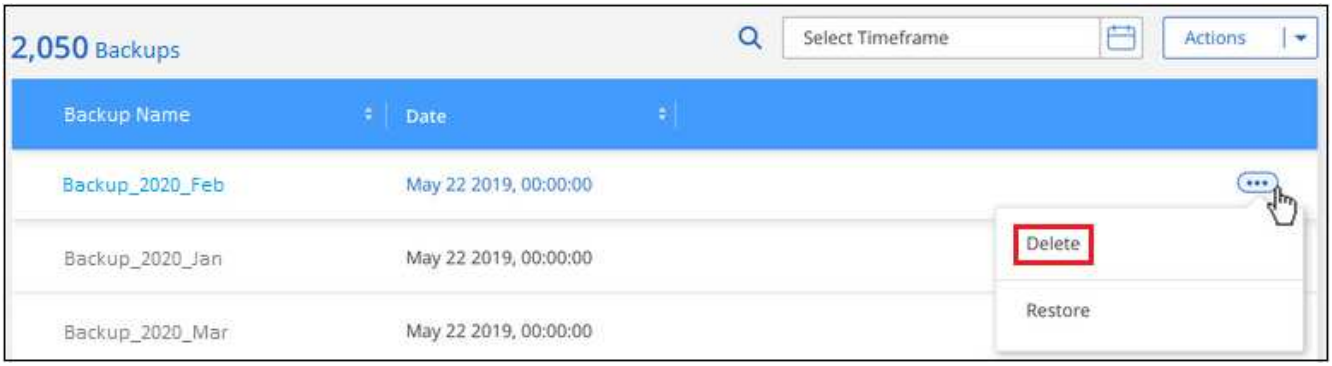
1. From the **Kubernetes** tab, click ••• for the source volume and select **Details & Backup List**.



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**.

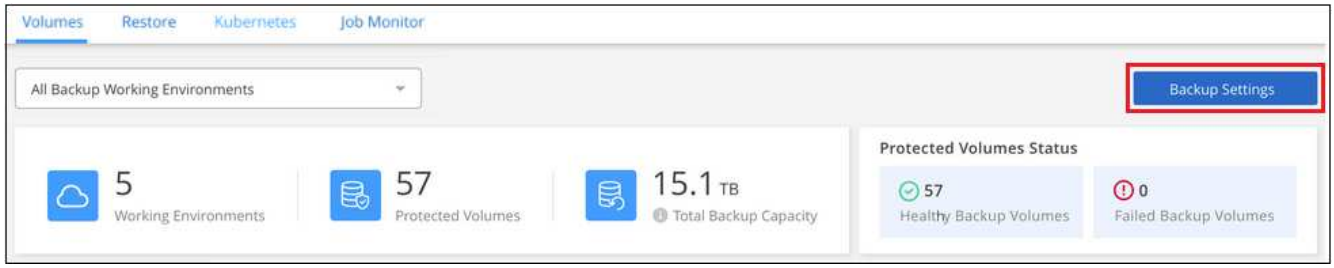
Disabling Cloud Backup for a working environment

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.

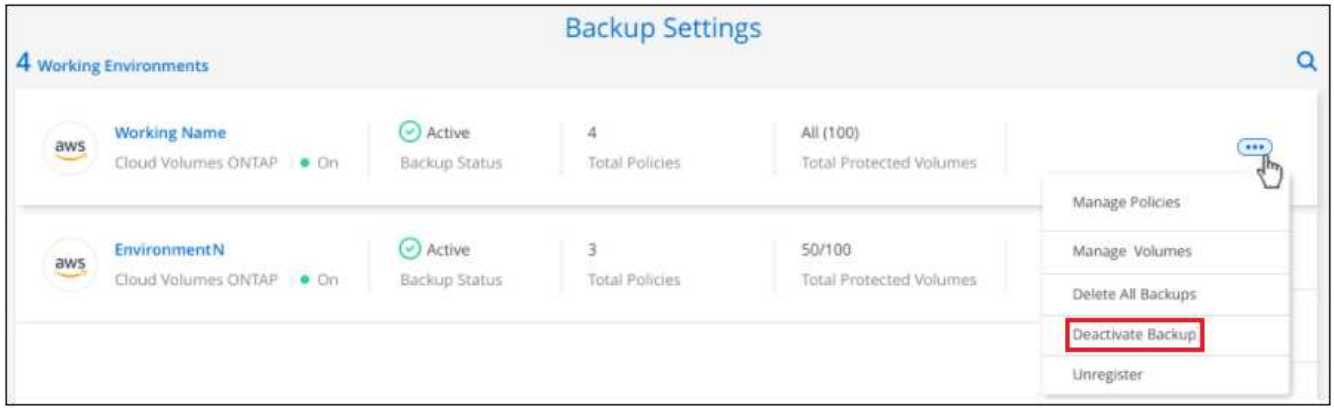
Note that you'll continue to be charged by your cloud provider for object storage costs for the capacity that your backups use unless you delete the backups.

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.

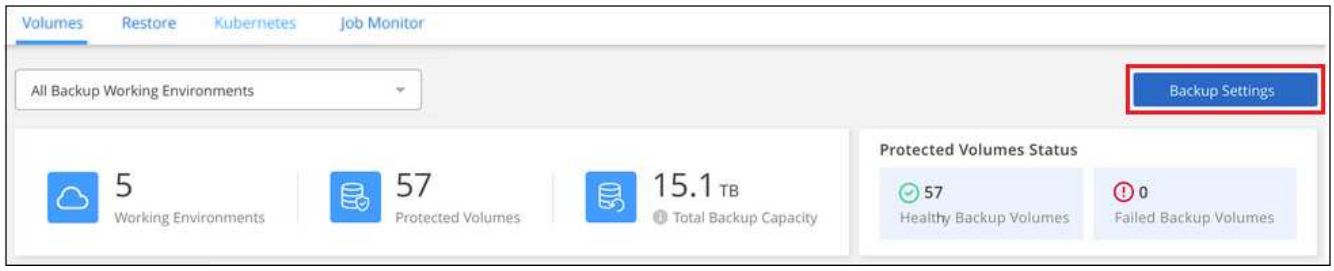
Before you can unregister Cloud Backup, you must perform the following steps, in this order:

- 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

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

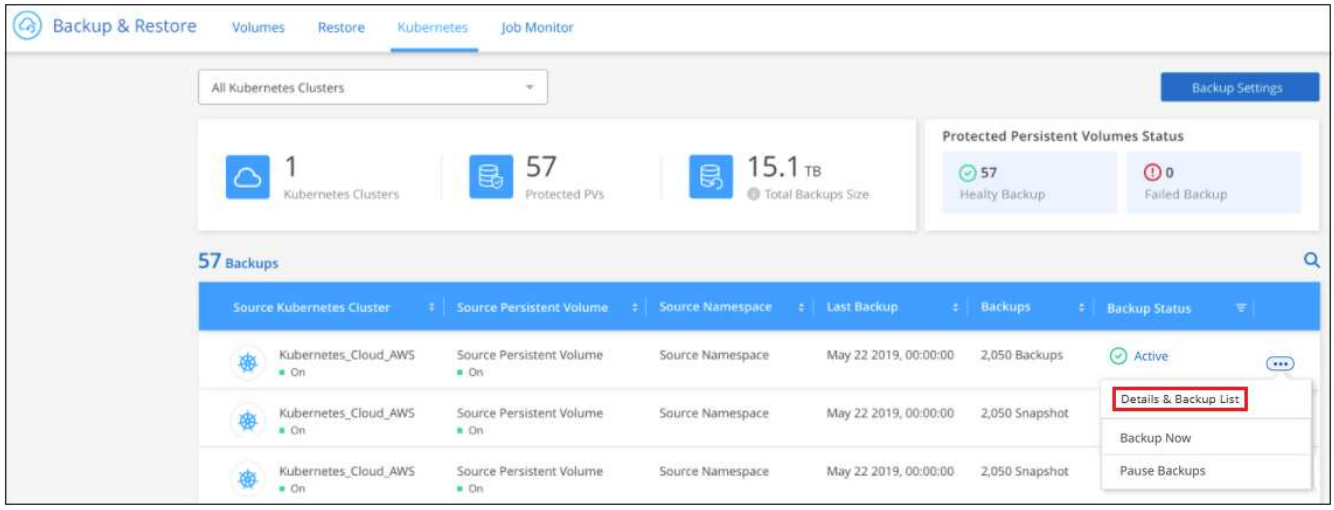
Restoring volumes from a Kubernetes backup file

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.

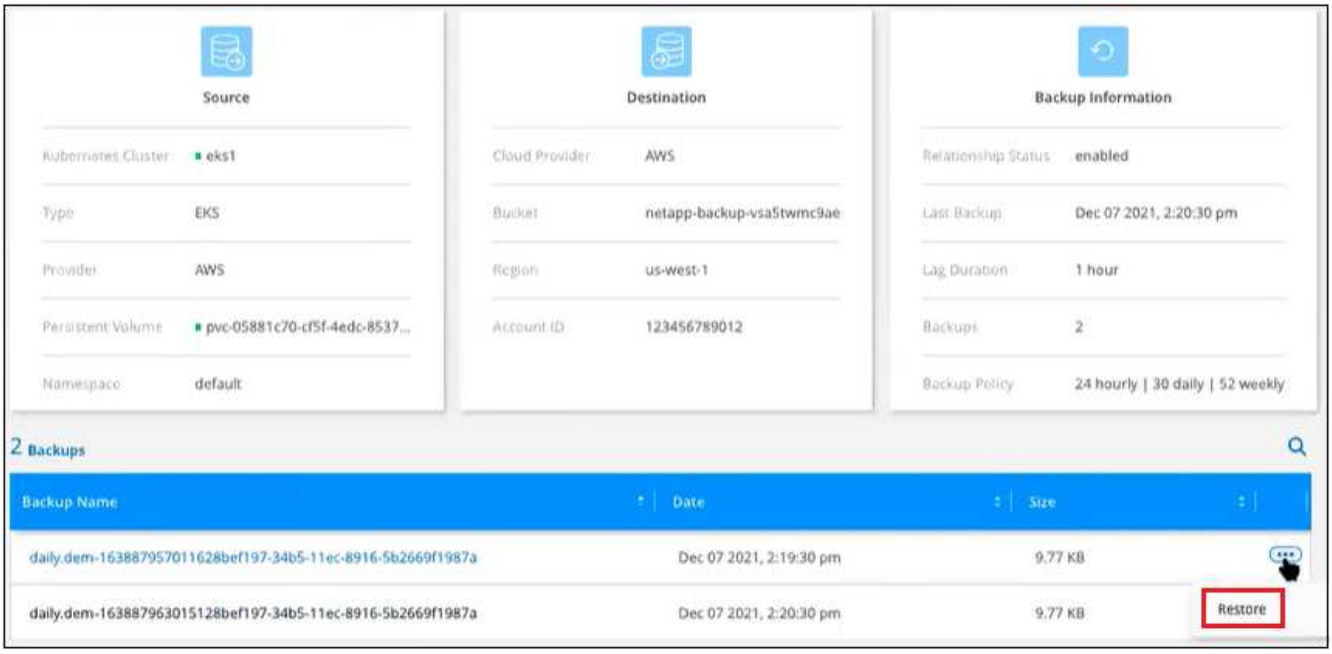
Steps

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 **Volume Details**.

   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.

Back up and restore on-premises applications data

Protect your on-premises applications data

You can integrate Cloud Backup for Applications with Cloud Manager and on-premises SnapCenter to back up the application consistent Snapshots from on-premises ONTAP to cloud. When required you can restore from cloud to on-premises SnapCenter Server.

You can back up Oracle and Microsoft SQL applications data from on-premises ONTAP to either Amazon Web Services or Microsoft Azure.

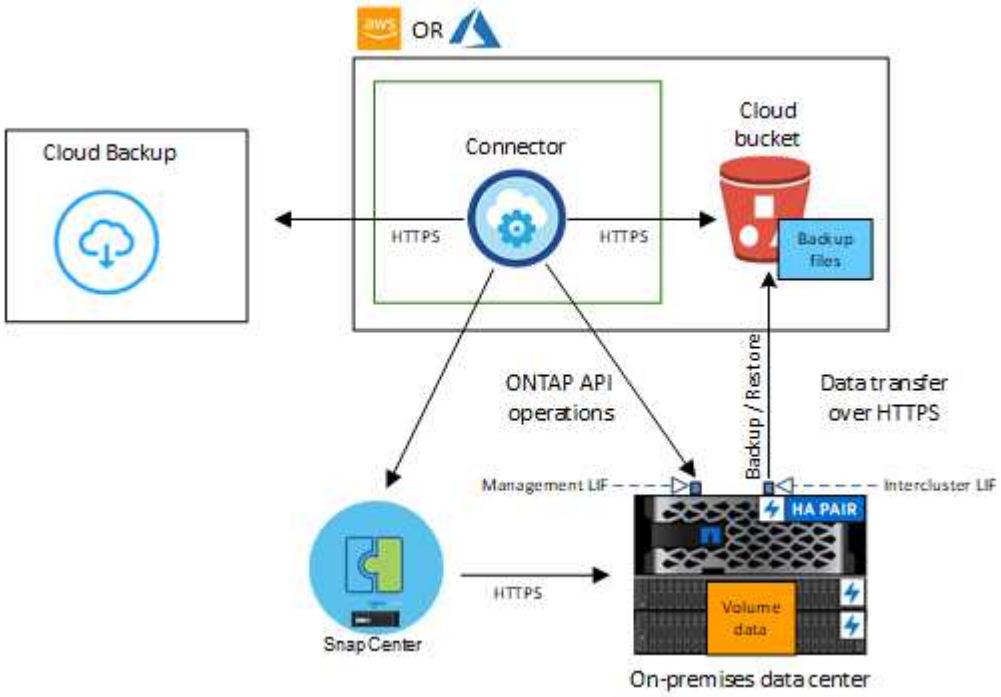
You should be using SnapCenter Software 4.6.

Requirements

Read the following requirements to make sure that you have a supported configuration before you start backing up application data to cloud services.

- ONTAP 9.8 or later
- Cloud Manager 3.9
- SnapCenter Server 4.6
- At least one backup per application should be available in SnapCenter Server
- At least one daily, weekly, or monthly policy in SnapCenter with no label or same label as that of the Cloud Backup for Applications policy in Cloud Manager.

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



Protection Policies

You should use the one of the policies defined in Cloud Backup for Applications to back up the application data to cloud.

Custom policies are not supported.

Policy Name	Label	Retention Value
1 Year Daily LTR	Daily	366
5 Years Daily LTR	Daily	1830
7 Year Weekly LTR	Weekly	370
10 Year Monthly LTR	Monthly	120

The labels and retention value of these policies can be modified using the REST API until the policy is associated with an application. Only one policy can be associated with an application and once associated, you cannot dissociate.

In addition to the Cloud Backup for Applications policies, you would also need at least one SnapCenter policy to back up the application data to cloud.

Back up on-premises applications data to cloud

You can back up the applications data from ONTAP to cloud by integrating Cloud Backup for Applications with Cloud Manager and on-premises SnapCenter.

Register SnapCenter Server

Only a user with SnapCenterAdmin role can register the host on which SnapCenter Server 4.6 is running. You can register multiple SnapCenter Server hosts but once registered, you cannot remove the SnapCenter Server host.

Steps

1. In Cloud Manager UI, click **Backup & Restore** > **Applications**.
2. From the **Settings** drop-down, click **SnapCenter Servers**.
3. Click **Register SnapCenter Server**.
4. Specify the following details:
   a. In the SnapCenter Server field, specify the FQDN or IP address of the SnapCenter Server host.
   b. In the Port field, specify the port number on which the SnapCenter Server is running.

      You should ensure that the port is open for the communication to happen between SnapCenter Server and the Cloud Backup for Applications.

   c. In the Tags field, specify a site name, city name, or any custom name with which you want to tag the SnapCenter Server.

The tags are comma separated.

d. In the Username and Password field, specify the credentials of the user with SnapCenterAdmin role.

5. Click **Register**.

After you finish

Click **Backup & Restore** > **Applications** to view all the applications that are protected using the registered SnapCenter Server host.

For SQL Server databases, the Application Name column displays the name in *application_name (host name)* format. When you search by providing the name in *application_name (host name)* format, the SQL Server database details are not displayed.

The supported applications and their configurations are:

- Oracle database: Full backups (data + log) created with at least one daily, weekly, or monthly schedules.
- Microsoft SQL Server database:
  - Standalone, failover cluster instances, and availability groups
  - Full backups created with at least one daily, weekly, or monthly schedules

The following Oracle and SQL Server databases will not be displayed:

- Databases that have no backups
- Databases that have only on-demand or hourly policy
- Databases residing on RDM or VMDK

Back up applications data

You can protect one or more applications simultaneously to the cloud using a single policy. Only the default pre-canned policies can be assigned to protect the application.

You can protect only one application at a time if you are using the Cloud Manager GUI. However, if you are using REST APIs, you can protect multiple applications simultaneously.

If you are protecting an SQL Server instance, then cloud protection will be configured for all the volumes of the eligible databases in that instance.
If you are protecting an SQL Server availability group, then cloud protection will be configured for all the volumes of the databases in that availability group. However, based on the backup preference, the Snapshot will be copied form the respective volumes.

Steps

1. In Cloud Manager UI, click **Backup & Restore** > **Applications**.
2. Click [icon to select the action] corresponding to the application and click **Activate Backup**.
3. Add the working environment.

   Configure the ONTAP cluster that hosts the SVM on which the application is running. After adding the working environment for one of the applications, it can be reused for all the other applications residing on the same ONTAP cluster.

a. Select the SVM and click Add Working Environment.
b. In the Add Working Environment wizard:
    i. Specify the IP address of the ONTAP cluster.
    ii. Specify the admin credentials.

        Cloud Backup for Applications supports only cluster admin.

c. Click **Add Working Environment**.

4. Select and configure the cloud provider.

Configure Amazon Web Services

a. Specify the AWS account.
b. In the AWS Access Key field, specify the key.
c. In the AWS Secret Key field, specify the password.
d. Select the region where you want to create the backups.
e. Specify the IP addresses of the ONTAP clusters that were added as the working environments.

Configure Microsoft Azure

a. Specify the Azure subscription ID.
b. Select the region where you want to create the backups.
c. Either create a new resource group or use an existing resource group.
d. Specify the IP addresses of the ONTAP clusters that were added as the working environments.

5. In the Assign Policy page, select the policy and click **Next**.
6. Review the details and click **Activate Backup**.

Manage protection of applications

You can view the policies and backups. Depending upon the change in database, policies, or resource groups, you can refresh the updates from the Cloud Manager UI.

View policies

You can view all the default pre-canned policies. For each of these policies, when you view the details all the associated Cloud Backup for Applications policies and all the associated applications are listed.

1. Click **Backup & Restore** > **Applications**.
2. From the **Settings** drop-down, click **Policies**.
3. Click **View Details** corresponding to policy whose details you want to view.

   The associated Cloud Backup for Applications policies and all the applications are listed.

   You should not delete the Cloud Backup for Applications policies.

You can also view cloud extended SnapCenter policies, by running the `Get-SmResources` SnapCenter cmdlet.
The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running Get-Help command_name. Alternatively, you can also refer the SnapCenter Software Cmdlet Reference Guide.

View backups on cloud

You can view the backups on cloud in the Cloud Manager UI.

1. Click **Backup & Restore** > **Applications**.
2. Click [icon to select the action] corresponding to the application and click **View Details**.

> The time taken for the backups to be listed depends on ONTAP's default replication schedule (maximum of 1 hour) and Cloud Manager (maximum of 6 hours).

- For Oracle databases, both data and log backups, SCN number for each backup, end date for each backup are listed. You can select only the data backup and restore the database to on-premises SnapCenter Server.
- For Microsoft SQL Server databases, only the full backups and the end date for each backup are listed. You can select the backup and restore the database to on-premises SnapCenter Server.
- For Microsoft SQL Server instance, backups are not listed instead only the databases under that instance is listed.

> The backups created before enabling cloud protection are not listed for restore.

You can also view these backups by running the `Get-SmBackup` SnapCenter cmdlet.
The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running Get-Help command_name. Alternatively, you can also refer the SnapCenter Software Cmdlet Reference Guide.

Database layout change

When volumes are added to the database, SnapCenter Server will label the snapshots on the new volumes automatically as per the policy and the schedule. These new volumes will not have the object store endpoint and you should refresh by executing the following steps:

1. Click **Backup & Restore** > **Applications**.
2. From the **Settings** drop-down, click **SnapCenter Servers**.
3. Click [icon to select the action] corresponding to the SnapCenter Server hosting the application and click **Refresh**.

   The new volumes are discovered.

4. Click [icon to select the action] corresponding to the application and click **Refresh Protection** to enable cloud protection for the new volume.

If a storage volume is removed from the application after configuring the cloud service, for new backups SnapCenter Server will only label the snapshots on which the application is residing. If the removed volume is not used by any other applications, then you should manually delete the object store relationship.
If you update the application inventory, it will contain the current storage layout of the application.

Policy or resource group change

If there is a change to the SnapCenter policy or resource group, you should refresh the protection.

1. Click **Backup & Restore** > **Applications**.
2. Click [icon to select the action] corresponding to the application and click **Refresh Protection**.

Monitor Jobs

Jobs are created for all the Cloud Backup operations. You can monitor all the jobs and all the sub tasks that are performed as part of each task.

1. Click **Backup & Restore** > **Job Monitoring**.

   When you initiate an operation, a window appears stating that the job is initiated. You can click the link to monitor the job.

2. Click the primary task to view the sub tasks and status of each of these sub tasks.

Configure CA Certificates

If you have CA certificates, you should manually copy the root CA certificates to the connector machine.

However, if you do not have CA certificates, you can proceed without configuring CA certificates.

Steps

1. Copy the certificate to the volume that can be accessed from the docker agent.
   - `cd /var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/mkdir sc_certs`
   - `chmod 777 sc_certs`
2. Copy the RootCA certificate files to the above folder on the connector machine.

   ```
   cp <path on connector>/<filename>
   /var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/sc_certs
   ```

3. Copy the CRL file to the volume which can be accessed from the docker agent.
   - `cd /var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/mkdir sc_crl`
   - `chmod 777 sc_crl`
4. Copy the CRL files to the above folder on the connector machine.

   ```
   cp <path on connector>/<filename>
   /var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/sc_crl
   ```

5. After copying the certificates and CRL files, restart the Cloud Backup for Apps service.
   - `sudo docker exec cloudmanager_snapcenter sed -i 's/skipSCCertValidation: true/skipSCCertValidation: false/g' /opt/netapp/cloudmanager-snapcenter-agent/config/config.yml`
   - `sudo docker restart cloudmanager_snapcenter`

Restore applications data

Restore Oracle database

You can only restore the Oracle database to the same SnapCenter Server host, same SVM, or to the same database host. For a RAC database, the data will be restored to the on-premises node where the backup was created.

Only full database with control file restore is supported. If the archive logs are not present in the AFS, you should specify the location that contains the archive logs required for recovery.

Steps

1. In Cloud Manager UI, click **Backup & Restore** > **Applications**.
2. In the **Filter By** field, select the filter **Type** and from the drop-down select **Oracle**.
3. Click **View Details** corresponding to the database that you want to restore and click **Restore**.
4. On the Restore Type page, perform the following actions:
   a. Select **Control files** if you want to restore control file along with full database.
   b. Select **Change database state if needed for restore and recovery** to change the state of the database to the state required to perform restore and recovery operations.

      The various states of a database from higher to lower are open, mounted, started, and shutdown. You must select this check box if the database is in a higher state but the state must be changed to a lower state to perform a restore operation. If the database is in a lower state but the state must be changed to a higher state to perform the restore operation, the database state is changed automatically even if you do not select the check box.

      If a database is in the open state, and for restore the database needs to be in the mounted state, then the database state is changed only if you select this check box.
5. On the Recovery Scope page, perform the following actions:
   a. Specify the recovery scope.

If you…	Do this…
Want to recover to the last transaction	Select **All Logs**.
Want to recover to a specific System Change Number (SCN)	Select **Until SCN (System Change Number)**.
Want to recover to a specific data and time	Select **Date and Time**. You must specify the date and time of the database host's time zone.
Do not want to recover	Select **No recovery**.

If you…	Do this…
Want to specify any external archive log locations	If the archive logs are not present in the AFS, you should specify the location that contains the archive logs required for recovery.

b. Select the check box if you want to open the database after recovery.

In a RAC setup, only the RAC instance that is used for recovery is opened after recovery.

6. Review the details and click **Restore**.

Restore SQL Server database

You can restore SQL Server database either to the same host or to the alternate host. Recovery of log backups and reseed of availability groups are not supported.

Steps

1. In Cloud Manager UI, click **Backup & Restore** > **Applications**.
2. In the **Filter By** field, select the filter **Type** and from the drop-down select **SQL**.
3. Click **View Details** to view all the available backups.
4. Select the backup and click **Restore**.
5. Select the location where you want to restore the database files.

Option	Description
Restore the database to the same host where the backup was created	Select this option if you want to restore the database to the same SQL server where the backups are taken.
Restore the database to an alternate host	Select this option if you want the database to be restored to a different SQL server in the same or different host where backups are taken. Select a host name, provide a database name (optional), select an instance, and specify the restore paths. The file extension provided in the alternate path must be same as the file extension of the original database file. If the **Restore the database to an alternate host** option is not displayed in the Restore Scope page, clear the browser cache.

6. On the **Pre Restore Options** page, select one of the following options:

- Select **Overwrite the database with same name during restore** to restore the database with the same name.
- Select **Retain SQL database replication settings** to restore the database and retain the existing replication settings.

7. On the **Post Restore Options** page, to specify the database state for restoring additional transactional logs, select one of the following options:
   - Select **Operational, but unavailable** if you are restoring all of the necessary backups now.

     This is the default behavior, which leaves the database ready for use by rolling back the uncommitted transactions. You cannot restore additional transaction logs until you create a backup.

   - Select **Non-operational, but available** to leave the database non-operational without rolling back the uncommitted transactions.

     Additional transaction logs can be restored. You cannot use the database until it is recovered.

   - Select **Read-only mode, and available** to leave the database in read-only mode.

     This option undoes uncommitted transactions, but saves the undone actions in a standby file so that recovery effects can be reverted.

     If the Undo directory option is enabled, more transaction logs are restored. If the restore operation for the transaction log is unsuccessful, the changes can be rolled back. The SQL Server documentation contains more information.

8. Review the details and click **Restore**.

Reference

AWS S3 archival storage classes and restore retrieval times

Cloud Backup supports two S3 archival storage classes and most regions.

Supported S3 archival storage classes for Cloud Backup

When backup files are initially created they're stored in S3 *Standard* storage. This tier is optimized for storing data that's infrequently accessed; but that also allows you to access it immediately. After 30 days the backups transition to the S3 *Standard-Infrequent Access* storage class to save on costs.

If your source clusters are running 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 (typically more than 30 days) for further cost optimization. Data in these tiers can't be accessed immediately when needed, and will require a higher retrieval cost, so you need to consider how often you may need to restore data from these archived backup files. See the section about restoring data from archival storage.

Note that when you configure Cloud Backup with this type of lifecycle rule, you must not configure any lifecycle rules when setting up the bucket in your AWS account.

Learn about S3 storage classes.

Restoring data from archival storage

While storing older backup files in archival storage is much less expensive than Standard or Standard-IA storage, accessing data from a backup file in archive storage for restore operations will take a longer amount of time and will cost more money.

How much does it cost to restore data from Amazon S3 Glacier and Amazon S3 Glacier Deep Archive?

There are 3 restore priorities you can choose when retrieving data from Amazon S3 Glacier, and 2 restore priorities when retrieving data from Amazon S3 Glacier Deep Archive. S3 Glacier Deep Archive costs less than S3 Glacier:

Archive Tier	Restore Priority & Cost		
	High	**Standard**	**Low**
S3 Glacier	Fastest retrieval, highest cost	Slower retrieval, lower cost	Slowest retrieval, lowest cost
S3 Glacier Deep Archive		Faster retrieval, higher cost	Slower retrieval, lowest cost

Each method has a different per-GB retrieval fee and per-request fee. For detailed S3 Glacier pricing by AWS Region, visit the Amazon S3 pricing page.

How long will it take to restore my objects archived in Amazon S3 Glacier?

There are 2 parts that make up the total restore time:

- **Retrieval time**: The time to retrieve the backup file from archive and place it in Standard storage. This is sometimes called the "rehydration" time. The retrieval time is different depending on the restore priority you choose.

Archive Tier	Restore Priority & Retrieval Time		
	High	**Standard**	**Low**
S3 Glacier	3-5 minutes	3-5 hours	5-12 hours
S3 Glacier Deep Archive		12 hours	48 hours

- **Restore time**: The time to restore the data from the backup file in Standard storage. This time is no different than the typical restore operation directly from Standard storage - when not using an archival tier.

For more information about Amazon S3 Glacier and S3 Glacier Deep Archive retrieval options, refer to the Amazon FAQ about these storage classes.

Azure archival tiers and restore retrieval times

Cloud Backup supports one Azure archival access tier and most regions.

Supported Azure Blob access tiers for Cloud Backup

When backup files are initially created they're stored in the *Cool* access tier. This tier is optimized for storing data that's infrequently accessed; but when needed, can be accessed immediately.

If your source clusters are running ONTAP 9.10.1 or greater, you can choose to tier backups from *Cool* to *Azure Archive* storage after a certain number of days (typically more than 30 days) for further cost optimization. Data in this tier can't be accessed immediately when needed, and will require a higher retrieval cost, so you need to consider how often you may need to restore data from these archived backup files. See the next section about restoring data from archival storage.

Note that when you configure Cloud Backup with this type of lifecycle rule, you must not configure any lifecycle rules when setting up the container in your Azure account.

Learn about Azure Blob access tiers.

Restoring data from archival storage

While storing older backup files in archival storage is much less expensive than Cool storage, accessing data from a backup file in Azure Archive for restore operations will take a longer amount of time and will cost more money.

How much does it cost to restore data from Azure Archive?

There are two restore priorities you can choose when retrieving data from Azure Archive:

- **High**: Fastest retrieval, higher cost
- **Standard**: Slower retrieval, lower cost

Each method has a different per-GB retrieval fee and per-request fee. For detailed Azure Archive pricing by Azure Region, visit the Azure pricing page.

How long will it take to restore my data archived in Azure Archive?

There are 2 parts that make up the restore time:

- **Retrieval time**: The time to retrieve the archived backup file from Azure Archive and place it in Cool storage. This is sometimes called the "rehydration" time. The retrieval time is different depending on the restore priority you choose:
  - **High**: < 1 hour
  - **Standard**: < 15 hours
- **Restore time**: The time to restore the data from the backup file in Cool storage. This time is no different than the typical restore operation directly from Cool storage - when not using an archival tier.

For more information about Azure Archive retrieval options, refer to this Azure FAQ.

Cross-account and cross-region configurations

These topics describe how to configure Cloud Backup for cross account configurations when using different cloud providers.

- Configure Cloud Backup for multi-account access in AWS
- Configure Cloud Backup for multi-account access in Azure

Configure backup for multi-account access in AWS

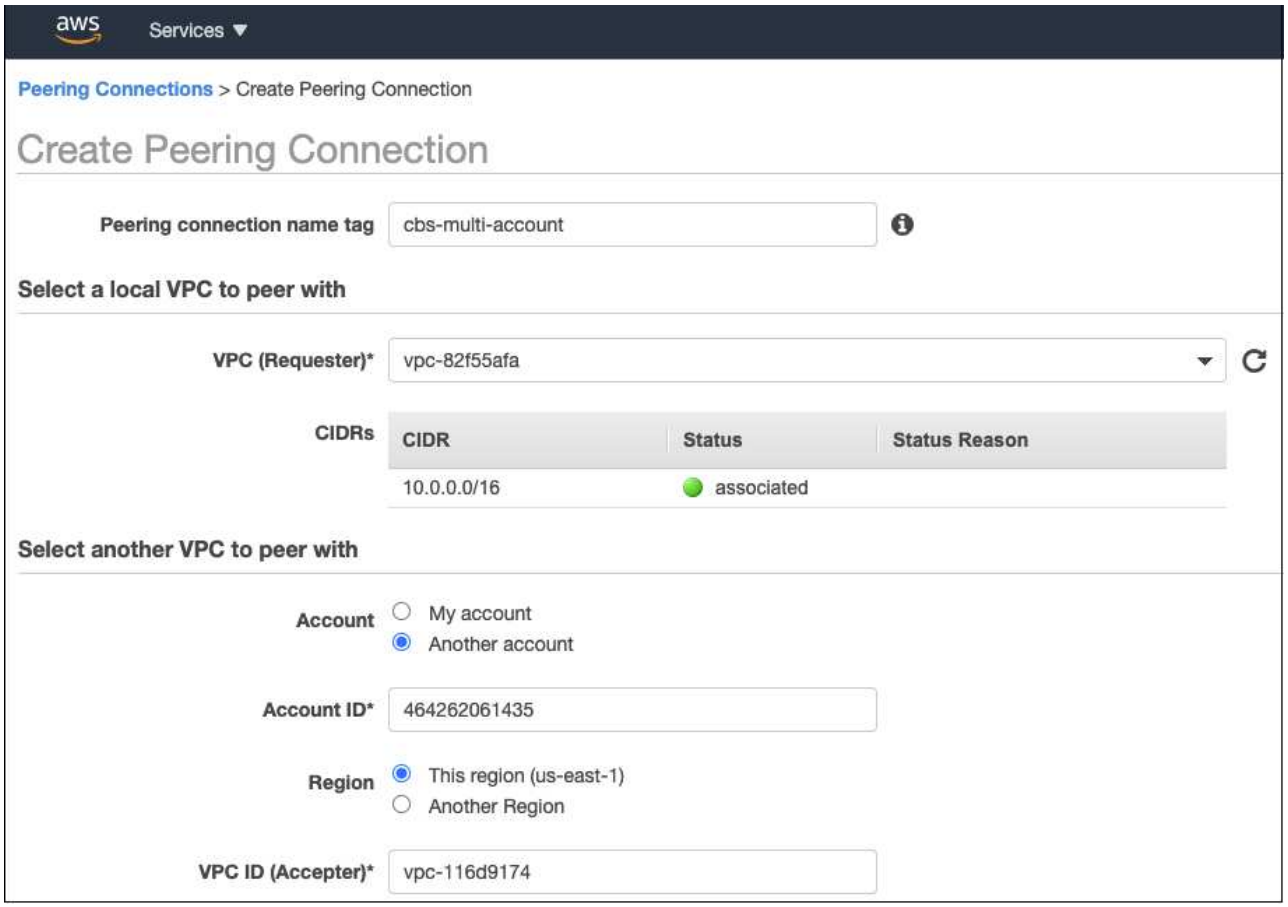
Cloud Backup enables you to create backup files in an AWS account that is different than where your source Cloud Volumes ONTAP volumes reside. And both of those accounts can be different than the account where the Cloud Manager Connector resides.

These steps are required only when you are backing up Cloud Volumes ONTAP data to Amazon S3.

Follow the steps below to set up your configuration in this manner.

Set up VPC peering between accounts

1. Log in to second account and Create Peering Connection:
   a. Select a local VPC: Select the VPC of the second account.
   b. Select another VPC: Enter the account ID of the first account.
   c. Select the Region where the Cloud Manager Connector is running. In this test setup both accounts are running in same region.
   d. VPC ID: Log into first account and enter the acceptor VPC ID. This is the VPC ID of the Cloud Manager Connector.



A Success dialog displays.

The status of the peering connection shows as Pending Acceptance.

2. Log into the first account and accept the peering request:

a. Click **Yes**.

The connection now shows as Active. We have also added a Name tag to identify the peering connection called `cbs-multi-account`.

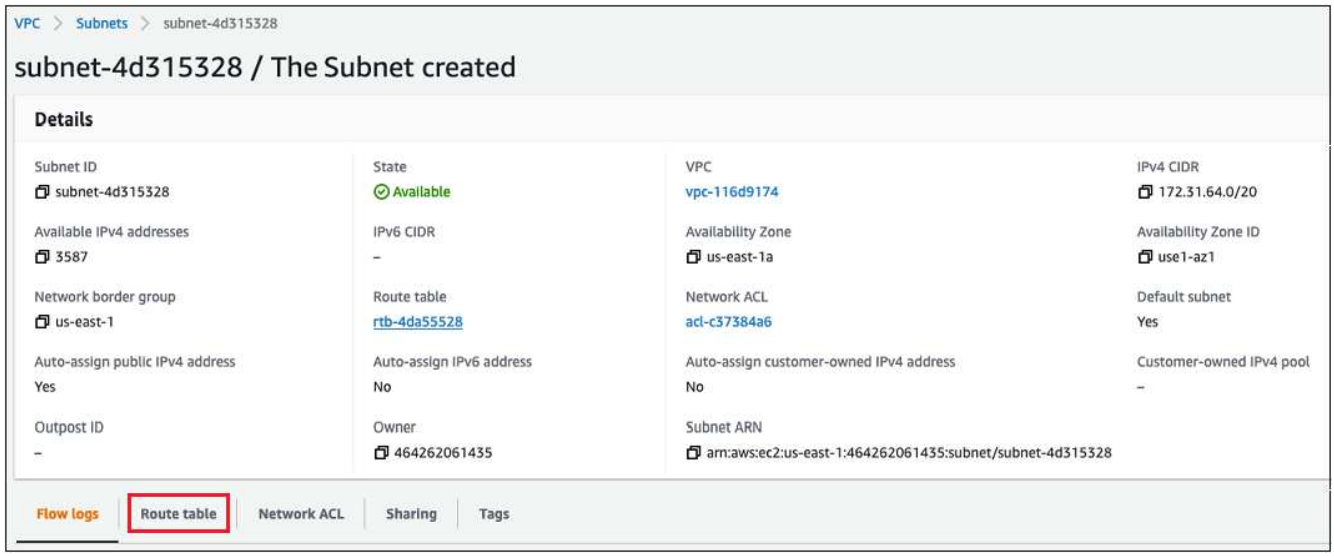
Name	Peering Connection	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs	Requester Owner	Accepter Owner
	pcx-004715531514cb0d8	Active	vpc-0647747d | M…	vpc-116d9174	10.2.0.0/24	172.31.0.0/16	464262061435	464262061435
estycvoconnect	pcx-0305041f9cc2dfbdb	Active	vpc-116d9174	vpc-445d4f21	172.31.0.0/16	10.129.0.0/20	464262061435	759995470648
cbs-multi-account	pcx-049758069d9b7c140	Active	vpc-82f55afa	vpc-116d9174	10.0.0.0/16	172.31.0.0/16	733004784675	464262061435
hill-vpc-peer-chen	pcx-0d0e5c7fc4360254d	Active	vpc-0d12df59528f…	vpc-824dc0e4 | nf…	10.0.0.0/24	10.20.30.0/24	464262061435	464262061435

b. Refresh the peering connection in the second account and notice that the status changes to Active.

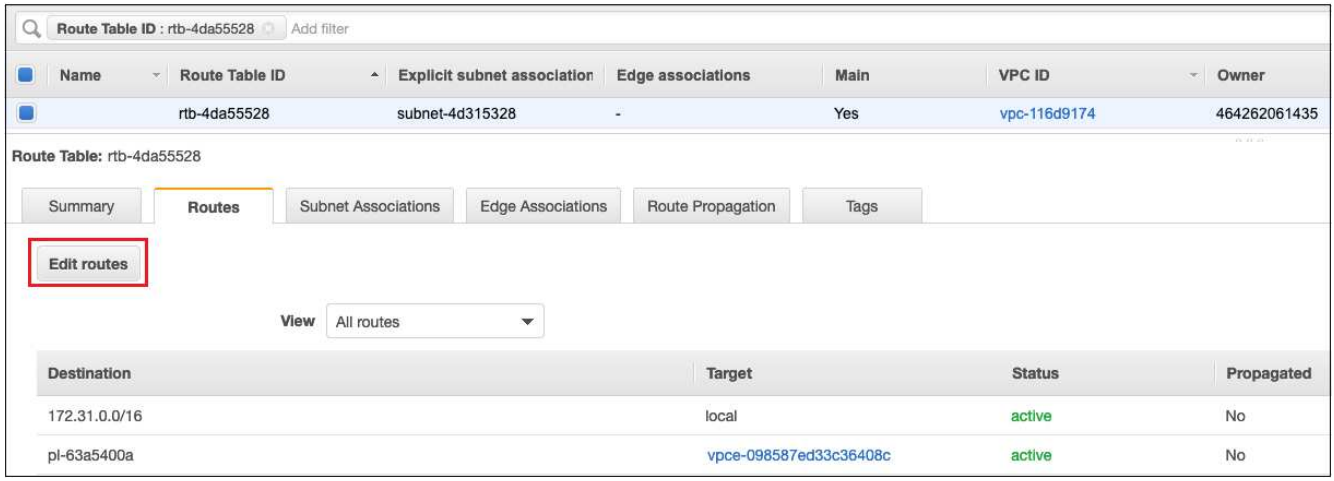
Name	Peering Connection	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs	Requester Owner	Accepter Owner
cbs-multi-account	pcx-049758069d9b7c140	Active	vpc-82f55afa | VP…	vpc-116d9174	10.0.0.0/16	172.31.0.0/16	733004784675	464262061435
New_Peering	pcx-6d55ca04	Active	vpc-b16c90d4 | V…	vpc-fc2aa39a | De…	172.31.0.0/16	192.168.0.0/16	733004784675	733004784675

Add a route to the route tables in both accounts

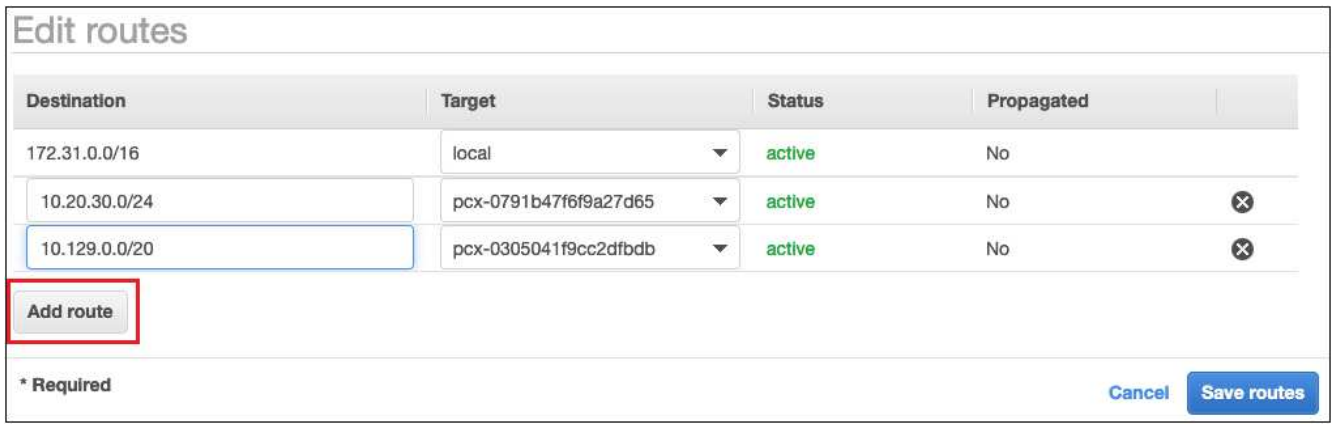
1. Go to VPC > Subnet > Route table.



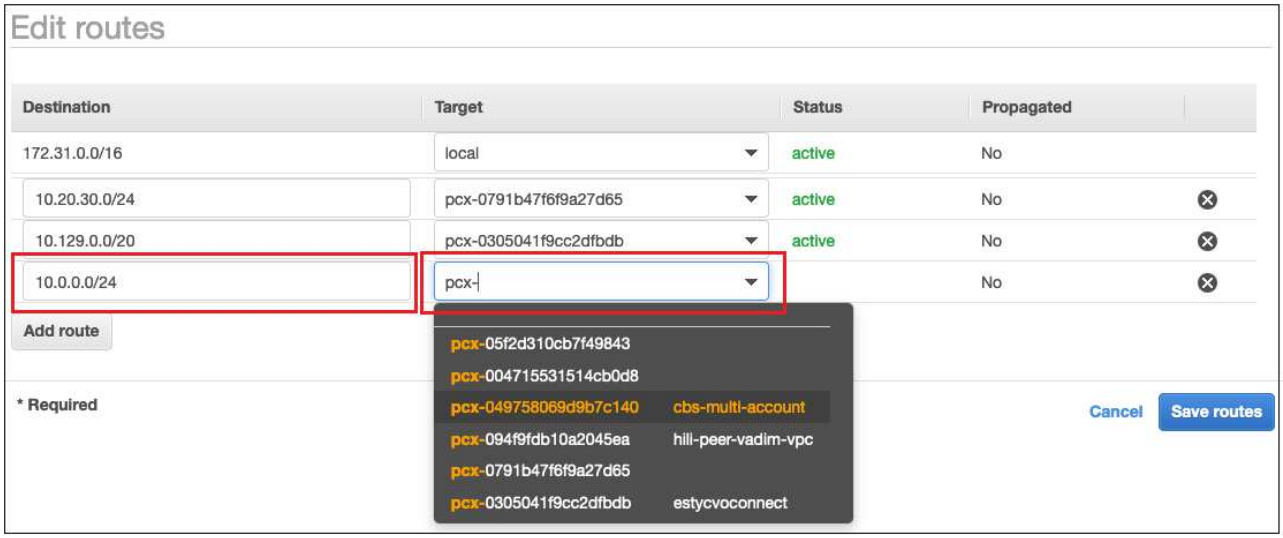
2. Click on the Routes tab.



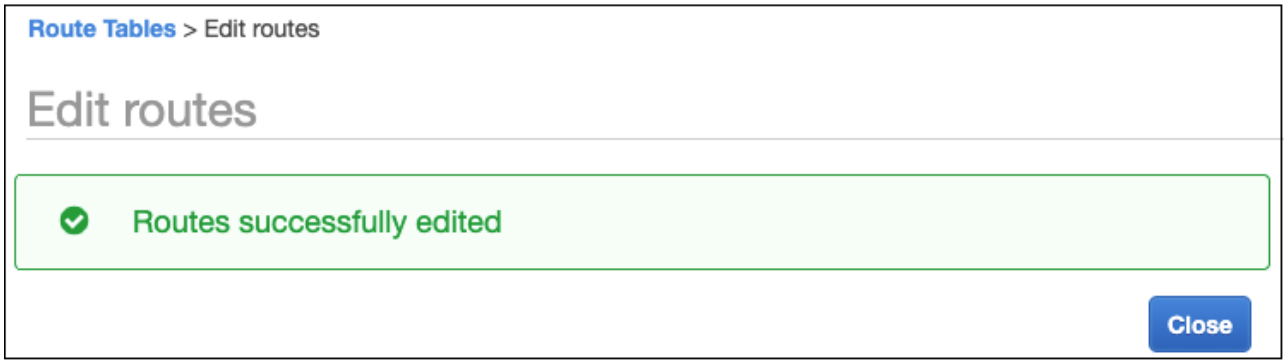
3. Click **Edit routes**.



4. Click **Add route**, and from the Target drop-down list select **Peering Connection**, and then select the peering connection that you created.
   a. In the Destination, enter the other account's subnet CIDR.

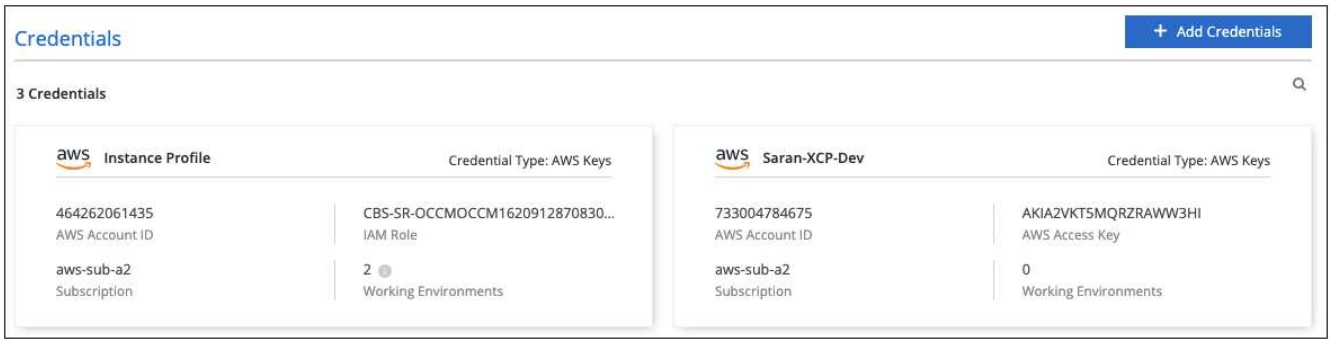


b. Click **Save routes** and a Success dialog displays.

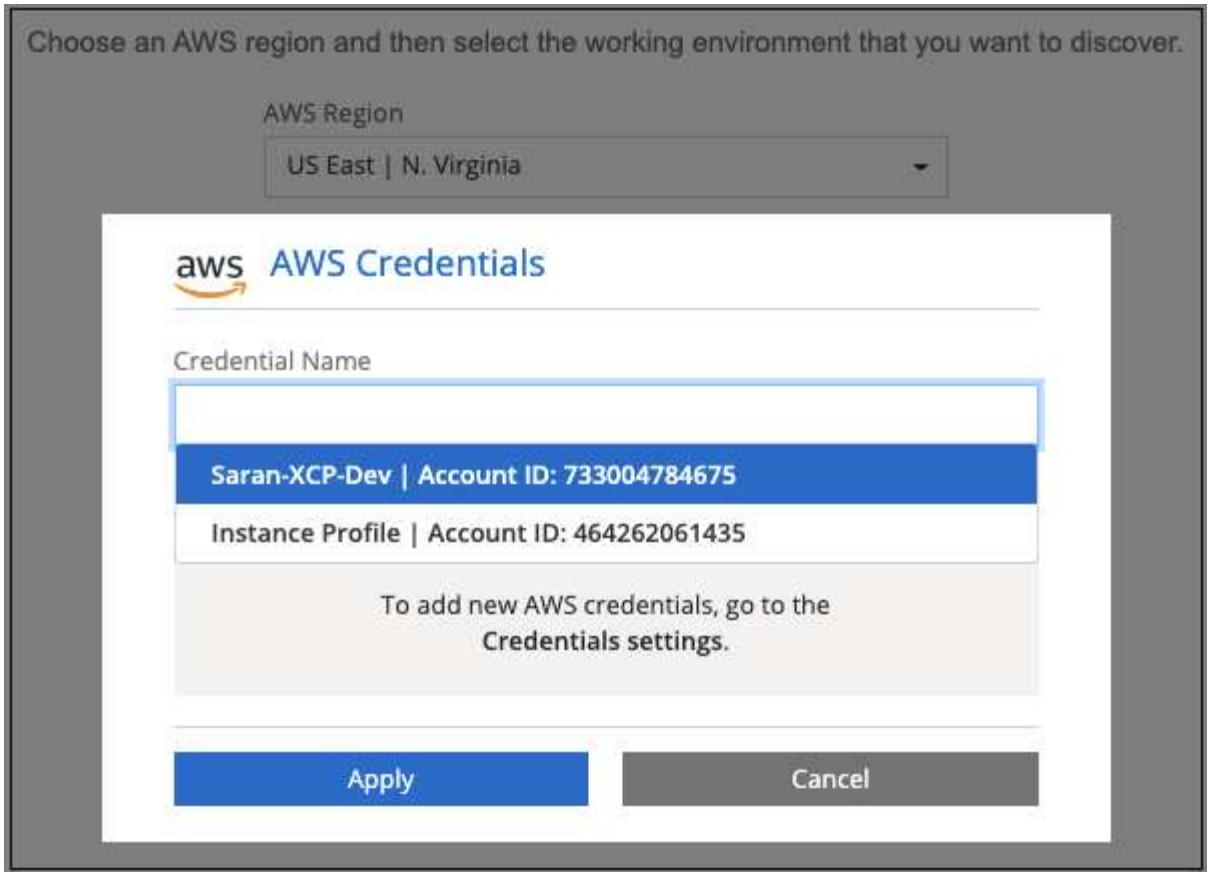


Add the second AWS account credentials in Cloud Manager

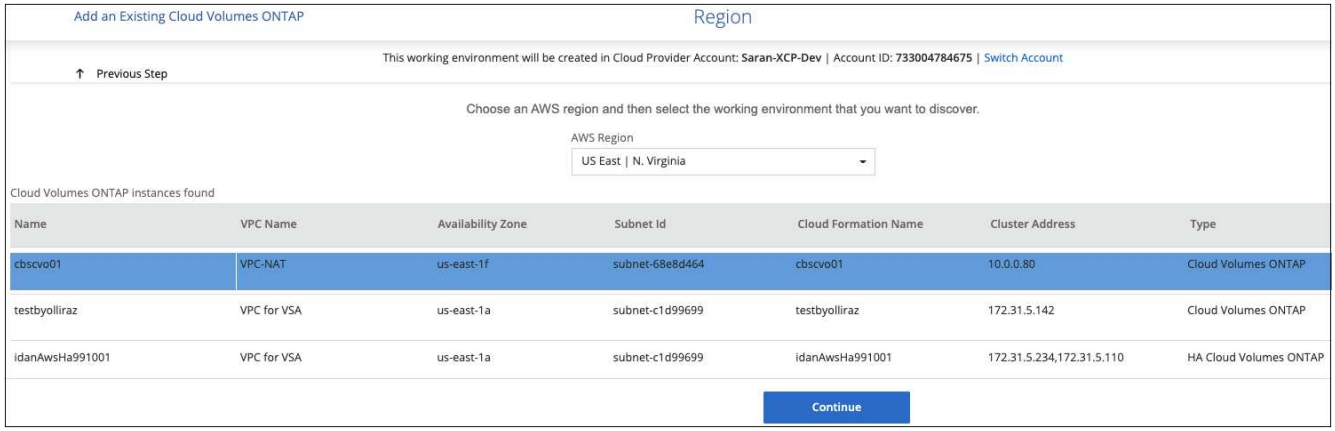
1. Add the second AWS account, for example, *Saran-XCP-Dev*.



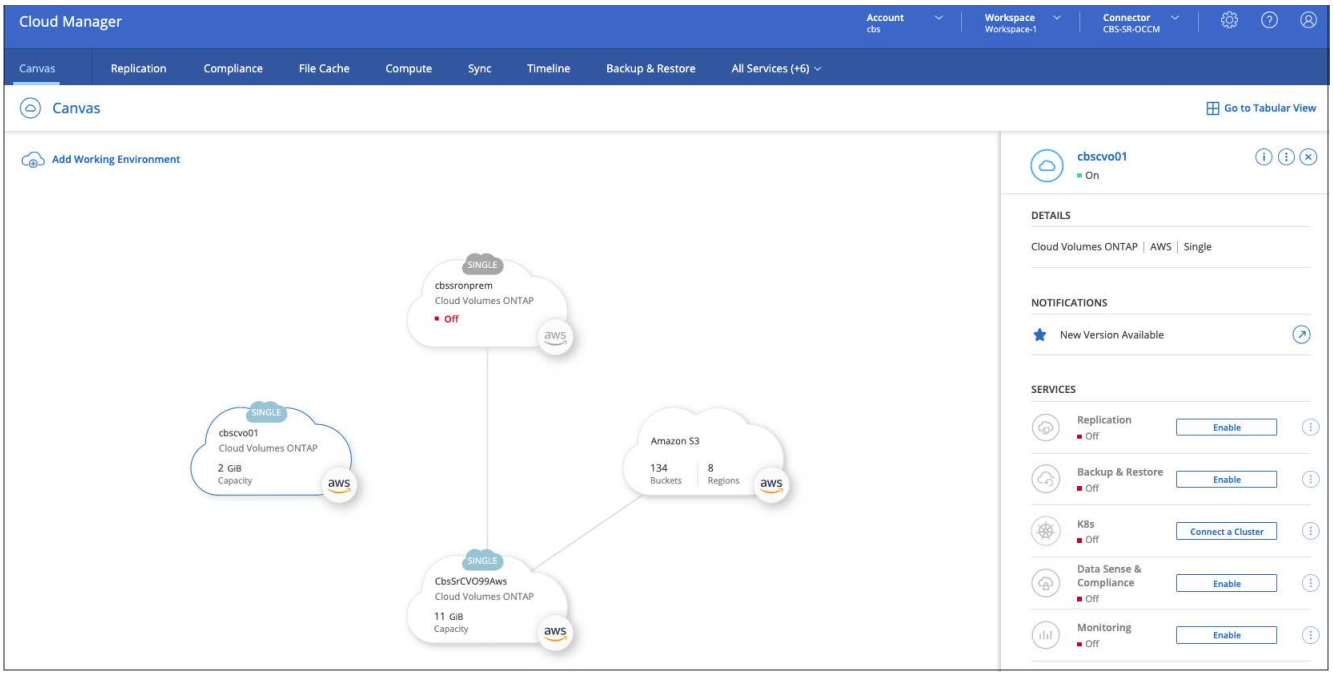
2. In the Discover Cloud Volumes ONTAP page, select the newly added credentials.



3. Select the Cloud Volumes ONTAP system you want to discover from second account. You can also deploy a new Cloud Volumes ONTAP system in the second account.

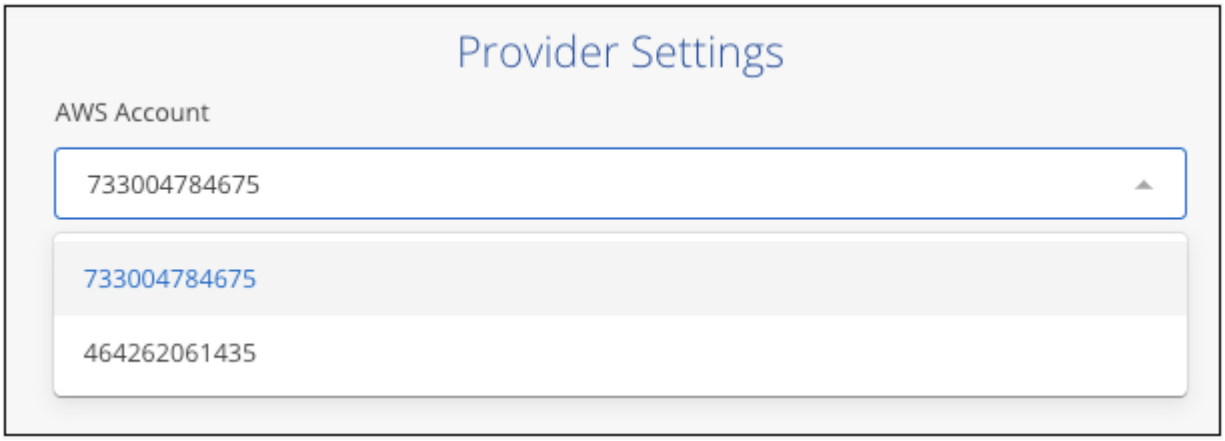


The Cloud Volumes ONTAP system from the second account is now added to Cloud Manager which is running in a different account.



Enable backup in the other AWS account

1. In Cloud Manager, enable backup for the Cloud Volumes ONTAP system running in the first account, but select the second account as the location for creating the backup files.



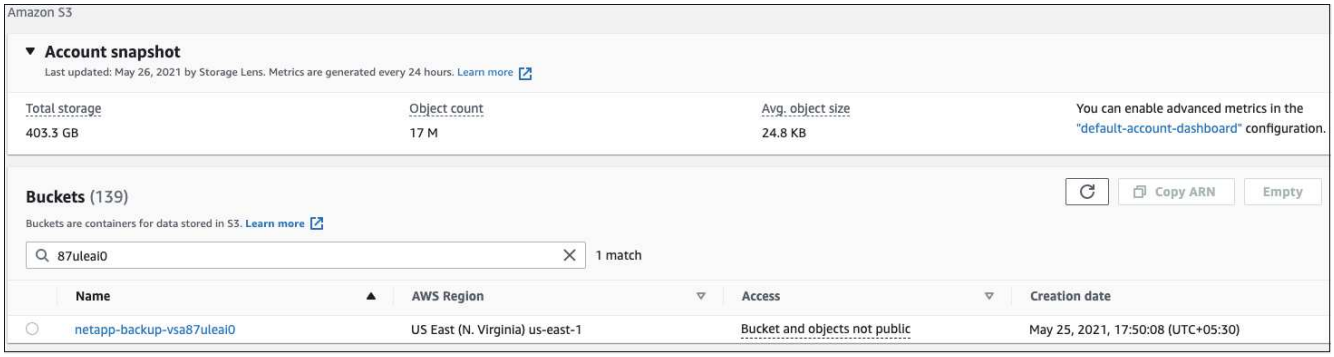
2. Then select a backup policy and the volumes you want to back up, and Cloud Backup attempts to create a new bucket in the selected account.

   However, adding the bucket to the Cloud Volumes ONTAP system will fail because Cloud Backup uses the instance profile to add the bucket and the Cloud Manager instance profile doesn't have access to the resources in the second account.

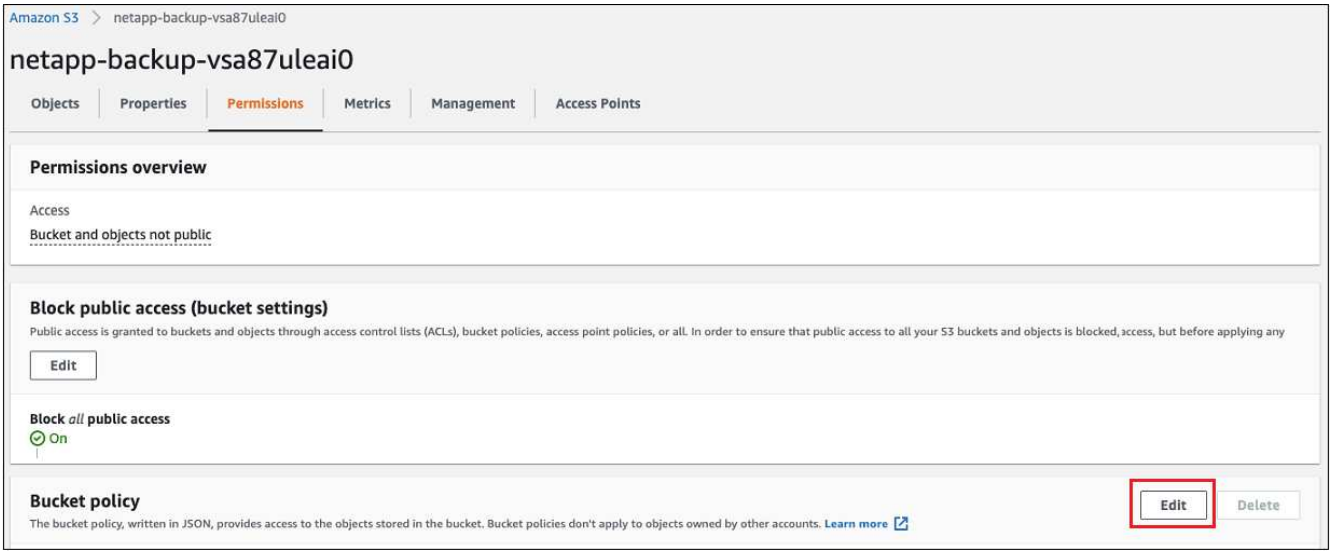
3. Get the working environment ID for the Cloud Volumes ONTAP system.

Cloud Backup creates every bucket with the prefix `Netapp-backup-` and will include the working environment ID; for example: `87ULeA10`

4. In the EC2 portal, go to S3 and search for the bucket with name ending with `87uLeA10` and you'll see the bucket name displayed as `Netapp-backup-vsa87uLeA10`.



5. Click on the bucket, then click the Permissions tab, and then click **Edit** in the Bucket policy section.



6. Add a bucket policy for the newly created bucket to provide access to the Cloud Manager's AWS account, and then Save the changes.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicRead",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::464262061435:root"
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::netapp-backup-vsa87uleai0",
        "arn:aws:s3:::netapp-backup-vsa87uleai0/*"
      ]
    }
  ]
}
```

Note that "AWS": "arn:aws:iam::464262061435:root" gives complete access this bucket for all resources in account 464262061435. If you want to reduce it to specific role, level, you can update the policy with specific role(s). If you are adding individual roles, ensure that occm role also added, otherwise backups will not get updated in the Cloud Backup UI.

For example: "AWS": "arn:aws:iam::464262061435:role/cvo-instance-profile-version10-d8e-IamInstanceRole-IKJPJ1HC2E7R"

7. Retry enabling Cloud Backup on the Cloud Volumes ONTAP system and this time it should be successful.

Configure backup for multi-account access in Azure

Cloud Backup enables you to create backup files in an Azure account that is different than where your source Cloud Volumes ONTAP volumes reside. And both of those accounts can be different than the account where the Cloud Manager Connector resides.

These steps are required only when you are backing up Cloud Volumes ONTAP data to Azure Blob storage.

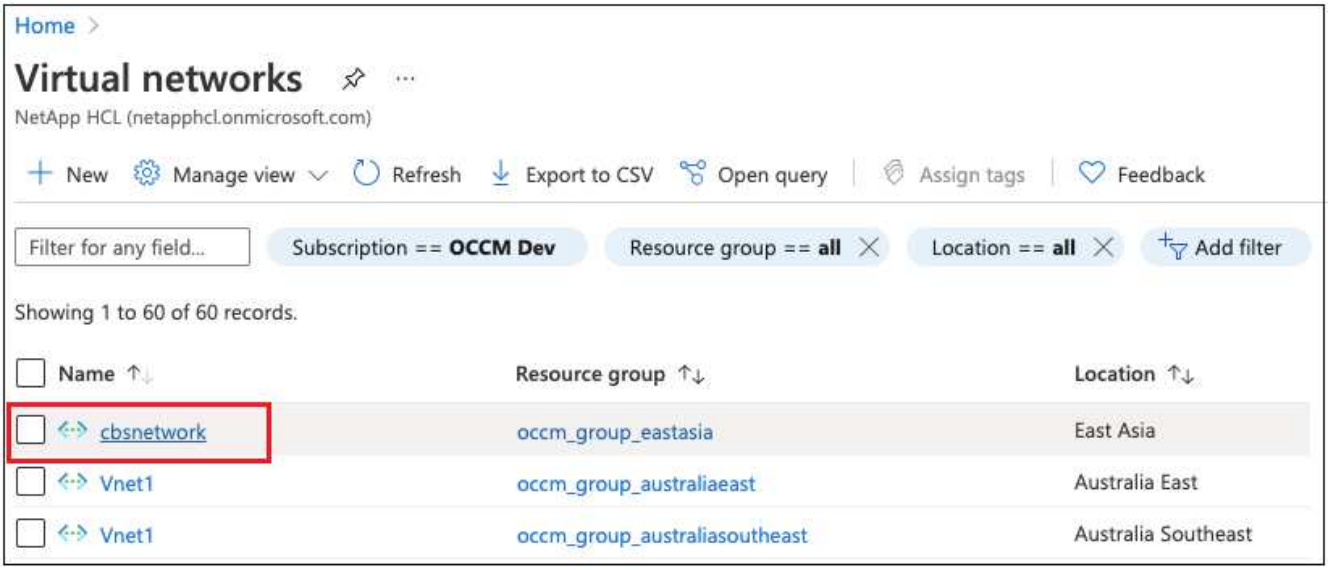
Just follow the steps below to set up your configuration in this manner.

Set up VNet peering between accounts

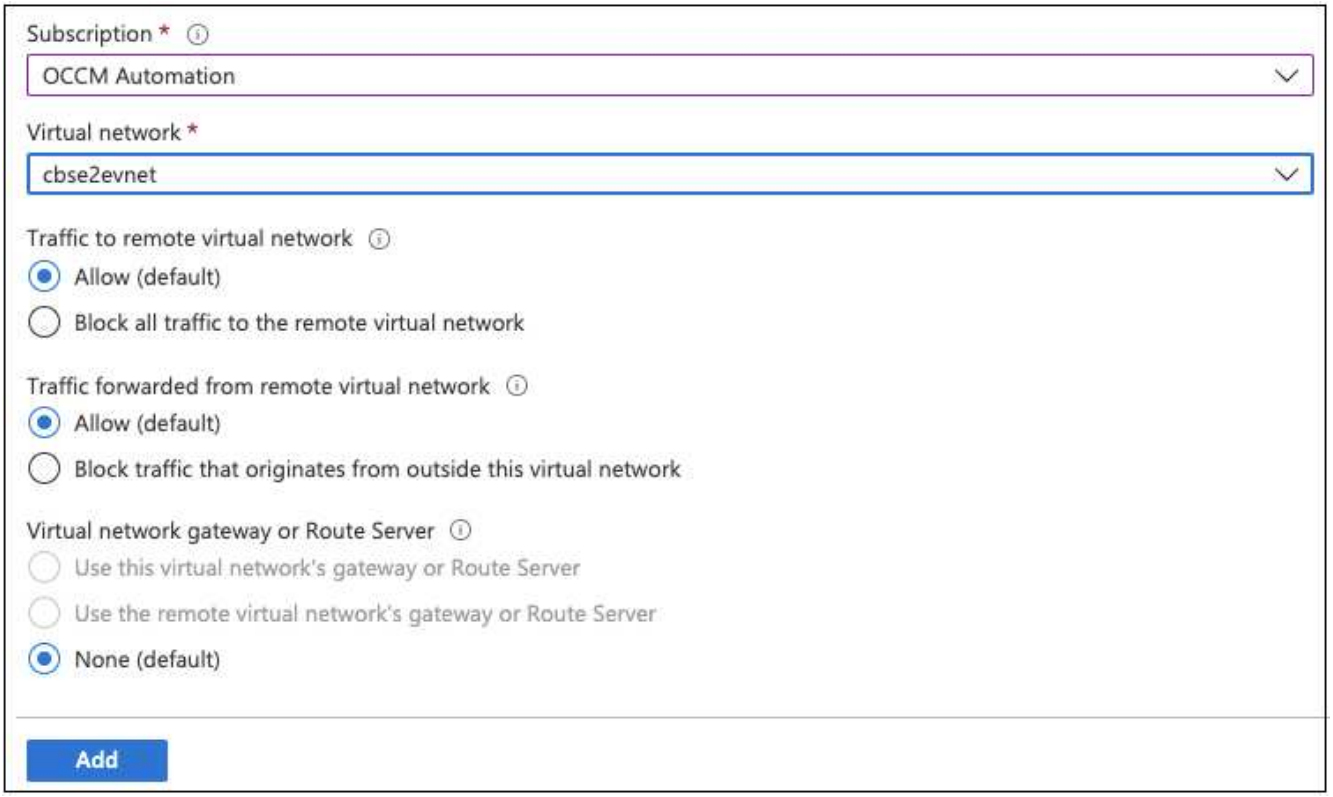
Note that if you want Cloud Manager to manage your Cloud Volumes ONTAP system in a different account/region, then you need to setup VNet peering. VNet peering is not required for storage account

connectivity.

1. Log in to the Azure portal and from home, select Virtual Networks.
2. Select the subscription you are using as subscription 1 and click on the VNet where you want to set up peering.

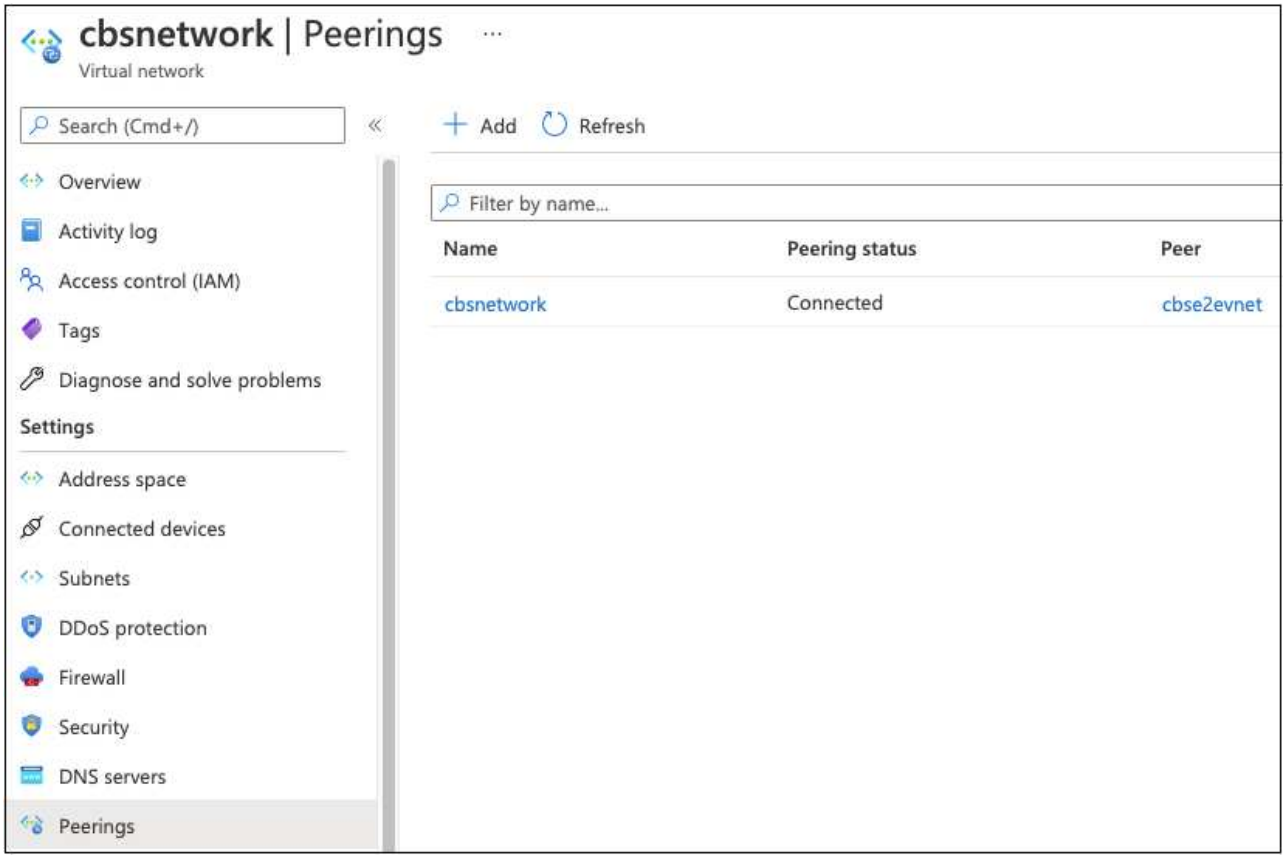


3. Select **cbsnetwork** and from the left panel, click on **Peerings**, and then click **Add**.

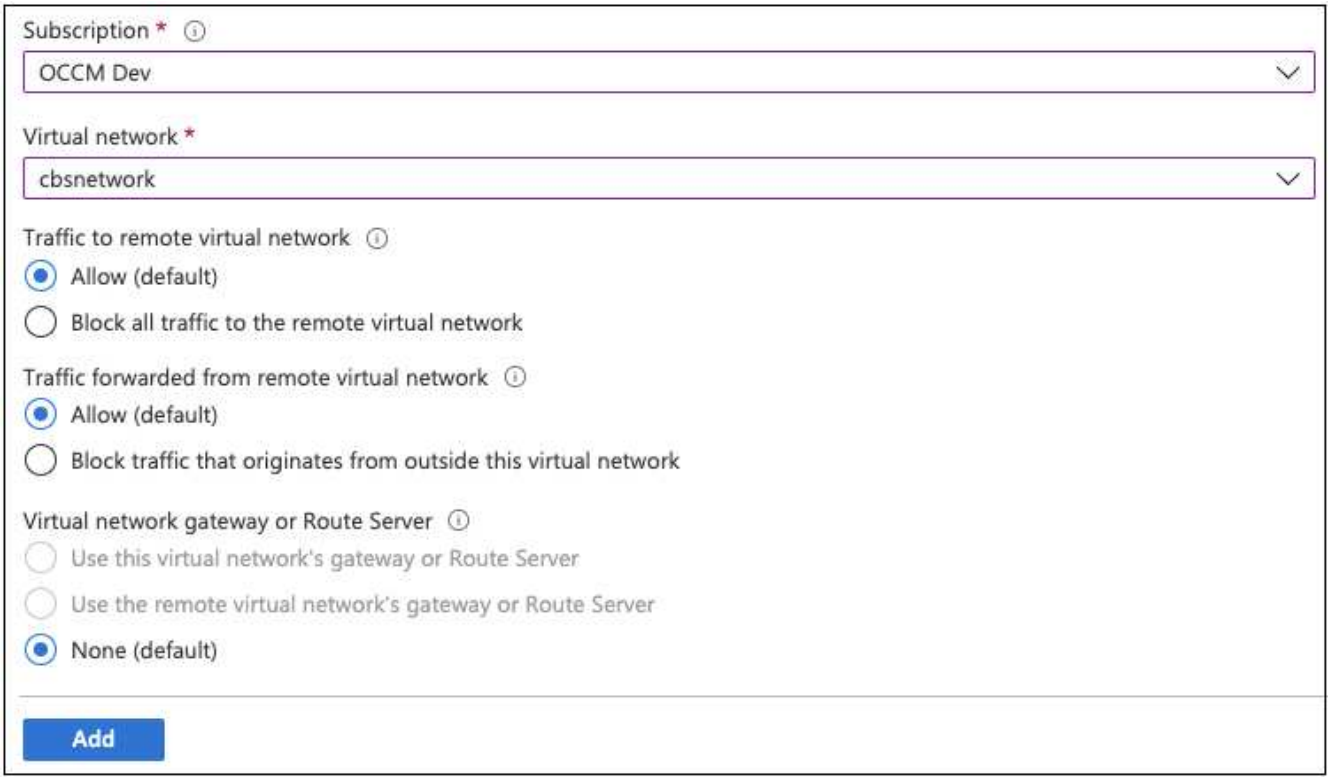


4. Enter the following information on the Peering page and then click **Add**.
   - Peering link name for this network: you can give any name to identify the peering connection.
   - Remote virtual network peering link name: enter a name to identify the remote VNet.

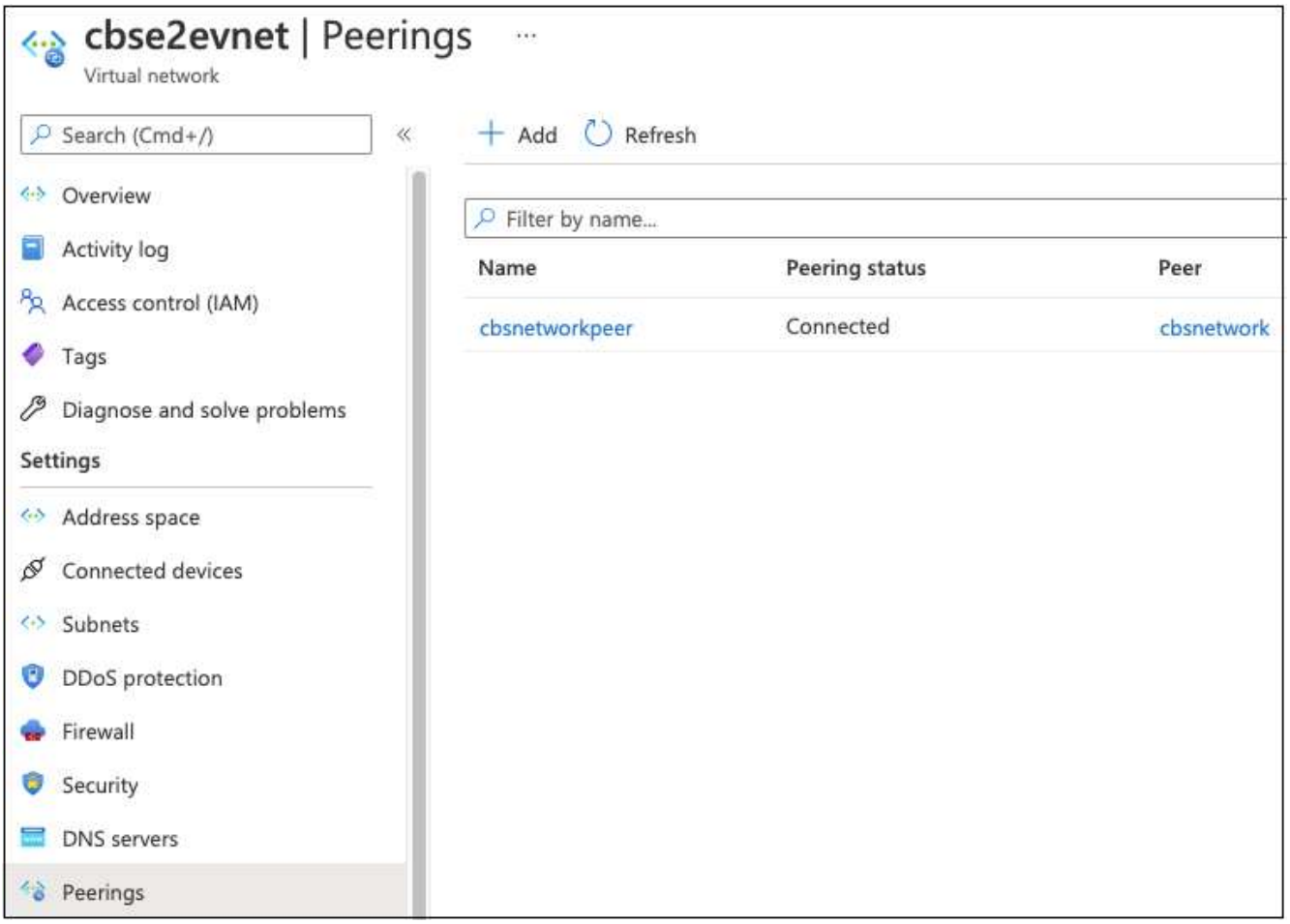
- Keep all the selections as default values.
- Under subscription, select the subscription 2.
- Virtual network, select the virtual network in subscription 2 to which you want to set up the peering.



5. Perform the same steps in subscription 2 VNet and specify the subscription and remote VNet details of subscription 1.



The peering settings are added.



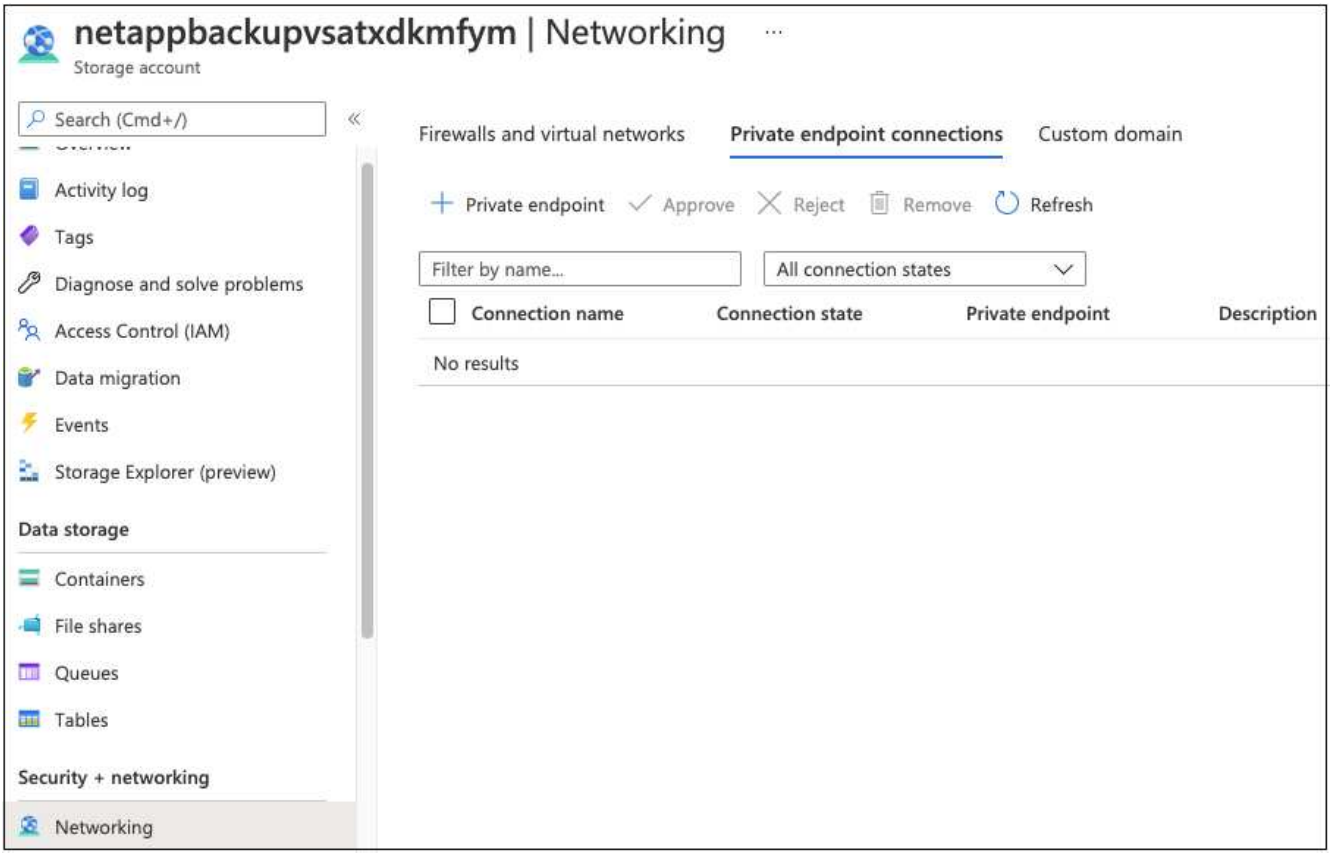
Create a private endpoint for the storage account

Now you need to create a private endpoint for the storage account. In this example, the storage account is created in subscription 1 and the Cloud Volumes ONTAP system is running in subscription 2.

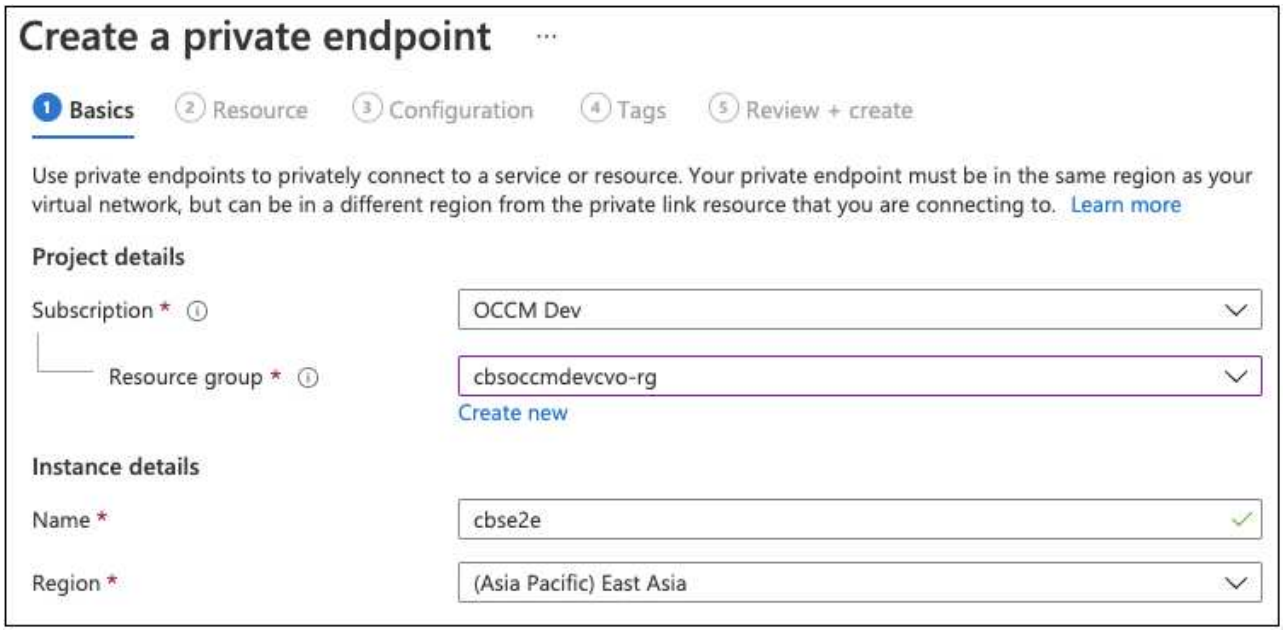
You need network contributor permission to perform the following action.


```
{
  "id": "/subscriptions/d333af45-0d07-4154-
943dc25fbbce1b18/providers/Microsoft.Authorization/roleDefinitions/4d97b98
b-1d4f-4787-a291-c67834d212e7",
  "properties": {
    "roleName": "Network Contributor",
    "description": "Lets you manage networks, but not access to them.",
    "assignableScopes": [
      "/"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Authorization/*/read",
          "Microsoft.Insights/alertRules/*",
          "Microsoft.Network/*",
          "Microsoft.ResourceHealth/availabilityStatuses/read",
          "Microsoft.Resources/deployments/*",
          "Microsoft.Resources/subscriptions/resourceGroups/read",
          "Microsoft.Support/*"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

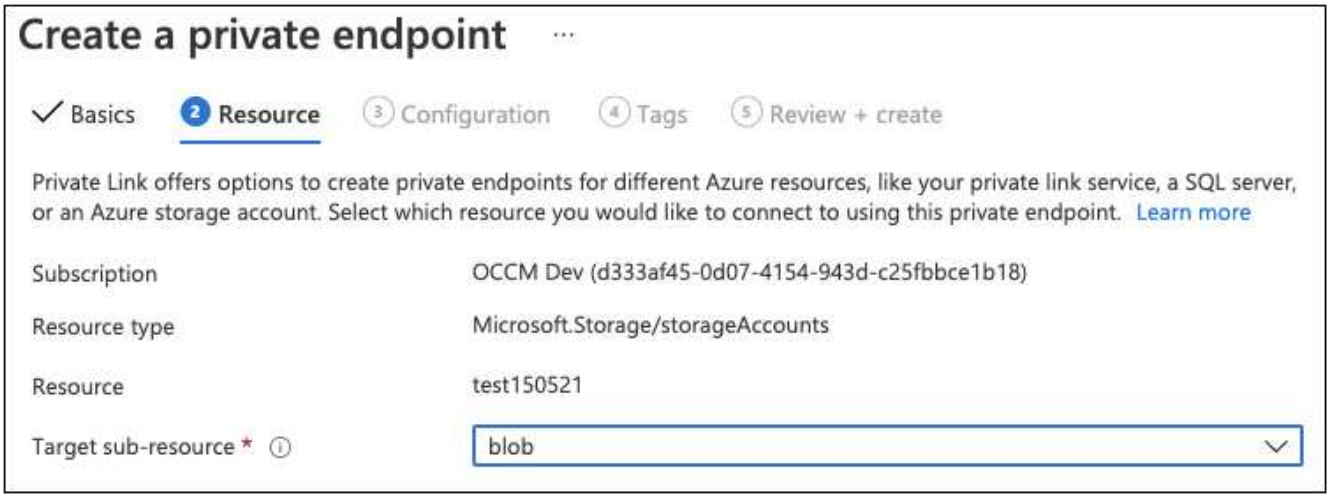

1. Go to the storage account > Networking > Private endpoint connections and click **+ Private endpoint**.



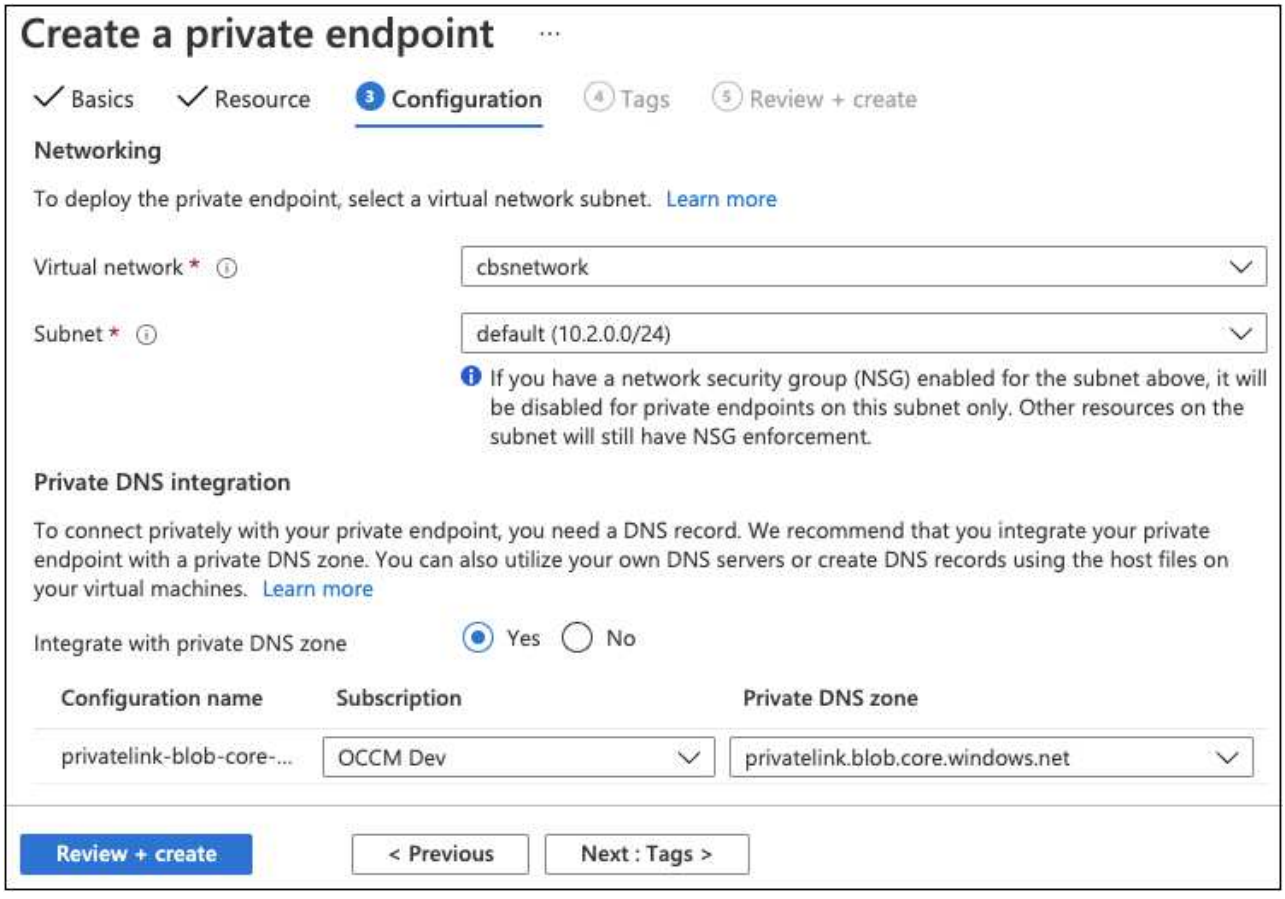
2. In the Private Endpoint *Basics* page:
   - Select subscription 2 (where the Cloud Manager Connector and Cloud Volumes ONTAP system are deployed) and the resource group.
   - Enter an endpoint name.
   - Select the region.



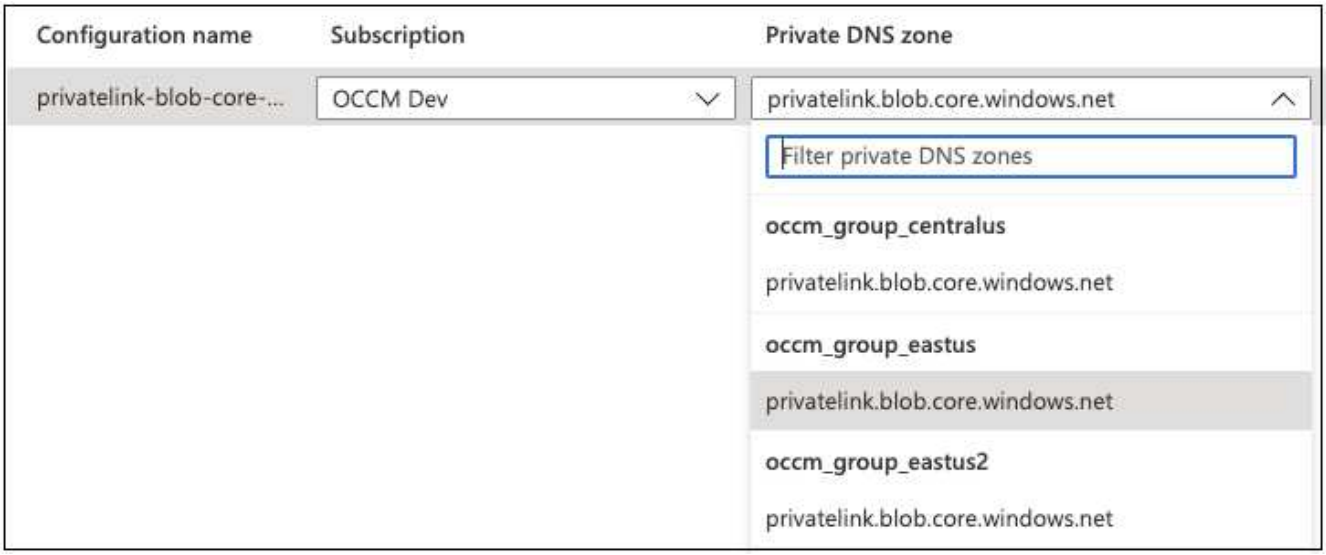
3. In the *Resource* page, select Target sub-resource as **blob**.



4. In the Configuration page:
   - Select the virtual network and subnet.
   - Click the **Yes** radio button to "Integrate with private DNS zone".



5. In the Private DNS zone list, ensure that the Private Zone is selected from the correct Region, and click **Review + Create**.



Now the storage account (in subscription 1) has access to the Cloud Volumes ONTAP system which is running in subscription 2.

6. Retry enabling Cloud Backup on the Cloud Volumes ONTAP system and this time it should be successful.

Knowledge and support

Register for support

Unresolved directive in task-support-registration.adoc - include::https://raw.githubusercontent.com/NetAppDocs/cloud-manager-family/main/_include/support-registration.adoc[]

Get help

Unresolved directive in task-get-help.adoc - include::https://raw.githubusercontent.com/NetAppDocs/cloud-manager-family/main/_include/get-help.adoc[]

Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

http://www.netapp.com/us/legal/copyright.aspx

Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

http://www.netapp.com/us/legal/netapptmlist.aspx

Patents

A current list of NetApp owned patents can be found at:

https://www.netapp.com/us/media/patents-page.pdf

Privacy policy

https://www.netapp.com/us/legal/privacypolicy/index.aspx

Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

- Notice for Cloud Manager 3.9
- Notice for the Cloud Backup
- Notice for Single File Restore