



# **Back up and restore ONTAP data**

## **Cloud Backup**

NetApp  
June 20, 2022

This PDF was generated from <https://docs.netapp.com/us-en/cloud-manager-backup-restore/gcp/concept-ontap-backup-to-cloud.html> on June 20, 2022. Always check docs.netapp.com for the latest.

# Table of Contents

- Back up and restore ONTAP data ..... 1
  - Protect your ONTAP cluster data using Cloud Backup ..... 1
  - Backing up Cloud Volumes ONTAP data to Google Cloud Storage ..... 7
  - Backing up on-premises ONTAP data to Google Cloud Storage..... 13
  - Backing up on-premises ONTAP data to StorageGRID..... 21
  - Managing backups for your ONTAP systems..... 27
  - Restoring ONTAP data from backup files..... 43

# 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 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 and searchable file catalogs 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 Google	Google Cloud Storage

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

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

### Support for sites with no internet connectivity

Cloud Backup can be used in a site with no internet connectivity (also known as an "offline" or "dark" site) to back up volume data from local on-premises ONTAP systems to local NetApp StorageGRID systems. In this case, you'll need to deploy the Cloud Manager Connector (minimum version 3.9.19) in the dark site. See [Backing up on-premises ONTAP data to StorageGRID](#) for details.

## 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 Volume or File Restore using Search & Restore, certain resources are provisioned by your cloud provider and there is per-TiB cost associated with the amount of data that is scanned by your search requests.
  - In Google, a new bucket is deployed, and the [Google Cloud BigQuery services](#) are provisioned on an account/project level.
- If you need to restore volume data from a backup file that has been moved to archival storage, then there's 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. The third option is to purchase licenses directly from NetApp. Read the [Licensing](#) section for details.

## Licensing

Cloud Backup is available in a few licensing options:

- Pay As You Go (PAYGO) subscription
- Bring Your Own License (BYOL)

A 30-day free trial is available when you initially sign up with a PAYGO subscription.

### 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.

[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 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 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 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. 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

These limitations apply to both the Search & Restore and the Browse & Restore methods of restoring files; unless called out specifically.

- Browse & Restore can restore up to 100 individual files at a time.
- Search & Restore can restore 1 file 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.
- You can't restore individual files if the backup file resides in archival storage.
- File level restore using Search & Restore is not supported when the Connector is installed on a site without internet access (dark site).



# 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.

A screenshot of a 'Provider Settings' form. It has two dropdown menus. The first is labeled 'Google Cloud Project' and has 'Default Project' selected. The second is labeled 'Region' and has 'us-east-2' selected. The form has a light gray background and a white border.

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.

### Define Policy

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

**Policy - Retention & Schedule**

☒ Create a New Policy ☐ Select an Existing Policy

☐ Hourly

Number of backups to retain

24

☒ Daily

Number of backups to retain

30

☐ Weekly

Number of backups to retain

52

☐ Monthly

Number of backups to retain

12

**DP Volumes**

Data protection volume backups use the same retention period as defined in the source SnapMirror relationship by default. Use the API if you want to change this value

**Google Cloud Storage Bucket**

Cloud Manager will create the Google Cloud Storage Bucket after you complete the wizard

5

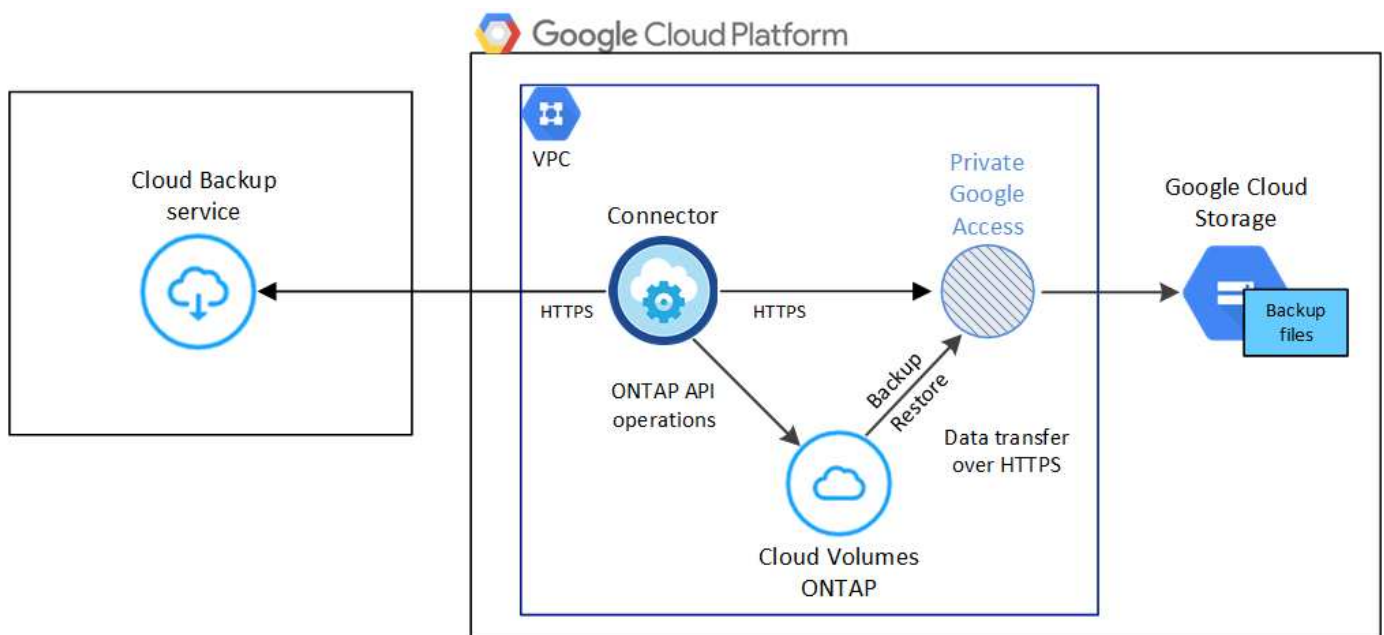
### Select the volumes that you want to back up

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

Minimum of ONTAP 9.7P5; ONTAP 9.8P11 and later is recommended.

## 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](#).

## Verify or add permissions to the Connector

To use the Cloud Backup Search & Restore functionality, you need to have specific permissions in the role for the Connector so that it can access the Google Cloud BigQuery service. See the permissions below, and follow the steps if you need to modify the policy.

1. In [Cloud Console](#), go to the **Roles** page.
2. Using the drop-down list at the top of the page, select the project or organization that contains the role that you want to edit.
3. Click a custom role.
4. Click **Edit Role** to update the role's permissions.
5. Click **Add Permissions** to add the following new permissions to the role.

```
bigquery.jobs.get  
bigquery.jobs.list  
bigquery.jobs.listAll  
bigquery.datasets.create  
bigquery.datasets.get  
bigquery.jobs.create  
bigquery.tables.get  
bigquery.tables.getData  
bigquery.tables.list  
bigquery.tables.create
```

6. Click **Update** to save the edited role.

## 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.

The screenshot shows the 'Details & Credentials' configuration page. At the top, there's a header 'Details & Credentials'. Below it, a section for 'Project' shows 'Project1' (Google Cloud Project) and 'MPAWSSubscription1222' (Marketplace Subscription), with an 'Edit Project' button. The main area is split into two columns: 'Details' and 'Credentials'. In the 'Details' column, there's a 'Working Environment Name (Cluster Name)' field with 'TamiVSA', a 'Service Account' toggle switch that is turned on, a 'Service Account Name' dropdown menu showing 'ServiceAccount1', and an 'Add Labels' button with the text 'Optional Field | Up to four labels'. In the 'Credentials' column, there's a 'User Name' field with 'admin', a 'Password' field with masked characters, and a 'Confirm Password' field with masked characters.

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**.

 A screenshot of a 'Provider Settings' form. It has two sections. The first section is labeled 'Google Cloud Project' and contains a dropdown menu with 'Default Project' selected. The second section is labeled 'Region' and contains a dropdown menu with 'us-east-2' selected.

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**.

### Define Policy

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

**Policy - Retention & Schedule**    ☒ Create a New Policy    ☐ Select an Existing Policy

☐ Hourly

Number of backups to retain

24

↑ ↓

☒ Daily

Number of backups to retain

30

↑ ↓

☐ Weekly

Number of backups to retain

52

↑ ↓

☐ Monthly

Number of backups to retain

12

↑ ↓

---

**DP Volumes**    Data protection volume backups use the same retention period as defined in the source SnapMirror relationship by default. Use the API if you want to change this value

---

**Google Cloud Storage Bucket**    Cloud Manager will create the Google Cloud Storage Bucket after you complete the wizard

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.

57 Volumes						
<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Volume_Name_1 <small>On</small>	RW	SVM_Name_1	0.25 TB	10 TB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume_Name_2 <small>On</small>	RW	SVM_Name_1	0.25 TB	10 TB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume_Name_3 <small>On</small>	RW	SVM_Name_1	0.25 TB	10 TB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume_Name_4 <small>On</small>	DP	SVM_Name_2	0.25 TB	10 TB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume_Name_5 <small>On</small>	RW	SVM_Name_1	0.25 TB	10 TB	⊖ Not Active

☒ Automatically back up future volumes on all storage VMs with the selected backup policy ⓘ

◦ 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 volumes or files 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 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.

## 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 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.

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 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.

**Define Policy**

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

**Policy - Retention & Schedule**

☒ Create a New Policy ☐ Select an Existing Policy

☐ Hourly Number of backups to retain 24

☒ Daily Number of backups to retain 30

☐ Weekly Number of backups to retain 52

☐ Monthly Number of backups to retain 12

**DP Volumes** Data protection volume backups use the same retention period as defined in the source SnapMirror relationship by default. Use the API if you want to change this value

**Google Cloud Storage Bucket** Cloud Manager will create the Google Cloud Storage Bucket after you complete the wizard

## 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

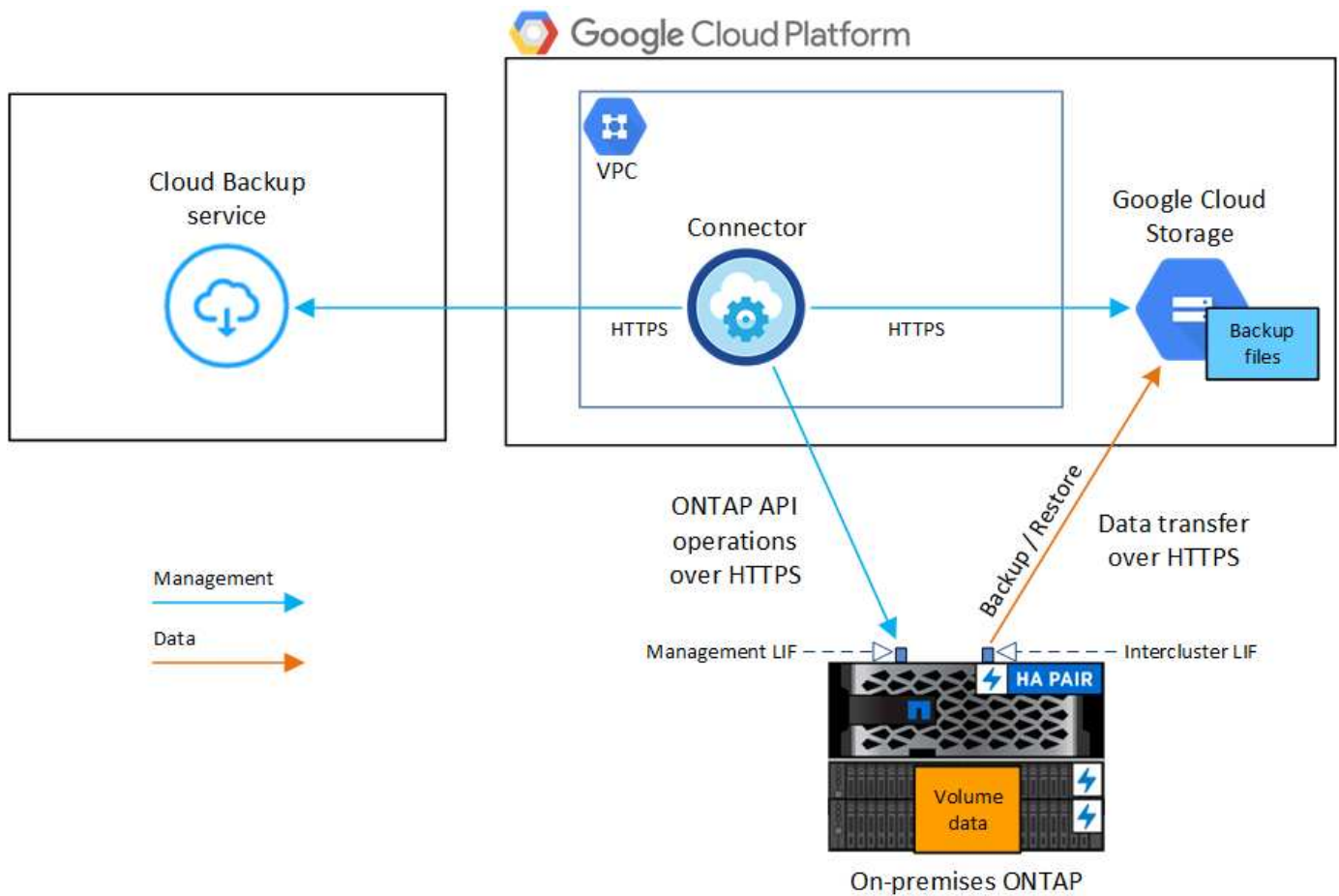
Read the following requirements to make sure you have a supported configuration before you start backing up on-premises volumes to Google Cloud storage.

There are two connection methods you can use when configuring backups from on-premises ONTAP systems to Google Cloud Storage.

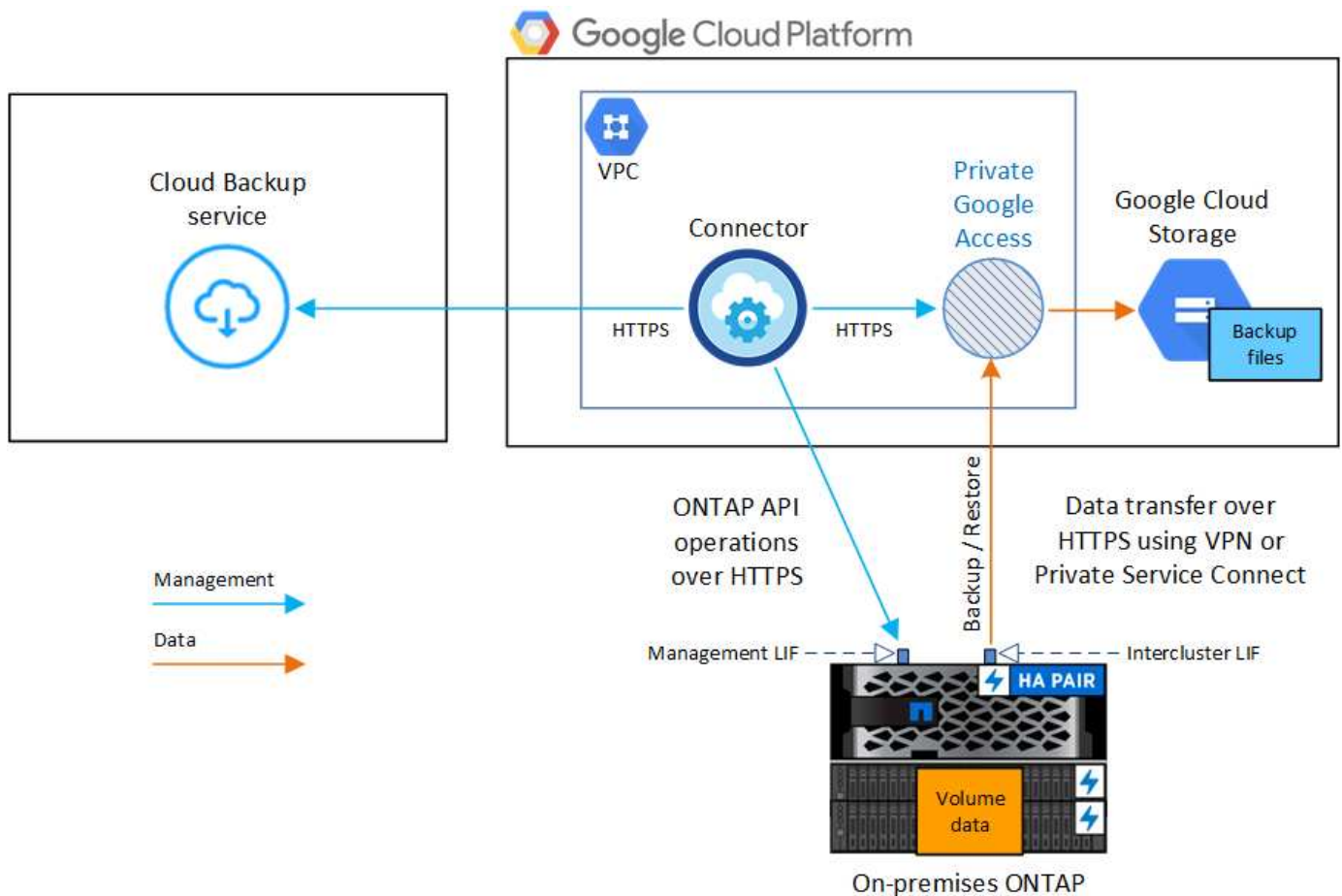
- Public connection - Directly connect the ONTAP system to Google Cloud Storage using a public Google endpoint.
- Private connection - Use a VPN or Private Service Connect and route traffic through a Private Google Access interface that uses a private IP address.

The following image shows the **public connection** method and the connections that you need to prepare between the components:





The following image shows the **private connection** method and the connections that you need to prepare between the components:



## 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

- Minimum of ONTAP 9.7P5; ONTAP 9.8P11 and later is recommended.
- 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).

## Verify or add permissions to the Connector

To use the Cloud Backup Search & Restore functionality, you need to have specific permissions in the role for

the Connector so that it can access the Google Cloud BigQuery service. See the permissions below, and follow the steps if you need to modify the policy.

### Steps

1. In [Cloud Console](#), go to the **Roles** page.
2. Using the drop-down list at the top of the page, select the project or organization that contains the role that you want to edit.
3. Click a custom role.
4. Click **Edit Role** to update the role's permissions.
5. Click **Add Permissions** to add the following new permissions to the role.

```
bigquery.jobs.get  
bigquery.jobs.list  
bigquery.jobs.listAll  
bigquery.datasets.create  
bigquery.datasets.get  
bigquery.jobs.create  
bigquery.tables.get  
bigquery.tables.getData  
bigquery.tables.list  
bigquery.tables.create
```

6. Click **Update** to save the edited role.

### Verify license requirements

- Before you can activate Cloud Backup for your cluster, you'll need to either 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 your 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 use 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 a Google subscription for the object storage space where your backups will be located.

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 backups will be stored when you set up the service.

### 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**.

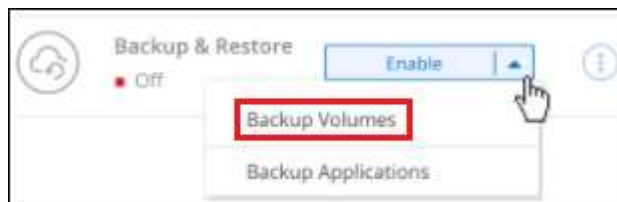
You'll need to enter the keys in Cloud Backup later when you configure the backup service.

## Enabling Cloud Backup

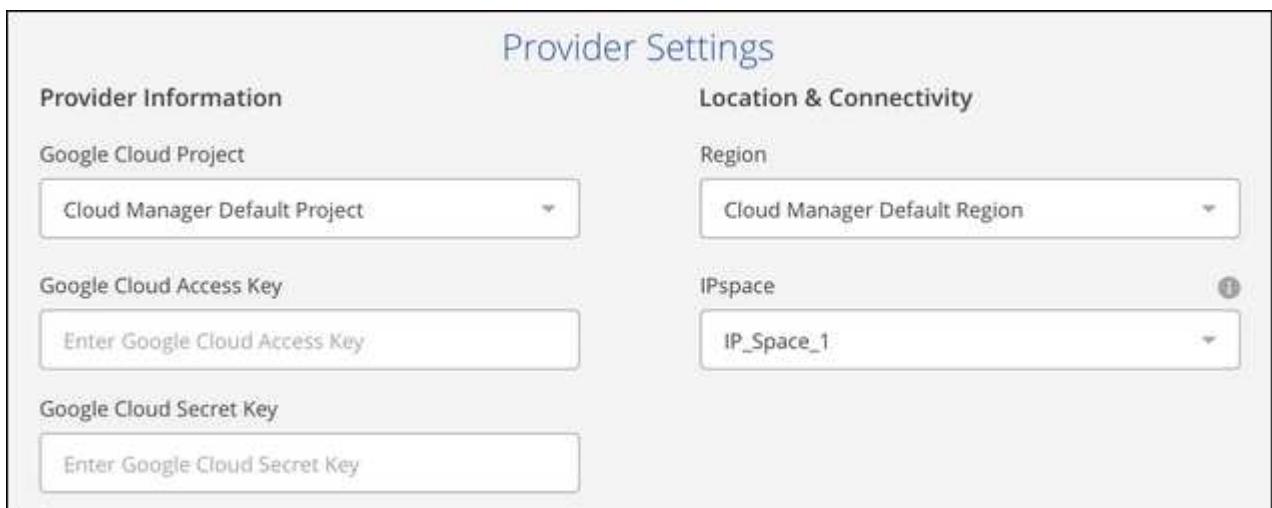
Enable Cloud Backup at any time directly from the on-premises working environment.

### 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. If you don't have an existing Cloud Backup license for your account, you'll be prompted at this point to

select the type of charging method that you want to use. You can subscribe to a pay-as-you-go (PAYGO) Cloud Manager Marketplace offering from Google (or if you have multiple subscriptions you'll need to select one), or purchase and activate a Cloud Backup BYOL license from NetApp. [Learn how to set up Cloud Backup licensing](#).

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

### Define Policy

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

**Policy - Retention & Schedule**   ☒ Create a New Policy   ☐ Select an Existing Policy

☐ Hourly   Number of backups to retain   24

☒ Daily   Number of backups to retain   30

☐ Weekly   Number of backups to retain   52

☐ Monthly   Number of backups to retain   12

**DP Volumes**

Data protection volume backups use the same retention period as defined in the source SnapMirror relationship by default. Use the API if you want to change this value

**Google Cloud Storage Bucket**

Cloud Manager will create the Google Cloud Storage Bucket after you complete the wizard

See [the list of existing policies](#).

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 ).

57 Volumes							
<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Backup Status	
<input checked="" type="checkbox"/>	Volume_Name_1 On	RW	SVM_Name_1	0.25 TB	10 TB	<input type="radio"/>	Not Active
<input checked="" type="checkbox"/>	Volume_Name_2 On	RW	SVM_Name_1	0.25 TB	10 TB	<input type="radio"/>	Not Active
<input checked="" type="checkbox"/>	Volume_Name_3 On	RW	SVM_Name_1	0.25 TB	10 TB	<input type="radio"/>	Not Active
<input checked="" type="checkbox"/>	Volume_Name_4 On	DP	SVM_Name_2	0.25 TB	10 TB	<input type="radio"/>	Not Active
<input checked="" type="checkbox"/>	Volume_Name_5 On	RW	SVM_Name_1	0.25 TB	10 TB	<input type="radio"/>	Not Active
<input checked="" type="checkbox"/> Automatically back up future volumes on all storage VMs with the selected backup policy ⓘ							

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 volumes or files 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.
  - The Connector can be installed in a site with or without internet access.
  - 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.

### Provider Settings

<b>Provider Information</b> Storage Server: <input type="text" value="Enter Storage Server"/> Access Key: <input type="text" value="Access Key"/> Secret Key: <input type="text" value="Secret Key"/>	<b>Connectivity</b> IPspace: <input type="text" value="IP_Space_1"/>
---	--

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.

### Define Policy

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

**Policy - Retention & Schedule**

☐ Create a New Policy
 ☒ Select an Existing Policy

Select Policy

Default Policy (30 Daily)

**DP Volumes**

Data protection volume backups use the same retention period as defined in the source SnapMirror relationship by default. Use the API if you want to change this value

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.

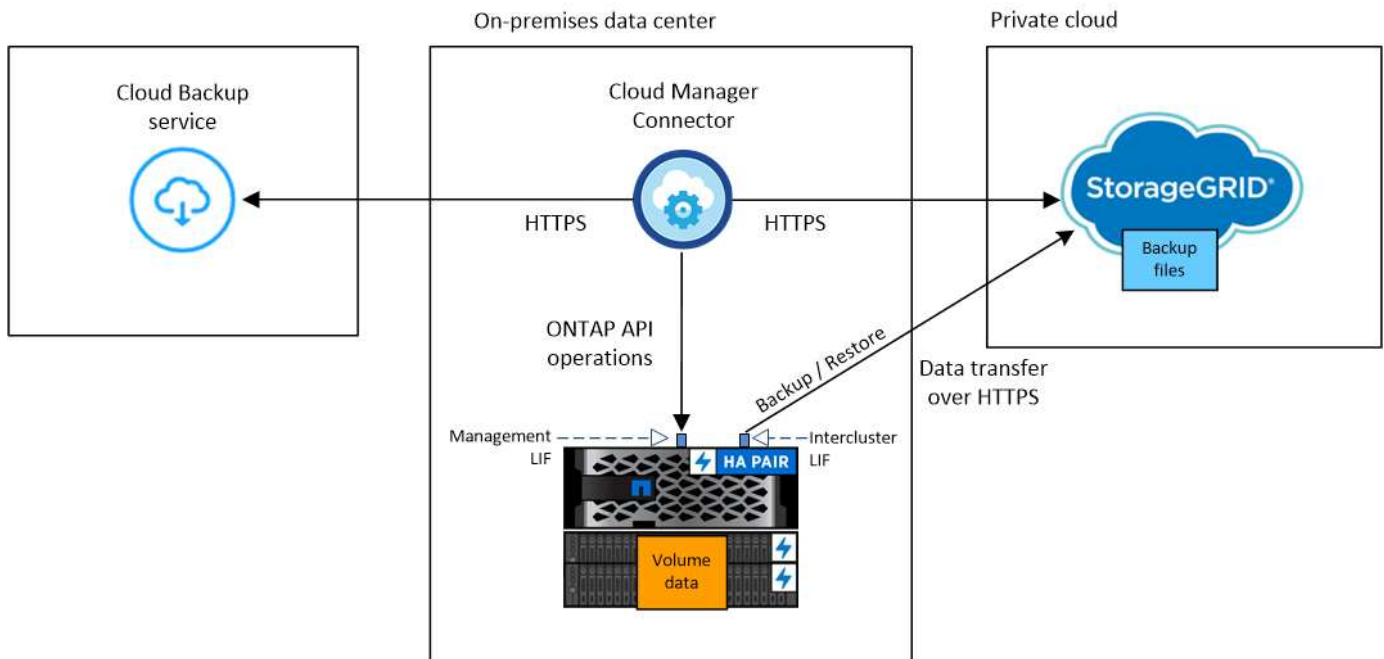


An S3 bucket is created automatically in the service account indicated by the S3 access key and secret key you entered, and the backup files are stored there.

## 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:



When the Connector and on-premises ONTAP system are installed in an on-prem location without internet access, the StorageGRID system must be located in the same on-prem data center.

## 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

- Minimum of ONTAP 9.7P5; ONTAP 9.8P11 and later is recommended.
- 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 (not required when the Connector is installed in a "dark" site).
- 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 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. The Connector can be installed in a site with or without internet access.

- [Learn about Connectors](#)
- [Installing the Connector on a Linux host with internet access](#)
- [Installing the Connector on a Linux host without internet access](#)
- [Switching between Connectors](#)



Cloud Backup functionality is built into the Cloud Manager Connector. When installed in a site with no internet connectivity, you'll need to update the Connector software periodically to get access to new features. Check the [Cloud Backup What's New](#) to see the new features in each Cloud Backup release, and then you can follow the steps to [upgrade the Connector software](#) when you want to use new features.

## 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 (not required when the Connector is installed in a "dark" site)

## License requirements

Before you can activate Cloud Backup for your cluster, you'll 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](#).



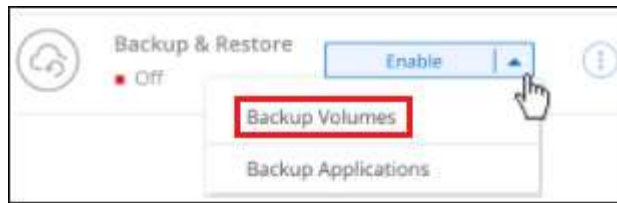
PAYGO licensing is not supported when backing up files to StorageGRID.

## 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 (not required when the Connector is installed in a "dark" site).

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).

Select Volumes

57 Volumes

<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Volume_Name_1 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_2 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_3 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_4 On	DP	SVM_Name_2	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_5 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active

☒ Automatically back up future volumes on all storage VMs with the selected backup policy ⓘ

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 or individual files from a backup file](#) to 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.



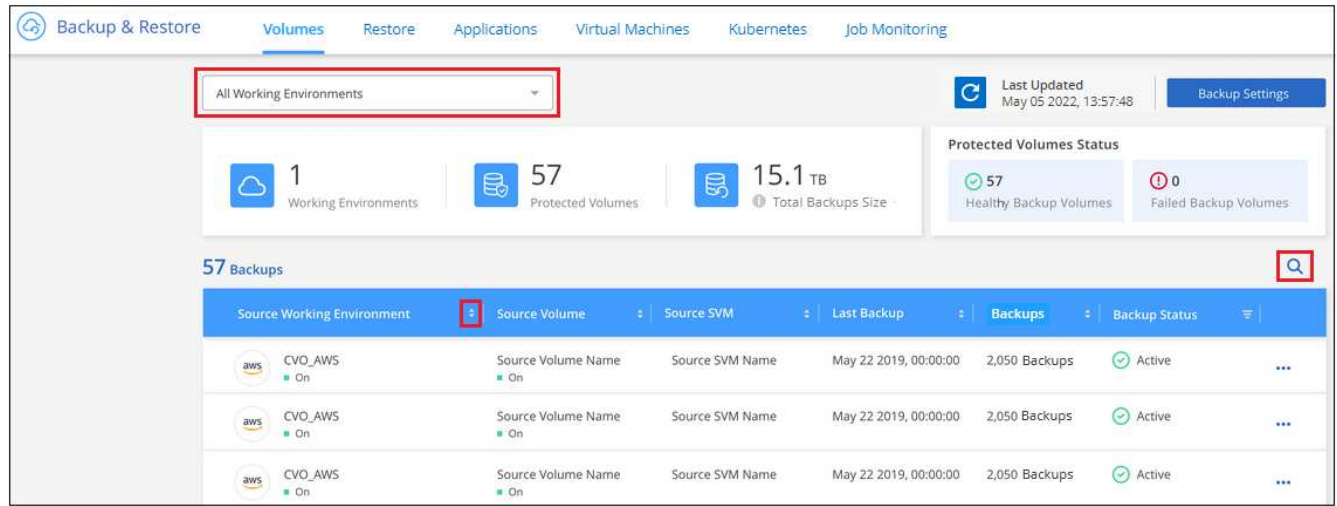
Do not manage or change backup files directly from your cloud provider environment. This may corrupt the files and will result in an unsupported configuration.

## 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.



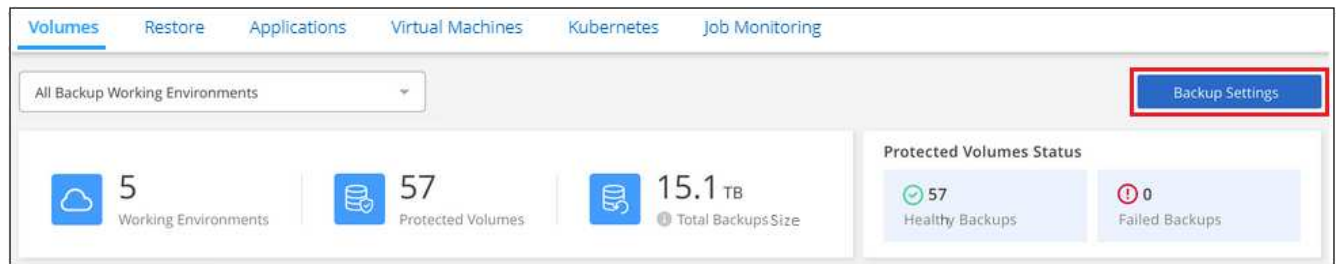
If you are looking for specific volumes in certain working environments, you can refine the list by working environment and volume, or you can use the search filter.

## Enabling and disabling backups of volumes

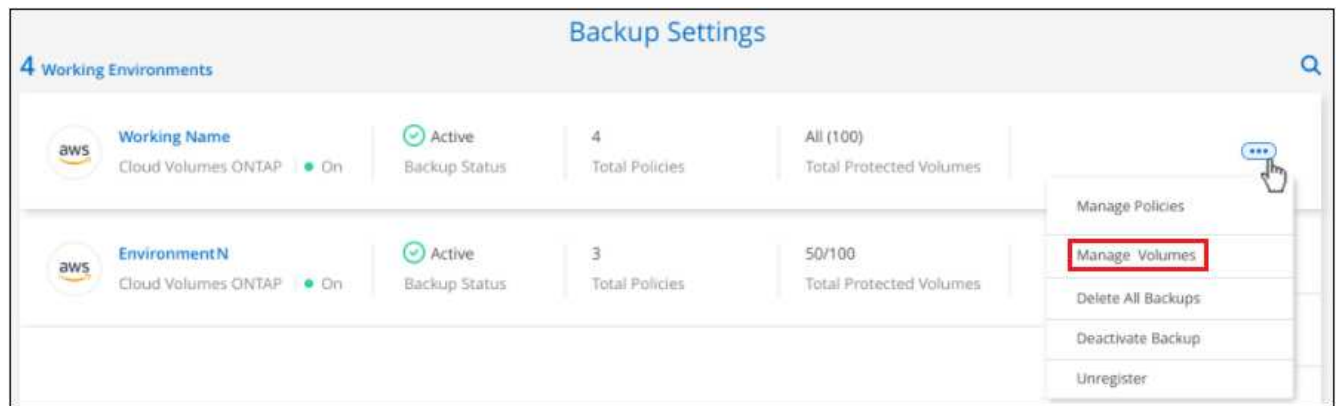
You can stop backing up a volume if you do not need backup copies of that volume and you do not want to pay for the cost to store the backups. You can also add a new volume to the backup list if it is not currently being backed up.

## Steps

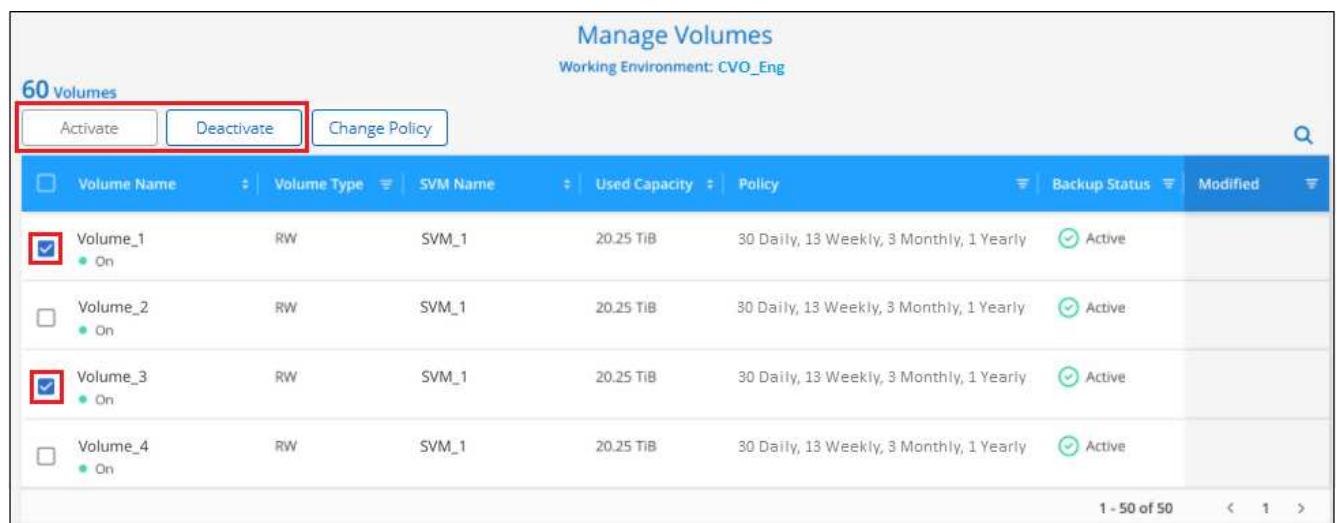
1. From the **Volumes** tab, select **Backup Settings**.



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.



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

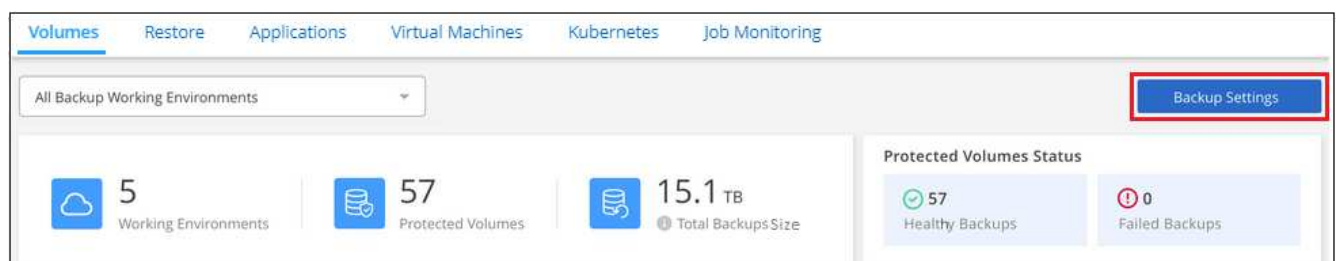
**Note:** When stopping a volume from being backed up you'll continue to be charged by your cloud provider for object storage costs for the capacity that the backups use unless you [delete the backups](#).

## Editing an existing backup policy

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

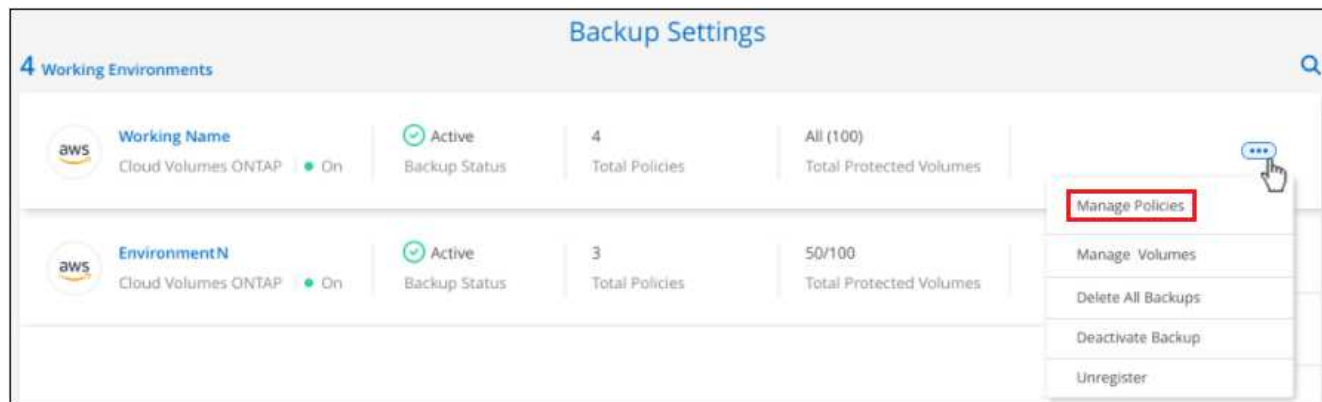
### Steps

1. From the **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, you also have the option to enable or disable tiering of backups to archival storage after a certain number of days.

+



Archival Policy

Backups reside in Cool Azure Blob storage for frequently accessed data. Optionally, you can tier backups to Azure Archive storage for further cost optimization.

Azure

☒ Tier Backups to Archival

Archive after (Days)

Access Tier  

Azure Archive

---

Archival Policy

Backups reside in S3 Standard storage for frequently accessed data. Optionally, you can tier backups to either S3 Glacier or S3 Glacier Deep Archive storage for further cost optimization.

AWS

☒ Tier Backups to Archival

Archive after (Days)

Storage Class  

S3 Glacier

S3 Glacier

S3 Glacier Deep Archive

+

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.

## 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**.

Volumes Restore Applications Virtual Machines Kubernetes Job Monitoring

All Backup Working Environments

Backup Settings

5

Working Environments

57

Protected Volumes

15.1 TB

Total Backups Size

Protected Volumes Status

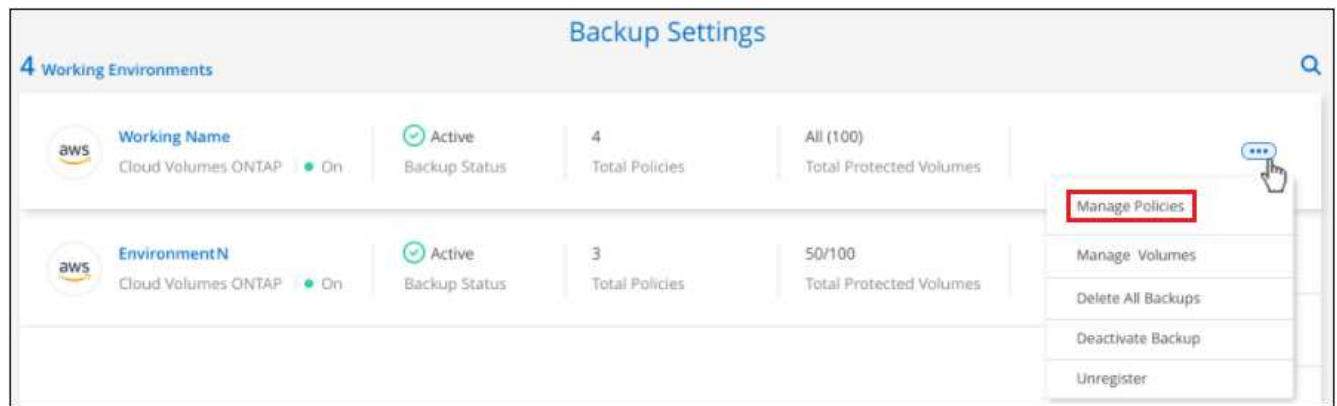
57

Healthy Backups

0

Failed Backups

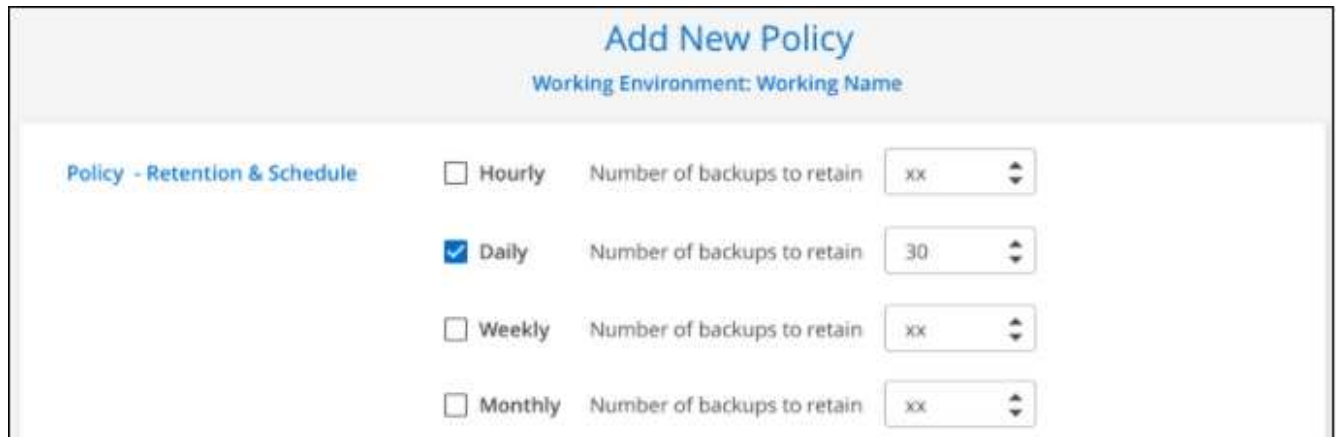
2. From the *Backup Settings* page, click ... for the working environment where you want to add the new policy, and select **Manage Policies**.



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, you also have the option to enable or disable tiering of backups to archival storage after a certain number of days.

+

Archival Policy

Backups reside in Cool Azure Blob storage for frequently accessed data. Optionally, you can tier backups to Azure Archive storage for further cost optimization.

Azure

☒ Tier Backups to Archival

Archive after (Days)

Access Tier

---

Archival Policy

Backups reside in S3 Standard storage for frequently accessed data. Optionally, you can tier backups to either S3 Glacier or S3 Glacier Deep Archive storage for further cost optimization.

AWS

☒ Tier Backups to Archival

Archive after (Days)

Storage Class  


S3 Glacier  
 S3 Glacier Deep Archive

## 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**.

Volumes

Restore

Applications

Virtual Machines

Kubernetes

Job Monitoring

All Backup Working Environments

Backup Settings

5 Working Environments

57 Protected Volumes

15.1 TB Total Backups Size

Protected Volumes Status

57 Healthy Backups

0 Failed Backups

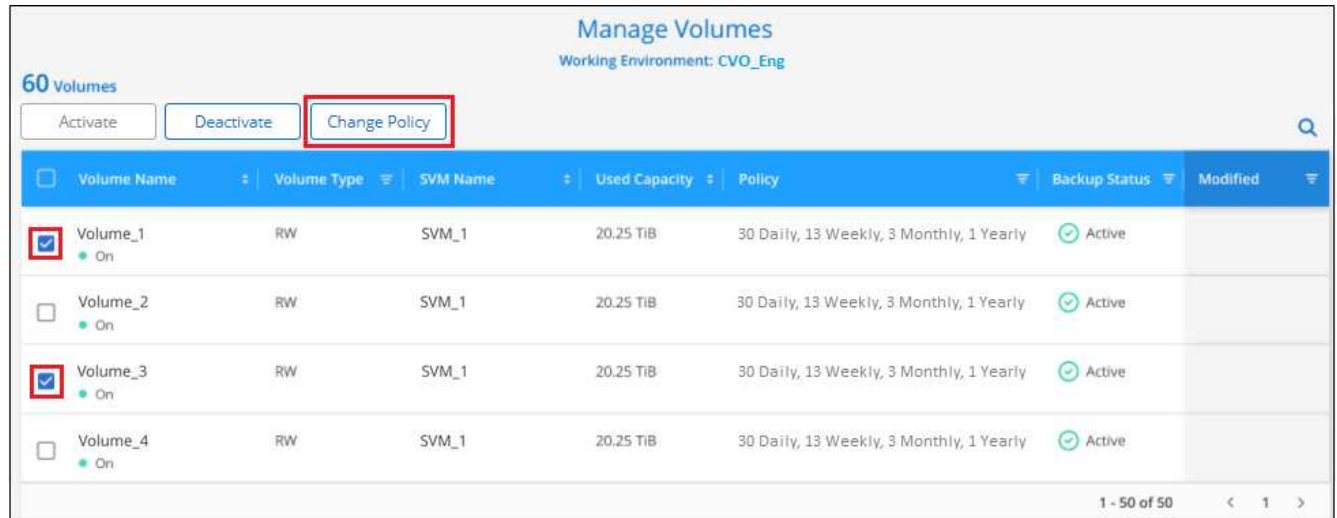
2. From the *Backup Settings* page, click ... for the working environment where the volumes exist, and select **Manage Volumes**.

Backup Settings

4 Working Environments

Working Name	Backup Status	Total Policies	Total Protected Volumes	
Cloud Volumes ONTAP On	Active	4	All (100)	...
EnvironmentN Cloud Volumes ONTAP On	Active	3	50/100	<div>             Manage Policies             <div> <div>Manage Volumes</div> <div>Delete All Backups</div> <div>Deactivate Backup</div> <div>Unregister</div> </div> </div>

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

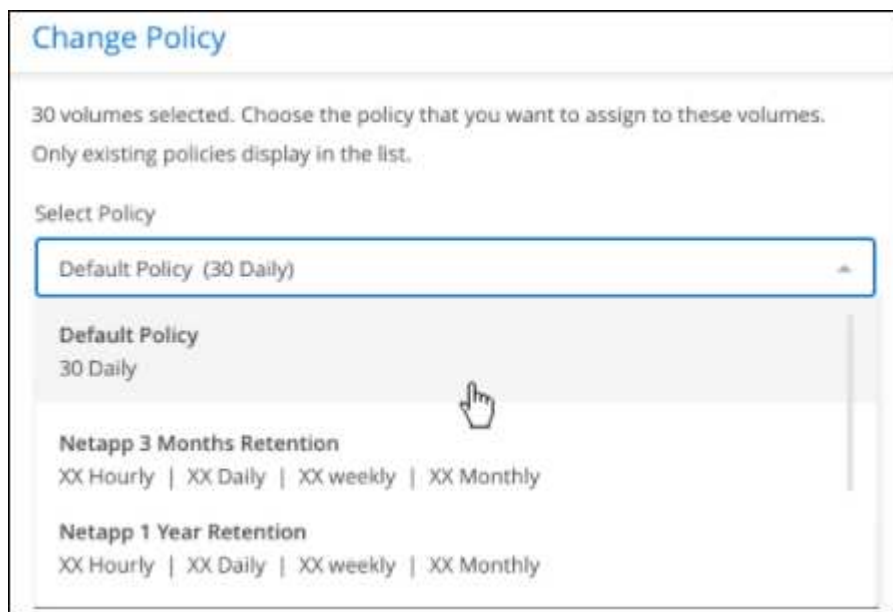


The screenshot shows the 'Manage Volumes' interface. At the top, it says '60 Volumes' and 'Working Environment: CVO\_Eng'. Below this are three buttons: 'Activate', 'Deactivate', and 'Change Policy' (which is highlighted with a red box). Below the buttons is a table with columns: Volume Name, Volume Type, SVM Name, Used Capacity, Policy, Backup Status, and Modified. The table contains four rows of data. The first and third rows have their checkboxes selected (checked).

<input type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Policy	Backup Status	Modified
<input checked="" type="checkbox"/>	Volume_1 On	RW	SVM_1	20.25 TiB	30 Daily, 13 Weekly, 3 Monthly, 1 Yearly	Active	
<input type="checkbox"/>	Volume_2 On	RW	SVM_1	20.25 TiB	30 Daily, 13 Weekly, 3 Monthly, 1 Yearly	Active	
<input checked="" type="checkbox"/>	Volume_3 On	RW	SVM_1	20.25 TiB	30 Daily, 13 Weekly, 3 Monthly, 1 Yearly	Active	
<input type="checkbox"/>	Volume_4 On	RW	SVM_1	20.25 TiB	30 Daily, 13 Weekly, 3 Monthly, 1 Yearly	Active	

At the bottom right, it says '1 - 50 of 50' and has navigation arrows.

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



The screenshot shows the 'Change Policy' page. It says '30 volumes selected. Choose the policy that you want to assign to these volumes. Only existing policies display in the list.' Below this is a 'Select Policy' section with a dropdown menu showing 'Default Policy (30 Daily)'. Below the dropdown is a list of policies: 'Default Policy 30 Daily', 'Netapp 3 Months Retention', and 'Netapp 1 Year Retention'. A hand cursor is pointing at the 'Default Policy 30 Daily' option.

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

## Setting a backup policy to be assigned to new volumes

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

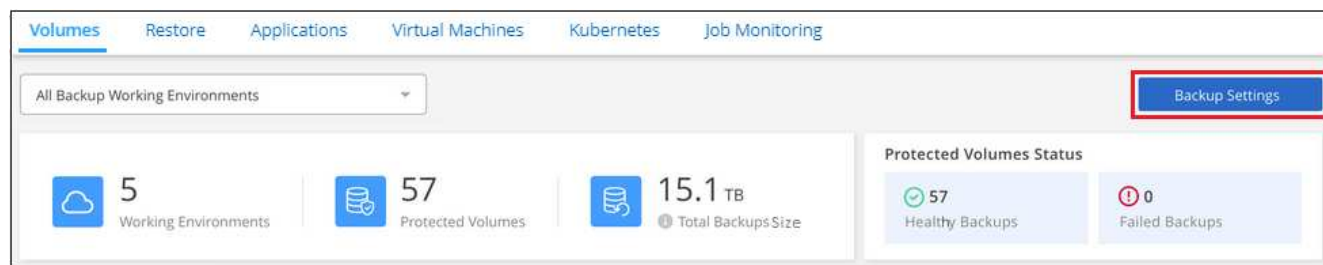
Note that the policy that you want to apply to the volumes must already exist. [See how to add a new backup policy for a working environment.](#)

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

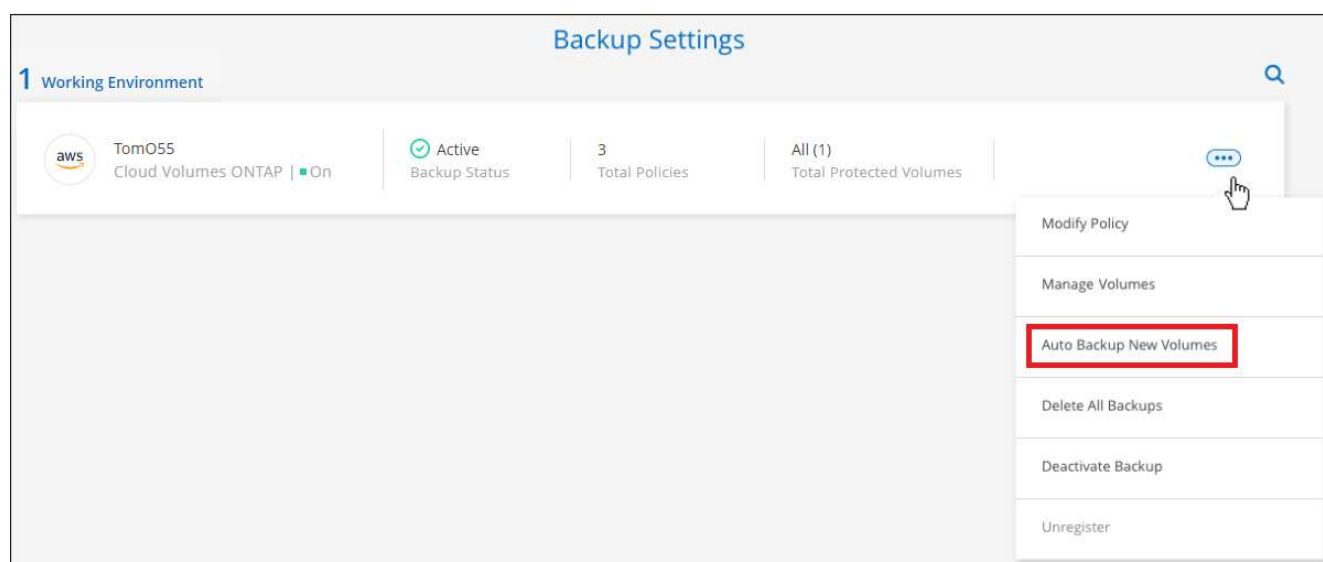
future.

## Steps

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



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



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

### Auto Backup New Volumes

☒ Automatically back up new volumes on all SVMs for Working Environment TomO55

Choose the policy that will be assigned to new volumes. Only existing policies are shown in the list.

Select Backup Policy

CloudBackupService-1611307085985\_V2 (30 Daily) ▼

Save

Cancel

## Result

Now this backup policy will be applied to any new volume created in this working environment using Cloud Manager, System Manager, or the ONTAP CLI.

## 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.

Note that when creating an ad-hoc backup, a Snapshot is created on the source volume. Since this Snapshot is not part of a normal Snapshot schedule, it will not rotate off. You may want to manually delete this Snapshot from the source volume once the backup is complete. This will allow blocks related to this Snapshot to be freed up. The name of the Snapshot will begin with `cbs-snapshot-adhoc-`. [See how to delete a Snapshot using the ONTAP CLI.](#)



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**.

**Volumes** | Restore | Applications | Virtual Machines | Kubernetes | Job Monitoring

All Backup Working Environments

Backup Settings

1 Working Environments | 57 Protected Volumes | 15.1 TB Total Backup Capacity

**Protected Volumes Status**

57 Healthy Backup Volumes | 0 Failed Backup Volumes

57 Backups

Source Working Environment	Source Volume	Source SVM	Last Backup	Backups	Backup Status
CVO_AWS	Volume_1	SVM_1	May 22 2019, 00:00:00	2,050 Backups	Active
CVO_AWS	Volume_2	SVM_1	May 22 2019, 00:00:00	2,050 Backups	
CVO_AWS	Volume_3	SVM_1	May 22 2019, 00:00:00	2,050 Backups	

Context Menu for Volume\_1:

- Details & Backup List
- Backup Now
- Pause Backups

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**.

**Volumes** | Restore | Applications | Virtual Machines | Kubernetes | Job Monitoring

All Backup Working Environments

Backup Settings

1 Working Environments | 57 Protected Volumes | 15.1 TB Total Backup Capacity

**Protected Volumes Status**

57 Healthy Backup Volumes | 0 Failed Backup Volumes

57 Backups

Source Working Environment	Source Volume	Source SVM	Last Backup	Backups	Backup Status
CVO_AWS	Volume_1	SVM_1	May 22 2019, 00:00:00	2,050 Backups	Active
CVO_AWS	Volume_2	SVM_1	May 22 2019, 00:00:00	2,050 Backups	
CVO_AWS	Volume_3	SVM_1	May 22 2019, 00:00:00	2,050 Backups	

Context Menu for Volume\_1:

- Details & Backup List
- Backup Now
- Pause Backups



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

Source

Working Environment Working Environment N...  
Type Cloud Volumes ONTAP (HA)  
Provider AWS  
Volume Volume Name  
SVM SVM Name

Destination

Cloud Provider AWS  
Region us-east-1  
Bucket netapp-backup  
Account ID 012345678901234567890

Backup Information

Relationship Status Active  
Last Backup Oct 05 2021, 2:41:33 pm  
Lag Duration 14 days 3 hours, 38 mi...  
Backups 2,050  
Backup Policy Netapp7YearsRetention

2,050 Backups

Select Timeframe

Actions

Backup Name	Date	Size	
Backup_2020_Jan	May 22 2019, 00:00:00	19,001	...
Backup_2020_Mar	May 22 2019, 00:00:00	19,002	...
Backup_2020_Apr	May 22 2019, 00:00:00	19,009	...

## 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. 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**.

VolumesRestoreApplicationsVirtual MachinesKubernetesJob Monitoring

All Backup Working Environments

Backup Settings

5 Working Environments

57 Protected Volumes

15.1 TB Total Backups Size

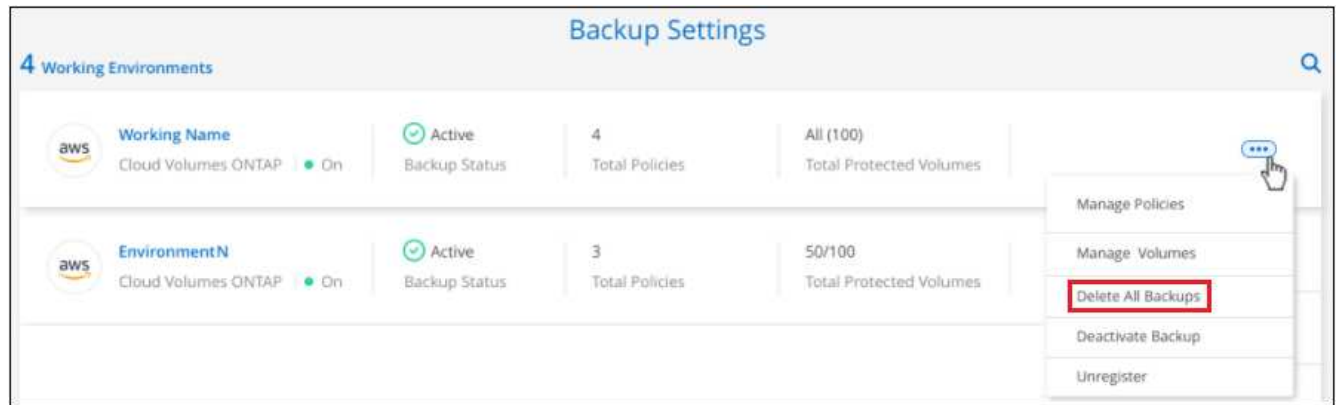
Protected Volumes Status

57 Healthy Backups

0 Failed Backups



2. Click ... for the working environment 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**.

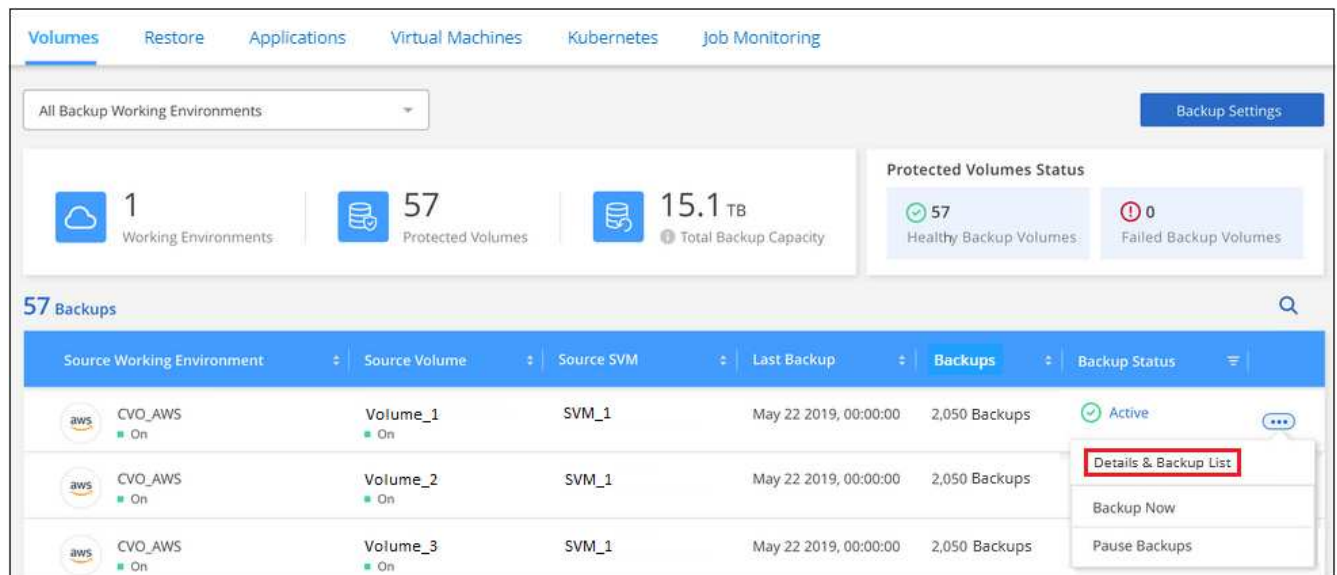
### Deleting all backup files for a volume

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.

The screenshot displays the NetApp backup management interface. It is divided into three main sections: Source, Destination, and Backup Information. Below these is a table of backups and an Actions menu.

Source		Destination		Backup Information	
Working Environment	Working Environment N...	Cloud Provider	AWS	Relationship Status	Active
Type	Cloud Volumes ONTAP (HA)	Region	us-east-1	Last Backup	Oct 05 2021, 2:41:33 pm
Provider	AWS	Bucket	netapp-backup	Lag Duration	14 days 3 hours, 38 mi...
Volume	Volume Name	Account ID	012345678901234567890	Backups	2,050
SVM	SVM Name			Backup Policy	Netapp7YearsRetention

2,050 Backups

Backup Name	Date	Size	
Backup_2020_Jan	May 22 2019, 00:00:00	19,001	...
Backup_2020_Mar	May 22 2019, 00:00:00	19,002	...
Backup_2020_Apr	May 22 2019, 00:00:00	19,009	...

Actions: Select Timeframe, Actions

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

The screenshot shows the same interface as before, but with the 'Actions' menu open. The 'Delete All Backups' option is highlighted with a red box and a mouse cursor. The 'Download Backup Report' option is also visible.

2,050 Backups

Backup Name	Date	
Backup_2020_Jan	May 22 2019, 00:00:00	
Backup_2020_Mar	May 22 2019, 00:00:00	...

Actions: Select Timeframe, Actions

Delete All Backups

Download Backup Report

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**.

Navigation: Volumes | Restore | Applications | Virtual Machines | Kubernetes | Job Monitoring

All Backup Working Environments Backup Settings

1 Working Environments

57 Protected Volumes

15.1 TB Total Backup Capacity

**Protected Volumes Status**

57 Healthy Backup Volumes

0 Failed Backup Volumes

57 Backups Search

Source Working Environment	Source Volume	Source SVM	Last Backup	Backups	Backup Status	
CVO_AWS On	Volume_1 On	SVM_1	May 22 2019, 00:00:00	2,050 Backups	Active	...
CVO_AWS On	Volume_2 On	SVM_1	May 22 2019, 00:00:00	2,050 Backups		<div>Details &amp; Backup List</div> <div>Backup Now</div> <div>Pause Backups</div>
CVO_AWS On	Volume_3 On	SVM_1	May 22 2019, 00:00:00	2,050 Backups		

The list of all backup files is displayed.

**Source**

Working Environment Working Environment N...

Type Cloud Volumes ONTAP (HA)

Provider AWS

Volume Volume Name

SVM SVM Name

**Destination**

Cloud Provider AWS

Region us-east-1

Bucket netapp-backup

Account ID 012345678901234567890

**Backup Information**

Relationship Status Active

Last Backup Oct 05 2021, 2:41:33 pm

Lag Duration 14 days 3 hours, 38 mi...

Backups 2,050

Backup Policy Netapp7YearsRetention

2,050 Backups Search Select Timeframe Calendar Actions

Backup Name	Date	Size	
Backup_2020_Jan	May 22 2019, 00:00:00	19,001	...
Backup_2020_Mar	May 22 2019, 00:00:00	19,002	...
Backup_2020_Apr	May 22 2019, 00:00:00	19,009	...

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

2,050 Backups Search Select Timeframe Calendar Actions

Backup Name	Date	
Backup_2020_Feb	May 22 2019, 00:00:00	...
Backup_2020_Jan	May 22 2019, 00:00:00	
Backup_2020_Mar	May 22 2019, 00:00:00	

Delete

Restore

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

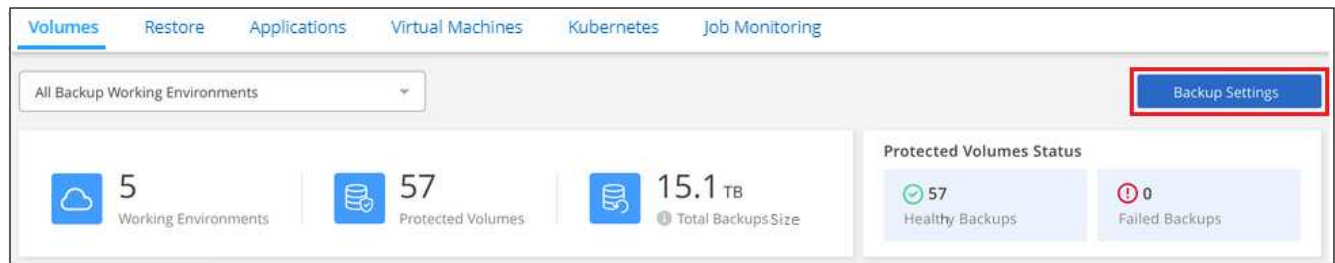
## Disabling Cloud Backup for a working environment

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.

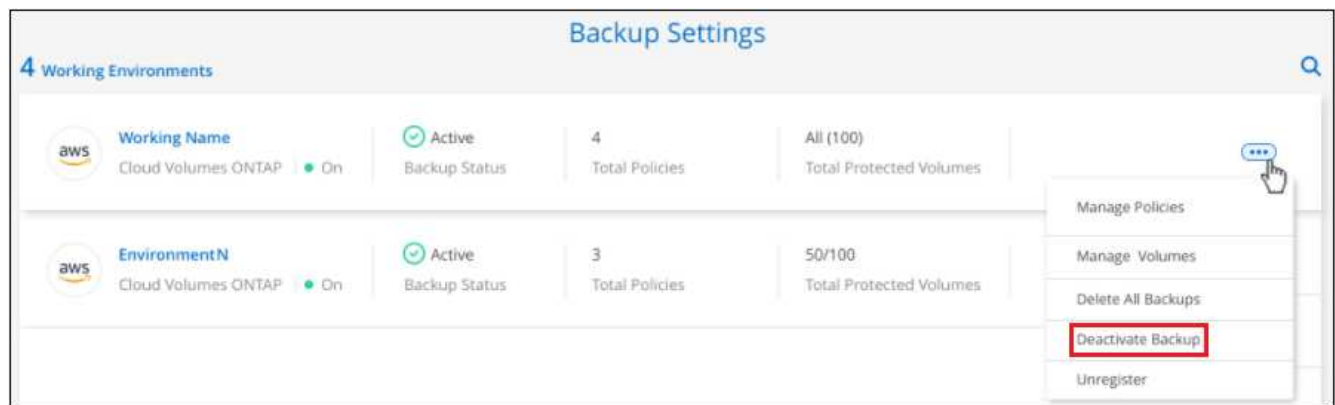
Note that you'll continue to be charged by your cloud provider for object storage costs for the capacity that your backups use unless you [delete the backups](#).

### Steps

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



2. From the *Backup Settings* page, click ... for the working environment 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.

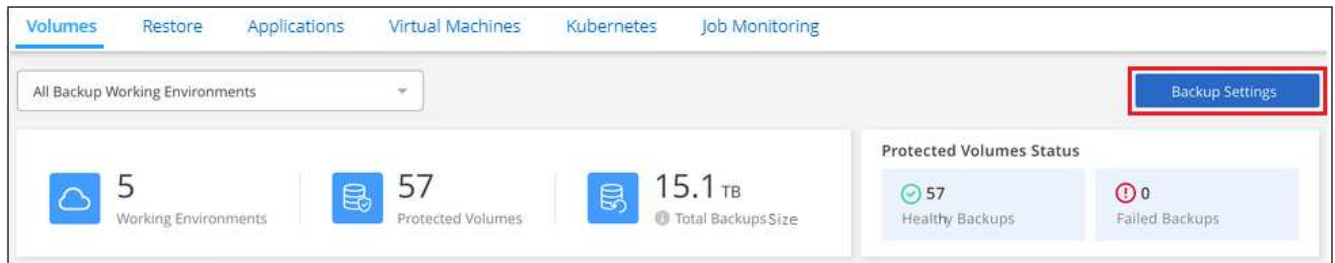
Before you can unregister Cloud Backup, you must perform the following steps, in this order:

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

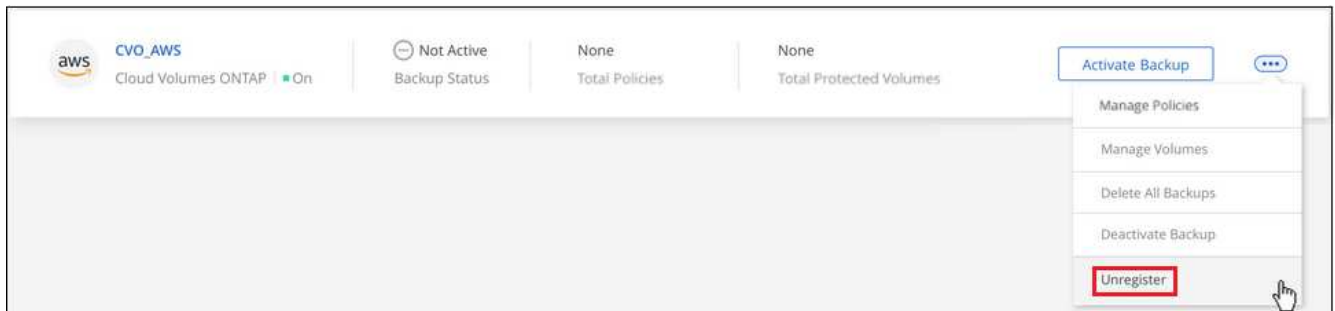
The unregister option is not available until these two actions are complete.

## 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 ONTAP 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 original 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 original 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.

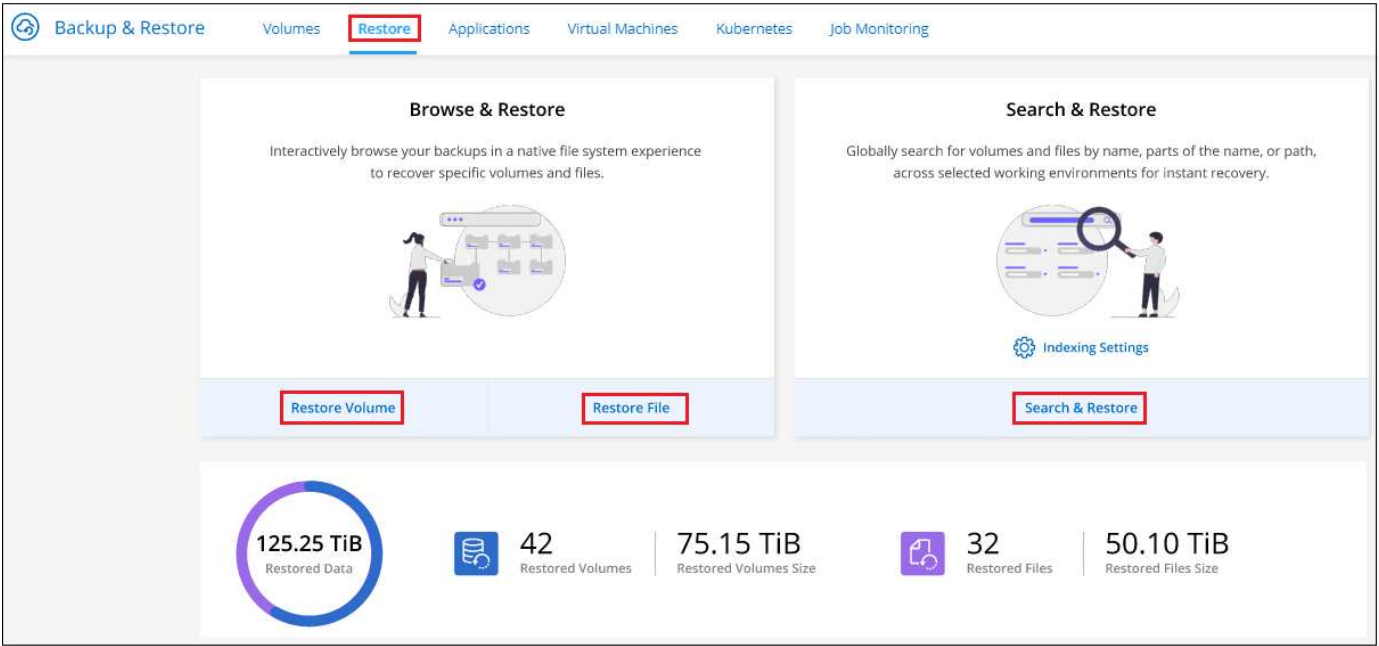
A valid Cloud Backup license is required to restore data from backup files to a production system.

# 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 to restore a specific volume or file from the last week or month — 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 to restore 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 <b>all backup files</b> by partial or full volume name, partial or full file name, size range, and additional search filters
Volume and file restore works with backup files stored in Amazon S3, Azure Blob, Google Cloud, and NetApp StorageGRID.	Volume and file restore works with backup files stored in Amazon S3 and Google Cloud
Restore volumes and files from StorageGRID in sites with no internet access	Not supported in dark sites

Browse & Restore	Search & Restore
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 and private clouds	Browse for results across public clouds and local Snapshots copies
No additional cloud provider resources required	Additional bucket and AWS or Google resources required per account
No additional cloud provider costs required	Cost associated with AWS or Google resources when scanning your backups and volumes for search results

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 file, you should know the name of the volume or file you want to restore, the name of the working environment where the volume resides, and the approximate date of the backup file that you want to restore from.

**Note:** If the backup file for the volume that you want to restore resides in archival storage (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.

### 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
Google Cloud Storage	Cloud Volumes ONTAP in Google On-premises ONTAP system	Cloud Volumes ONTAP in Google On-premises ONTAP system
NetApp StorageGRID	On-premises ONTAP system	On-premises ONTAP system

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

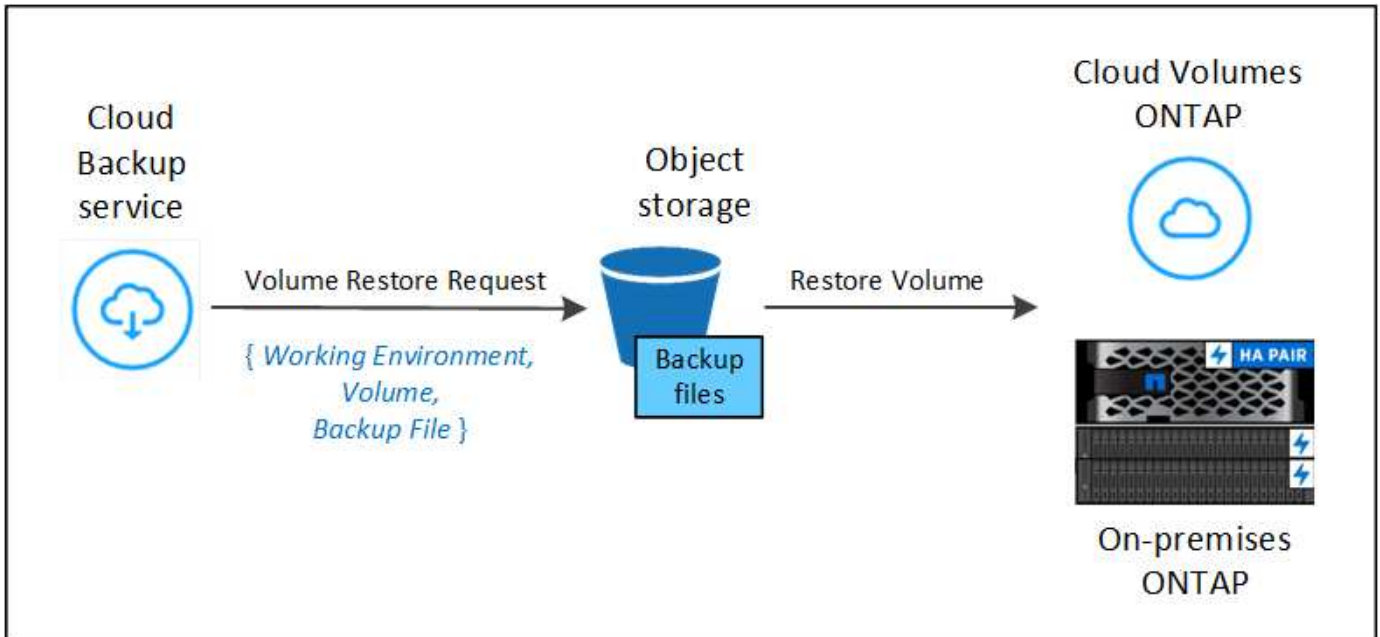


If the backup file resides in archival storage, only volume restore is supported. File restore is not currently supported from archival storage when using Browse & Restore.



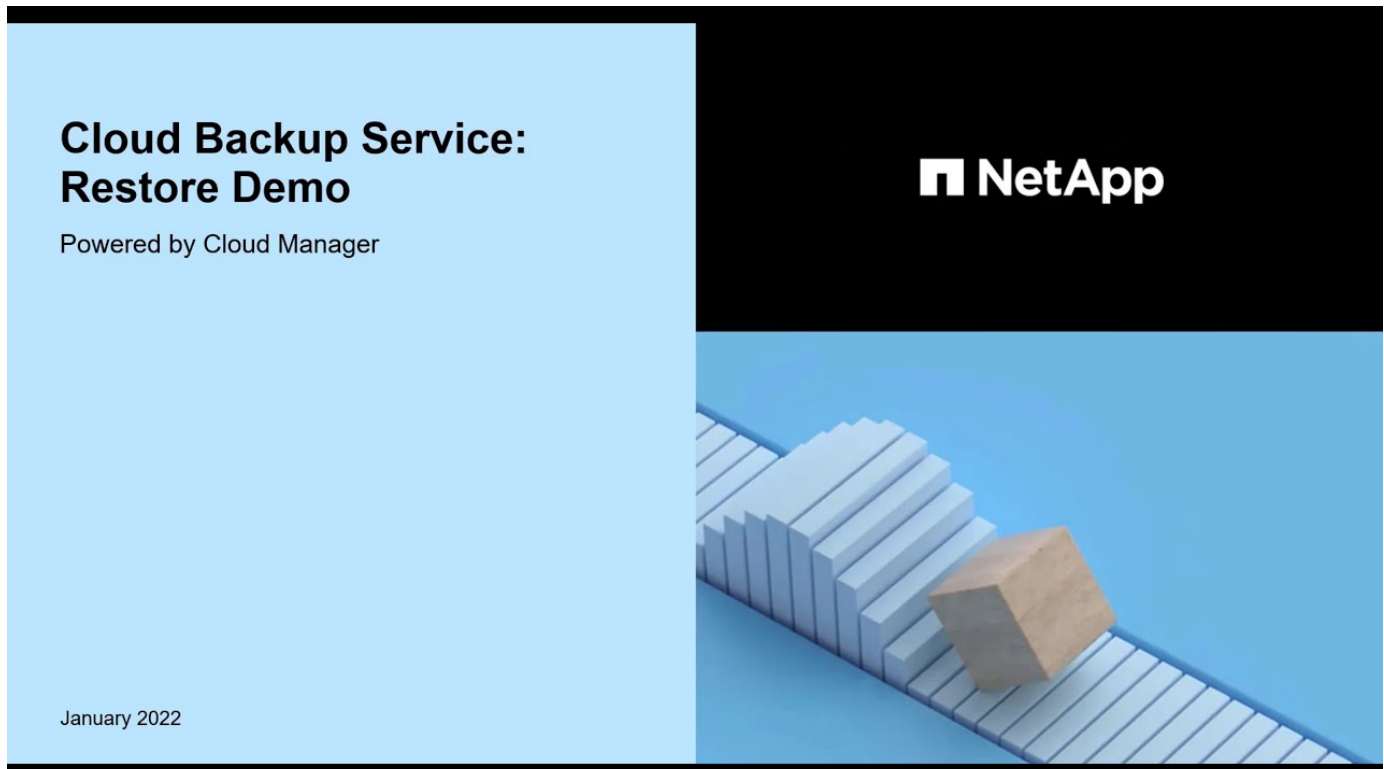
## Restoring volumes using Browse & Restore

When you restore a volume from a backup file, Cloud Backup creates a *new* volume using the data from the backup. You can restore the data to a volume in the original 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.

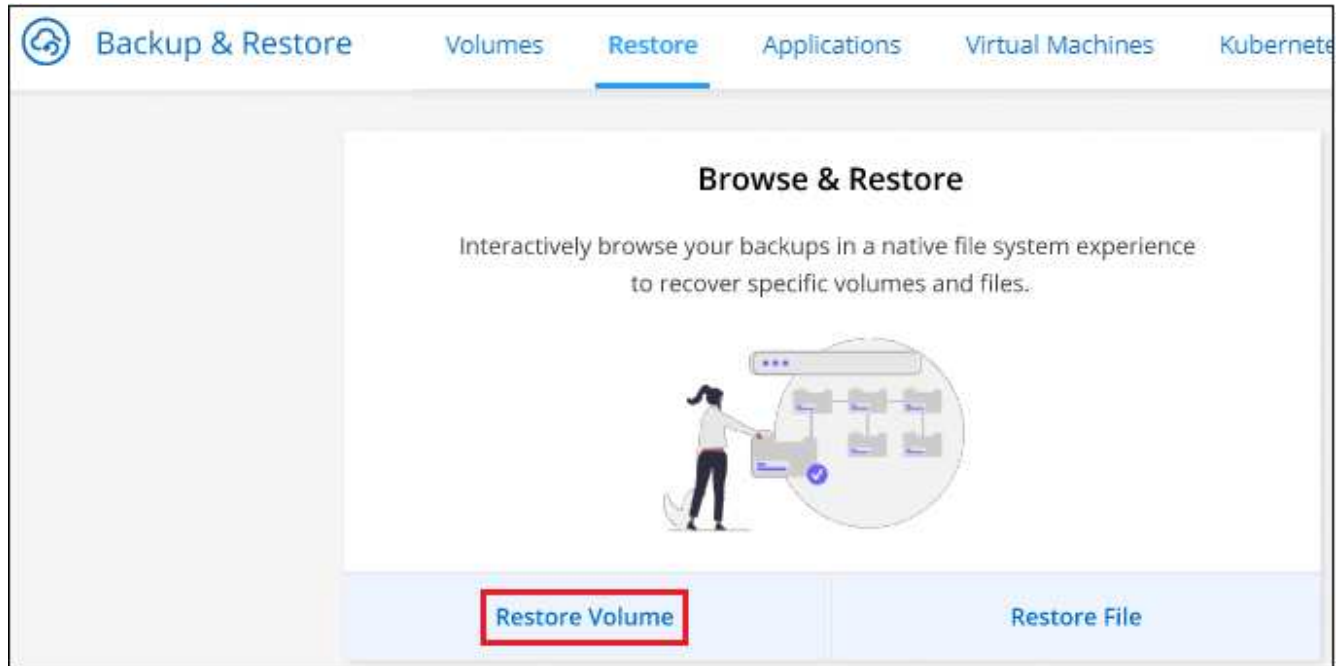
The following video shows a quick walkthrough of restoring a volume:



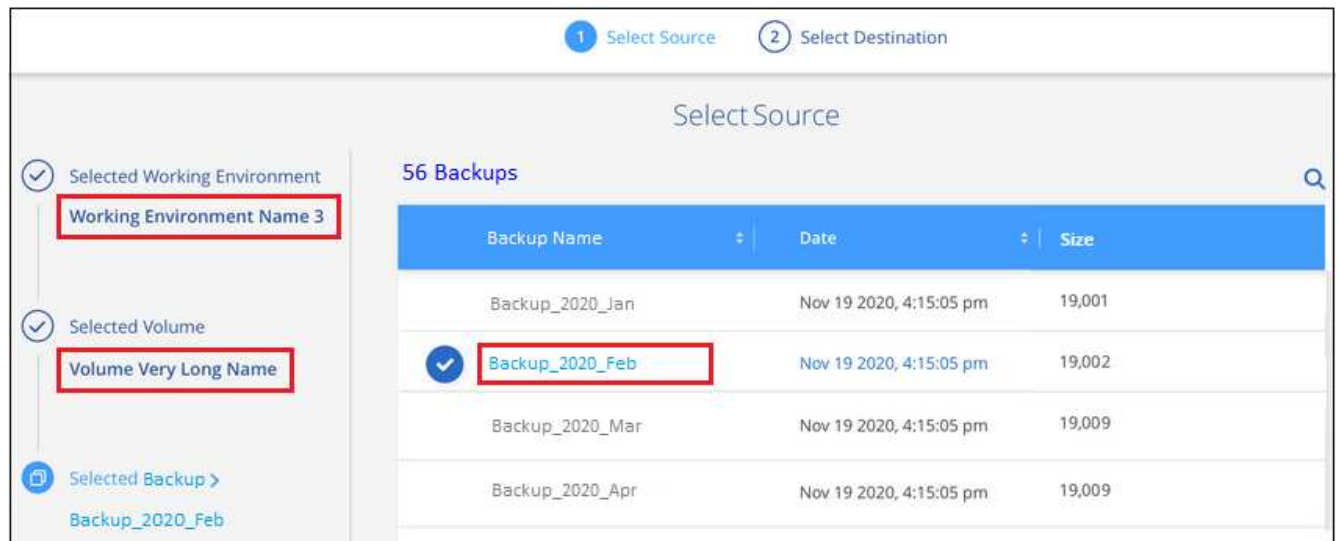


## Steps

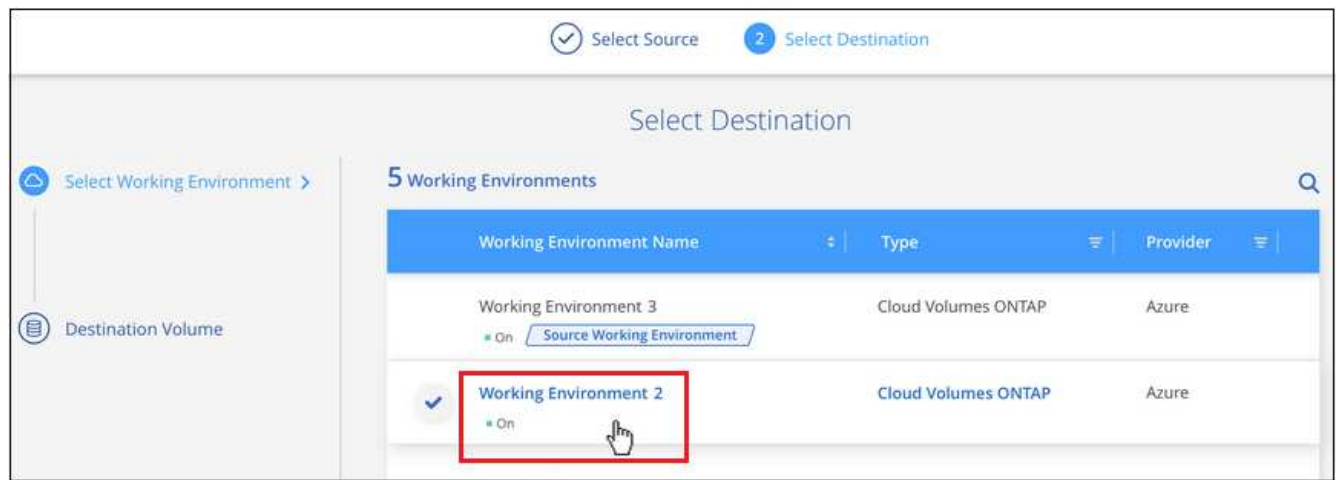
1. Select the **Backup & Restore** service.
2. Click the **Restore** tab and the Restore Dashboard is displayed.
3. From the *Browse & Restore* section, click **Restore Volume**.



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 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, enter the FQDN of the StorageGRID server and the port that ONTAP should use for HTTPS communication with 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.

The screenshot shows the 'Select Destination' page with configuration fields. On the left, the 'Selected Working Environment' is 'Working Environment Name 2' and the 'Destination Volume' is 'General\_restore'. The main area has a blue information box stating: 'A new volume will be created in the working environment based on the backup you selected'.

Configuration fields:

- Volume Name:** General\_restore
- Storage VM:** svm1
- Restore Priority:** Low

**Volume Information:**

- Volume Size: 50.00 GB
- Backup Policy: CloudBackupService
- Protocol: NFS

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.

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

## Result

Cloud Backup 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 an ONTAP volume backup, you can choose to restore individual files instead of restoring the entire volume. You can restore files to an existing volume in the original 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. So if you want to restore files to different volumes, you'll need to run the restore process multiple times.



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, or you can restore the entire volume from the archived backup and then access the files you need, or you can restore files using Search & Restore.

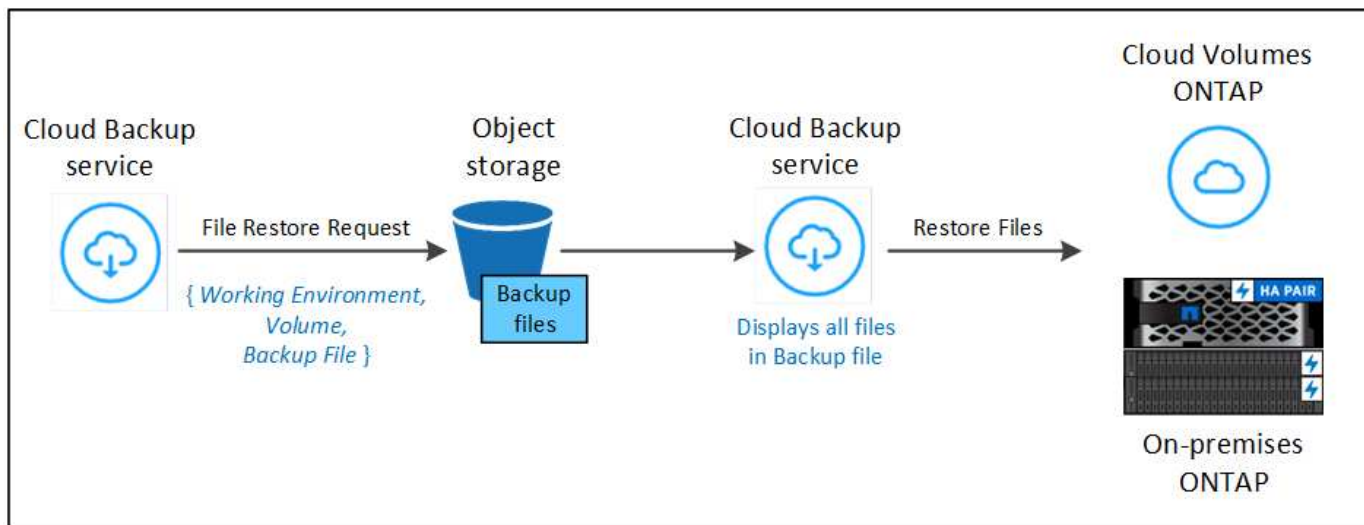
### Prerequisites

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

### 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. Cloud Backup displays the folders and files that exist within the selected backup 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.

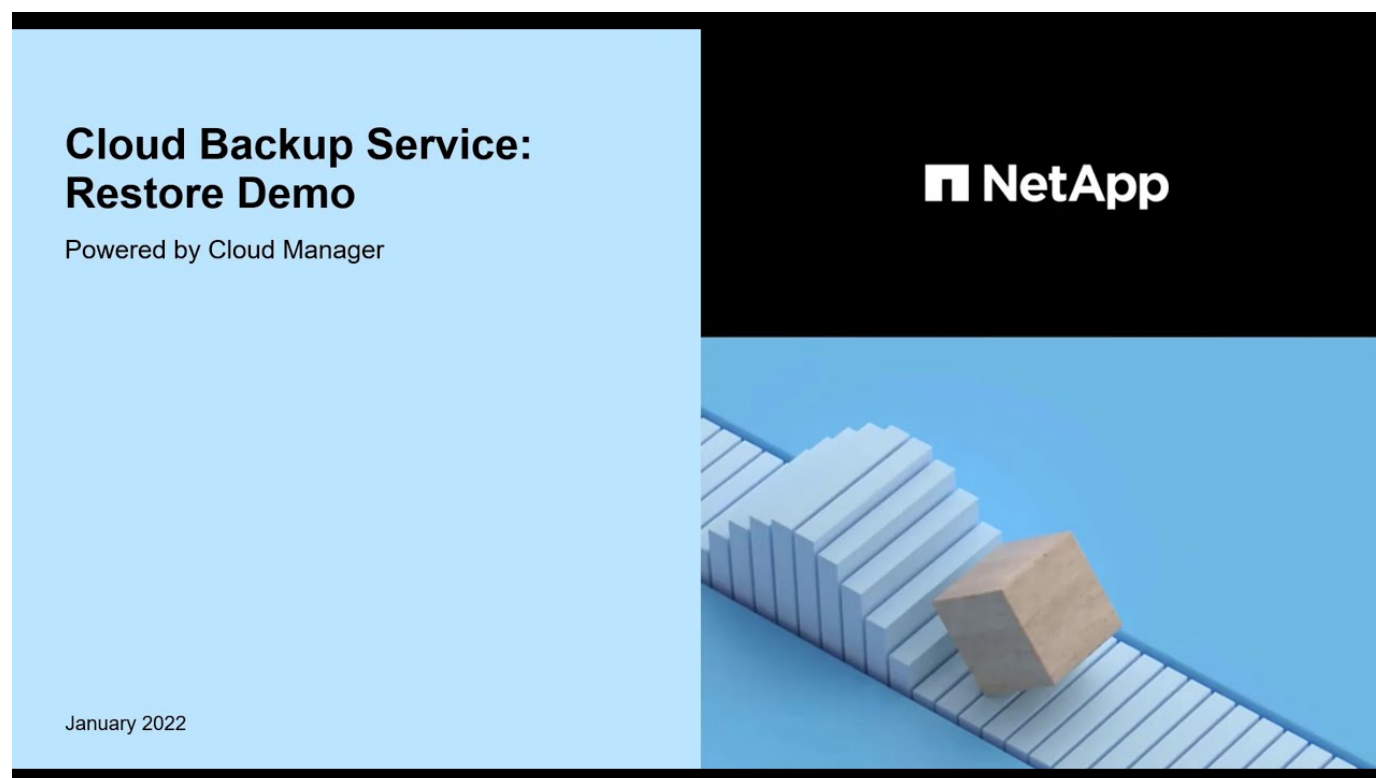


As you can see, you need to know the working environment name, volume name, backup file date, and file name to perform a file restore.

### Restoring files using Browse & Restore

Follow these steps to restore files to a volume from an ONTAP 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.

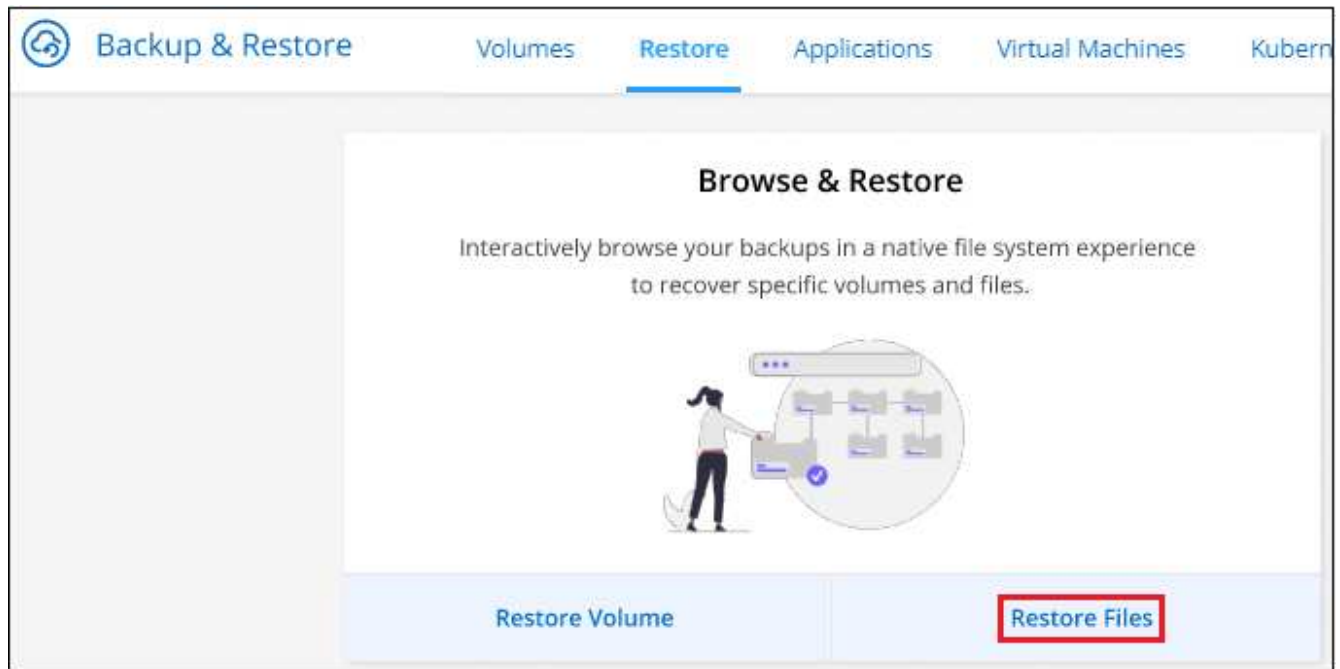
The following video shows a quick walkthrough of restoring a single file:



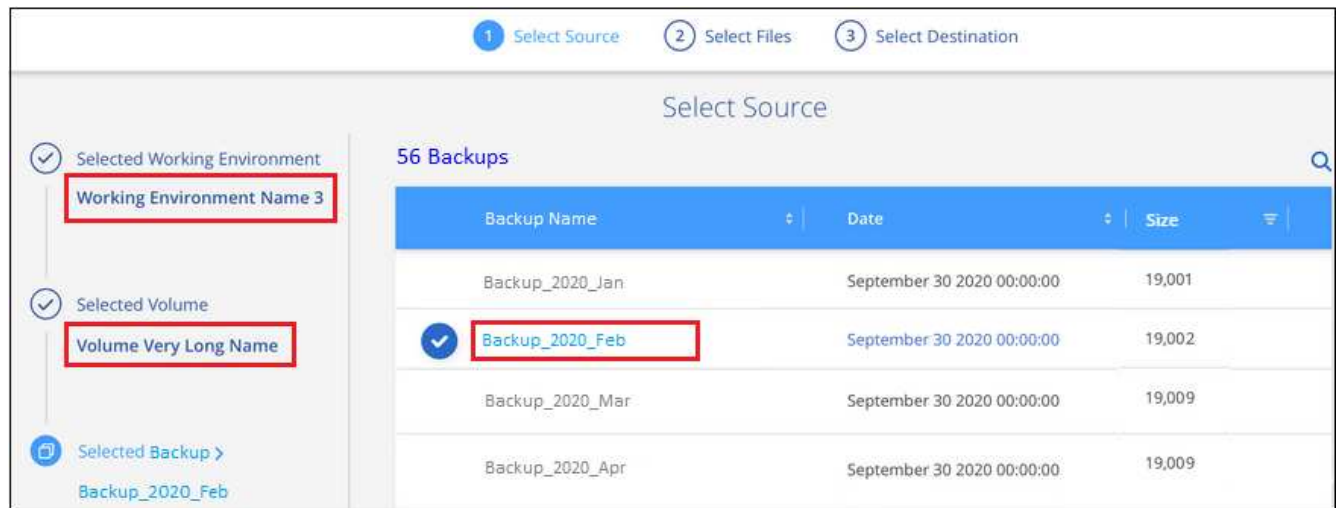
### Steps

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

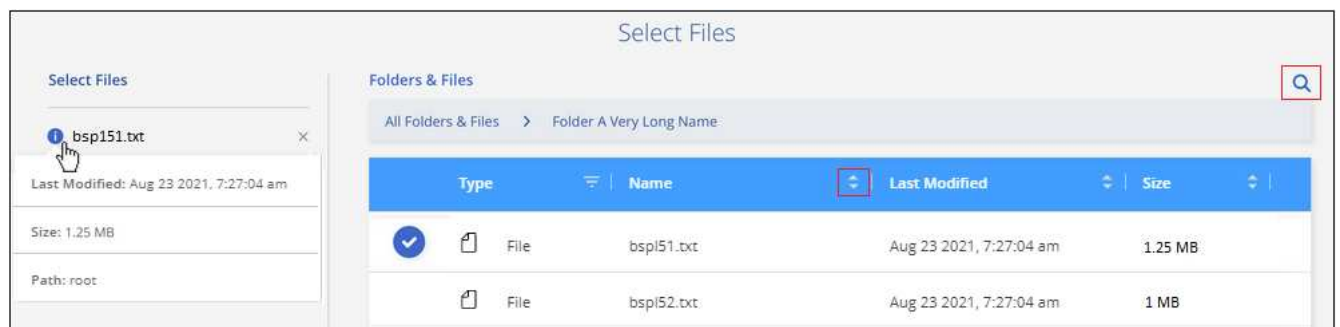
- From the *Browse & Restore* section, click **Restore Files**.




- 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.



- Click **Continue** and the list of folders and files from the volume backup are displayed.

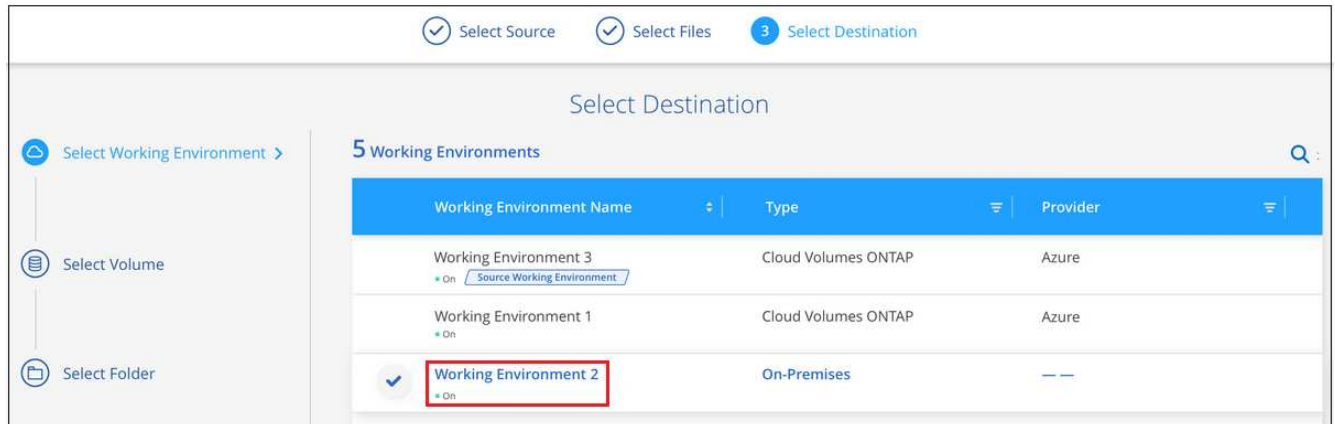


6. In the *Select Files* page, select the file or files that you want to restore and click **Continue**. To assist you in finding the file:

- 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.

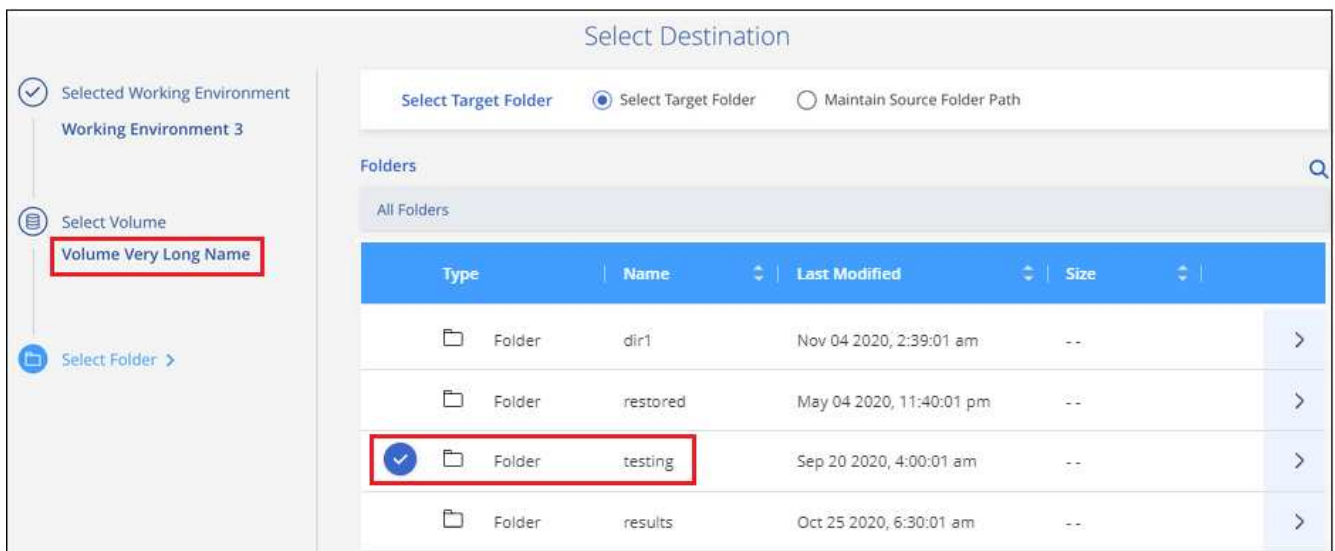
7. In the *Select Destination* page, select the **Working Environment** where you want to restore the files.



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 Google Cloud Storage, enter the IPspace in the ONTAP cluster where the destination volumes reside, and the Access Key and Secret Key needed to access the object storage.
- When restoring from StorageGRID, enter the FQDN of the StorageGRID server and the port that ONTAP should use for HTTPS communication with StorageGRID, enter the Access Key and Secret Key needed to access the object storage, and 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.

## Restoring ONTAP data using Search & Restore

You can restore a volume or individual files from an ONTAP 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.

The search operation also looks across all local Snapshot copies that exist for your ONTAP volumes too. Since restoring data from a local Snapshot copy can be faster and less costly than restoring from a backup file, you may want to restore data from the Snapshot. You can restore the Snapshot as a new volume from the Volume Details page on the Canvas.

When you restore a volume from a backup file, Cloud Backup creates a *new* volume using the data from the backup. You can restore the data as a volume in the original 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 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, and that file restore from archival storage is not currently supported.

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

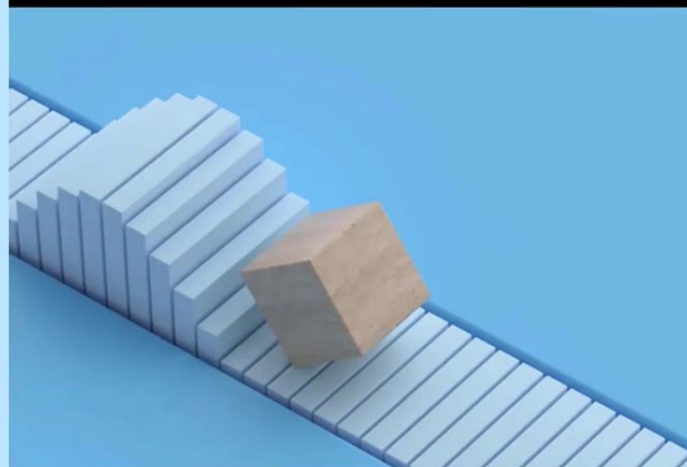
The following video shows a quick walkthrough of restoring a single file:

# Cloud Backup : Search and Restore

Indexed Catalog Preview Feature

February 2022

© 2022 NetApp, Inc. All rights reserved.



## 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
Google Cloud Storage	Cloud Volumes ONTAP in Google On-premises ONTAP system	Cloud Volumes ONTAP in Google On-premises ONTAP system
NetApp StorageGRID	Not currently supported	

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.
- Google Cloud requirements:
  - Specific Google BigQuery permissions must be added to the user role that provides Cloud Manager with permissions. [Make sure all the permissions are configured correctly.](#)

Note that if you were already using Cloud Backup with a Connector you configured in the past, you'll



need to add the BigQuery permissions to the Cloud Manager user role now. These are new, and they are required for Search & Restore.

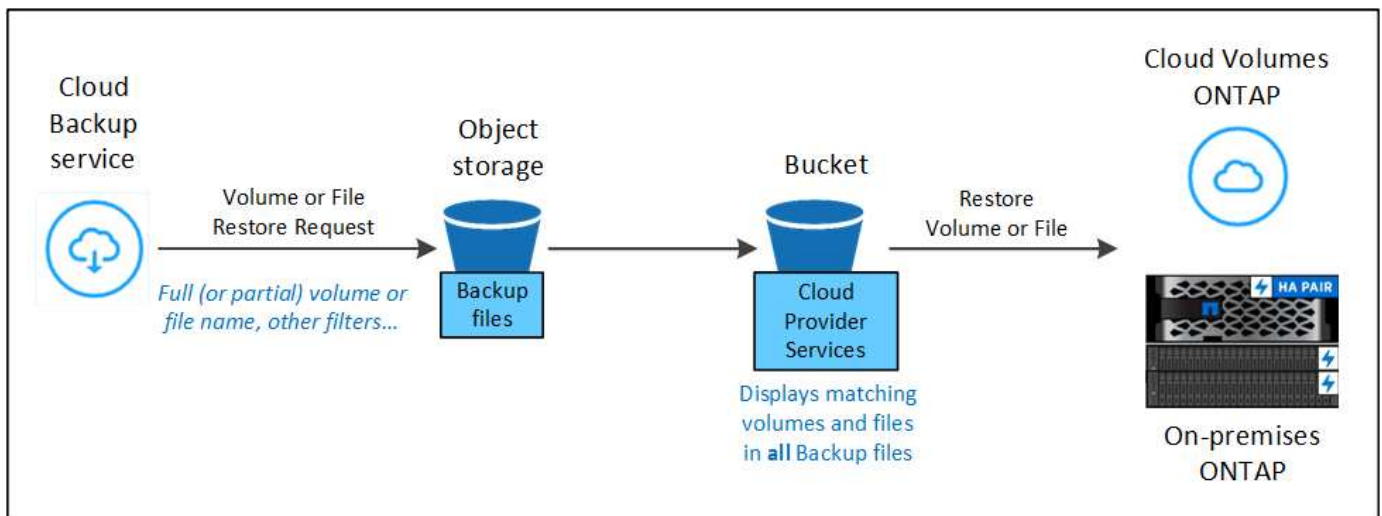
## Search & Restore process

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.
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 locations that have a file or volume that matches your search criteria.

4. Click **View All Backups** for the location 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 performs the following actions:

- For backups stored in Google Cloud, it provisions a new bucket, and the [Google Cloud BigQuery services](#)

are provisioned on an account/project level.

If Indexing has already been enabled 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".

The image shows a composite screenshot of the AWS Backup console's 'Search & Restore' section. It illustrates the steps to enable indexing for working environments. At the top, two panels show the 'Search & Restore' header and a description: 'Globally search for volumes and files by name, parts of the name, or path, across selected working environments for instant recovery.' The left panel shows a button 'Enable Indexing for Working Environments' highlighted with a red box. The right panel shows an 'Indexing Settings' link highlighted with a red box. Red arrows point from these elements to a larger screenshot below. This larger screenshot shows the 'Indexing Settings for Working Environments' page. It includes a table with three working environments. The first is 'Active', the second is 'Not Active' with an 'Enable Indexing' button highlighted in a red box, and the third is 'In Progress'.

Indexing Settings for Working Environments		
Enable Indexing for each working environment where you'll want to use Search & Restore.		
	<b>Working Environment Name # 1</b> Cloud Volumes ONTAP   ● On	✔ Active Index Catalog Status
	<b>Working Environment Name # 2</b> Cloud Volumes ONTAP   ● On	⊖ Not Active Index Catalog Status <b>Enable Indexing</b>
	<b>Working Environment Name # 3</b> Cloud Volumes ONTAP   ● On	🔄 In Progress Index Catalog Status Enable Indexing

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 transparently updated hourly with incremental changes to stay current.

## Restoring volumes and files using Search & Restore

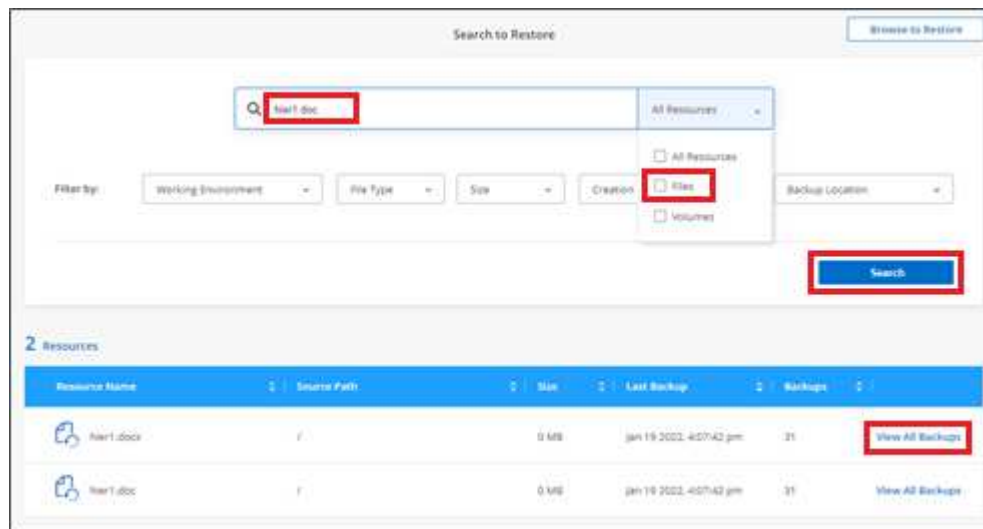
After you have [enabled Indexing for your working environment](#), you can restore volumes or files using Search & Restore. This allows you to use a broad range of filters to find the exact file or volume that you want to restore from all backup files.

### Steps

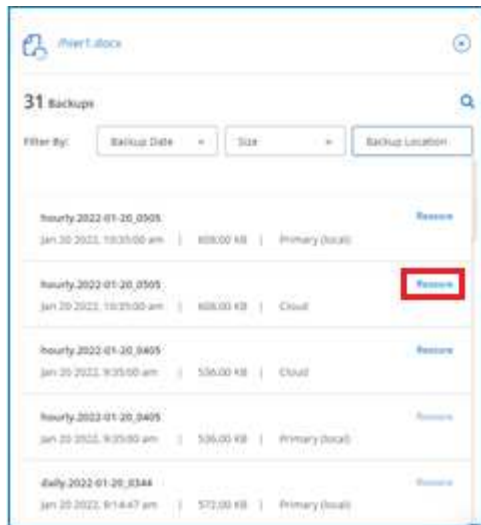
1. Select the **Backup & Restore** service.
2. Click the **Restore** tab and the Restore Dashboard is displayed.
3. From the *Search & Restore* section, click **Search & Restore**.



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 from the cloud.

Note that the results also identify local volume Snapshot copies that contain the file in your search. The **Restore** button is not functional for Snapshots at this time, but if you want to restore the data from the Snapshot copy instead of from the Backup file, write down the name and location of the volume, open the Volume Details page on the Canvas, and use the **Restore from Snapshot copy** option.

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.

## Copyright Information

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

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

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

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

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

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

## Trademark Information

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