



Cloud Backup documentation

Cloud Backup

NetApp
July 14, 2022

This PDF was generated from <https://docs.netapp.com/us-en/cloud-manager-backup-restore/aws/index.html> on July 14, 2022. Always check docs.netapp.com for the latest.

Table of Contents

Cloud Backup documentation	1
What's new with Cloud Backup	2
13 July 2022	2
14 June 2022	2
8 June 2022	2
2 May 2022	3
4 April 2022	4
3 March 2022	4
14 February 2022	5
2 January 2022	5
28 November 2021	5
5 November 2021	6
4 October 2021	6
2 September 2021	7
1 August 2021	7
7 July 2021	7
7 June 2021	8
5 May 2021	8
Get started	10
Learn about Cloud Backup	10
Set up licensing for Cloud Backup	12
Back up and restore ONTAP data	18
Protect your ONTAP cluster data using Cloud Backup	18
Backing up Cloud Volumes ONTAP data to Amazon S3	24
Backing up on-premises ONTAP data to Amazon S3	32
Backing up on-premises ONTAP data to StorageGRID	44
Managing backups for your ONTAP systems	51
Restoring ONTAP data from backup files	65
Back up and restore Kubernetes data	82
Protect your Kubernetes cluster data using Cloud Backup	82
Backing up Kubernetes persistent volume data to Amazon S3	85
Managing backups for your Kubernetes systems	92
Restoring Kubernetes data from backup files	103
Back up and restore on-premises applications data	105
Protect your on-premises applications data	105
Back up on-premises applications data to cloud	106
Manage protection of applications	109
Restore applications data	112
Back up and restore Virtual Machines data	115
Protect your virtual machines data	115
Back up datastores to the cloud	117
Manage protection of virtual machines	118
Restore virtual machines from the cloud	120

Cloud Backup APIs	121
Getting started	121
Example using the APIs	123
API reference	126
Reference	127
AWS S3 archival storage classes and restore retrieval times	127
Azure archival tiers and restore retrieval times	128
Cross-account and cross-region configurations	129
Knowledge and support	145
Register for support	145
Get help	146
Legal notices	148
Copyright	148
Trademarks	148
Patents	148
Privacy policy	148
Open source	148

Cloud Backup documentation

What's new with Cloud Backup

Learn what's new in Cloud Backup.

13 July 2022

Support has been added to back up SnapLock Enterprise volumes

Now you can use Cloud Backup to back up SnapLock Enterprise volumes to public and private clouds. This feature requires that your ONTAP system is running ONTAP 9.11.1 or later. SnapLock Compliance volumes, however, aren't currently supported.

Now you can create backup files in the public cloud when using an on-premises Connector

In the past you needed to deploy the Connector in the same cloud provider as where you were creating backup files. Now you can use a Connector deployed in your premises to create backup files from on-prem ONTAP systems to Amazon S3, Azure Blob, and Google Cloud Storage. (An on-prem Connector was always required when creating backup files on StorageGRID systems.)

Additional features are available when creating backup policies for ONTAP systems

- Backup on a yearly schedule is now available. The default retention value is 1 for yearly backups, but you can change this value if you want to have access to many previous years' backup files.
- You can name your backup policies so you can identify your policies with more descriptive text.

14 June 2022

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

If your on-prem ONTAP cluster resides in a site with no internet access, also known as a dark site or offline site, now you can use Cloud Backup to back up volume data to a NetApp StorageGRID system that resides in the same site. This functionality requires that the Cloud Manager Connector (version 3.9.19 or greater) is also deployed in the offline site.

[See how to install the Connector in your offline site.](#)

[See how to back up ONTAP data to StorageGRID in your offline site.](#)

8 June 2022

Cloud Backup for Virtual Machines 1.1.0 is now GA

You can protect data on your virtual machines by integrating the SnapCenter Plug-in for VMware vSphere with Cloud Manager. You can back up datastores to the cloud and restore virtual machines back to the on-premises SnapCenter Plug-in for VMware vSphere with ease.

[Learn more about protecting virtual machines to cloud.](#)

Cloud Restore instance is not needed for ONTAP Browse & Restore functionality

A separate Cloud Restore instance/virtual machine used to be required for file-level Browse & Restore operations from S3 and Blob storage. This instance shut down when not in use — but it still added some time and cost when restoring files. This functionality has been replaced with a no-cost container that gets deployed on the Connector when needed. It provides the following advantages:

- No added cost for file-level restore operations
- Faster file-level restore operations
- Support for Browse & Restore operations for files from the cloud when the Connector is installed on your premises

Note that the Cloud Restore instance/VM will be removed automatically if you were previously using it. A Cloud Backup process will run once a day to delete all old Cloud Restore instances. This change is completely transparent — there is no effect on your data, and you won't notice any changes to your backup or restore jobs.

Browse & Restore support for files from Google Cloud and StorageGRID storage

With the addition of the container for Browse & Restore operations (as described above), file restore operations now can be performed from backup files stored in Google Cloud and StorageGRID systems. Now Browse & Restore can be used to restore files across all public cloud providers and from StorageGRID. [See how to use Browse & Restore to restore volumes and files from your ONTAP backups.](#)

Drag and drop to enable Cloud Backup to S3 storage

If the Amazon S3 destination for your backups exists as a working environment on the Canvas, you can drag your on-prem ONTAP cluster or Cloud Volumes ONTAP system (installed in AWS) onto the Amazon S3 working environment to initiate the setup wizard.

Automatically apply a backup policy to newly created volumes in Kubernetes clusters

If you added new persistent volumes to your Kubernetes clusters after Cloud Backup was activated, in the past you needed to remember to configure backups for those volumes. Now you can select a policy that will be applied automatically to newly created volumes [from the Backup Settings page](#) for clusters that have already activated Cloud Backup.

Cloud Backup APIs are now available for managing backup and restore operations

The APIs are available at <https://docs.netapp.com/us-en/cloud-manager-automation/cbs/overview.html>. See [this page](#) for an overview of the APIs.

2 May 2022

Search & Restore is now supported with backup files in Google Cloud Storage

The Search & Restore method of restoring volumes and files was introduced in April for users who store their backup files in AWS. Now the capability is available for users who store their backup files in Google Cloud Storage. [See how to restore your volumes and files using Search & Restore.](#)

Configure a backup policy to be applied automatically to newly created volumes in Kubernetes clusters

If you added new persistent volumes to your Kubernetes clusters after Cloud Backup was activated, in the past you needed to remember to configure backups for those volumes. Now you can select a policy that will be applied automatically to newly created volumes. This option is available in the setup wizard when activating Cloud Backup for a new Kubernetes cluster.

Cloud Backup now requires a license before being activated on a working environment

There are a few changes to how licensing is implemented with Cloud Backup:

- You must sign up for a PAYGO Marketplace subscription from your cloud provider, or purchase a BYOL license from NetApp, before you can activate Cloud Backup.
- The 30-day Free Trial is available only when using a PAYGO subscription from your cloud provider - it is not available when using the BYOL license.
- The Free Trial starts the day the Marketplace subscription starts. For example, if you activate the Free Trial after you have been using a Marketplace subscription for 30 days for a Cloud Volumes ONTAP system, the Cloud Backup Trial will not be available.

[Learn more about the available licensing models.](#)

4 April 2022

Cloud Backup for Applications 1.1.0 (powered by SnapCenter) is now GA

The new Cloud Backup for Applications capability enables you to offload existing application consistent Snapshots (backups) for Oracle and Microsoft SQL from on-premises primary storage to cloud object storage in Amazon S3 or Azure Blob.

When required, you can restore this data from cloud to on-premises.

[Learn more about protecting on-premises applications data to the cloud.](#)

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

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

3 March 2022

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

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

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

14 February 2022

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

In the past you could assign only a single backup policy to all volumes in a cluster. Now you can create multiple backup policies for a single cluster and apply different policies to different volumes. [See how to create new backup policies for a cluster and assign them to selected volumes.](#)

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

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

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

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

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

2 January 2022

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

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

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

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

28 November 2021

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

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

Enhanced functionality to back up DP volumes

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

5 November 2021

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

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

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

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

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

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

4 October 2021

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

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

TCO calculator is available to compare Cloud Backup costs

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

Ability to unregister Cloud Backup for a working environment

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

2 September 2021

Ability to create an on-demand backup of a volume

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

[See how to create an on-demand backup.](#)

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

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

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

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

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

1 August 2021

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

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

An Hourly backup policy is now supported

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

7 July 2021

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

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

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

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

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

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

7 June 2021

Limitations lifted for DP volumes when using ONTAP 9.8 or greater

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

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

5 May 2021

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

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

Now you can use System Manager to perform Cloud Backup operations

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

Backup policies have been improved with a few enhancements

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

Miscellaneous backup and restore improvements

- When configuring the cloud destination for your backup files, now you can select a different region than the region in which the Cloud Volumes ONTAP system resides.

- The number of backup files you can create for a single volume has been increased from 1,019 to 4,000.
- In addition to the earlier ability to delete all backup files for a single volume, now you can delete just a single backup file for a volume, or you can delete all backup files for an entire working environment, if needed.

Get started

Learn about Cloud Backup

Cloud Backup is a service for Cloud Manager working environments that provides backup and restore capabilities for protection and long-term archive of your data. Backups are automatically generated and stored in an object store in your public or private cloud account.

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

[Learn more about Cloud Backup.](#)

Backup & Restore can be used to:

- Back up and Restore ONTAP volumes from Cloud Volumes ONTAP and on-premises ONTAP systems. [See detailed features here.](#)
- Back up and Restore Kubernetes persistent volumes. [See detailed features here.](#)
- Back up the application consistent Snapshots from on-premises ONTAP to cloud using Cloud Backup for Applications. [See detailed features here.](#)
- Back up datastores to the cloud and restore virtual machines back to the on-premises vCenter using Cloud Backup for VMware. [See detailed features here.](#)



When the Cloud Manager Connector is deployed in a Government region in the cloud, or in a site without internet access (a dark site), Cloud Backup only supports backup and restore operations from ONTAP systems. When using these alternate deployment methods, Cloud Backup does not support backup and restore operations from Kubernetes clusters, Applications, or Virtual Machines.

How Cloud Backup works

When you enable Cloud Backup on a Cloud Volumes ONTAP or on-premises ONTAP system, the service performs a full backup of your data. Volume snapshots are not included in the backup image. After the initial backup, all additional backups are incremental, which means that only changed blocks and new blocks are backed up. This keeps network traffic to a minimum.

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

The following image shows the relationship between each component:



Where backups reside

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

- In AWS, Cloud Manager enables the [Amazon S3 Block Public Access feature](#) on the S3 bucket.
- In StorageGRID, Cloud Manager uses an existing storage account for the object store bucket.

Backups are taken at midnight

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

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

Backup copies are associated with your NetApp account

Backup copies are associated with the [NetApp account](#) in which the Connector resides.

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

Set up licensing for Cloud Backup

You can license Cloud Backup by purchasing a pay-as-you-go (PAYGO) marketplace subscription from your cloud provider, or by purchasing a bring-your-own-license (BYOL) from NetApp. A valid license is required to activate Cloud Backup on a working environment, to create backups of your production data, and to restore backup data to a production system.

A few notes before you read any further:

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

[Learn more about the costs related to using Cloud Backup.](#)

30-day free trial

A Cloud Backup 30-day free trial is available from the pay-as-you-go subscription in your cloud provider's marketplace. The free trial starts at the time that you subscribe to the marketplace listing. Note that if you pay for the marketplace subscription when deploying a Cloud Volumes ONTAP system, and then start your Cloud Backup free trial 10 days later, you'll have 20 days to use the free trial.

When the free trial ends, you'll be switched over automatically to the PAYGO subscription without interruption. If you decide not to continue using Cloud Backup, just [unregister Cloud Backup from the working environment](#) before the trial ends and you won't be charged.

Use a Cloud Backup PAYGO subscription

For pay-as-you-go, you'll pay your cloud provider for object storage costs and for NetApp backup licensing costs on an hourly basis in a single subscription. You should subscribe even if you have a free trial or if you bring your own license (BYOL):

- Subscribing ensures that there's no disruption of service after your free trial ends. When the trial ends, you'll be charged hourly according to the amount of data that you back up.
- If you back up more data than allowed by your BYOL license, then data backup continues through your pay-as-you-go subscription. For example, if you have a 10 TiB BYOL license, all capacity beyond the 10 TiB is charged through the PAYGO subscription.

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

There are a few PAYGO plans for Cloud Backup:

- A "Cloud Backup" package that enables you to back up Cloud Volumes ONTAP data and on-premises ONTAP data.
- A "CVO Professional" package that enables you to bundle Cloud Volumes ONTAP and Cloud Backup. This includes unlimited backups for Cloud Volumes ONTAP volumes charged against this license (backup capacity is not counted against the license). This option doesn't enable you to back up on-premises ONTAP data.

[Learn more about these capacity-based license packages.](#)

Use these links to subscribe to Cloud Backup from your cloud provider marketplace:

- AWS: [Go to the Cloud Manager Marketplace offering for pricing details.](#)

Use an annual contract

Pay for Cloud Backup annually by purchasing an annual contract.

When using AWS, there are two annual contracts available from the [AWS Marketplace page](#) for Cloud Volumes ONTAP and on-premises ONTAP systems. They're available in 1-, 2-, or 3-year terms:

- A "Cloud Backup" plan that enables you to back up Cloud Volumes ONTAP data and on-premises ONTAP data.

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

- A "CVO Professional" plan that enables you to bundle Cloud Volumes ONTAP and Cloud Backup. This includes unlimited backups for Cloud Volumes ONTAP volumes charged against this license (backup capacity is not counted against the license). This option doesn't enable you to back up on-premises ONTAP data.

See the [Cloud Volumes ONTAP licensing topic](#) to learn more about this licensing option.

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

Use a Cloud Backup BYOL license

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

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

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

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

You use the Digital Wallet page in Cloud Manager to manage BYOL licenses. You can add new licenses, update existing licenses, and view license status from the Digital Wallet.

Obtain your Cloud Backup license file

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

If you're running Cloud Backup in an on-premises site that doesn't have internet access, meaning that you've deployed the Cloud Manager Connector on a host in the offline on-premises site, you'll need to obtain the license file from an internet-connected system. Activating the license using the serial number and NSS account is not available for offline (dark site) installations.

Steps

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

Software Licenses

Serial Number

481*

Serial #	Cluster SN	License Name	License Key	Host ID	Value	End Date
Serial #	Cluster SN	License Name		Host ID	Value	End Date
4810		CLOUD_BKP_SERVICE	Get NetApp License File		100	12/31/9998

- 3. In the **License Key** column, click **Get NetApp License File**.
- 4. Enter your Cloud Manager Account ID (this is called a Tenant ID on the support site) and click **Submit** to download the license file.

Get License

SERIAL NUMBER:

4810

LICENSE:

CLOUD_BKP_SERVICE

SALES ORDER:

3005

TENANT ID:

Enter Tenant ID

Example: account-xxxxxxxx

Cancel

Submit

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

Add Cloud Backup BYOL licenses to your account

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

Steps

1. From the Cloud Manager left navigation menu, click **Digital Wallet** and then select the **Data Services Licenses** tab.
2. Click **Add License**.
3. In the *Add License* dialog, enter the license information and click **Add License**:

- If you have the backup license serial number and know your NSS account, select the **Enter Serial Number** option and enter that information.

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

- If you have the backup license file (required when installed in a dark site), select the **Upload License File** option and follow the prompts to attach the file.

The image displays two screenshots of the 'Add Cloud Backup License' dialog box. The left screenshot shows the 'Enter Serial Number' option selected, with fields for 'Serial Number' and 'NetApp Support Site Account'. The right screenshot shows the 'Upload License File' option selected, with instructions and an 'Upload' button.

Add Cloud Backup License

A Backup License must be installed with an active subscription. A Backup license enables you to use Cloud Backup for a certain period of time and for a maximum amount of backup space.

☒ Enter Serial Number ☐ Upload License File

Serial Number

Enter Serial Number

NetApp Support Site Account

Select Support Site Account

Add Backup License Cancel

☐ Enter Serial Number ☒ Upload License File

To install a license, follow these instructions:

- 1 Obtain the license file from the "System > Software Licenses" tab at [NetApp Support Site](#). You will need to provide your cloud service serial number and Cloud Manager Account ID.
- 2 Click Upload File and then select the file.

Upload License File

Upload License File

Upload

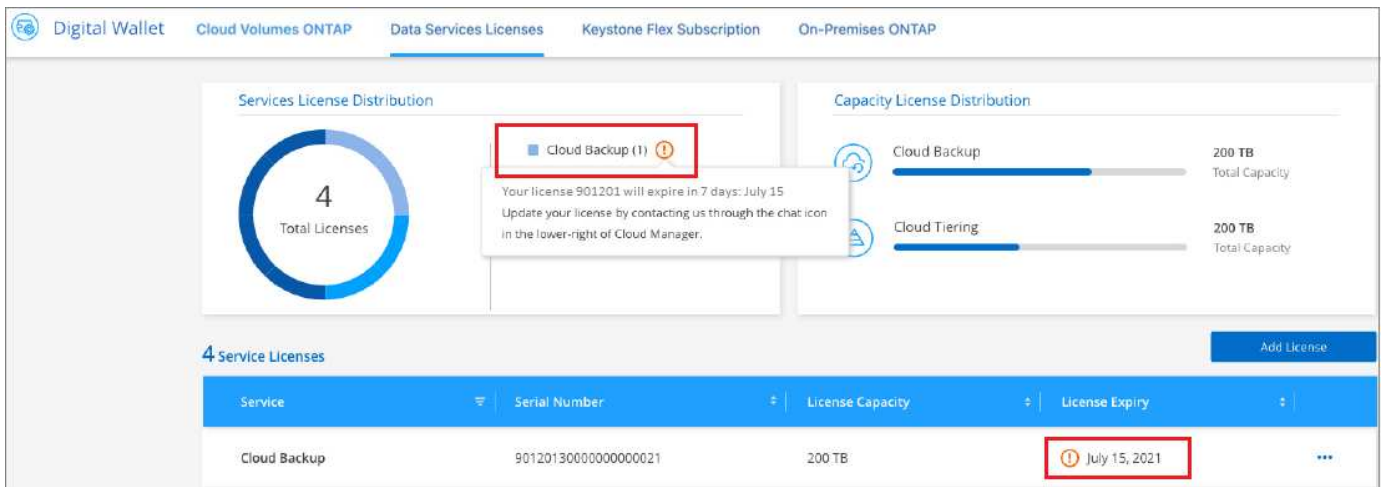
Add Backup License Cancel

Result

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

Update a Cloud Backup BYOL license

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



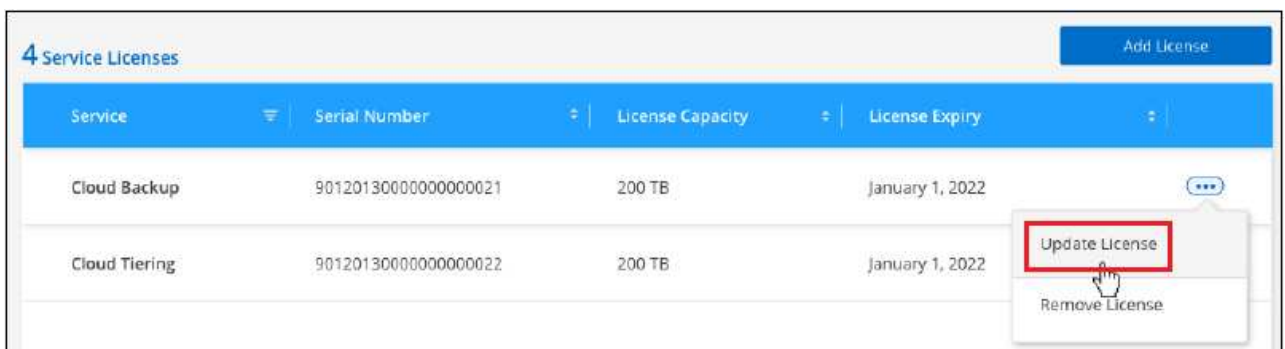
You can update your Cloud Backup license before it expires so that there is no interruption in your ability to back up and restore your data.

Steps

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

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

2. If Cloud Manager can't automatically update the license (for example, when installed in a dark site), then you'll need to manually upload the license file.
 - a. You can [obtain the license file from the NetApp Support Site](#).
 - b. On the Digital Wallet page *Data Services Licenses* tab, click ... for the service serial number you are updating, and click **Update License**.



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

Result

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

BYOL license considerations

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

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

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

Two things can happen when your BYOL license expires:

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

Once you renew your BYOL subscription, Cloud Manager automatically updates the license. If Cloud Manager can't access the license file over the secure internet connection (for example, when installed in a dark site), you can obtain the file yourself and manually upload it to Cloud Manager. For instructions, see [how to update a Cloud Backup license](#).

Systems that were shifted over to a PAYGO license are returned to the BYOL license automatically. And systems that were running without a license will stop seeing the warnings.

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.
- Name your backup policies so it is easy to see what each policy is used for.
- 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 AWS	Amazon S3

Source Working Environment	Backup File Destination
On-premises ONTAP system	Amazon S3 NetApp StorageGRID

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

Backup File	Destination Working Environment	
Location	Volume Restore	File Restore
Amazon S3	Cloud Volumes ONTAP in AWS On-premises ONTAP system	Cloud Volumes ONTAP in AWS On-premises ONTAP system
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. Both volume and file restore are also supported in this configuration. In this case, you'll need to deploy the Cloud Manager Connector (minimum version 3.9.20) 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 AWS, [Amazon Athena](#) and [AWS Glue](#) resources are deployed in a new S3 bucket.
- 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 with the following consumption models:

- **BYOL**: A license purchased from NetApp that can be used with any cloud provider.
- **PAYGO**: An hourly subscription from your cloud provider's marketplace.
- **Annual**: An annual contract from your cloud provider's marketplace.



If you purchase a BYOL license from NetApp, you also need to subscribe to the PAYGO offering from your cloud provider's marketplace. Your license is always charged first, but you'll be charged from the hourly rate in the marketplace in these cases:

- If you exceed your licensed capacity
- If the term of your license expires

If you have an annual contract from a marketplace, all Cloud Backup consumption is charged against that contract. You can't mix and match an annual marketplace contract with a BYOL.

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.](#)

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.](#)

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

Annual contract

When using AWS, two annual contracts are available for 12, 24, or 36 month terms:

- A "Cloud Backup" plan that enables you to back up Cloud Volumes ONTAP data and on-premises ONTAP data.

- A "CVO Professional" plan that enables you to bundle Cloud Volumes ONTAP and Cloud Backup. This includes unlimited backups for Cloud Volumes ONTAP volumes charged against this license (backup capacity is not counted against the license).

[Learn how to set up annual contracts.](#)

How Cloud Backup works

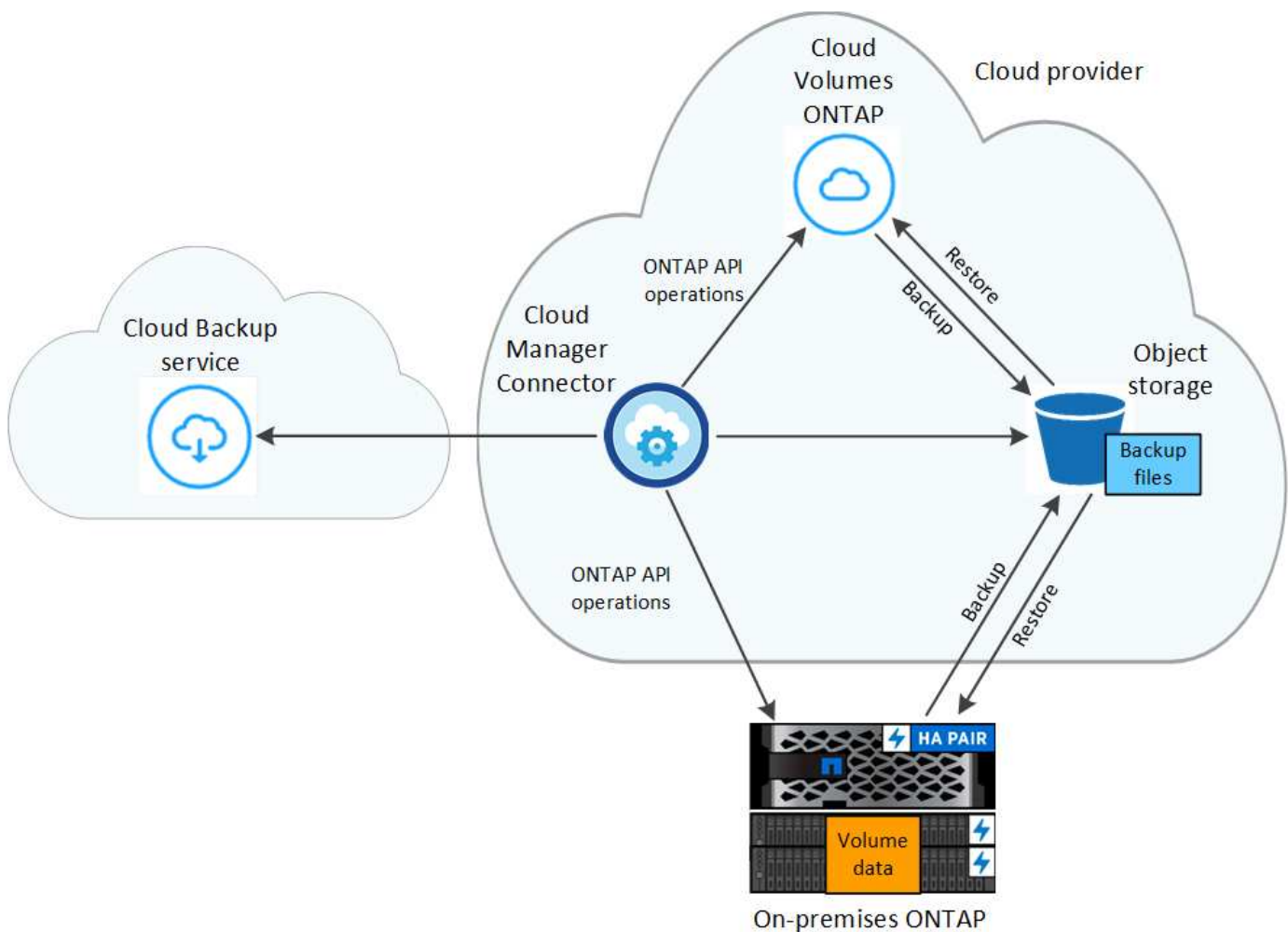
When you enable Cloud Backup on a Cloud Volumes ONTAP or on-premises ONTAP system, the service performs a full backup of your data. Volume snapshots are not included in the backup image. After the initial backup, all additional backups are incremental, which means that only changed blocks and new blocks are backed up. This keeps network traffic to a minimum.

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



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

The following image shows the relationship between each component:



Where backups reside

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

- In AWS, Cloud Manager enables the [Amazon S3 Block Public Access feature](#) on the S3 bucket.
- In StorageGRID, Cloud Manager uses an existing storage account for the object store bucket.

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

Supported storage classes or access tiers

- In AWS, backups start in the *Standard* storage class and transition to the *Standard-Infrequent Access* storage class after 30 days.

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

- In 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 the other volumes after Backup is activated.

You can choose a combination of hourly, daily, weekly, monthly, and yearly 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 (and so obsolete backups don't continue to take up space in the cloud).

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 the following types of volumes:

- FlexVol read-write volumes
- SnapMirror data protection (DP) destination volumes
- SnapLock Enterprise volumes (requires ONTAP 9.11.1 or later)

FlexGroup volumes and SnapLock Compliance 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 Amazon S3

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

Quick start

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

1

Verify support for your configuration

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

2

Enable Cloud Backup on your new or existing system

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



3

Enter the provider details

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

A screenshot of a 'Provider Settings' form. The form is titled 'Provider Settings' at the top center. It is divided into two main sections: 'Provider Information' on the left and 'Location & Connectivity' on the right. Under 'Provider Information', there are three fields: 'AWS Account' (a dropdown menu with 'AWS_Account_1' selected), 'AWS Access Key' (a text input field with placeholder text 'Enter AWS Access Key'), and 'AWS Secret Key' (a text input field with placeholder text 'Enter AWS Secret Key'). Under 'Location & Connectivity', there is a 'Region' dropdown menu with 'us-east-2' selected, an 'Encryption' section with a settings icon, and 'Encryption Key Type: AWS SSE-S3' with a 'Change Key' link.

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, monthly, or yearly backups, or select one of the system-defined policies that provide more options. You can also change the number of backup copies you want to retain.

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

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.

Cloud Backup will create the S3 bucket after you complete the wizard

Policy Type

☒ Create a new Policy

☐ Select an existing Policy

Name	Default_Policy_Name	⌵
Labels & Retention	30 Daily	⌵
Archival Policy	<div>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.</div> <div><input checked="" type="checkbox"/> Tier Backups to Archive</div> <div><div>Archive After (Days)</div><div>30</div></div> <div><div>Storage Class</div><div>S3 Glacier</div></div>	⌶

5

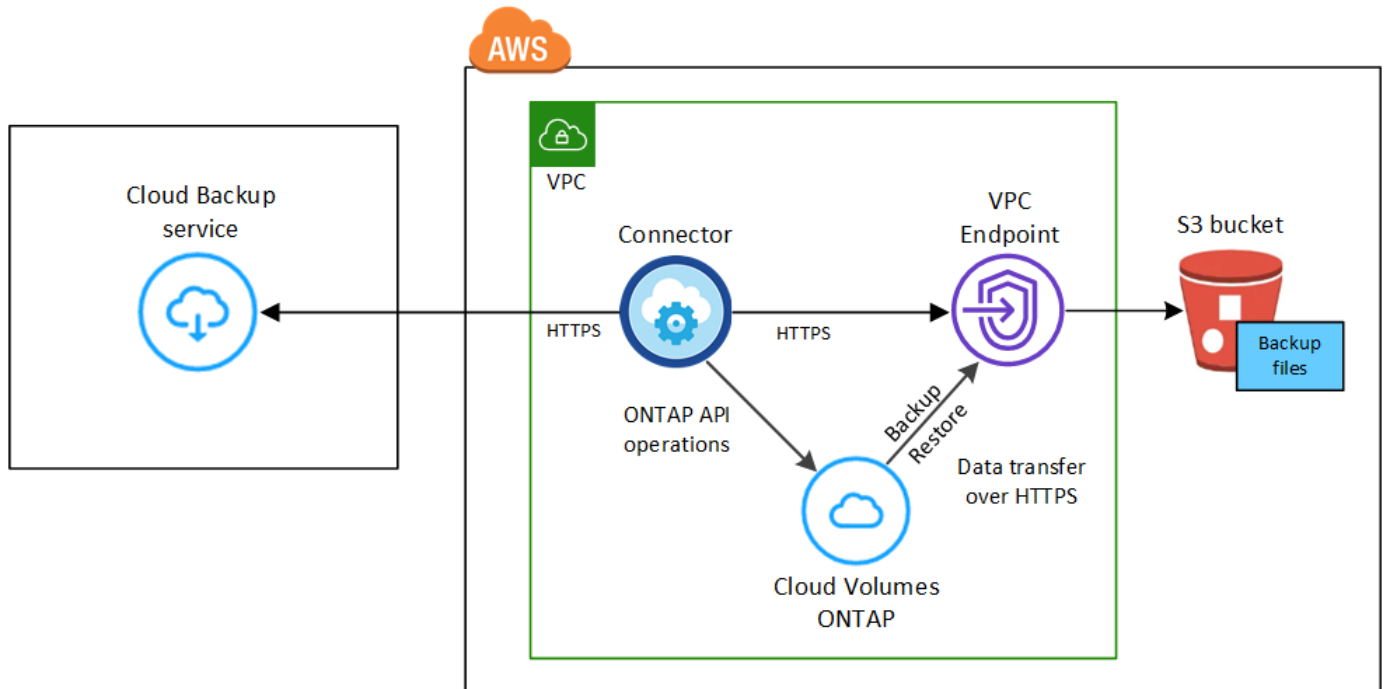
Select the volumes that you want to back up

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

Requirements

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

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



Supported ONTAP versions

Minimum of ONTAP 9.6; ONTAP 9.8P11 and later is recommended.

License requirements

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

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

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

For Cloud Backup BYOL licensing, you need the serial number from NetApp that enables you to use the service for the duration and capacity of the license. [Learn how to manage your BYOL licenses](#).

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

Supported AWS regions

Cloud Backup is supported in all AWS regions [where Cloud Volumes ONTAP is supported](#); including AWS GovCloud regions.

Required setup for creating backups in a different AWS account

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

Required information for using customer-managed keys for data encryption

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

AWS permissions required

The IAM role that provides Cloud Manager with permissions must include S3 permissions from the latest [Cloud Manager policy](#).

Here are the specific permissions from the policy:

```

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

```

If you deployed the Connector using version 3.9.15 or greater, these permissions should be part of the IAM role already. Otherwise you'll need to add the missing permissions. Specifically the "athena" and "glue" permissions, as they are required for Search & Restore.

Enabling Cloud Backup on a new system

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

See [Launching Cloud Volumes ONTAP in AWS](#) for requirements and details for creating your Cloud Volumes ONTAP system.

Steps

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



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

Result

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

What's next?

You can [start and stop backups for volumes or change the backup schedule](#).

You can also [restore entire volumes or individual files from a backup file](#) to a Cloud Volumes ONTAP system in AWS, or to an on-premises ONTAP system.

Enabling Cloud Backup on an existing system

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

Steps

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

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



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

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

- b. The region where the backups will be stored. This can be a different region than where the Cloud Volumes ONTAP system resides.

- c. Whether you'll use the default Amazon S3 encryption keys or choose your own customer-managed keys from your AWS account to manage encryption of your data. ([See how to use your own encryption keys](#)).

Provider Settings

Provider Information

AWS Account
AWS_Account_1

AWS Access Key
Enter AWS Access Key

AWS Secret Key
Enter AWS Secret Key

Location & Connectivity

Region
us-east-2

Encryption

Encryption Key Type: AWS SSE-S3 [Change Key](#)

3. Enter the backup policy details that will be used for your default policy and click **Next**. You can select an existing policy, or you can create a new policy by entering your selections in each section:
- Enter the name for the default policy. You don't need to change the name.
 - Define the backup schedule and choose the number of backups to retain. [See the list of existing policies you can choose](#).
 - When using ONTAP 9.10.1 and greater, you can choose to tier backups to either S3 Glacier or S3 Glacier Deep Archive storage after a certain number of days for further cost optimization. [Learn more about using archival tiers](#).

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.

i Cloud Backup will create the S3 bucket after you complete the wizard

Policy Type

☒ Create a new Policy ☐ Select an existing Policy

Name Default_Policy_Name

Labels & Retention 30 Daily

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.

☒ Tier Backups to Archive

Archive After (Days) 30

Storage Class S3 Glacier

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.

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
<input checked="" type="checkbox"/> 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).
- 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.
 - Click **Activate Backup** and Cloud Backup starts taking the initial backups of each selected volume.

Result

Cloud Backup starts taking the initial backups of each selected volume and the Volume Backup Dashboard is displayed so you can monitor the state of the backups.

What's next?

You can [start and stop backups for volumes or change the backup schedule](#).

You can also [restore entire volumes or individual files from a backup file](#) to a Cloud Volumes ONTAP system in AWS, or to an on-premises ONTAP system.

Backing up on-premises ONTAP data to Amazon S3

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

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

Quick start

Get started quickly by following these steps. Details for each step are provided in the following sections in this topic.

1

Identify the configuration method you'll use

Choose whether you'll connect your on-premises ONTAP cluster directly to AWS S3 over the public internet, or whether you'll use a VPN or AWS Direct Connect and route traffic through a private VPC Endpoint interface to

AWS S3.

[See the available connection methods.](#)

2

Prepare your Cloud Manager Connector

If you already have a Connector deployed in your AWS VPC or on your premises, then you're all set. If not, then you'll need to create a Connector to back up ONTAP data to AWS S3 storage. You'll also need to customize network settings for the Connector so that it can connect to AWS S3.

[See how to create a Connector and how to define required network settings.](#)

3

Prepare your on-premises ONTAP cluster

Discover your ONTAP cluster in Cloud Manager, verify that the cluster meets minimum requirements, and customize network settings so the cluster can connect to AWS S3.

[See how to get your on-premises ONTAP cluster ready.](#)

4

Prepare Amazon S3 as your backup target

Set up permissions for the Connector to create and manage the S3 bucket. You'll also need to set up permissions for the on-premises ONTAP cluster so it can read and write data to the S3 bucket.

Optionally, you can set up your own custom-managed keys for data encryption instead of using the default Amazon S3 encryption keys. [See how to get your AWS S3 environment ready to receive ONTAP backups.](#)

5

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. Then follow the setup wizard to define the default backup policy and number of backups to retain, and select the volumes you want to back up.

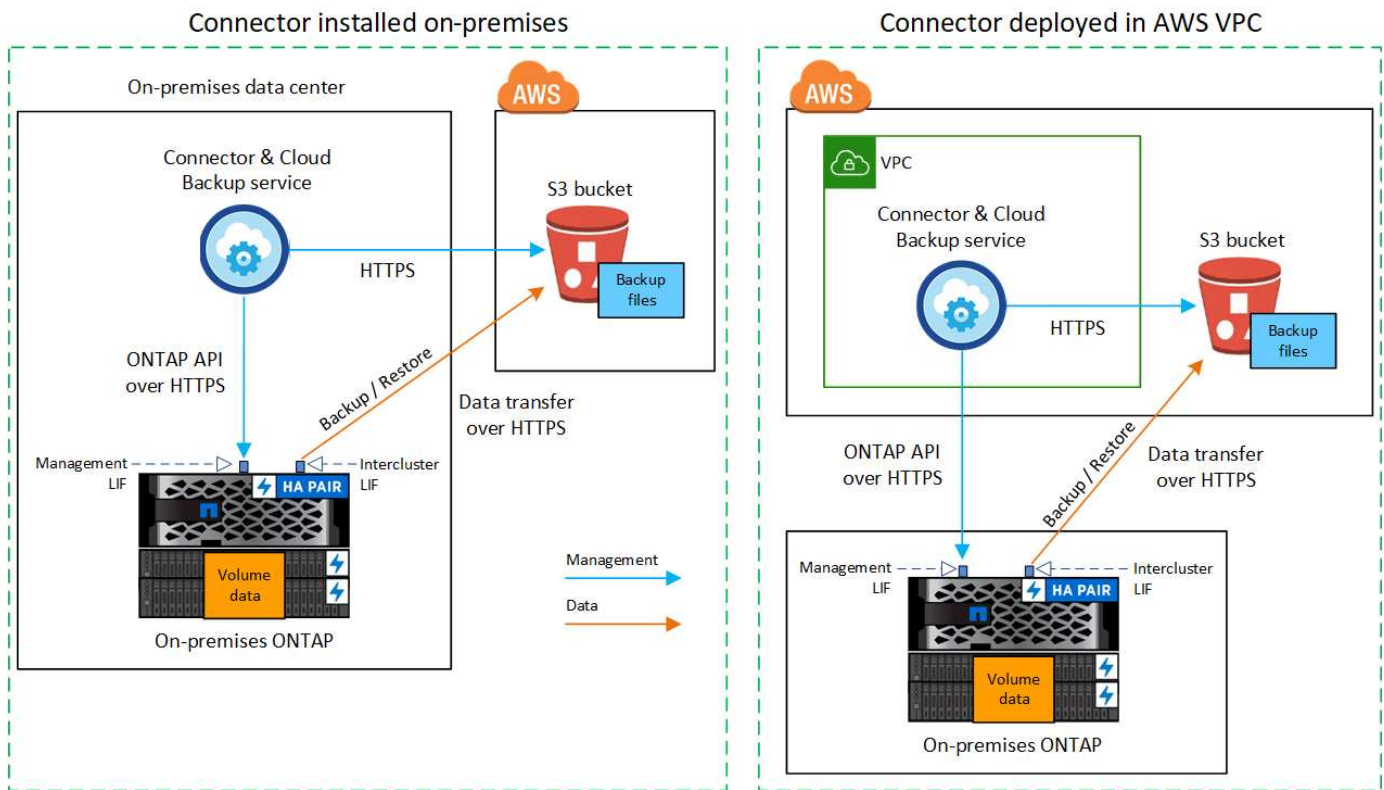
[See how to activate Cloud Backup on your volumes.](#)

Network diagrams for connection options

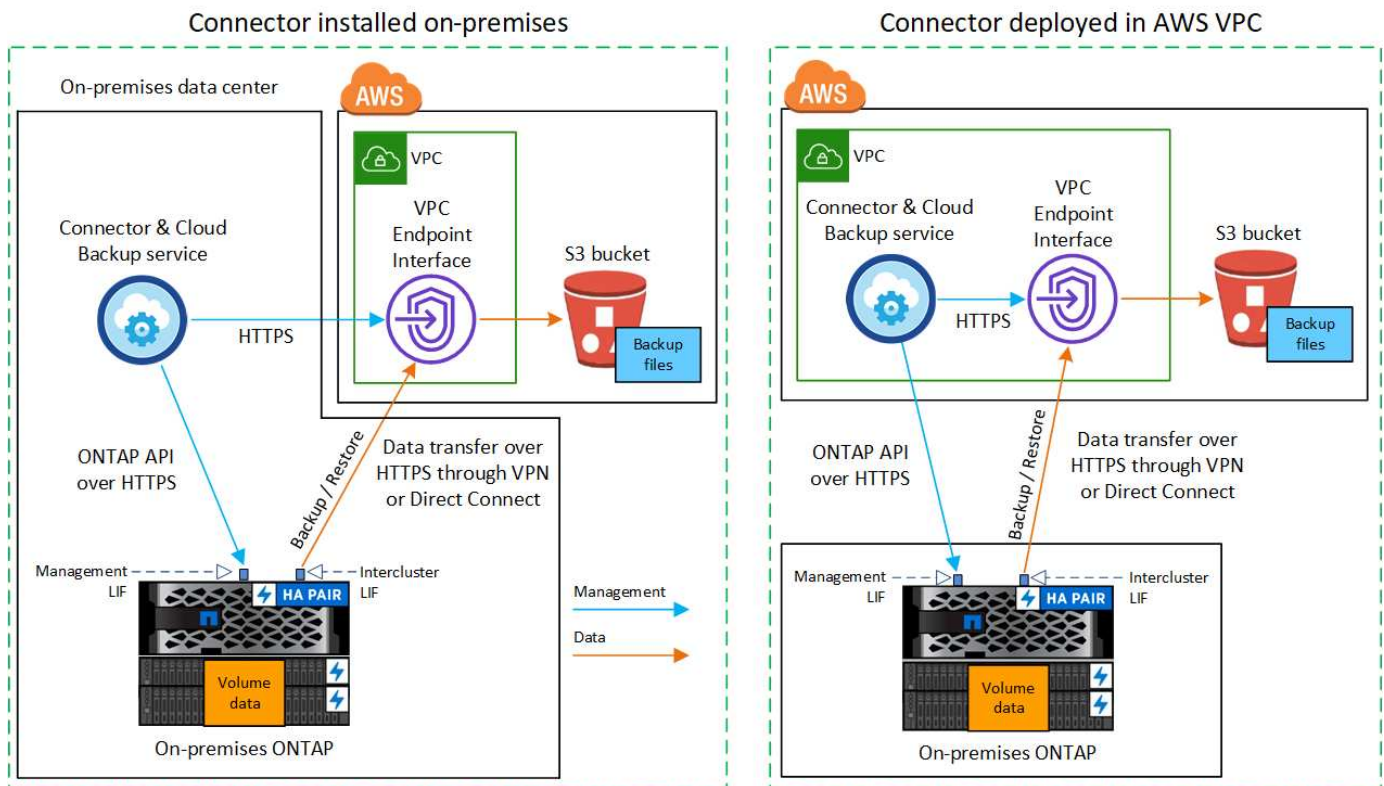
There are two connection methods you can use when configuring backups from on-premises ONTAP systems to AWS S3.

- Public connection - Directly connect the ONTAP system to AWS S3 using a public S3 endpoint.
- Private connection - Use a VPN or AWS Direct Connect and route traffic through a VPC Endpoint interface that uses a private IP address.

The following diagram shows the **public connection** method and the connections that you need to prepare between the components. You can use a Connector that you've installed on your premises, or a Connector that you've deployed in the AWS VPC.



The following diagram shows the **private connection** method and the connections that you need to prepare between the components. You can use a Connector that you've installed on your premises, or a Connector that you've deployed in the AWS VPC.



Prepare your Connector

The Cloud Manager Connector is the main software for Cloud Manager functionality. A Connector is required to back up and restore your ONTAP data.

Creating or switching Connectors

If you already have a Connector deployed in your AWS VPC or on your premises, then you're all set. If not, then you'll need to create a Connector in either of those locations to back up ONTAP data to AWS S3 storage. You can't use a Connector that's deployed in another cloud provider.

- [Learn about Connectors](#)
- [Getting started with Connectors](#)
- [Installing a Connector in AWS](#)
- [Installing a Connector in your premises](#)

Connector networking requirements

- Ensure that the network where the Connector is installed enables the following connections:
 - An HTTPS connection over port 443 to the Cloud Backup service and to your S3 object storage ([see the list of endpoints](#))
 - An HTTPS connection over port 443 to your ONTAP cluster management LIF
- [Ensure that the Connector has permissions to manage the S3 bucket.](#)
- If you have a Direct Connect or VPN connection from your ONTAP cluster to the VPC, and you want communication between the Connector and S3 to stay in your AWS internal network (a **private** connection), you'll need to enable a VPC Endpoint interface to S3. [See how to set up a VPC endpoint interface.](#)

Prepare your ONTAP cluster

Discover your ONTAP cluster in Cloud Manager

You need to discover your on-premises ONTAP cluster in Cloud Manager before you can start backing up volume data. You'll need to know the cluster management IP address and the password for the admin user account to add the cluster.

[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 cluster requires an inbound HTTPS connection from the Connector to the cluster management LIF.
- An intercluster LIF is required on each ONTAP node that hosts the volumes you want to back up. These intercluster LIFs must be able to access the object store.

The cluster initiates an outbound HTTPS connection over port 443 from the intercluster LIFs to Amazon S3 storage for backup and restore operations. ONTAP reads and writes data to and from object storage — the object storage never initiates, it just responds.

- The intercluster LIFs 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 these LIFs are associated with. That might be the "Default" IPspace or a custom IPspace that you created.

If you are using a different IPspace than "Default", then you might need to create a static route to get access to the object storage.

All intercluster LIFs within the IPspace must have access to the object store. If you can't configure this for the current IPspace, then you'll need to create a dedicated IPspace where all intercluster LIFs have access to the object store.

- DNS servers must have been configured for the storage VM where the volumes are located. See how to [configure DNS services for the SVM](#).
- Update firewall rules, if necessary, to allow Cloud Backup 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).
- If you are using a Private VPC Interface Endpoint in AWS for the S3 connection, then in order for HTTPS/443 to be used, you'll need to load the S3 endpoint certificate into the ONTAP cluster. [See how to set up a VPC endpoint interface and load the S3 certificate.](#)
- [Ensure that your ONTAP cluster has permissions to access the S3 bucket.](#)

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 AWS, or purchase and activate a Cloud Backup BYOL license from NetApp. These licenses are for your account and can be used across multiple systems.
 - For Cloud Backup PAYGO licensing, you'll need a subscription to the [AWS Cloud Manager Marketplace offering](#) to 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 an AWS subscription for the object storage space where your backups will be located.

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

Prepare your AWS environment

Set up S3 permissions

You'll need to configure two sets of permissions:

- Permissions for the Connector to create and manage the S3 bucket.
- Permissions for the on-premises ONTAP cluster so it can read and write data to the S3 bucket.

Steps

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


```

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

```

If you deployed the Connector using version 3.9.15 or greater, these permissions should be part of the IAM role already. Otherwise you'll need to add the missing permissions. Specifically the "athena" and "glue" permissions, as they're required for Search & Restore. See the [AWS Documentation: Editing IAM policies](#).

2. When activating the service, the Backup wizard will prompt you to enter an access key and secret key. These credentials are passed to the ONTAP cluster so that ONTAP can back up and restore data to the S3 bucket. For that, you'll need to create an IAM user with the following permissions:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource": "arn:aws:s3:::netapp-backup-*",
      "Effect": "Allow",
      "Sid": "backupPolicy"
    }
  ]
}

```

See the [AWS Documentation: Creating a Role to Delegate Permissions to an IAM User](#) for details.

Set up customer-managed AWS keys for data encryption

If you want to use the default Amazon S3 encryption keys to encrypt the data passed between your on-prem cluster and the S3 bucket, then you are all set because the default installation uses that type of encryption.

If you want to use your own customer-managed keys for data encryption instead of using the default keys, then you'll need to have the encryption managed keys already set up before you start the Cloud Backup wizard.

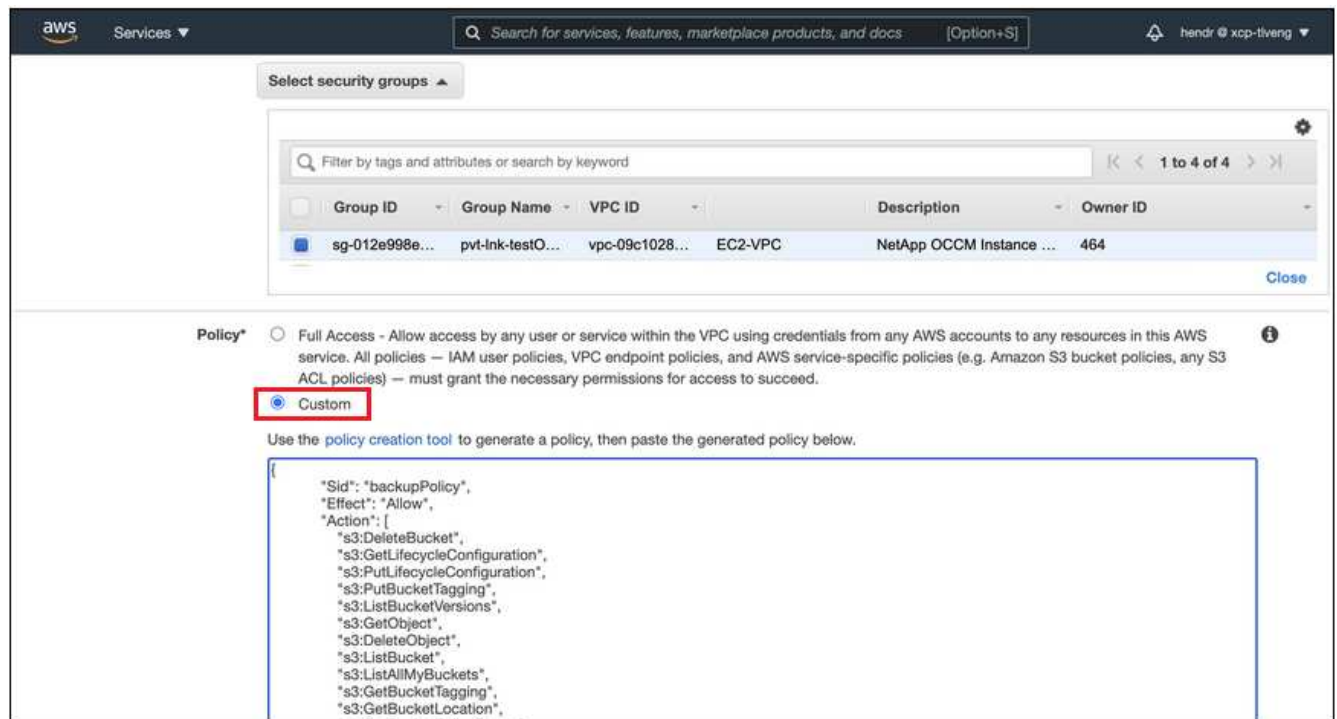
[See how to use your own keys.](#)

Configure your system for a private connection using a VPC endpoint interface

If you want to use a standard public internet connection, then all the permissions are set by the Connector and there is nothing else you need to do. This type of connection is shown in the [first diagram](#).

If you want to have a more secure connection over the internet from your on-prem data center to the VPC, there's an option to select an AWS PrivateLink connection in the Backup activation wizard. It's required if you plan to use a VPN or AWS Direct Connect to connect your on-premises system through a VPC Endpoint interface that uses a private IP address. This type of connection is shown in the [second diagram](#).

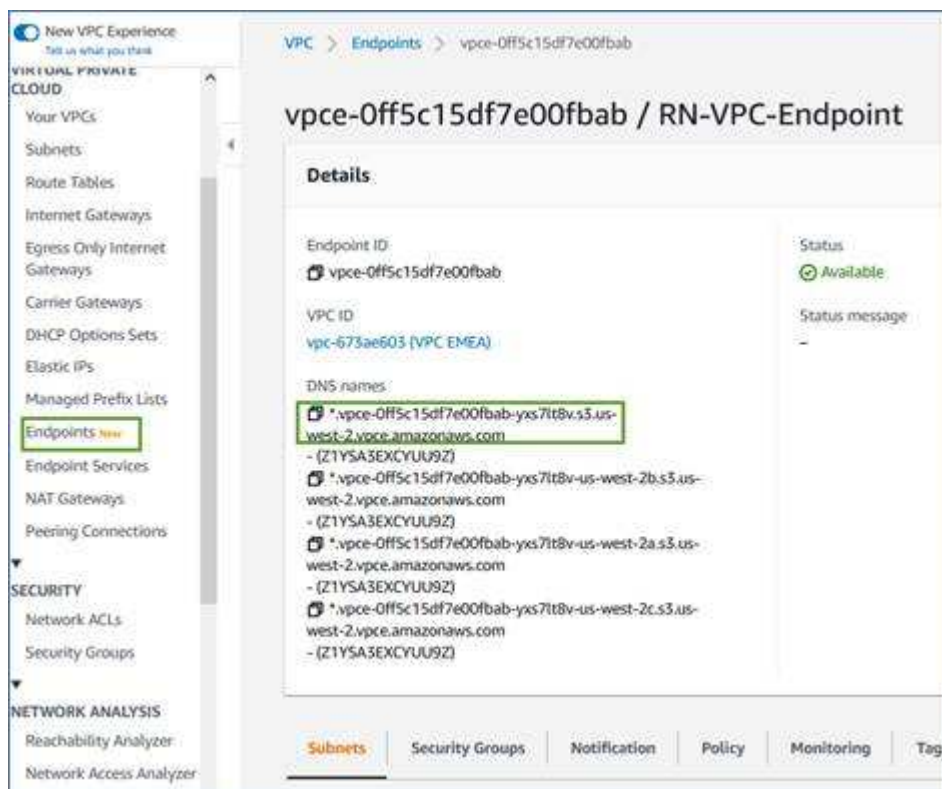
1. Create an Interface endpoint configuration using the Amazon VPC console or the command line. [See details about using AWS PrivateLink for Amazon S3.](#)
2. Modify the security group configuration that's associated with the Cloud Manager Connector. You must change the policy to "Custom" (from "Full Access"), and you must [add the S3 permissions from the backup policy](#) as shown earlier.



If you're using port 80 (HTTP) for communication to the private endpoint, you're all set. You can enable Cloud Backup on the cluster now.

If you're using port 443 (HTTPS) for communication to the private endpoint, you must copy the certificate from the VPC S3 endpoint and add it to your ONTAP cluster, as shown in the next 4 steps.

3. Obtain the DNS name of the endpoint from the AWS Console.



4. Obtain the certificate from the VPC S3 endpoint. You do this by [logging into the VM that hosts the Cloud Manager Connector](#) and running the following command. When entering the DNS name of the endpoint, add “bucket” to the beginning, replacing the “*”:

```
[ec2-user@ip-10-160-4-68 ~]$ openssl s_client -connect bucket.vpce-0ff5c15df7e00fbab-yxs7lt8v.s3.us-west-2.vpce.amazonaws.com:443 -showcerts
```

5. From the output of this command, copy the data for the S3 certificate (all data between, and including, the BEGIN / END CERTIFICATE tags):

```
Certificate chain
0 s:/CN=s3.us-west-2.amazonaws.com`
  i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
-----BEGIN CERTIFICATE-----
MIIM6zCCC9OgAwIBAgIQA7MGJ4FaDBR8uL0KR3oltTANBgkqhkiG9w0BAQsFADBG
...
...
GqvbOz/oO2NWLLFCqI+xmKLCmiPrZy+/6Af+HH2MLCM4EsI2b+IpBmPkriWnnxo=
-----END CERTIFICATE-----
```

6. Log into the ONTAP cluster CLI and apply the certificate you copied using the following command (substitute your own storage VM name):

```
cluster1::> security certificate install -vserver cluster1 -type server-ca
Please enter Certificate: Press <Enter> when done
```

Enable 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.

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



2. Select Amazon Web Services as your provider and click **Next**.


3. Enter the provider details and click **Next**.

- a. The AWS Account, the AWS Access Key, and the Secret Key used to store the backups.

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

- b. The AWS region where the backups will be stored.

- c. Whether you'll use the default Amazon S3 encryption keys, or choose your own customer-managed keys from your AWS account, to manage encryption of your data. ([See how to use your own keys](#)).



The screenshot shows the 'Provider Settings' form. It is divided into two main sections: 'Provider Information' on the left and 'Location & Connectivity' on the right. Under 'Provider Information', there are three fields: 'AWS Account' (a dropdown menu showing 'AWS_Account_1'), 'AWS Access Key' (a text input field with placeholder text 'Enter AWS Access Key'), and 'AWS Secret Key' (a text input field with placeholder text 'Enter AWS Secret Key'). Under 'Location & Connectivity', there is a 'Region' dropdown menu showing 'us-east-2'. Below the region section is an 'Encryption' section with a header and an information icon. It shows 'Encryption Key Type: AWS SSE-S3' and a 'Change Key' link with a pencil icon.

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 AWS (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. Enter the networking details and click **Next**.

- a. The IPspace in the ONTAP cluster where the volumes you want to back up reside. The intercluster LIFs for this IPspace must have outbound internet access.

- b. Optionally, choose whether you'll use an AWS PrivateLink that you have previously configured. [See details about using AWS PrivateLink for Amazon S3](#).

Networking

IPspace
IP_Space_1

☒ **Private Link Configuration**

Select Private Link

	Name	VPC	Endpoint ID
<input type="radio"/>	Private_Link_Name_001	vpce0-012345678901234567890 (Default)	vpce0-012345678901234567890
<input type="radio"/>	Private_Link_Name_002	vpce0-012345678901234567890 (k8s)	vpce0-012345678901234567890

6. Enter the backup policy details that will be used for your default policy and click **Next**. You can select an existing policy, or you can create a new policy by entering your selections in each section:
 - a. Enter the name for the default policy. You don't need to change the name.
 - b. Define the backup schedule and choose the number of backups to retain. [See the list of existing policies you can choose.](#)
 - c. When using ONTAP 9.10.1 and greater, you can choose to tier backups to either S3 Glacier or S3 Glacier Deep Archive storage after a certain number of days for further cost optimization. [Learn more about using archival tiers.](#)

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.

i Cloud Backup will create the S3 bucket after you complete the wizard

Policy Type ☒ Create a new Policy ☐ Select an existing Policy

Name	Default_Policy_Name	⌵
Labels & Retention	30 Daily	⌵
Archival Policy	<p>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.</p> <p><input checked="" type="checkbox"/> Tier Backups to Archive</p> <p>Archive After (Days) <input type="text" value="30"/> Storage Class <input type="text" value="S3 Glacier"/></p>	

7. 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
<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.

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

Result

Cloud Backup starts taking the initial backups of each selected volume and the Volume Backup Dashboard is displayed so you can monitor the state of the backups.

What's next?

You can [start and stop backups for volumes or change the backup schedule](#).

You can also [restore entire volumes or individual files from a backup file](#) to a Cloud Volumes ONTAP system in AWS, or to an on-premises ONTAP system.

Backing up on-premises ONTAP data to 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

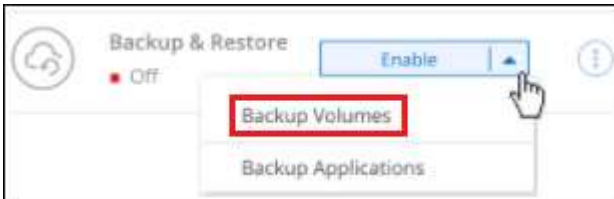
- You have discovered the on-premises cluster and added it to a working environment in Cloud Manager. See [Discovering ONTAP clusters](#) for details.
 - The cluster is running ONTAP 9.7P5 or later.
 - The cluster has a SnapMirror license — it is included as part of the Premium Bundle or Data Protection 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

Provider Information

Storage Server

Enter Storage Server

Access Key

Access Key

Secret Key

Secret Key

Connectivity

IPspace

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, monthly, or yearly 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 Type

☒ Create a new Policy
 ☐ Select an existing Policy

Name	Default_Policy_Name	▼
Labels & Retention	30 Daily	▼

5

Select the volumes that you want to back up

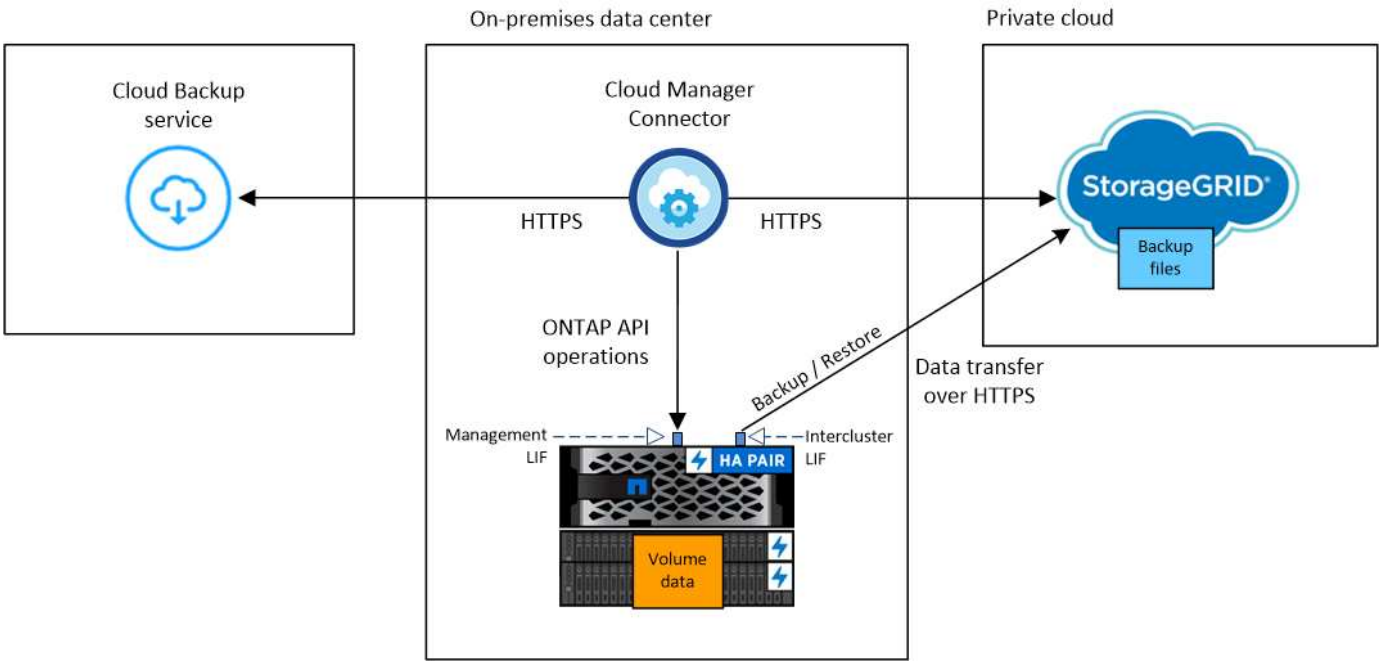
Identify which volumes you want to back up using the default backup policy in the Select Volumes page. If you want to assign different backup policies to certain volumes, you can create additional policies and apply them to volumes later.

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 the StorageGRID Gateway Node 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 the StorageGRID Gateway Node
 - 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.](#)



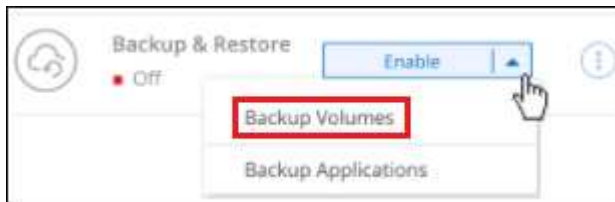
PAYGO licensing is not supported when backing up files to StorageGRID.

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 Gateway Node 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. Enter the backup policy details that will be used for your default policy and click **Next**. You can select an existing policy, or you can create a new policy by entering your selections in each section:
 - a. Enter the name for the default policy. You don't need to change the name.
 - b. Define the backup schedule and choose the number of backups to retain. [See the list of existing policies you can choose.](#)

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 Type

☒ Create a new Policy
 ☐ Select an existing Policy

Name

Default_Policy_Name ▼

Labels & Retention

30 Daily ▼

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 <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 ⓘ

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.



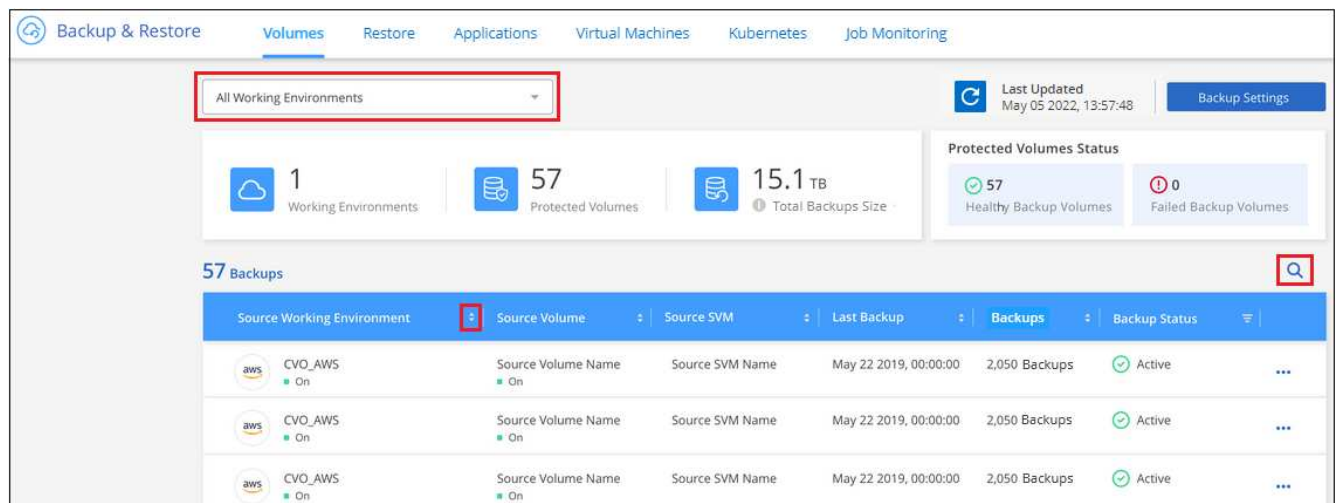
Do not manage or change backup files directly from your cloud provider environment. This may corrupt the files and will result in an unsupported configuration.

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. From the Cloud Manager left navigation menu, click **Backup & Restore**.
2. Click the **Volumes** tab to view the list of volumes for Cloud Volumes ONTAP and on-premises ONTAP systems.



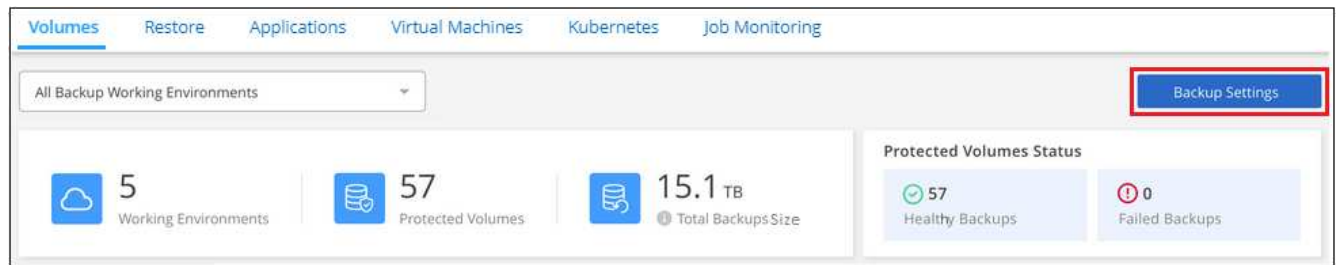
If you are looking for specific volumes in certain working environments, you can refine the list by working environment and volume, or you can use the search filter.

Enabling and disabling backups of volumes

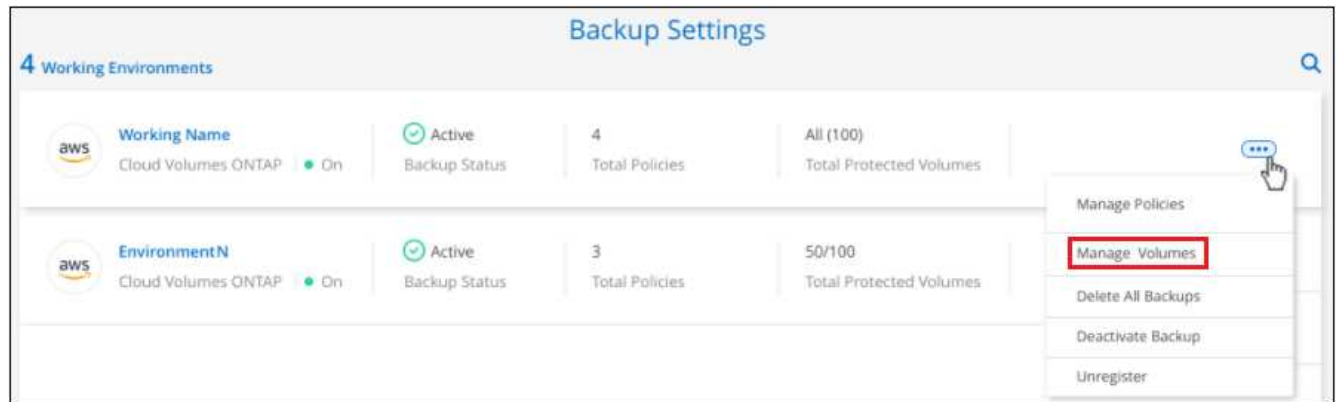
You can stop backing up a volume if you do not need backup copies of that volume and you do not want to pay for the cost to store the backups. You can also add a new volume to the backup list if it is not currently being backed up.

Steps

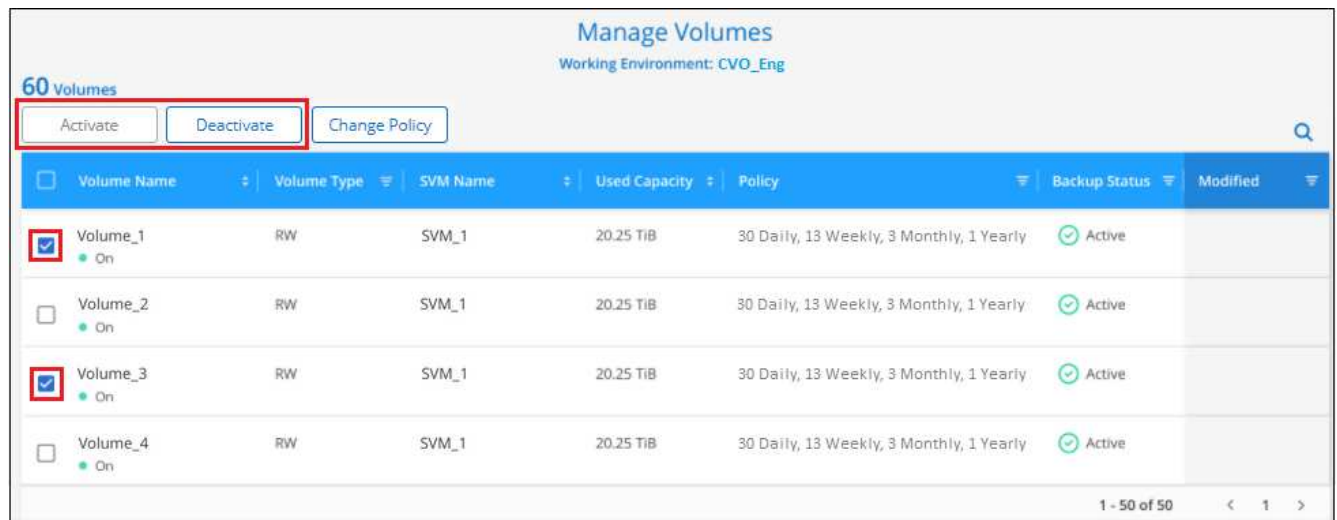
1. From the **Volumes** tab, select **Backup Settings**.



- From the *Backup Settings* page, click ... for the working environment and select **Manage Volumes**.



- 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.



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

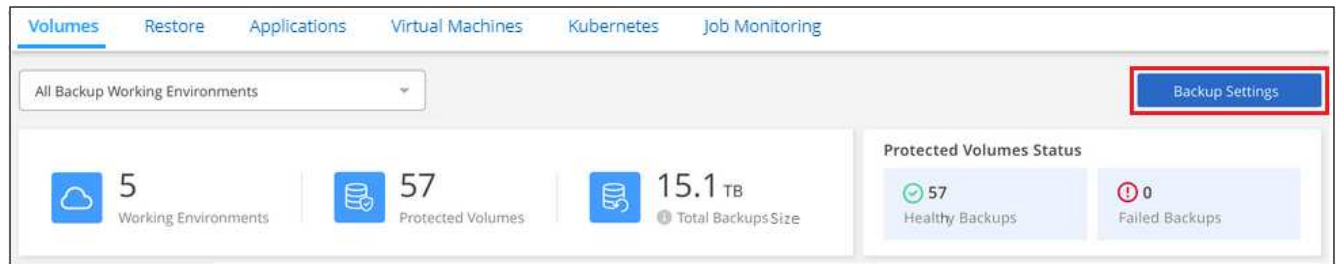
Note: When stopping a volume from being backed up you'll continue to be charged by your cloud provider for object storage costs for the capacity that the backups use unless you [delete the backups](#).

Editing an existing backup policy

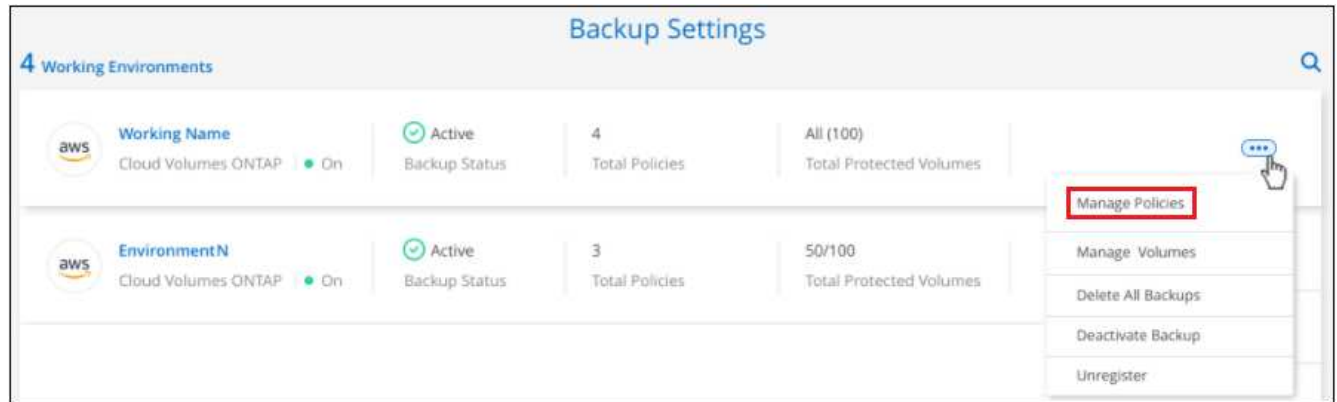
You can change the attributes for a backup policy that is currently applied to volumes in a working environment. Changing the backup policy affects all existing volumes that are using the policy.

Steps

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



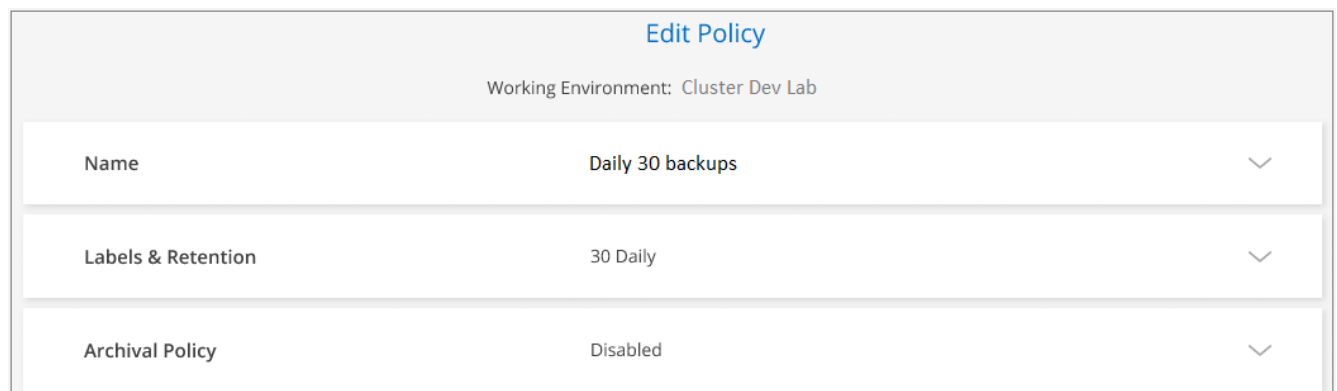
2. From the *Backup Settings* page, click ... for the working environment where you want to change the settings, and select **Manage Policies**.



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.

[Learn more about using AWS archival storage.](#)

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

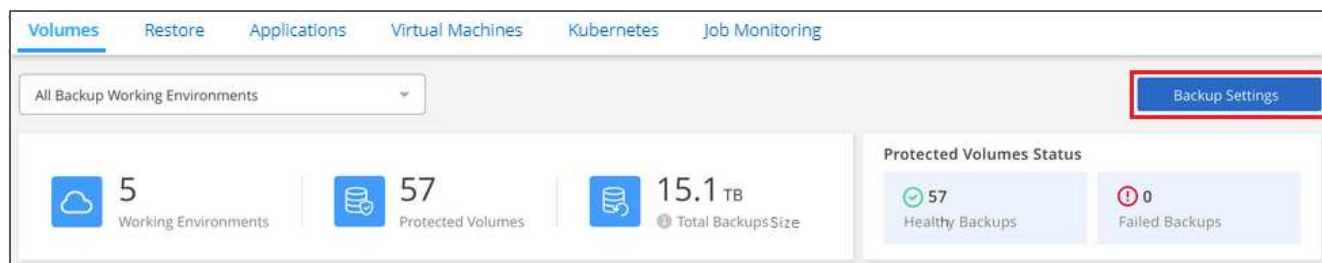
Adding a new backup policy

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

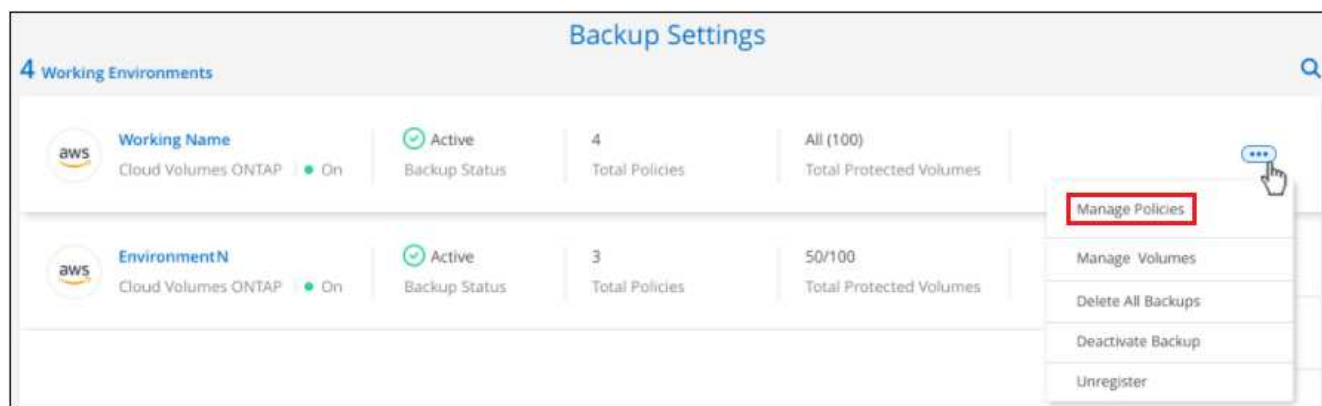
If you want to apply a new backup policy to certain volumes in a working environment, you first need to add the backup policy to the working environment. Then you can [apply the policy to volumes in that working environment](#).

Steps

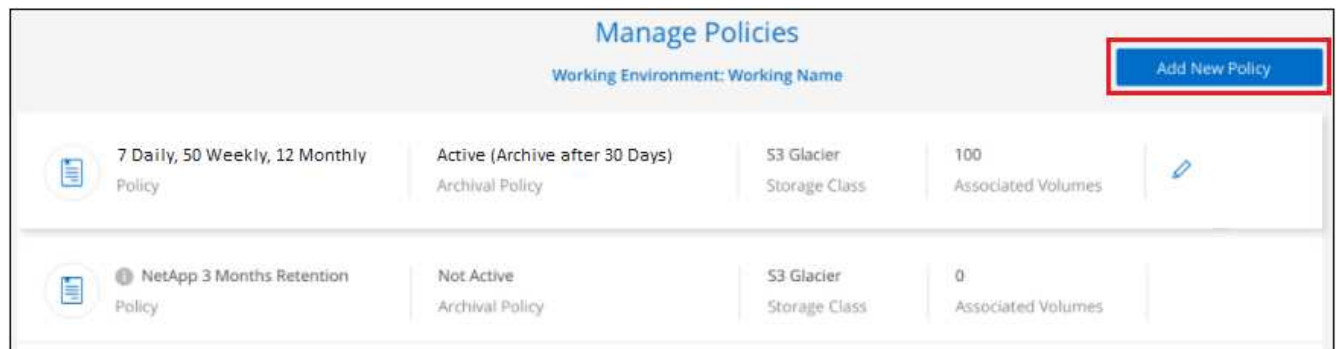
1. From the **Volumes** tab, select **Backup Settings**.



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



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



- 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.

[Learn more about using AWS archival storage.](#)

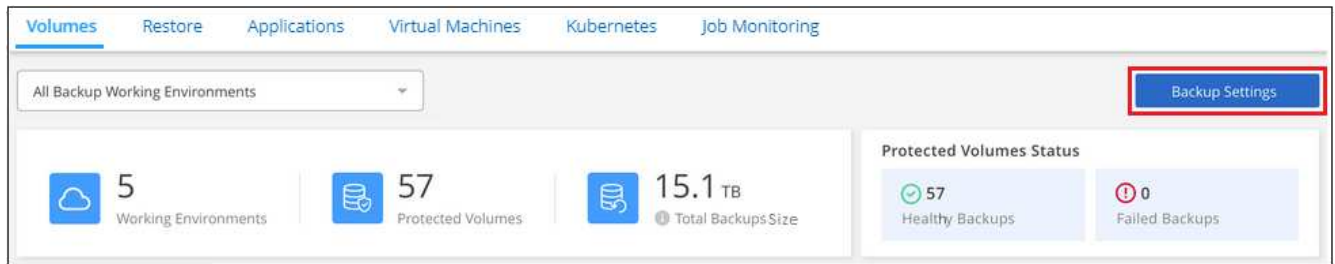
Changing the policy assigned to existing volumes

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

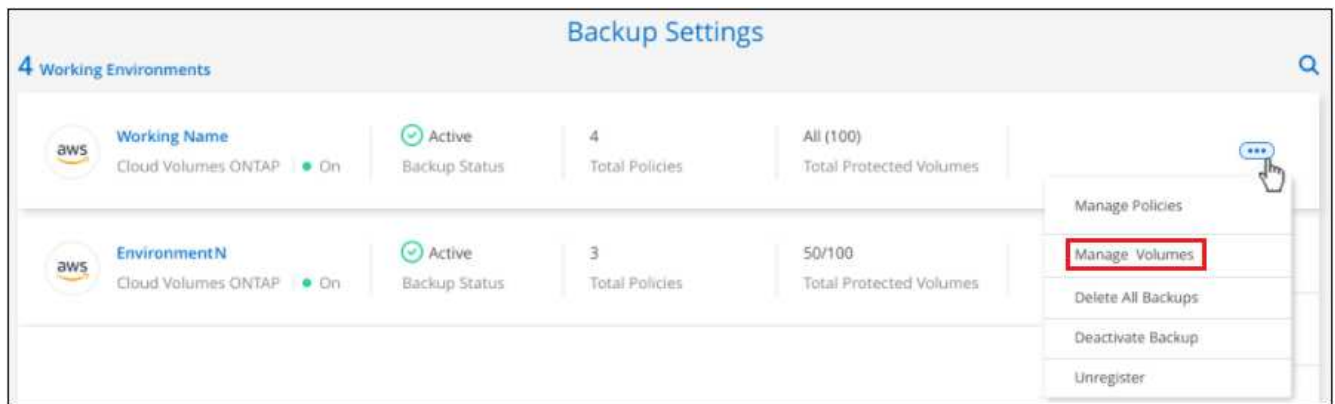
Note that the policy that you want to apply to the volumes must already exist. [See how to add a new backup policy for a working environment](#).

Steps

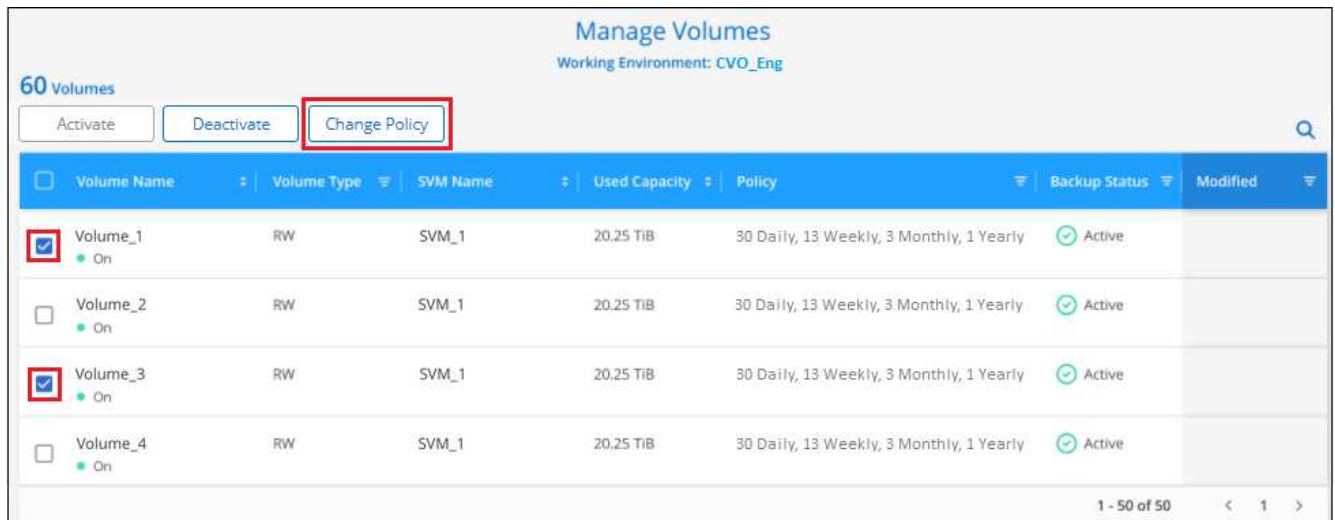
1. From the **Volumes** tab, select **Backup Settings**.



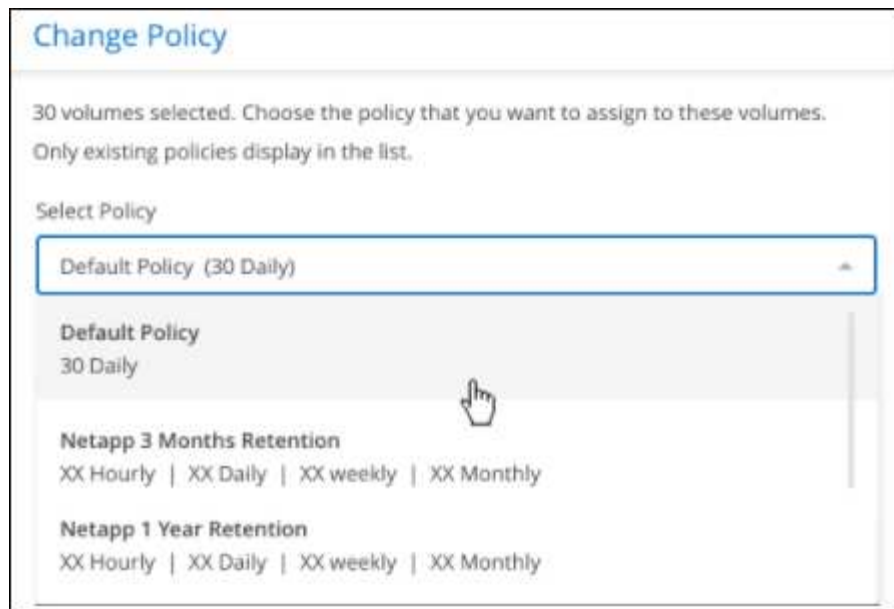
2. From the *Backup Settings* page, click ... for the working environment where the volumes exist, and select **Manage Volumes**.



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



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



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

Setting a backup policy to be assigned to new volumes

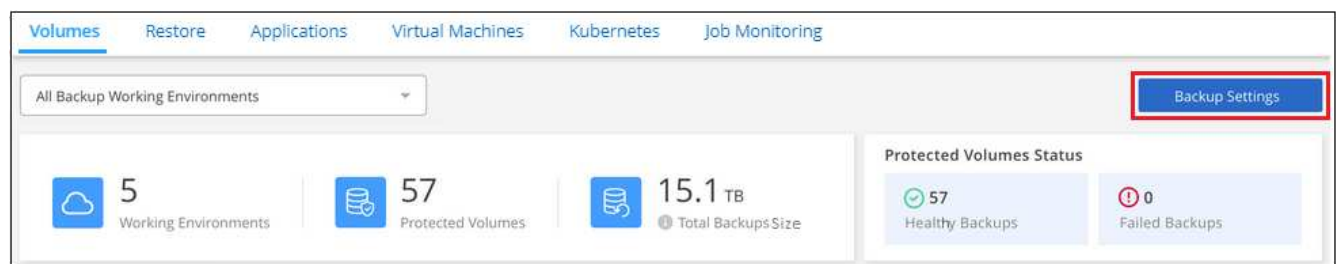
If you did not select the option to automatically assign a backup policy to newly created volumes when you first activated Cloud Backup on your ONTAP cluster, you can choose this option in the *Backup Settings* page later. Having a backup policy assigned to newly created volumes ensures that all your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

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



- 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**.

The screenshot displays the 'Volumes' tab in the ONTAP management console. At the top, there are tabs for 'Volumes', 'Restore', 'Applications', 'Virtual Machines', 'Kubernetes', and 'Job Monitoring'. Below these, a dropdown menu shows 'All Backup Working Environments'. The main dashboard area includes three summary cards: '1 Working Environments', '57 Protected Volumes', and '15.1 TB Total Backup Capacity'. To the right, a 'Protected Volumes Status' section shows '57 Healthy Backup Volumes' and '0 Failed Backup Volumes'. Below this, a table titled '57 Backups' lists backup details. The table has columns for 'Source Working Environment', 'Source Volume', 'Source SVM', 'Last Backup', 'Backups', and 'Backup Status'. The first three rows show backups for 'CVO_AWS' on 'Volume_1', 'Volume_2', and 'Volume_3', all with a 'Last Backup' of 'May 22 2019, 00:00:00' and '2,050 Backups'. The 'Backup Status' for the first row is 'Active'. A dropdown menu is open for the first row, showing options: 'Details & Backup List', 'Backup Now' (highlighted with a red box), and '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**.

The screenshot shows the Cloud Backup dashboard. At the top, there are tabs for Volumes, Restore, Applications, Virtual Machines, Kubernetes, and Job Monitoring. Below the tabs, there's a dropdown menu for 'All Backup Working Environments' and a 'Backup Settings' button. The dashboard displays three main metrics: 1 Working Environment, 57 Protected Volumes, and 15.1 TB Total Backup Capacity. To the right, a 'Protected Volumes Status' section shows 57 Healthy Backup Volumes and 0 Failed Backup Volumes. Below this, a '57 Backups' section shows a table of backup details. A dropdown menu is open for the first backup, showing options: 'Details & Backup List' (highlighted with a red box), 'Backup Now', and 'Pause Backups'.

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	
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 along with details about the source volume, destination location, and backup details.

The screenshot shows the details page for a backup. It is divided into three main sections: Source, Destination, and Backup Information. The Source section shows Working Environment (Working Environment N...), Type (Cloud Volumes ONTAP (HA)), Provider (AWS), Volume (Volume Name), and SVM (SVM Name). The Destination section shows Cloud Provider (AWS), Region (us-east-1), Bucket (netapp-backup), and Account ID (012345678901234567890). The Backup Information section shows Relationship Status (Active), Last Backup (Oct 05 2021, 2:41:33 pm), Lag Duration (14 days 3 hours, 38 mi...), Backups (2,050), and Backup Policy (Netapp7YearsRetention). Below these sections, there's a '2,050 Backups' section with a search bar and a table of backup details.

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.



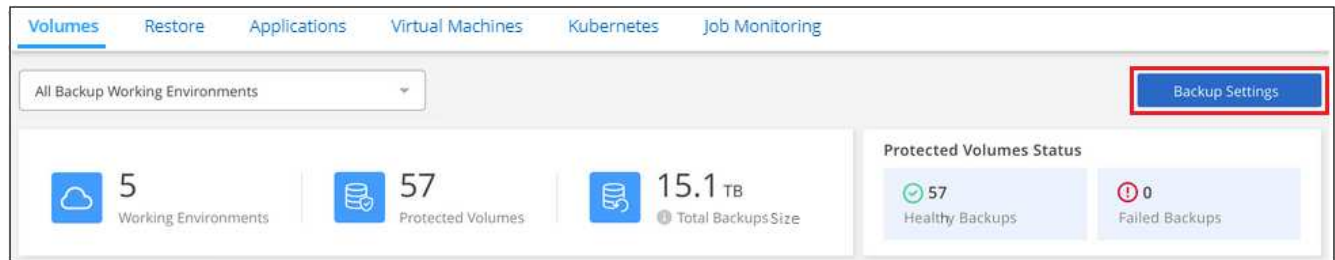
If you plan to delete a working environment or cluster that has backups, you must delete the backups **before** deleting the system. Cloud Backup doesn't automatically delete backups when you delete a system, and there is no current support in the UI to delete the backups after the system has been deleted.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

Deleting all backup files for a working environment

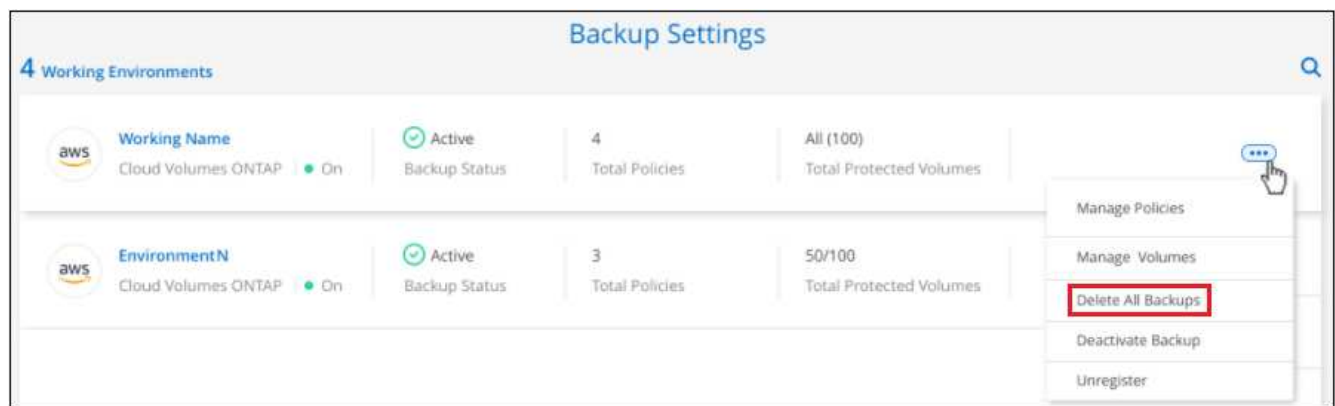
Deleting all backups for a working environment does not disable future backups of volumes in this working environment. If you want to stop creating backups of all volumes in a working environment, you can deactivate backups [as described here](#).

Steps

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



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 screenshot shows the NetApp Cloud Manager interface. At the top, there are tabs for Volumes, Restore, Applications, Virtual Machines, Kubernetes, and Job Monitoring. Below the tabs, there's a dropdown menu for "All Backup Working Environments" and a "Backup Settings" button. The main dashboard displays three metrics: 1 Working Environment, 57 Protected Volumes, and 15.1 TB Total Backup Capacity. To the right, a "Protected Volumes Status" section shows 57 Healthy Backup Volumes and 0 Failed Backup Volumes. Below this, a section titled "57 Backups" contains a table with columns: Source Working Environment, Source Volume, Source SVM, Last Backup, Backups, and Backup Status. The table lists three backup entries for CVO_AWS. A context menu is open for the first entry, showing options: "Details & Backup List" (highlighted with a red box), "Backup Now", and "Pause Backups".

The list of all backup files is displayed.

The screenshot shows the NetApp Cloud Manager interface with backup details. The top section is divided into three panels: "Source", "Destination", and "Backup Information". The "Source" panel shows Working Environment (Working Environment N...), Type (Cloud Volumes ONTAP (HA)), Provider (AWS), Volume (Volume Name), and SVM (SVM Name). The "Destination" panel shows Cloud Provider (AWS), Region (us-east-1), Bucket (netapp-backup), and Account ID (012345678901234567890). The "Backup Information" panel shows Relationship Status (Active), Last Backup (Oct 05 2021, 2:41:33 pm), Lag Duration (14 days 3 hours, 38 mi...), Backups (2,050), and Backup Policy (Netapp7YearsRetention). Below this, a section titled "2,050 Backups" contains a table with columns: Backup Name, Date, and Size. The table lists three backup entries: Backup_2020_Jan, Backup_2020_Mar, and Backup_2020_Apr. A context menu is open for the first entry, showing options: "Delete All Backups" (highlighted with a red box) and "Download Backup Report".

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

The screenshot shows the NetApp Cloud Manager interface with backup details. The top section is divided into three panels: "Source", "Destination", and "Backup Information". The "Source" panel shows Working Environment (Working Environment N...), Type (Cloud Volumes ONTAP (HA)), Provider (AWS), Volume (Volume Name), and SVM (SVM Name). The "Destination" panel shows Cloud Provider (AWS), Region (us-east-1), Bucket (netapp-backup), and Account ID (012345678901234567890). The "Backup Information" panel shows Relationship Status (Active), Last Backup (Oct 05 2021, 2:41:33 pm), Lag Duration (14 days 3 hours, 38 mi...), Backups (2,050), and Backup Policy (Netapp7YearsRetention). Below this, a section titled "2,050 Backups" contains a table with columns: Backup Name, Date, and Size. The table lists three backup entries: Backup_2020_Jan, Backup_2020_Mar, and Backup_2020_Apr. A context menu is open for the first entry, showing options: "Delete All Backups" (highlighted with a red box) and "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**.

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	Active
CVO_AWS	Volume_3	SVM_1	May 22 2019, 00:00:00	2,050 Backups	Active

The list of all backup files is displayed.

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**.



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

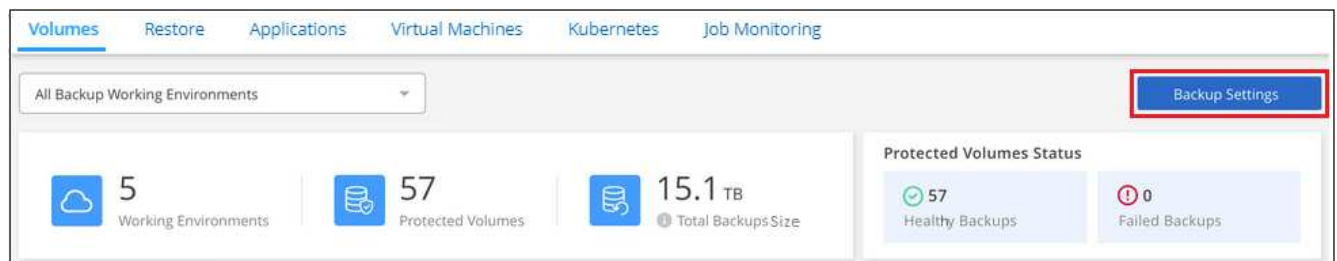
Disabling Cloud Backup for a working environment

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.

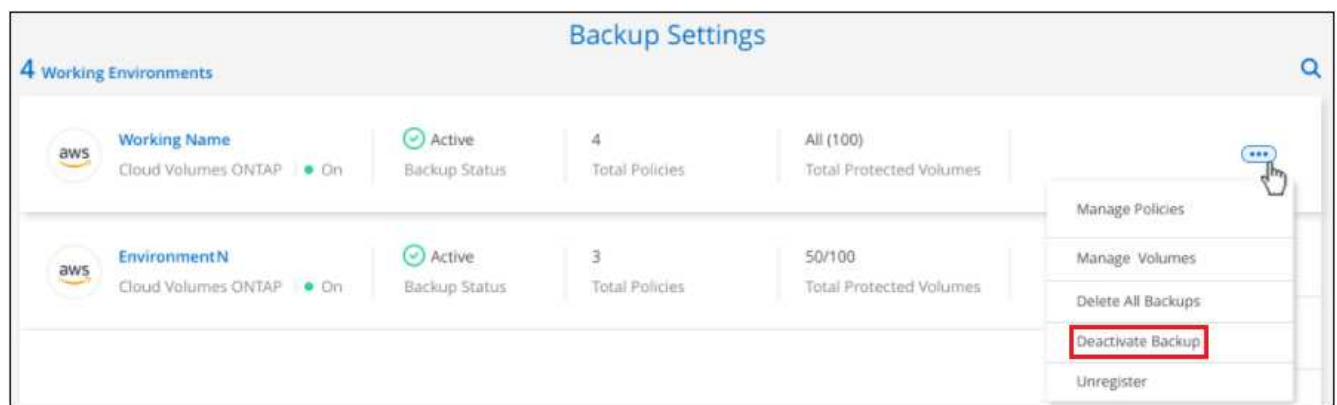
Note that you'll continue to be charged by your cloud provider for object storage costs for the capacity that your backups use unless you [delete the backups](#).

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.

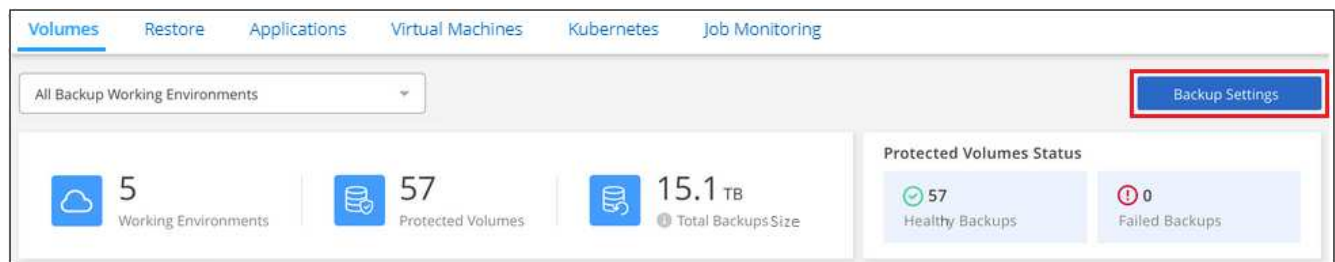
Before you can unregister Cloud Backup, you must perform the following steps, in this order:

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

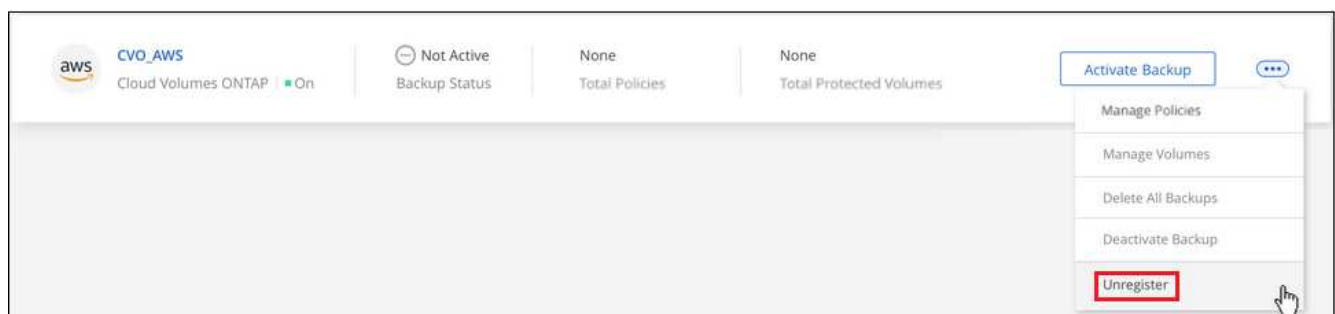
The unregister option is not available until these two actions are complete.

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.

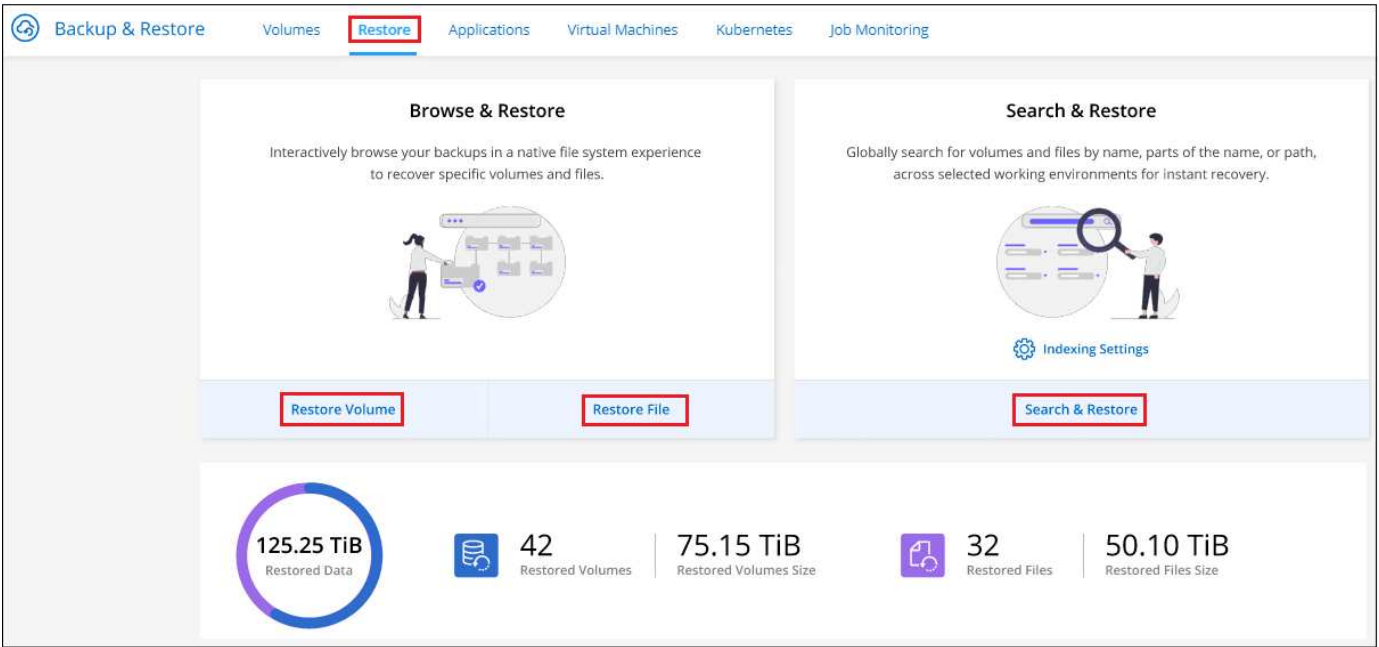
A valid Cloud Backup license is required to restore data from backup files to a production system.

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 Cloud Manager left navigation menu, 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 all backup files 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
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 public cloud provider resources required per account
No additional cloud provider costs required	Cost associated with public cloud provider 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.

[Learn more about restoring from AWS archival storage.](#)

Browse & Restore supported working environments and object storage providers

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

Backup File Location	Destination Working Environment	
	Volume Restore	File Restore

Backup File Location	Destination Working Environment	
Amazon S3	Cloud Volumes ONTAP in AWS	Cloud Volumes ONTAP in AWS
	On-premises ONTAP system	On-premises ONTAP system
NetApp StorageGRID	On-premises ONTAP system	On-premises ONTAP system

(¹) The Connector must be deployed in your Google Cloud Platform VPC for this support.

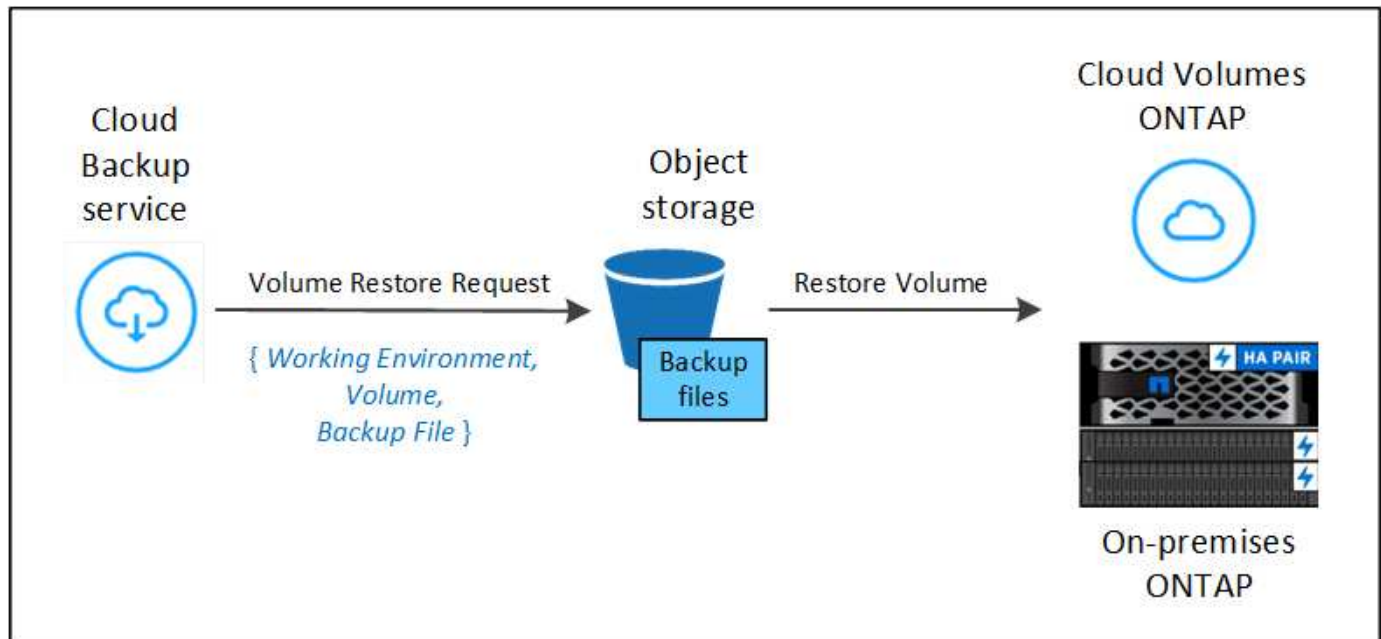
Note that references to "on-premises ONTAP systems" includes FAS, AFF, and ONTAP Select systems.



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:

Cloud Backup Service: Restore Demo

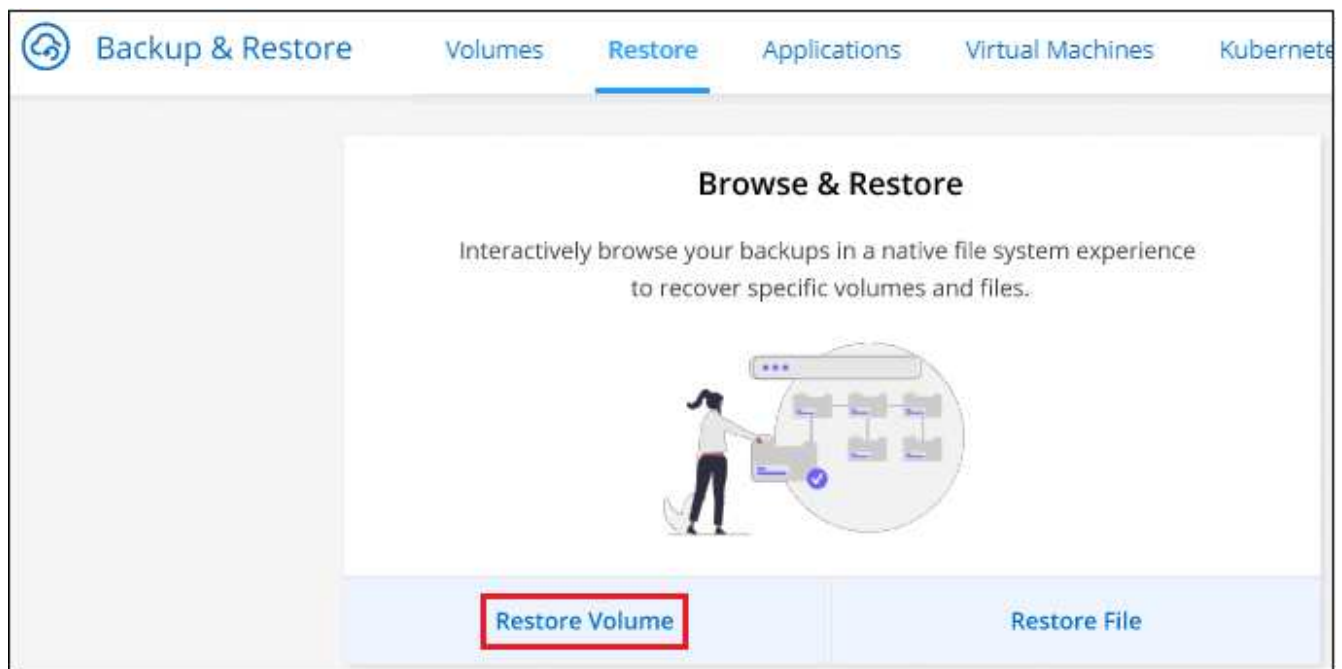
Powered by Cloud Manager

January 2022



Steps

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



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



5. Click **Continue**.

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



7. If you select an on-premises ONTAP system and you haven't already configured the cluster connection to the object storage, you are prompted for additional information:
- When restoring from Amazon S3, select the IPspace in the ONTAP cluster where the destination volume will reside, enter the access key and secret key for the user you created to give the ONTAP cluster access to the S3 bucket, and optionally choose a private VPC endpoint for secure data transfer.
 - When restoring from 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.

Select Destination				
<div> <div>✓</div> <div>Selected Working Environment</div> <div>Working Environment Name 2</div> </div> <div> <div>☰</div> <div>Destination Volume ></div> <div>General_restore</div> </div>	<div> <div>i</div> <div>A new volume will be created in the working environment based on the backup you selected</div> </div> <div> <div>Volume Name</div> <div>General_restore</div> </div> <div> <div>Storage VM</div> <div>svm1</div> </div> <div> <div>Restore Priority</div> <div>Low</div> </div> <div> <div>Volume Information</div> <table> <tr> <td>Volume Size: 50.00 GB</td> </tr> <tr> <td>Backup Policy: CloudBackupService</td> </tr> <tr> <td>Protocol: NFS</td> </tr> </table> </div>	Volume Size: 50.00 GB	Backup Policy: CloudBackupService	Protocol: NFS
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.

[Learn more about restoring from AWS archival storage.](#)

- 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

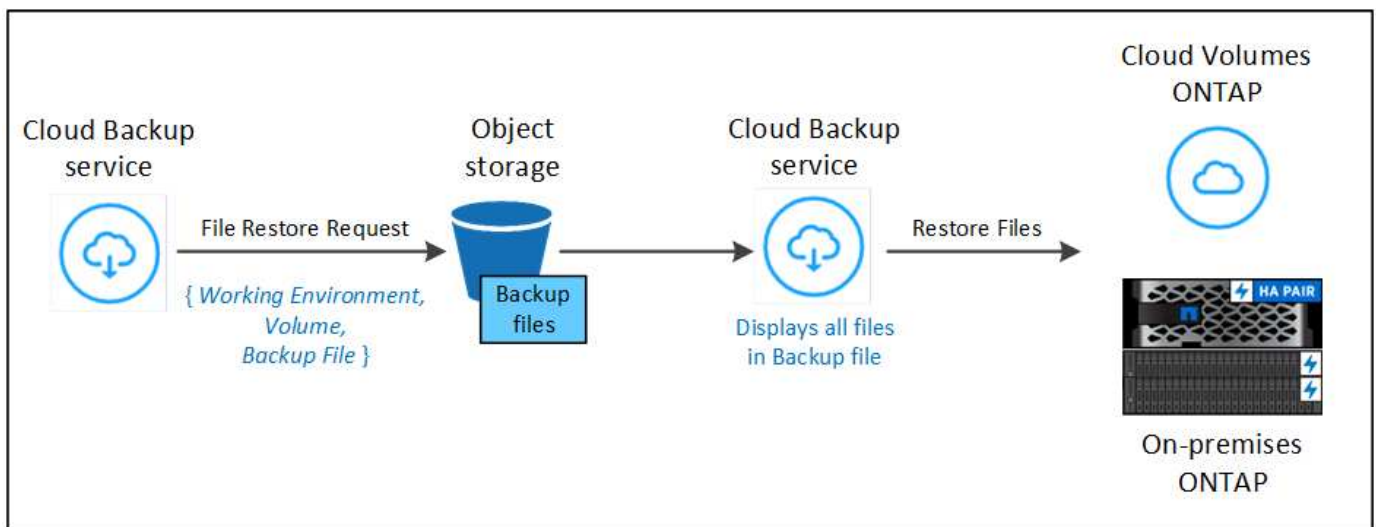
- The ONTAP version must be 9.6 or greater in your Cloud Volumes ONTAP or on-premises ONTAP systems to perform file restore operations.

- AWS cross-account restore requires manual action in the AWS console. See the AWS topic [granting cross-account bucket permissions](#) for details.

File Restore process

The process goes like this:

1. When you want to restore one or more files from a volume backup, click the **Restore** tab, click **Restore Files** under *Browse & Restore*, and select the backup file in which the file (or files) reside.
2. 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:

Cloud Backup Service: Restore Demo

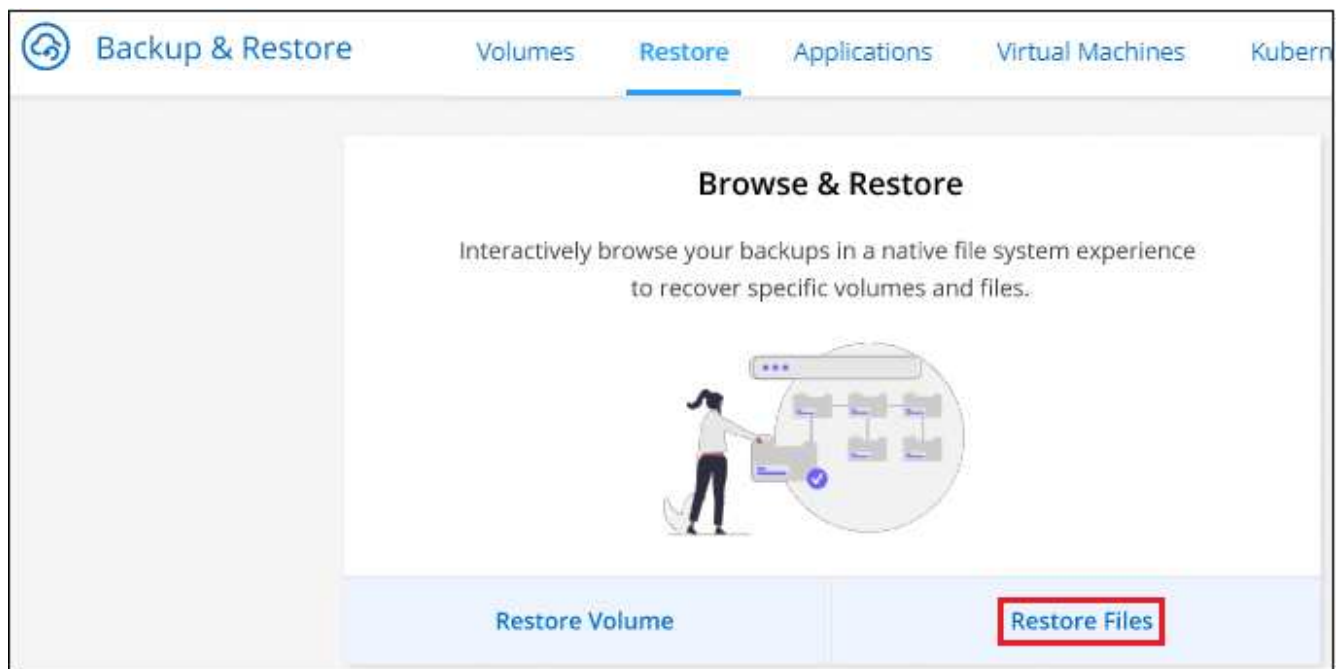
Powered by Cloud Manager

January 2022



Steps

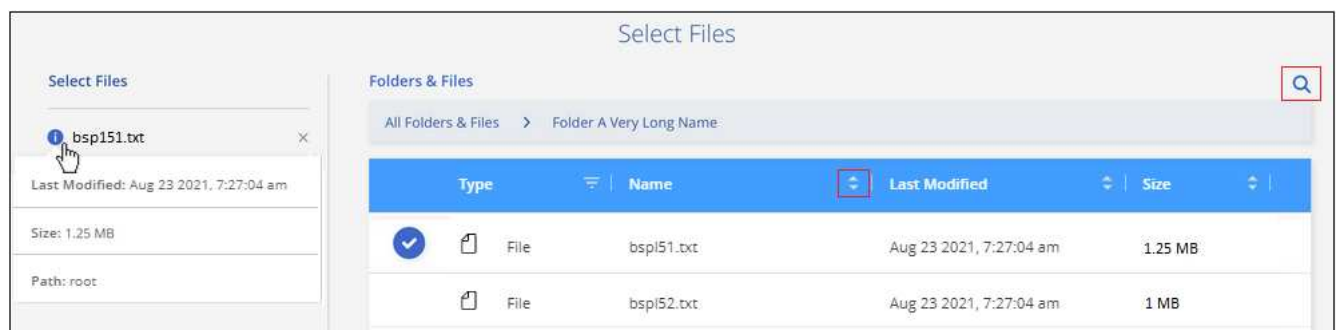
1. Select the **Backup & Restore** service.
2. Click the **Restore** tab and the Restore Dashboard is displayed.
3. From the *Browse & Restore* section, click **Restore Files**.



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



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

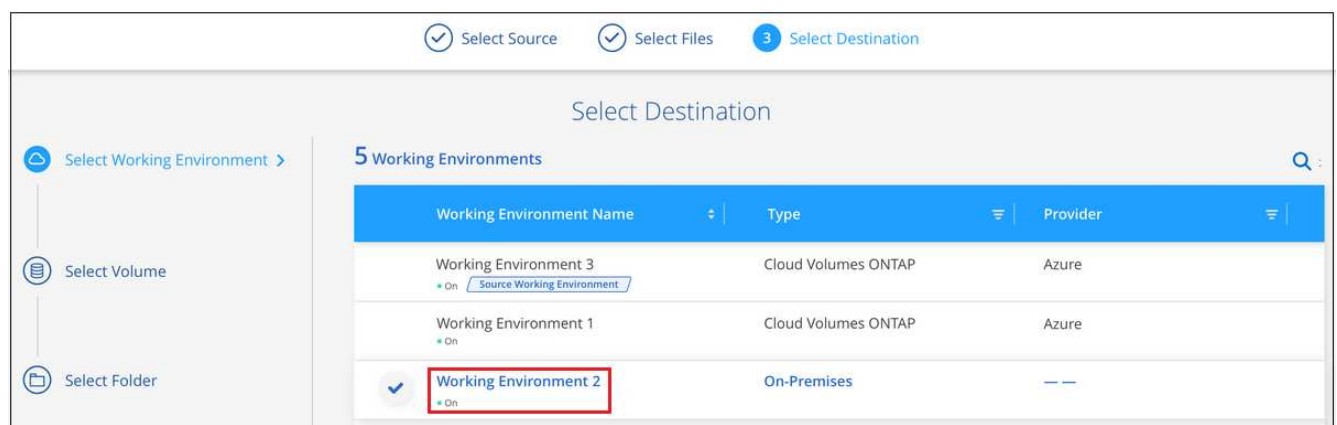


6. In the *Select Files* page, select the file or files that you want to restore and click **Continue**. To assist you in finding the file:

- 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.

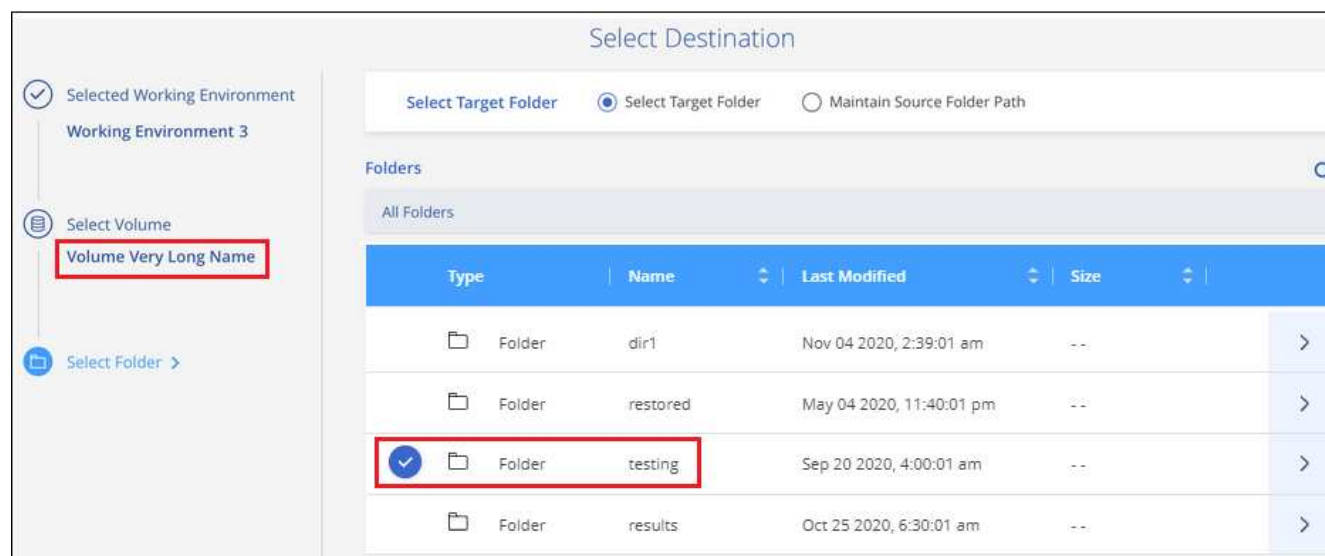
7. In the *Select Destination* page, select the **Working Environment** where you want to restore the files.




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

[Learn more about restoring from AWS archival storage.](#)

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

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



Search & Restore supported working environments and object storage providers

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

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

Backup File Location	Destination Working Environment	
NetApp StorageGRID	Not currently supported	



The Connector must be deployed in your cloud provider platform for this support. Search & Restore is not supported when the Connector is installed on your premises.

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

Prerequisites

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

Note that if you were already using Cloud Backup with a Connector you configured in the past, you'll need to add the Athena and Glue permissions to the Cloud Manager user role now. These are new, and they are required for Search & Restore.

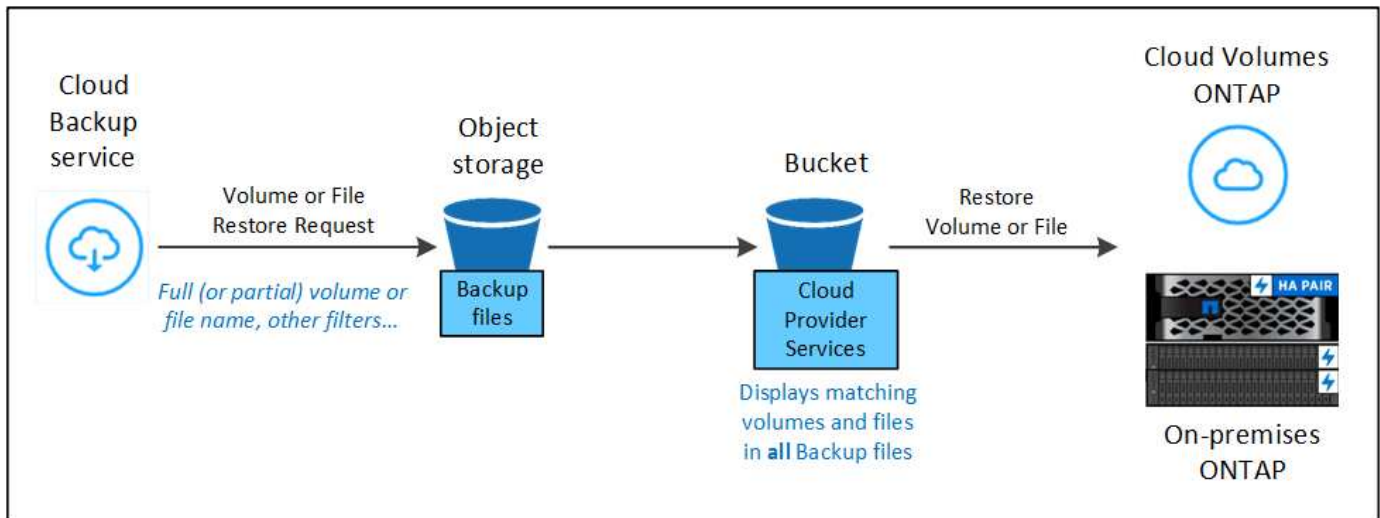
Search & Restore process

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:

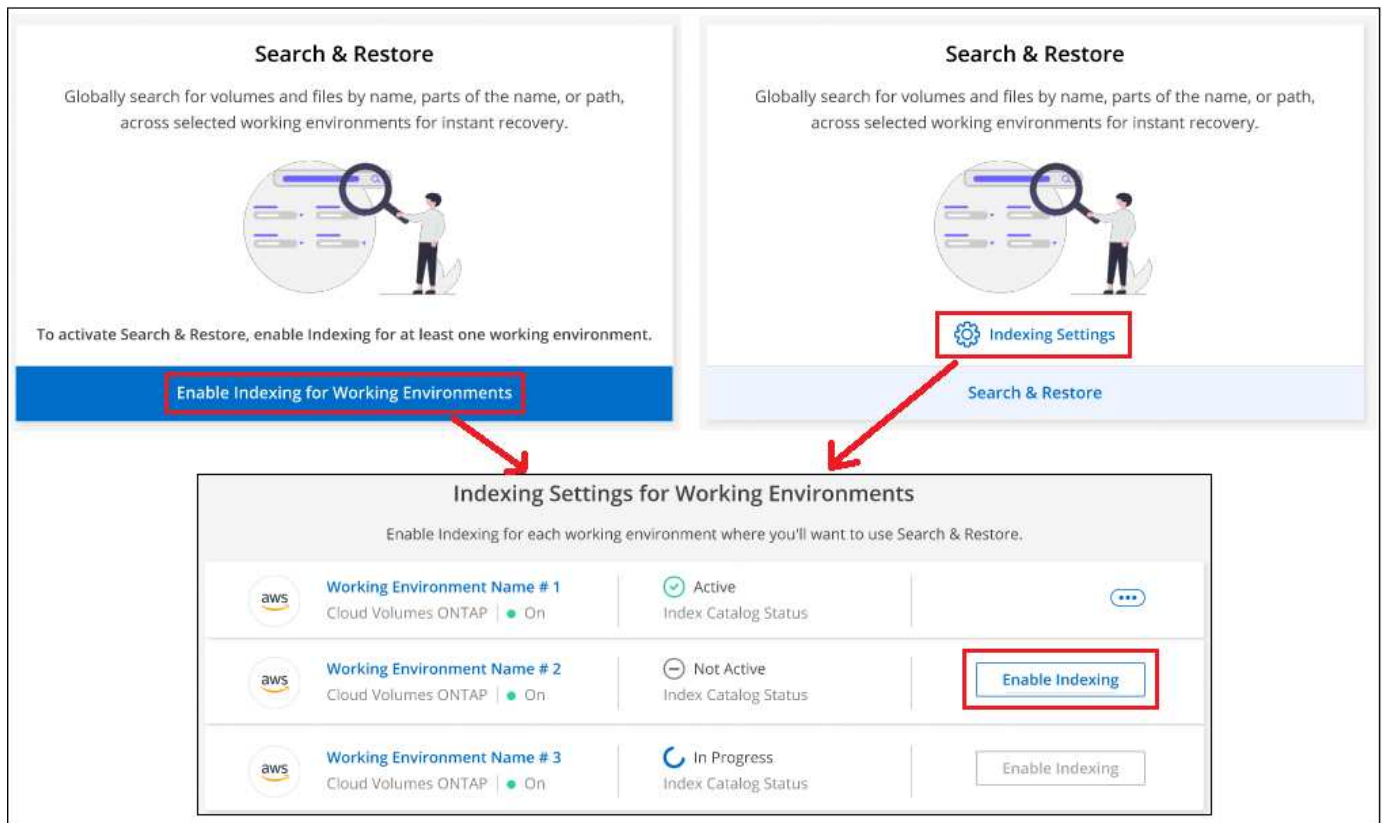
- For backups stored in AWS, it provisions a new S3 bucket and the [Amazon Athena interactive query service](#) and [AWS Glue serverless data integration service](#).

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".



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

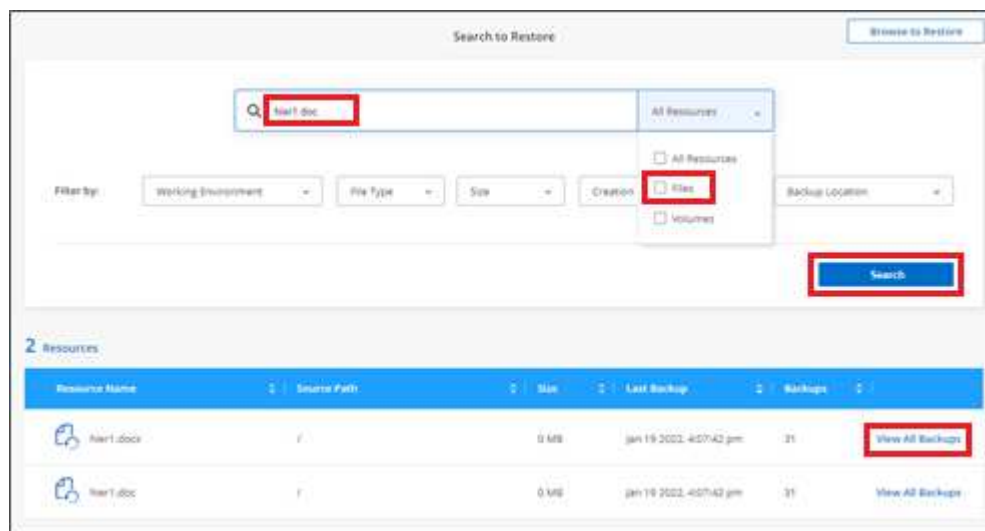
After you have [enabled Indexing for your working environment](#), you can restore volumes or files using Search & Restore. This allows you to use a broad range of filters to find the exact file or volume that you want to restore from all backup files.

Steps

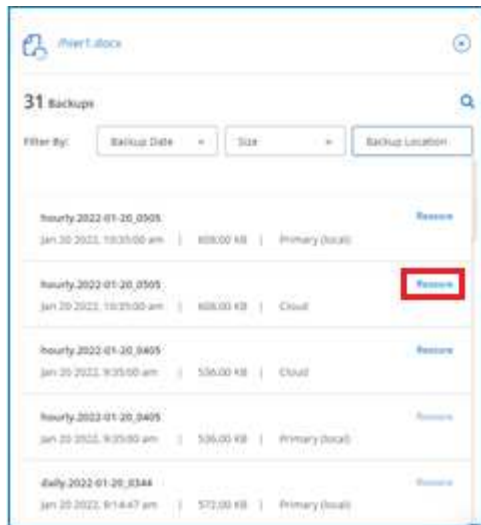
1. Select the **Backup & Restore** service.
2. Click the **Restore** tab and the Restore Dashboard is displayed.
3. From the *Search & Restore* section, click **Search & Restore**.



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.

Back up and restore Kubernetes data

Protect your Kubernetes cluster data using Cloud Backup

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

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

Features

Backup features:

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

Restore features:

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

Supported Kubernetes working environments and object storage providers

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

Source Working Environment	Backup File Destination
Kubernetes cluster in AWS	Amazon S3

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

Backup File Location	Destination Working Environment
Amazon S3	Kubernetes cluster in AWS

Cost

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

Resource charges

Resource charges are paid to the cloud provider for object storage capacity in the cloud. Since Cloud Backup

preserves the storage efficiencies of the source volume, you pay the cloud provider object storage costs for the data *after* ONTAP efficiencies (for the smaller amount of data after deduplication and compression have been applied).

Service charges

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

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

Licensing

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

Free trial

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

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

Pay-as-you-go subscription

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

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

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

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

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

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

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

[Learn how to set up a pay-as-you-go subscription.](#)

Bring your own license

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

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

[Learn how to manage your BYOL licenses.](#)

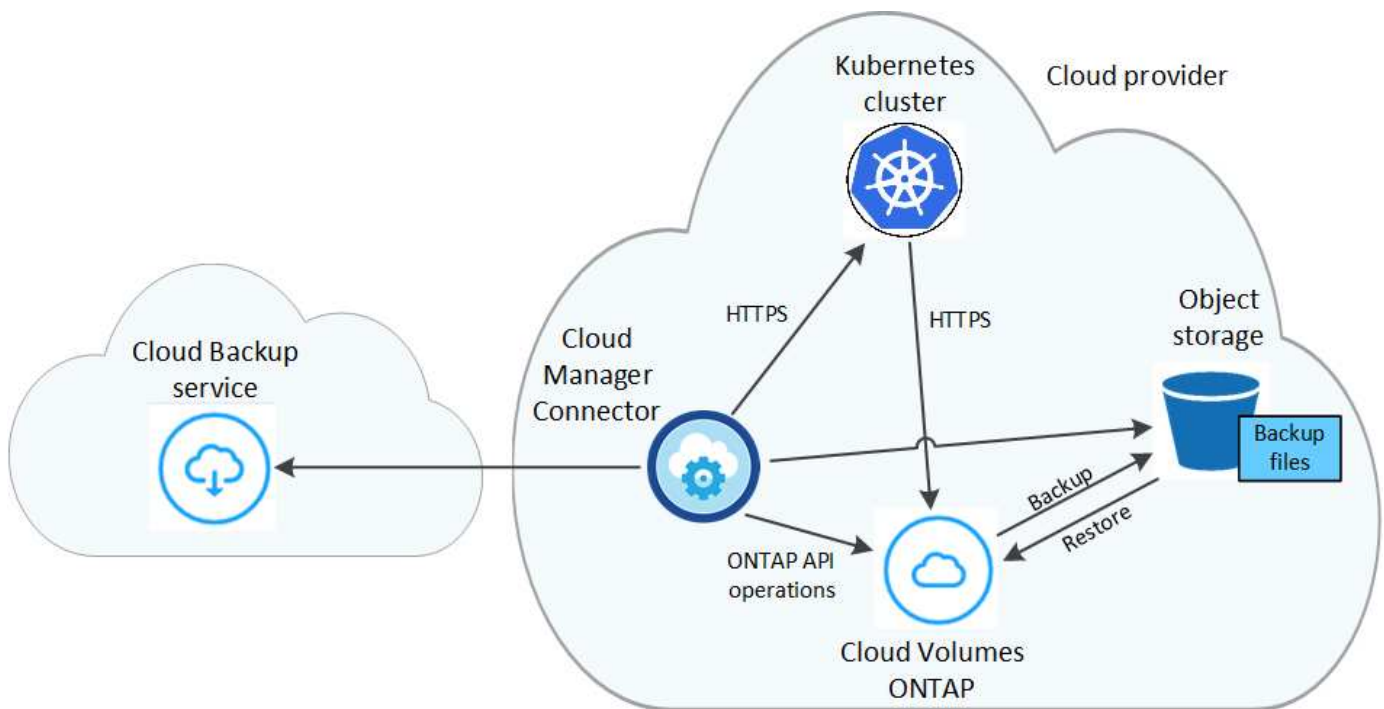
How Cloud Backup works

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



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

The following image shows the relationship between each component:



Supported storage classes or access tiers

- In AWS, backups start in the *Standard* storage class and transition to the *Standard-Infrequent Access* storage class after 30 days.

Customizable backup schedule and retention settings per cluster

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

and assign those policies to other volumes.

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

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

Supported volumes

Cloud Backup supports Persistent volumes (PVs).

Limitations

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

Backing up Kubernetes persistent volume data to Amazon S3

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

Quick start

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

1

Review prerequisites

- You have discovered the Kubernetes cluster as a Cloud Manager working environment.
 - Trident must be installed on the cluster, and the Trident version must be 21.1 or greater.
 - All PVCs that will be used to create persistent volumes that you want to back up must have "snapshotPolicy" set to "default".
 - The cluster must be using Cloud Volumes ONTAP on AWS for its' backend storage.
 - The Cloud Volumes ONTAP system must be running ONTAP 9.7P5 or later.
- You have a valid cloud provider subscription for the storage space where your backups will be located.
- You have subscribed to the [Cloud Manager Marketplace Backup offering](#), an [AWS annual contract](#), or you have purchased [and activated](#) a Cloud Backup BYOL license from NetApp.
- The IAM role that provides the Cloud Manager Connector with permissions includes S3 permissions from the latest [Cloud Manager policy](#).

2

Enable Cloud Backup on your existing Kubernetes cluster

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



3

Define the backup policy

The default policy backs up volumes every day and retains the most recent 30 backup copies of each volume. Change to hourly, daily, weekly, or monthly backups, or select one of the system-defined policies that provide more options. You can also change the number of backup copies you want to retain.

4

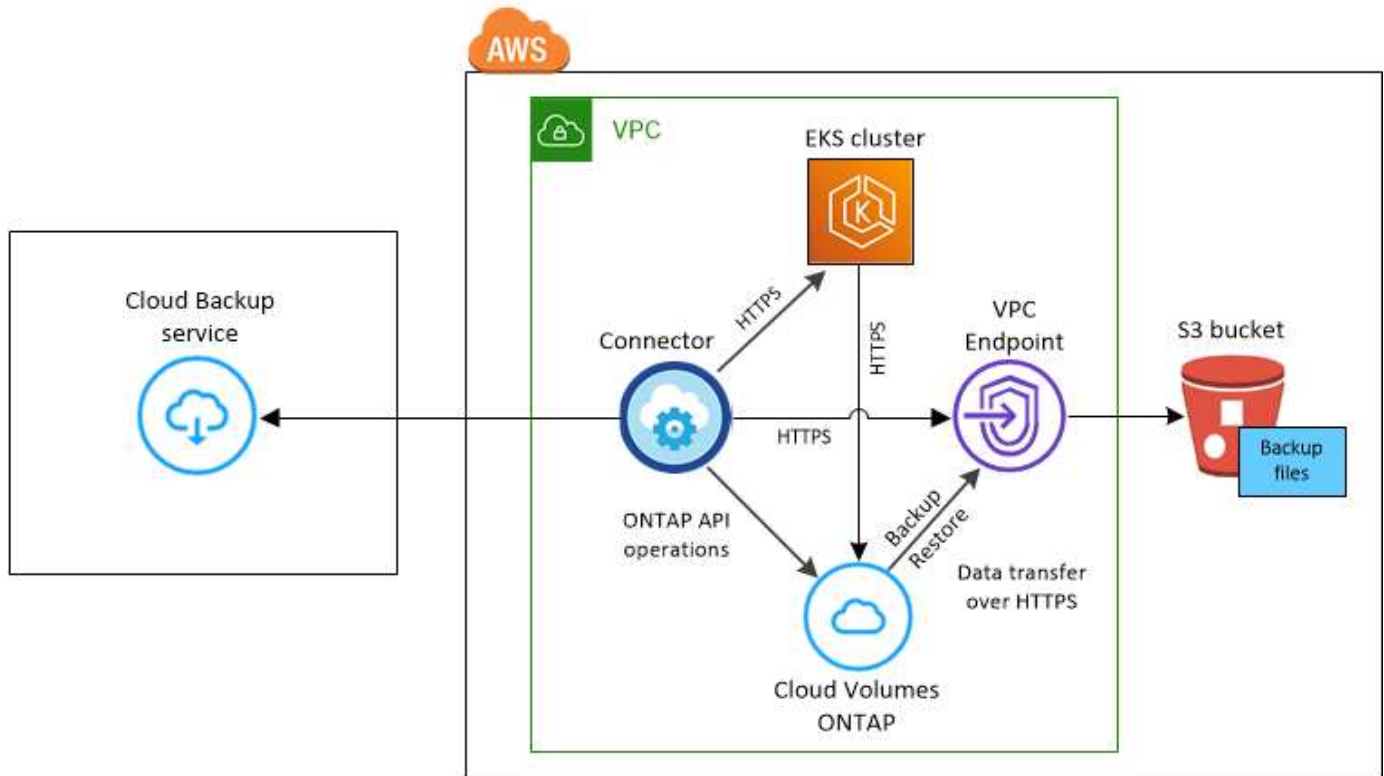
Select the volumes that you want to back up

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

Requirements

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

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



Note that the VPC Endpoint is optional.

Kubernetes cluster requirements

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

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

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

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

```

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

```

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

```

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

```

License requirements

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

subscription.

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

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

For Cloud Backup BYOL licensing, you need the serial number from NetApp that enables you to use the service for the duration and capacity of the license. [Learn how to manage your BYOL licenses](#).

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

Supported AWS regions

Cloud Backup is supported in all AWS regions [where Cloud Volumes ONTAP is supported](#).

AWS Backup permissions required

The IAM role that provides Cloud Manager with permissions must include S3 permissions from the latest [Cloud Manager policy](#).

Here are the specific S3 permissions from the policy:

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

Enabling Cloud Backup

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

Steps

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

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



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

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

Define Policy

Policy - Retention & Schedule

☐ Hourly
☒ Daily
☐ Weekly
☐ Monthly

Number of backups to retain

24

30

52

12

S3 Bucket Cloud Manager will create the S3 bucket after you complete the wizard

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

- To back up all volumes, check the box in the title row (☒ Volume Name).
- To back up individual volumes, check the box for each volume (☒ Volume_1).

Select Volumes

57 Volumes

<input checked="" type="checkbox"/>	Persistent Volume Name	Namespace	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Persistent Volume 1 <small>On</small>	Namespace 1	10 TB	⊖ Not Active
<input checked="" type="checkbox"/>	Persistent Volume 2 <small>On</small>	Namespace 1	10 TB	⊖ Not Active
<input checked="" type="checkbox"/>	Persistent Volume 3 <small>On</small>	Namespace 1	10 TB	⊖ Not Active
<input checked="" type="checkbox"/>	PV 1 <small>On</small>	Namespace 2	10 TB	⊖ Not Active
<input checked="" type="checkbox"/>	PV 2 <small>On</small>	Namespace 2	10 TB	⊖ Not Active

☒ Automatically back up all existing and future persistent volumes with the selected backup policy

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

Result

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

The Kubernetes Dashboard is displayed so you can monitor the state of the backups.

What's next?

You can [start and stop backups for volumes or change the backup schedule](#).

You can also [restore entire volumes from a backup file](#) as a new volume on the same or different Kubernetes cluster in AWS (in the same region).

Managing backups for your Kubernetes systems

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



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

Viewing the volumes that are being backed up

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

Steps

1. From the Cloud Manager left navigation menu, click **Backup & Restore**.
2. Click the **Kubernetes** tab to view the list of persistent volumes for Kubernetes systems.

Source K8s Cluster	Source Persistent Volume	Source Namespace	Last Backup	Backup Copies	Backup Status
aws eks1 Unknown	pvc-1704aa1f-af1d-49e9-87fd-6edd86125855 Unknown	default	Jun 09 2022, 10:00:24 am	20	Unknown
aws eks1 Unknown	pvc-1615f0a8-2d5d-44d0-b4e4-f365cc3fb4a6 Unknown	default	Jun 09 2022, 10:00:24 am	20	Unknown
aws eks1 Unknown	pvc-d1f839c1-d932-4f49-b620-33321dbe939e Unknown	trident	Jun 09 2022, 10:00:24 am	20	Unknown

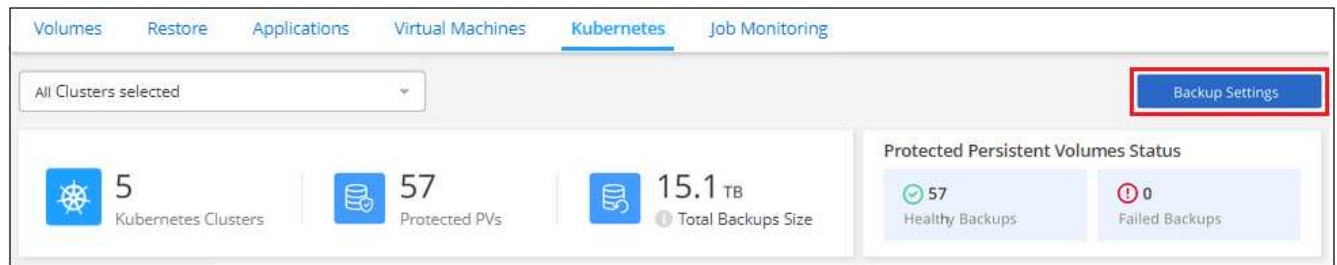
If you are looking for specific volumes in certain clusters, you can refine the list by cluster and volume, or you can use the search filter.

Enabling and disabling backups of volumes

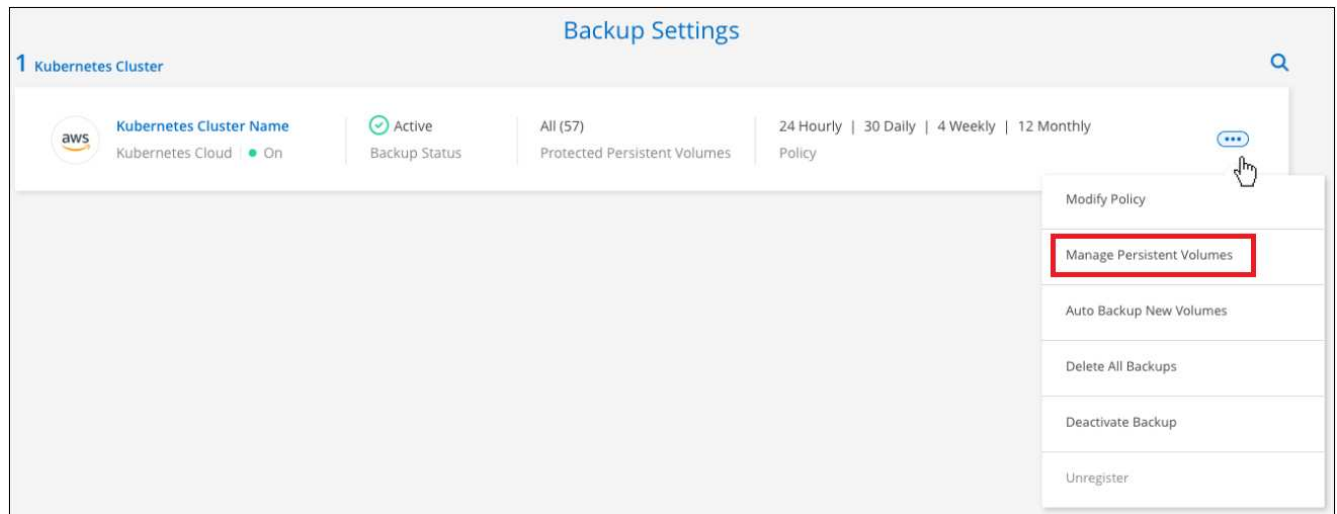
You can stop backing up a volume if you do not need backup copies of that volume and you do not want to pay for the cost to store the backups. You can also add a new volume to the backup list if it is not currently being backed up.

Steps

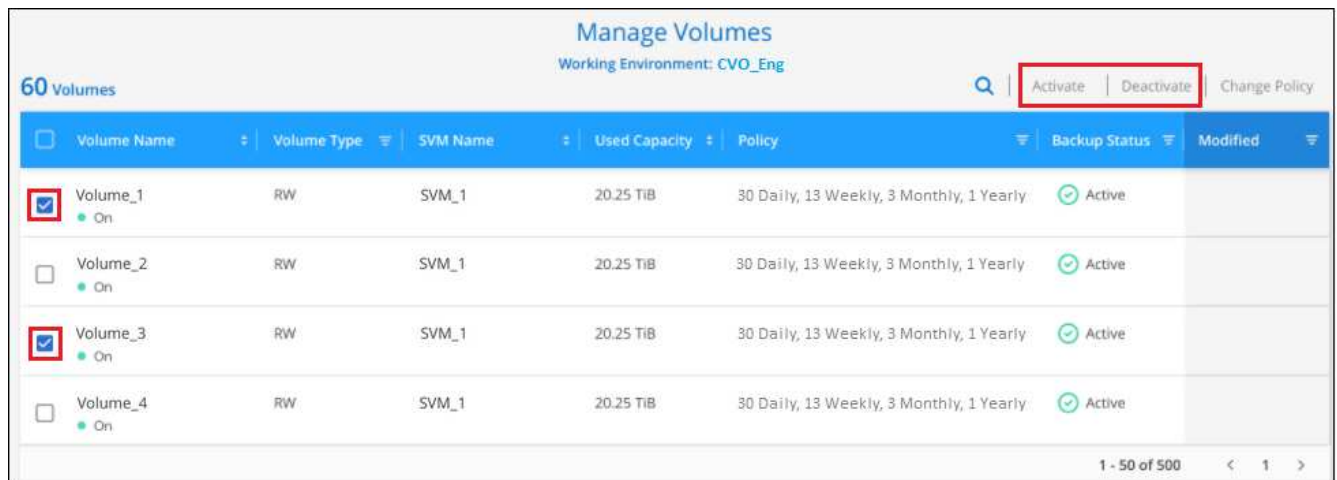
1. From the **Kubernetes** tab, select **Backup Settings**.



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



- 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.



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

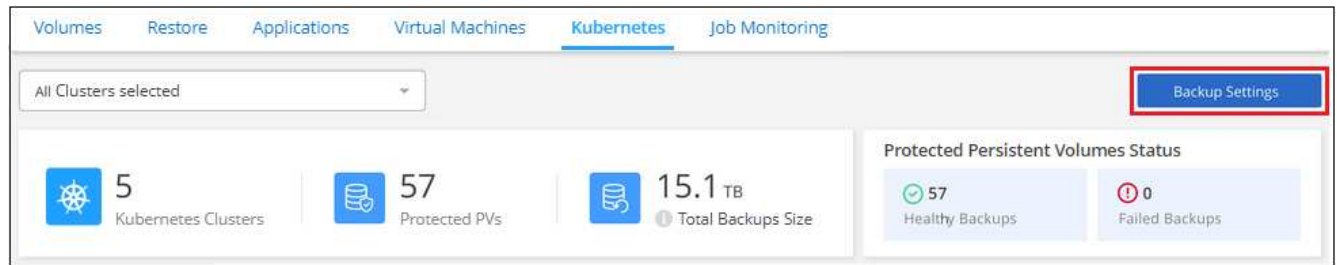
Note: When stopping a volume from being backed up you'll continue to be charged by your cloud provider for object storage costs for the capacity that the backups use unless you [delete the backups](#).

Editing an existing backup policy

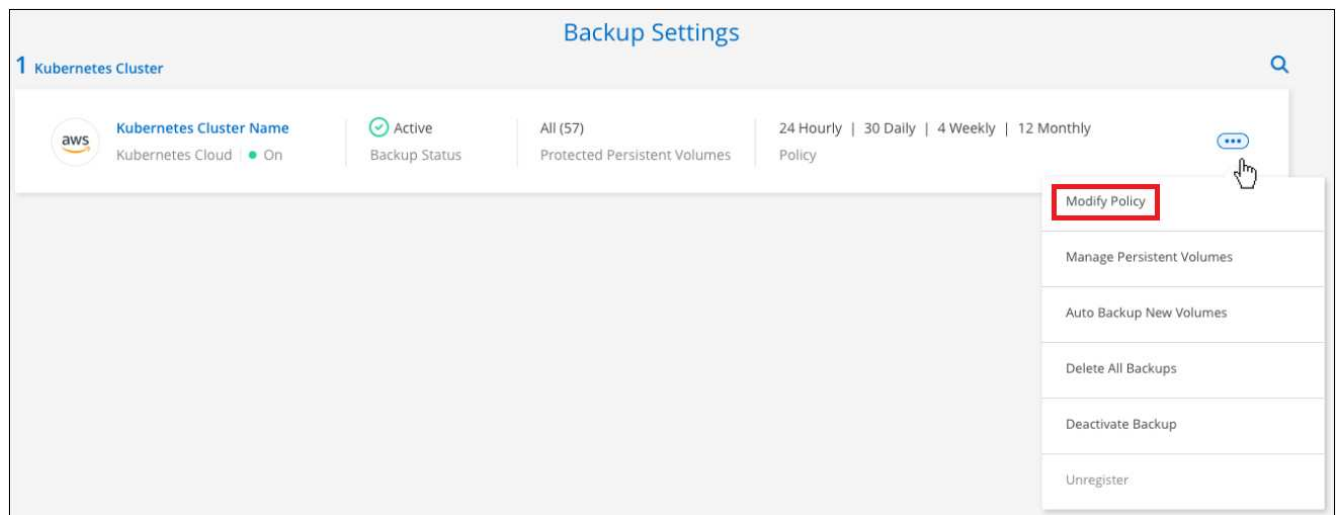
You can change the attributes for a backup policy that is currently applied to volumes in a working environment. Changing the backup policy affects all existing volumes that are using the policy.

Steps

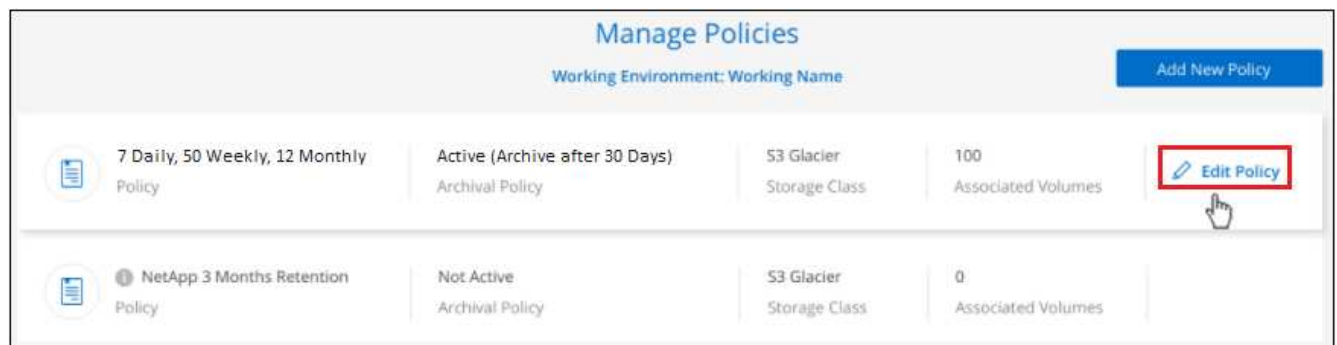
1. From the **Kubernetes** tab, select **Backup Settings**.



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



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



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

Edit Policy		
Working Environment: Cluster Dev Lab		
Name	Daily 30 backups	▼
Labels & Retention	30 Daily	▼
Archival Policy	Disabled	▼

Setting a backup policy to be assigned to new volumes

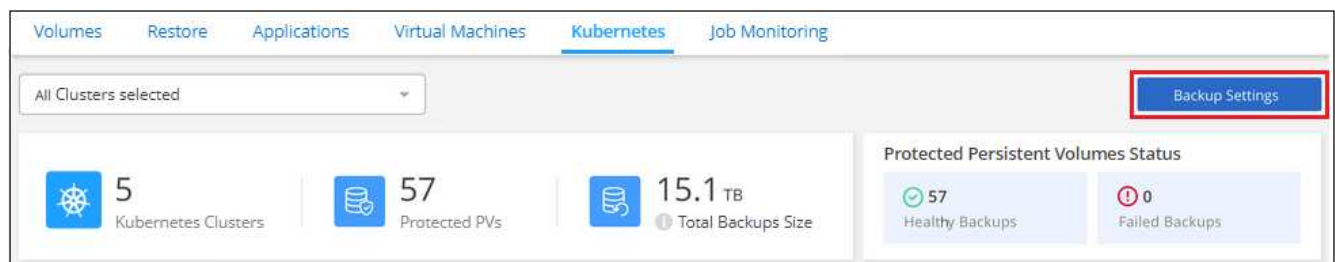
If you did not select the option to automatically assign a backup policy to newly created volumes when you first activated Cloud Backup on your Kubernetes cluster, you can choose this option in the *Backup Settings* page later. Having a backup policy assigned to newly created volumes ensures that all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

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

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

Steps

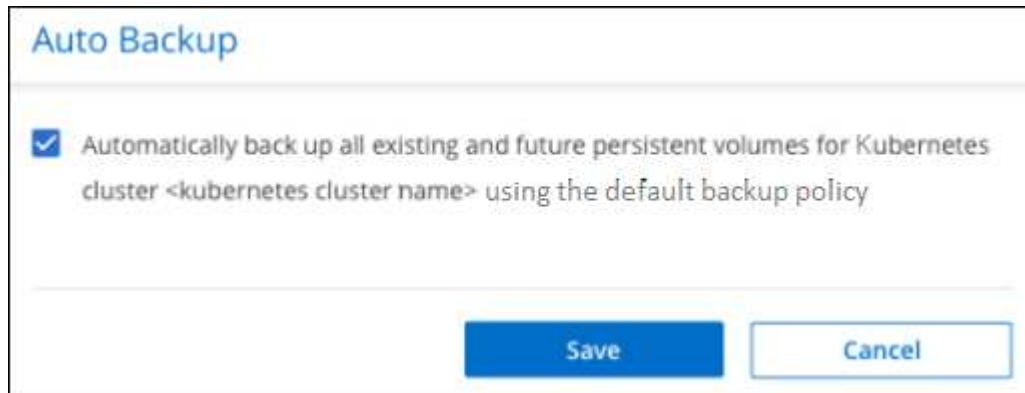
1. From the **Kubernetes** tab, select **Backup Settings**.



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



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



Result

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

Viewing the list of backups for each volume

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

This page also enables you perform the following tasks:

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

Steps

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

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

All Kubernetes Clusters

Backup Settings

1 Kubernetes Clusters | 57 Protected PVs | 15.1 TB Total Backups Size

Protected Persistent Volumes Status: 57 Healthy Backup | 0 Failed Backup

57 Backups

Source Kubernetes Cluster	Source Persistent Volume	Source Namespace	Last Backup	Backups	Backup Status
Kubernetes_Cloud_AWS	Source Persistent Volume	Source Namespace	May 22 2019, 00:00:00	2,050 Backups	Active
Kubernetes_Cloud_AWS	Source Persistent Volume	Source Namespace	May 22 2019, 00:00:00	2,050 Snapshot	
Kubernetes_Cloud_AWS	Source Persistent Volume	Source Namespace	May 22 2019, 00:00:00	2,050 Snapshot	

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

Kubernetes Cluster: eks1

Type: EKS

Provider: AWS

Persistent Volume: pvc-05881c70-cf5f-4edc-8537...

Namespace: default

Destination

Cloud Provider: AWS

Bucket: netapp-backup-vsa5twmc9ae

Region: us-west-1

Account ID: 123456789012

Backup Information

Relationship Status: enabled

Last Backup: Dec 07 2021, 2:20:30 pm

Lag Duration: 1 hour

Backups: 2

Backup Policy: 24 hourly | 30 daily | 52 weekly

2 Backups

Backup Name	Date	Size
daily-dem-163887957011628bef197-34b5-11ec-8916-5b2669f1987a	Dec 07 2021, 2:19:30 pm	9.77 KB
daily-dem-163887963015128bef197-34b5-11ec-8916-5b2669f1987a	Dec 07 2021, 2:20:30 pm	9.77 KB

Restore

Deleting backups

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



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

Deleting all backup files for a working environment

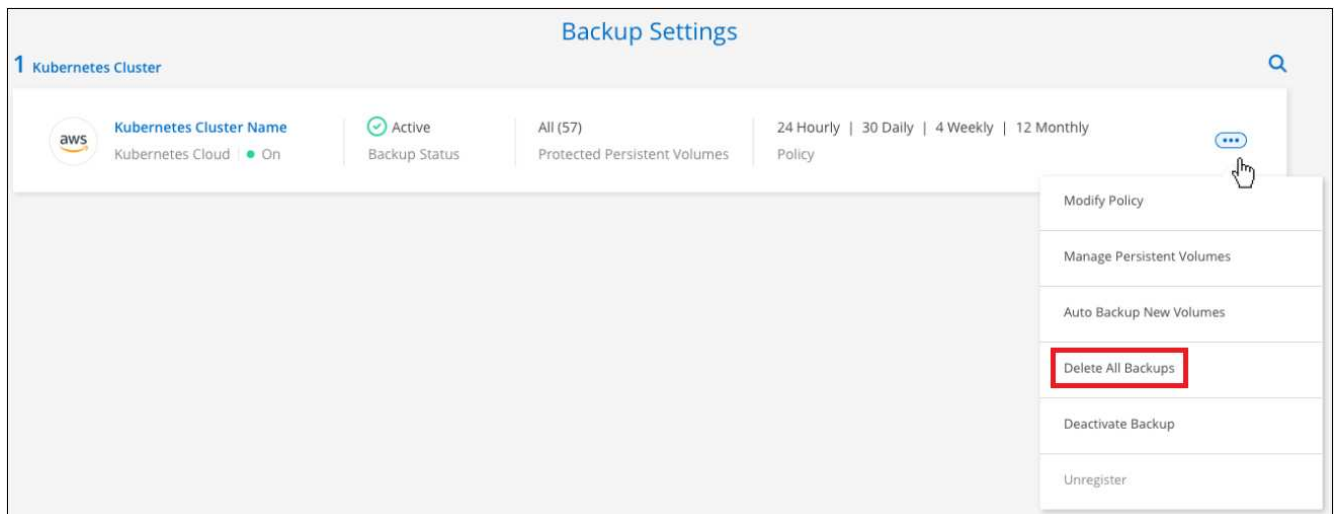
Deleting all backups for a working environment does not disable future backups of volumes in this working environment. If you want to stop creating backups of all volumes in a working environment, you can deactivate backups [as described here](#).

Steps

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



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



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

Deleting all backup files for a volume

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

You can [restart making backups for the volume](#) at any time from the Manage Backups page.

Steps

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

The screenshot shows the 'Backup & Restore' section of a management console. At the top, there are tabs for 'Volumes', 'Restore', 'Applications', 'Virtual Machines', 'Kubernetes' (selected), and 'Job Monitoring'. Below the tabs, a summary bar displays: 1 Kubernetes Clusters, 57 Protected PVs, and 15.1 TB Total Backups Size. To the right, a 'Protected Persistent Volumes Status' box shows 57 Healthy Backups and 0 Failed Backups. The main area lists 57 backups. The first backup row is selected, and a context menu is open with the following options: 'Details & Backup List' (highlighted with a red box), 'Backup Now', and 'Pause Backups'.

Source Kubernetes Cluster	Source Persistent Volume	Source Namespace	Last Backup	Backups	Backup Status
Kubernetes_Cloud_AWS	Source Persistent Volume	Source Namespace	May 22 2019, 00:00:00	2,050 Backups	Active
Kubernetes_Cloud_AWS	Source Persistent Volume	Source Namespace	May 22 2019, 00:00:00	2,050 Snapshot	
Kubernetes_Cloud_AWS	Source Persistent Volume	Source Namespace	May 22 2019, 00:00:00	2,050 Snapshot	

The list of all backup files is displayed.

The screenshot displays the 'Details & Backup List' for a specific backup. The details are organized into three columns: 'Source', 'Destination', and 'Backup Information'. Below the details, there is a table of 2,050 backups. The table has columns for 'Backup Name', 'Date', and 'Size'. The first three rows of the table are visible.

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 **Actions** > **Delete all Backups**.

The screenshot shows the 'Actions' dropdown menu for the backup list. The menu is open, and the 'Delete All Backups' option is highlighted with a red box. The 'Download Backup Report' option is also visible below it.

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

Deleting a single backup file for a volume

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

Steps

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

The screenshot shows the NetApp Backup & Restore interface with the **Kubernetes** tab selected. The top navigation bar includes **Backup & Restore**, **Volumes**, **Restore**, **Applications**, **Virtual Machines**, **Kubernetes**, and **Job Monitoring**. A dropdown menu for **All Kubernetes Clusters** is visible. The main content area shows a summary of 1 Kubernetes Cluster, 57 Protected PVS, and 15.1 TB Total Backups Size. To the right, a **Protected Persistent Volumes Status** section shows 57 Healthy Backups and 0 Failed Backups. Below this, a table lists 57 Backups. A dropdown menu is open for the first backup, showing options: **Details & Backup List**, **Backup Now**, and **Pause Backups**.

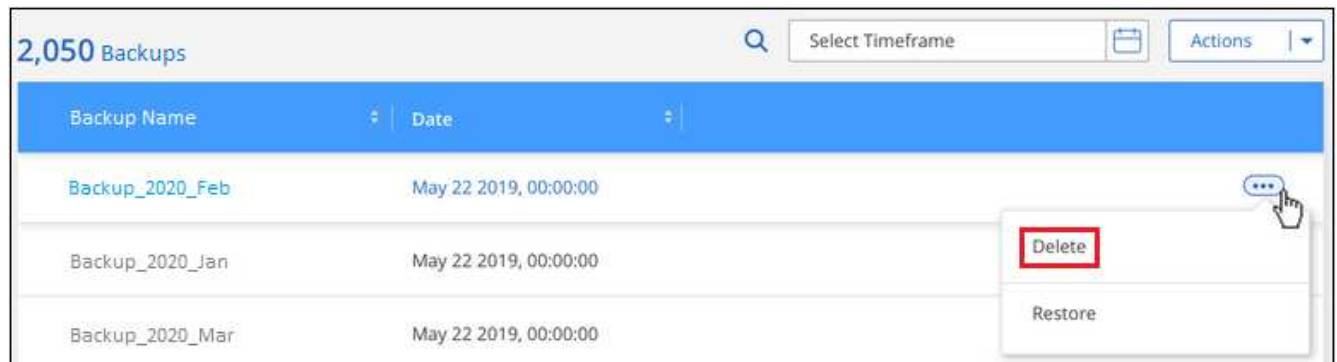
Source Kubernetes Cluster	Source Persistent Volume	Source Namespace	Last Backup	Backups	Backup Status
Kubernetes_Cloud_AWS	Source Persistent Volume	Source Namespace	May 22 2019, 00:00:00	2,050 Backups	Active
Kubernetes_Cloud_AWS	Source Persistent Volume	Source Namespace	May 22 2019, 00:00:00	2,050 Snapshot	
Kubernetes_Cloud_AWS	Source Persistent Volume	Source Namespace	May 22 2019, 00:00:00	2,050 Snapshot	

The list of all backup files is displayed.

The screenshot shows the NetApp Backup & Restore interface with the **Details & Backup List** view. The top navigation bar includes **Backup & Restore**, **Volumes**, **Restore**, **Applications**, **Virtual Machines**, **Kubernetes**, and **Job Monitoring**. The main content area is divided into three sections: **Source**, **Destination**, and **Backup Information**. Below these sections, a table lists 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

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



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

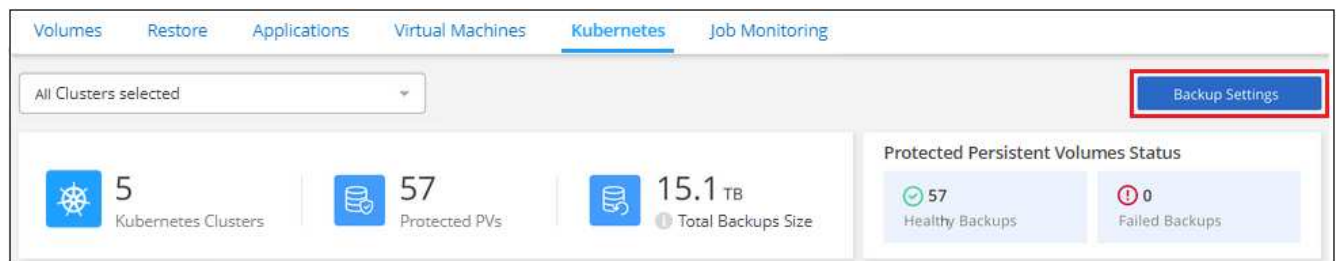
Disabling Cloud Backup for a working environment

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

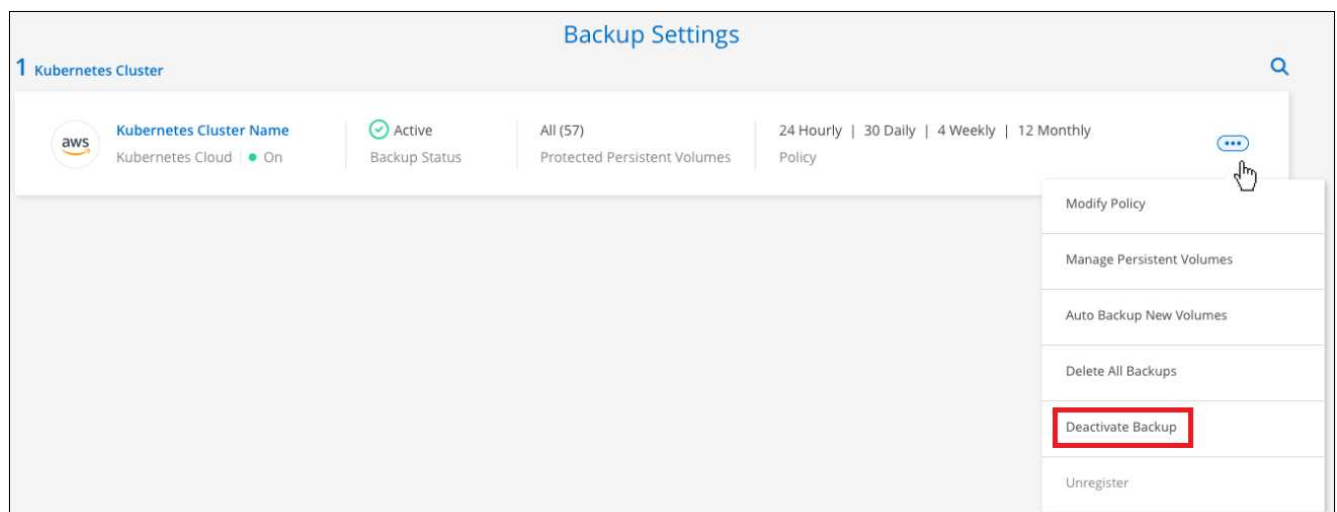
Note that you'll continue to be charged by your cloud provider for object storage costs for the capacity that your backups use unless you [delete the backups](#).

Steps

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



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



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



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

Unregistering Cloud Backup for a working environment

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

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

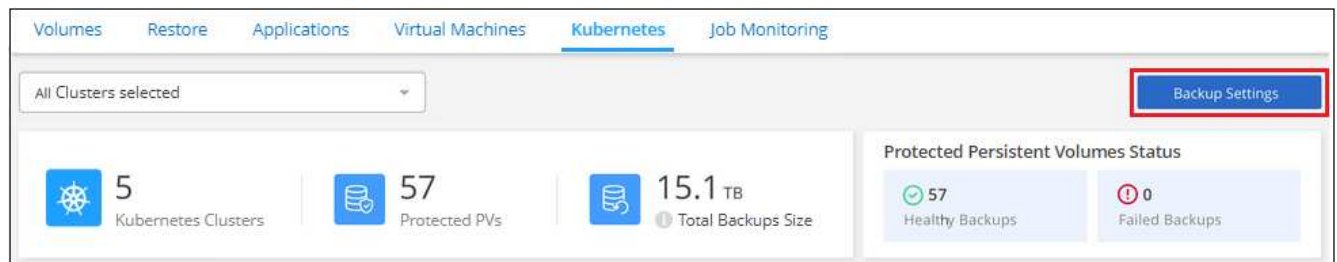
Before you can unregister Cloud Backup, you must perform the following steps, in this order:

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

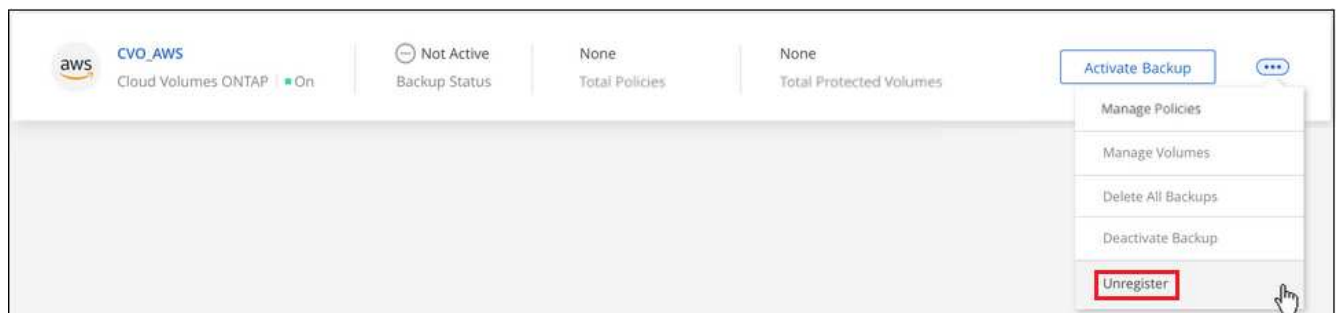
The unregister option is not available until these two actions are complete.

Steps

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



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



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

Restoring Kubernetes data from backup files

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

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

Supported working environments and object storage providers

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

Backup File Location	Destination Working Environment
Amazon S3	Kubernetes cluster in AWS

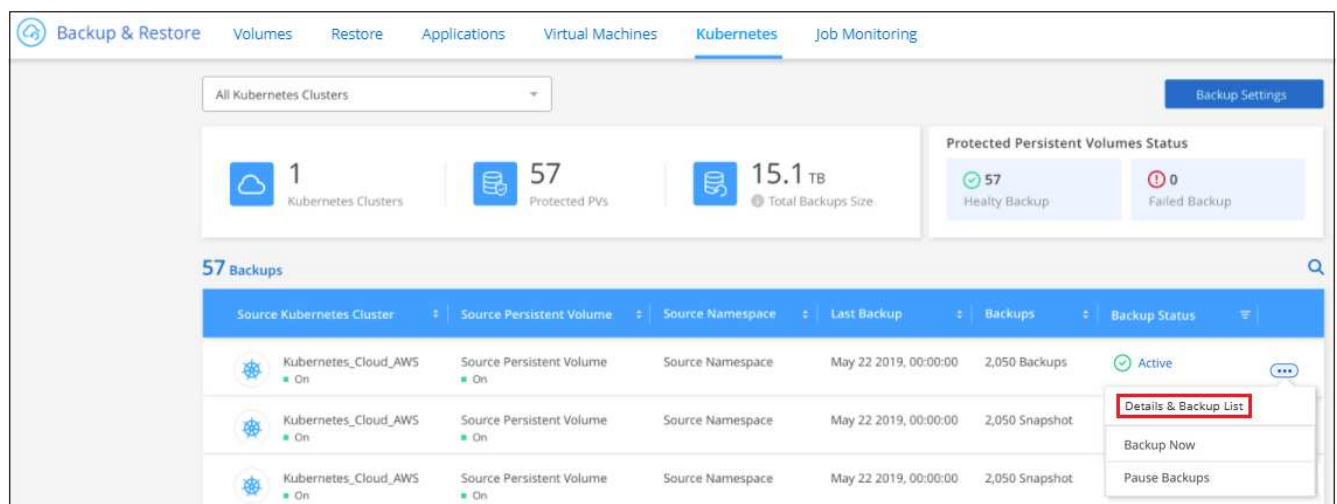
Restoring volumes from a Kubernetes backup file

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

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

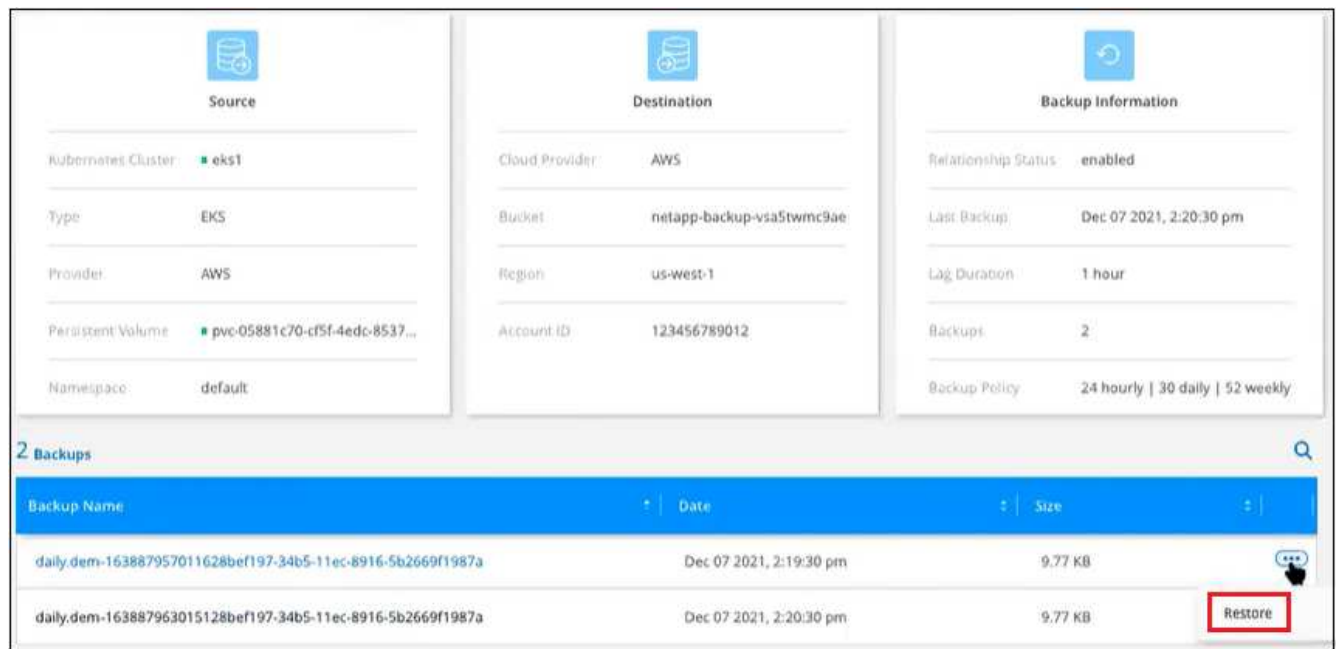
Steps

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



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

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



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

Select Destination

Select Kubernetes Cluster

eks1

Namespace

default

Storage Class

basic

PVC Name

pvc-05881c70-cf5f-4edc-8537-a0a5ce36f9a1-restore

Cancel

Restore

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

Result

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

Back up and restore on-premises applications data

Protect your on-premises applications data

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

You can back up Oracle and Microsoft SQL applications data from on-premises ONTAP systems to the following cloud providers:

- Amazon Web Services
- Microsoft Azure



You should be using SnapCenter Software 4.6.

For more information about Cloud Backup for Applications, refer to:

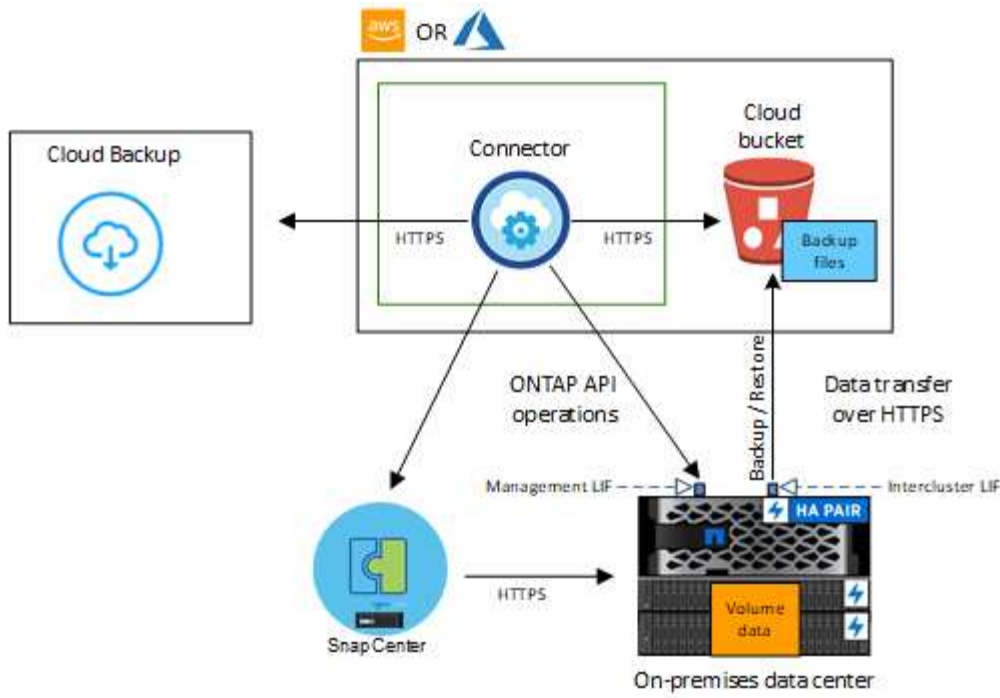
- [Application aware backup with Cloud Backup and SnapCenter](#)
- [Cloud backup for applications](#)

Requirements

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

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

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



Protection Policies

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



Custom policies are not supported.

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

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

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

Back up on-premises applications data to cloud

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

Register SnapCenter Server

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

Steps

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

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

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

The tags are comma separated.

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

5. Click **Register**.

After you finish

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



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

The supported applications and their configurations are:

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

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

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

Back up applications data

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



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

If you are protecting an SQL Server instance, then cloud protection will be configured for all the volumes of the eligible databases in that instance.

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

Steps

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

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

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

Cloud Backup for Applications supports only cluster admin.

- c. Click **Add Working Environment**.



You should not proceed until the working environment details are updated. It might take up to 30 minutes for the working environment details to be updated. After 30 minutes, you should close the wizard and retry from step 1 to view the working environment details.

After retrying if the working environment details are not updated, ensure that you have added the right working environment.

4. Select and configure the cloud provider.

Configure Amazon Web Services

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

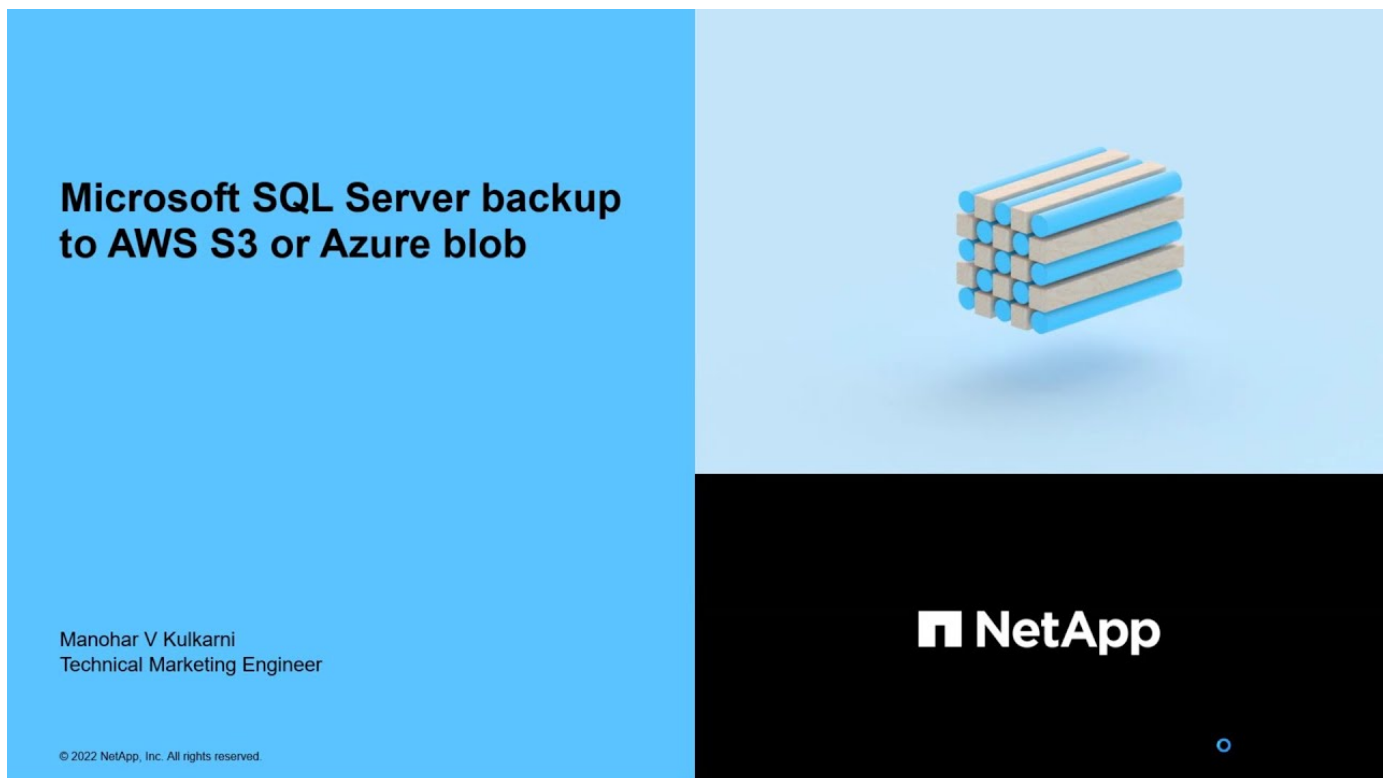
Configure Microsoft Azure

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

5. In the Assign Policy page, select the policy and click **Next**.

6. Review the details and click **Activate Backup**.

The following video shows a quick walkthrough of protecting a database:



Manage protection of applications

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

View policies

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

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

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



You should not delete the Cloud Backup for Applications policies.

You can also view cloud extended SnapCenter policies, by running the `Get-SmResources SnapCenter cmdlet`.

The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running `Get-Help command_name`. Alternatively, you can also refer the [SnapCenter Software Cmdlet Reference Guide](#).

View backups on cloud

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

1. Click **Backup & Restore > Applications**.
2. Click **...** corresponding to the application and click **View Details**.



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

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



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

You can also view these backups by running the `Get-SmBackup SnapCenter cmdlet`.

The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running `Get-Help command_name`. Alternatively, you can also refer the [SnapCenter Software Cmdlet Reference Guide](#).

Database layout change

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

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

The new volumes are discovered.

4. Click **...** corresponding to the application and click **Refresh Protection** to enable cloud protection for the new volume.

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

Policy or resource group change

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

1. Click **Backup & Restore > Applications**.
2. Click **...** corresponding to the application and click **Refresh Protection**.

Monitor Jobs

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

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

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

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

Configure CA Certificates

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

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

Steps

1. Copy the certificate to the volume that can be accessed from the docker agent.

```
° cd /var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/mkdir  
  sc_certs  
° chmod 777 sc_certs
```

2. Copy the RootCA certificate files to the above folder on the connector machine.

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

3. Copy the CRL file to the volume which can be accessed from the docker agent.

```
° cd /var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/mkdir sc_crl
° chmod 777 sc_crl
```

4. Copy the CRL files to the above folder on the connector machine.

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

5. After copying the certificates and CRL files, restart the Cloud Backup for Apps service.

```
° sudo docker exec cloudmanager_snapcenter sed -i 's/skipSCCertValidation:
true/skipSCCertValidation: false/g' /opt/netapp/cloudmanager-snapcenter-
agent/config/config.yml
° sudo docker restart cloudmanager_snapcenter
```

Restore applications data

Restore Oracle database

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

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

Steps

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

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

If a database is in the open state, and for restore the database needs to be in the mounted state, then the database state is changed only if you select this check box.

5. On the Recovery Scope page, perform the following actions:
 - a. Specify the recovery scope.

If you...	Do this...
Want to recover to the last transaction	Select All Logs .
Want to recover to a specific System Change Number (SCN)	Select Until SCN (System Change Number) .
Want to recover to a specific data and time	Select Date and Time . You must specify the date and time of the database host's time zone.
Do not want to recover	Select No recovery .
Want to specify any external archive log locations	If the archive logs are not present in the AFS, you should specify the location that contains the archive logs required for recovery.

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

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

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


Restore SQL Server database

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

Steps

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

Option	Description
Restore the database to the same host where the backup was created	Select this option if you want to restore the database to the same SQL server where the backups are taken.

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

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

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

7. On the **Post Restore Options** page, to specify the database state for restoring additional transactional logs, select one of the following options:

- Select **Operational, but unavailable** if you are restoring all of the necessary backups now.

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

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

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

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

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

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

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

Back up and restore Virtual Machines data

Protect your virtual machines data

You can protect data on your virtual machines by integrating the SnapCenter Plug-in for VMware vSphere with Cloud Manager. You can back up datastores to the cloud and restore virtual machines back to the on-premises SnapCenter Plug-in for VMware vSphere with ease.

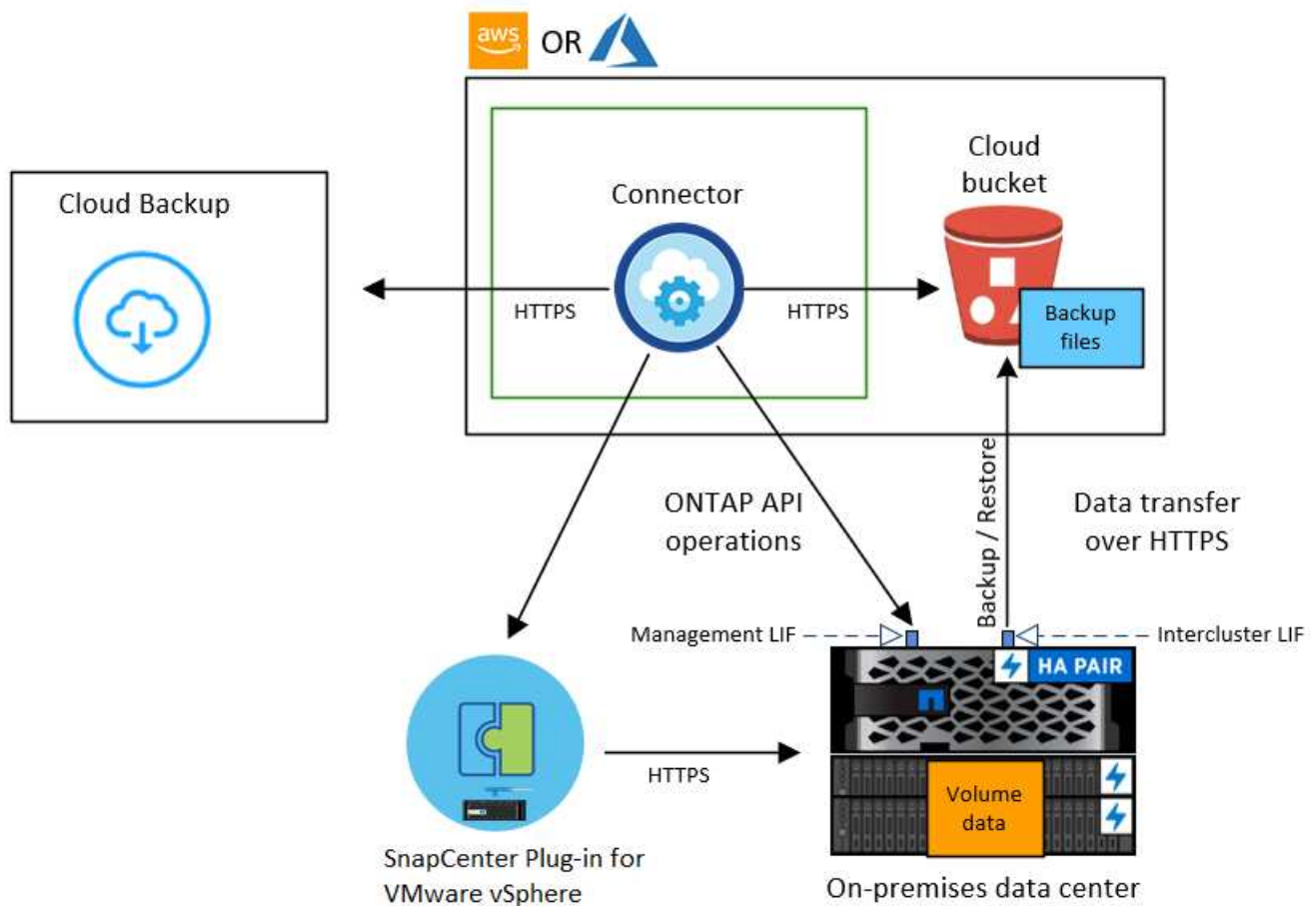
You can back up datastores to Amazon Web Services S3 or Microsoft Azure Blob.

Requirements

Read the following requirements to make sure that you have a supported configuration before you start backing up datastores and virtual machines to cloud services.

- SnapCenter Plug-in for VMware vSphere 4.6P1 or later
- ONTAP 9.8 or later
- Cloud Manager 3.9 or later
- At least one backup should have been taken in SnapCenter Plug-in for VMware vSphere 4.6P1.
- At least one daily, weekly, or monthly policy in SnapCenter Plug-in for VMware vSphere with no label or same label as that of the Cloud Backup for Virtual Machines policy in Cloud Manager.
- For a pre-canned policy, the schedule tier should be the same for the datastore in SnapCenter Plug-in for VMware vSphere and in the cloud.
- Ensure that there are no FlexGroup volumes in the datastore because backing up and restoring FlexGroup volumes are not supported.
- Ensure that none of the volumes are encrypted because restoring encrypted volumes are not supported.
- Disable "**_recent**" on the required resource groups. If you have "**_recent**" enabled for the resource group, then the backups of those resource groups cannot be used for data protection to cloud and subsequently cannot be used for the restore operation.
- Ensure that the destination datastore where the virtual machine will be restored has enough space to accommodate a copy of all virtual machine files such as VMDK, VMX, VMSSD, and so on.
- Ensure that the destination datastore does not have stale virtual machine files in the format of `restore_xxx_xxxxxx_filename` from the previous restore operation failures. You should delete the stale files before triggering a restore operation.

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



Protection Policies

You should use the one of the policies defined in the Cloud Backup for virtual machines to back up datastores to cloud.



Custom policies are not supported.

You can view the default policies by clicking **Backup & Restore > Virtual Machines > Policies** in Cloud Manager.

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

Back up datastores to the cloud

You can back up datastores to the cloud by integrating the SnapCenter Plug-in for VMware vSphere with Cloud Manager. This will help the VM administrators to easily and quickly back up and archive data for storage efficiency and accelerate cloud transition.



Ensure that you have met all the [requirements](#) before backing up datastores to the cloud.

Register SnapCenter Plug-in for VMware vSphere

You should register the SnapCenter Plug-in for VMware vSphere in Cloud Manager for the datastores and virtual machines to be displayed in Cloud Manager. Only a user with administrative access can register the SnapCenter Plug-in for VMware vSphere.



You can register multiple SnapCenter Plug-in for VMware vSphere. However, once registered, you cannot remove the SnapCenter Plug-in for VMware vSphere.

Steps

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

You should ensure that the port is open for communication to happen between SnapCenter Plug-in for VMware vSphere and Cloud Backup for Applications.

- c. In the Username and Password field, specify the credentials of the user with the administrator role.
5. Click **Register**.

After you finish

Click **Backup & Restore > Virtual Machines** to view all the datastores and virtual machines that are eligible for protection using the registered SnapCenter Plug-in for VMware vSphere.

Back up datastores

You can back up one or more datastores simultaneously to the cloud using a single policy. Only the default policies can be assigned to the datastore.

Steps

1. In Cloud Manager UI, click **Backup & Restore > Virtual Machines**.
2. Click **...** corresponding to the datastore that you want to back up and click **Activate Backup**.
3. Add the working environment.

Configure the ONTAP clusters that you want Cloud Manager to discover to back up your datastores. After adding the working environment for one of the datastores, it can be reused for all the other datastores residing on the same ONTAP cluster.

- a. Click **Add Working Environment** corresponding to the SVM.
 - b. In the Add Working Environment wizard:
 - i. Specify the IP address of the ONTAP cluster.
 - ii. Specify the credentials of the ONTAP cluster user.
 - c. Click **Add Working Environment**.
4. Select and configure the cloud provider.

Configure Amazon Web Services

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

Configure Microsoft Azure

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

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

Manage protection of virtual machines

You can view policies, datastores, and virtual machines before you back up and restore data. Depending upon the change in database, policies, or resource groups, you can refresh the updates from the Cloud Manager UI.

View policies

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

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

The associated Cloud Backup for Virtual Machines policies and all the virtual machines are listed.

View the datastores and virtual machines

The datastores and virtual machines that are protected using the registered SnapCenter Plug-in for VMware vSphere are displayed.

About this task

- Only NFS datastores are displayed.
- Only datastores for which at least one successful backup has been taken in SnapCenter Plug-in for VMware vSphere are displayed.

Steps

1. In Cloud Manager UI, click **Backup & Restore > Virtual Machines > Settings > SnapCenter Plug-in for VMware vSphere**.
2. Click the SnapCenter Plug-in for VMware vSphere for which you want to see the datastores and virtual machines.

Edit the SnapCenter Plug-in for VMware vSphere Instance

You can edit the details of the SnapCenter Plug-in for VMware vSphere in Cloud Manager

Steps

1. In Cloud Manager UI, click **Backup & Restore > Virtual Machines > Settings > SnapCenter Plug-in for VMware vSphere**.
2. Click and select **Edit**
3. Modify the details as required
4. Click **Save**.

Refresh Protection Status

When new volumes are added to the database, or if there is a change to the policy or resource group, you should refresh the protection.

1. Click **Backup & Restore > Virtual Machines**.
2. From the **Settings** drop-down, click **SnapCenter Plug-in for VMware vSphere**.
3. Click **...** corresponding to the SnapCenter Plug-in for VMware vSphere hosting the virtual machine and click **Refresh**.

The new changes are discovered.

4. Click **...** corresponding to the datastore and click **Refresh Protection** to enable cloud protection for the changes.

Monitor Jobs

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

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

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

monitor the job.

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

Restore virtual machines from the cloud

You can restore virtual machines from the cloud back to the on-premises vCenter. The backup will be restored to the exact same location from where the backup was taken. You cannot restore the backup to any other alternate location. You can restore virtual machines from the datastore or from the VMs view.



You cannot restore virtual machines that are spanned across datastores.

What you'll need

Ensure that you have met all the [requirements](#) before restoring virtual machines from the cloud.

Steps

1. In Cloud Manager, click **Backup & Restore > Virtual Machines > SnapCenter Plug-in for VMware vSphere** and select the SnapCenter Plug-in for VMware vSphere whose virtual machine you want to restore.



If the source virtual machine is moved to another location (vMotion), and if the user triggers a restore of that virtual machine from Cloud Manager, then the virtual machine will get restored to the original source location from where the backup was taken.

2. To restore from Datastore:
 - a. Click **...** corresponding to the datastore that you want to restore and click **View Details**.
 - b. Click **Restore** corresponding to the backup you want to restore.
 - c. Select the virtual machine that you want to restore from the backup and click **Next**.
 - d. Review the details and click **Restore**.
3. To restore from Virtual Machines:
 - a. Click **...** corresponding to the virtual machine that you want to restore and click **Restore**.
 - b. Select the backup through which you want to restore the virtual machine and click **Next**.
 - c. Review the details and click **Restore**.

The VM is restored to the same location from where the backup was taken.

Cloud Backup APIs

The Cloud Backup capabilities that are available through the web UI are also available through the RESTful API.

There are eight categories of endpoints defined within the Cloud Backup service:

- backup
- catalog
- cloud
- job
- license
- restore
- single file-level restore (SFR)
- working environment

Getting started

To get started with the Cloud Backup APIs, you'll need to obtain a user token, your Cloud Central account ID, and the Cloud Connector ID.

When making API calls, you'll add the user token in the Authorization header, and the Cloud Connector ID in the x-agent-id header. You should use the Cloud Central account ID in the APIs.

Steps

1. Obtain a user token from NetApp Cloud Central.

Make sure to generate the refresh token from the following xref:./ <https://services.cloud.netapp.com/refresh-token/>. The refresh token is an alpha-numeric string that you'll use to generate a user token.

```
curl --location --request POST 'https://netapp-cloud-  
account.auth0.com/oauth/token?=' \  
--header 'Content-Type: application/json' \  
-d '{  
  "grant_type": "refresh_token",  
  "refresh_token": "JxaVHn9cGkX92aPVCkhat3zxxxxxwsC9qMl_pLHkZtsVA",  
  "client_id": "Mu0V1ywgYteI6w1MbD15fKfVIUrNXGWC"  
}'
```

2. Obtain your NetApp Cloud Central account ID.

```
GET 'https://cloudmanager.cloud.netapp.com/tenancy/account' -H
'authority: cloudmanager.cloud.netapp.com'
Header:
-H 'accept: application/json'
-H 'accept-language: en-GB,en;q=0.9'
-H 'authorization: Bearer eyJhbGciOiJSUzI1NiIsInR.....
```

This API will return a response like the following. You can retrieve account ID by parsing the output from **[0].[accountPublicId]**.

```
[{"accountPublicId":"account-
i6vJXvZW","accountName":"rashidn","isSaas":true,"isGov":false,"isPrivate
PreviewEnabled":false,"is3rdPartyServicesEnabled":false,"accountSerial":
"96064469711530003565","userRole":"Role-1"}].....
```

3. Obtain the x-agent-id which contains the Cloud Manager Connector ID.

```
GET curl 'https://api.services.cloud.netapp.com/occm/list-occms/account-
OOnAR4ZS?excludeStandalone=true&source=saas' \
Header:
-H 'authority: api.services.cloud.netapp.com' \
-H 'accept: application/json' \
-H 'accept-language: en-GB,en;q=0.9' \
-H 'authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5.....
```

This API will return a response like the following. You can retrieve the agent id by parsing the output from **occm.[0].[agent].[agentId]**.

```
{
  "occms": [
    {
      "account": "account-OOOnAR4ZS",
      "accountName": "cbs",
      "occm": "imEdsEW4HyYTFbt8ZcNKTKDF05jMIe6Z",
      "agentId": "imEdsEW4HyYTFbt8ZcNKTKDF05jMIe6Z",
      "status": "ready",
      "occmName": "cbsgcpdevcntsg-asia",
      "primaryCallbackUri": "http://34.93.197.21",
      "manualOverrideUris": [],
      "automaticCallbackUris": [
        "http://34.93.197.21",
        "http://34.93.197.21/occmui",
        "https://34.93.197.21",
        "https://34.93.197.21/occmui",
        "http://10.138.0.16",
        "http://10.138.0.16/occmui",
        "https://10.138.0.16",
        "https://10.138.0.16/occmui",
        "http://localhost",
        "http://localhost/occmui",
        "http://localhost:1337",
        "http://localhost:1337/occmui",
        "https://localhost",
        "https://localhost/occmui",
        "https://localhost:1337",
        "https://localhost:1337/occmui"
      ],
      "createDate": "1652120369286",
      "agent": {
        "useDockerInfra": true,
        "network": "default",
        "name": "cbsgcpdevcntsg-asia",
        "agentId": "imEdsEW4HyYTFbt8ZcNKTKDF05jMIe6Zclients",
        "provider": "gcp",
        "systemId": "a3aa3578-bfee-4d16-9e10-"
      }
    }
  ]
}
```

Example using the APIs

The following example shows an API call to activate backup on Working Environment with a new policy that has daily, hourly, and weekly labels set and archive after days set as 180 days, in East-US-2 region in Azure cloud. Please note this enables backup only on Working Environment but no volumes are backed up. If you choose `"auto-backup-enabled": true` then any volumes already existing in the system would be backed up, plus future volumes added.

API Request

You'll see that we use the Cloud Central account ID "account-DpTFcxN3", Cloud Manager Connector ID "iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7lclients", and user token "Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IksrSXIPVFUzUWpZek1E...y6nyhBjwkeMwHc4ValobjUmju2x0xUH48g" in this command.

```

curl --location --request POST
'https://cloudmanager.cloud.netapp.com/account/account-
DpTFcxN3/providers/cloudmanager_cbs/api/v3/backup/working-
environment/VsaWorkingEnvironment-99hPYEgk' \
--header 'x-agent-id: iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Iks5rSx1PVFUzUWpZek1E...y6nyhBjwk
eMwHc4ValobjUmju2x0xUH48g' \
--data-raw '{
  "provider": "AZURE",
  "backup-policy": {
    "archive-after-days": 180,
    "rule": [
      {
        "label": "hourly",
        "retention": "2"
      },
      {
        "label": "daily",
        "retention": "30"
      },
      {
        "label": "weekly",
        "retention": "52"
      }
    ]
  },
  "ip-space": "Default",
  "region": "eastus2",
  "azure": {
    "resource-group": "rn-test-backup-rg",
    "subscription": "3beb4dd0-25d4-464f-9bb0-303d7cf5c0c2"
  }
}'

```

Response is a job ID that you can then monitor.

```

{
  "job-id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a"
}

```

Monitor the response.

```
curl --location --request GET
'https://cloudmanager.cloud.netapp.com/account/account-
DpTFcxN3/providers/cloudmanager_cbs/api/v1/job/1b34b6f6-8f43-40fb-9a52-
485b0dfe893a' \
--header 'x-agent-id: iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Iks5rSx1PVFUzUWpZek1E...hE9ss2Nub
K6wZRHUdSaORI7JvcOorUhJ8srqdiUiW6MvuGIFAQIh668of2M3dLbhVDBe8BBMtsa939UGnJx
7Qz6Eg'
```

Response.

```
{
  "job": [
    {
      "id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a",
      "type": "backup-working-environment",
      "status": "PENDING",
      "error": "",
      "time": 1651852160000
    }
  ]
}
```

Monitor until "status" is "COMPLETED".

```
{
  "job": [
    {
      "id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a",
      "type": "backup-working-environment",
      "status": "COMPLETED",
      "error": "",
      "time": 1651852160000
    }
  ]
}
```


What should I do when the token expires?

The user token from NetApp Cloud Central has an expiration date. To refresh the token, you need to call the API from step 1 again.

The API response includes an "expires_in" field that states when the token expires.

API reference

Documentation for each Cloud Backup API is available from <https://docs.netapp.com/us-en/cloud-manager-automation/cbs/overview.html>.

Reference

AWS S3 archival storage classes and restore retrieval times

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

Supported S3 archival storage classes for Cloud Backup

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

If your source clusters are running ONTAP 9.10.1 or greater, you can choose to tier backups to either S3 *Glacier* or S3 *Glacier Deep Archive* storage after a certain number of days (typically more than 30 days) for further cost optimization. Data in these tiers can't be accessed immediately when needed, and will require a higher retrieval cost, so you need to consider how often you may need to restore data from these archived backup files. See the section about [restoring data from archival storage](#).

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

[Learn about S3 storage classes](#).

Restoring data from archival storage

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

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

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

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

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

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

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

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

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

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

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

Azure archival tiers and restore retrieval times

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

Supported Azure Blob access tiers for Cloud Backup

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

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

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

[Learn about Azure Blob access tiers](#).

Restoring data from archival storage

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

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

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

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

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

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

There are 2 parts that make up the restore time:

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

For more information about Azure Archive retrieval options, refer to [this Azure FAQ](#).

Cross-account and cross-region configurations

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

- [Configure Cloud Backup for multi-account access in AWS](#)

Configure backup for multi-account access in AWS

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

These steps are required only when you are [backing up Cloud Volumes ONTAP data to Amazon S3](#).

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

Set up VPC peering between accounts

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

aws Services ▾

Peering Connections > Create Peering Connection

Create Peering Connection

Peering connection name tag ⓘ

Select a local VPC to peer with

VPC (Requester)* ⓘ

CIDRs	CIDR	Status	Status Reason
	10.0.0.0/16	● associated	

Select another VPC to peer with

Account ☐ My account ☒ Another account

Account ID*

Region ☒ This region (us-east-1) ☐ Another Region

VPC ID (Accepter)*

A Success dialog displays.

Success

A VPC peering connection (pcx-049758069d9b7c140) has been requested.
The owner of **vpc-116d9174** must accept the peering connection.

Requester VPC owner	733004784675 (This account)	Accepter VPC owner	464262061435
Requester VPC ID	vpc-82f55afa	Accepter VPC ID	vpc-116d9174
Requester VPC Region	us-east-1	Accepter VPC Region	us-east-1
Requester VPC CIDRs	10.0.0.0/16	Accepter VPC CIDRs	-

The status of the peering connection shows as Pending Acceptance.

<input type="checkbox"/>	Name	Peering Connection	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs	Requester Owner	Accepter Owner
<input checked="" type="checkbox"/>	cbs-multi-ac...	pcx-049758069d9...	Pending Acceptance	vpc-82f55afa VP...	vpc-116d9174	10.0.0.0/16	-	733004784675	464262061435
<input type="checkbox"/>	cbs-multi-peer	pcx-05f2d310cb7f...	Deleted	vpc-82f55afa VP...	vpc-116d9174	-	-	733004784675	464262061435
<input type="checkbox"/>	New_Peering	pcx-6d55ca04	Active	vpc-b16c90d4 V...	vpc-fc2aa39a De...	172.31.0.0/16	192.168.0.0/16	733004784675	733004784675

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

Create Peering Connection
Actions ▾

☐
Name

☐
cbs-multi-ac...

☐
estycvoconnect

☒
pcx-049758069d9b7c140

☐
hlll-vpc-peer-chen

Accept Request
Reject Request
Delete VPC Peering Connection
Edit ClassicLink Settings
Edit DNS Settings
Add/Edit Tags

Active

Active

Pending Acceptance

Active

Requester VPC

vpc-0647747d | M...

vpc-116d9174

vpc-82f55afa

vpc-0d12df59528f...

Accepter VPC

vpc-116d9174

vpc-445d4f21

vpc-116d9174

vpc-824dc0e4 | nf...

Requester CIDRs

10.2.0.0/24

172.31.0.0/16

10.0.0.0/16

10.0.0.0/24

Accepter CIDRs

172.31.0.0/16

10.129.0.0/20

-

10.20.30.0/24

Requester Owner

464262061435

464262061435

733004784675

464262061435

Accepter Owner

464262061435

759995470648

464262061435

464262061435

Accept VPC Peering Connection Request

Are you sure you want to accept this VPC peering connection request (pcx-049758069d9b7c140)?

Requester Account ID	733004784675	Acceptor Account ID	464262061435 (This account)
Requester VPC ID	vpc-82f55afa	Acceptor VPC ID	vpc-116d9174
Requester VPC Region	us-east-1	Acceptor VPC Region	us-east-1
Requester VPC CIDR	10.0.0.0/16	Acceptor VPC CIDR	-

Cancel
Yes, Accept

a. Click **Yes**.

Accept VPC Peering Connection Request

Your VPC Peering Connection has been established.

To send and receive traffic across this VPC peering connection, you must add a route to the peered VPC in one or more of your VPC route tables. [Learn more](#)

[Modify my route tables now](#)

Close

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

<input type="checkbox"/>	Name	Peering Connection	Status	Requester VPC	Acceptor VPC	Requester CIDRs	Acceptor CIDRs	Requester Owner	Acceptor Owner
<input type="checkbox"/>		pcx-004715531514cb0d8	Active	vpc-0647747d M...	vpc-116d9174	10.2.0.0/24	172.31.0.0/16	464262061435	464262061435
<input type="checkbox"/>	estycvoconnect	pcx-0305041f9cc2dfbdb	Active	vpc-116d9174	vpc-445d4f21	172.31.0.0/16	10.129.0.0/20	464262061435	759995470648
<input checked="" type="checkbox"/>	cbs-multi-account	pcx-049758069d9b7c140	Active	vpc-82f55afa	vpc-116d9174	10.0.0.0/16	172.31.0.0/16	733004784675	464262061435
<input type="checkbox"/>	hili-vpc-peer-chen	pcx-0d0e5c7fc4360254d	Active	vpc-0d12df59528f...	vpc-824dc0e4 nf...	10.0.0.0/24	10.20.30.0/24	464262061435	464262061435

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

<input type="checkbox"/>	Name	Peering Connection	Status	Requester VPC	Acceptor VPC	Requester CIDRs	Acceptor CIDRs	Requester Owner	Acceptor Owner
<input checked="" type="checkbox"/>	cbs-multi-account	pcx-049758069d9b7c140	Active	vpc-82f55afa VP...	vpc-116d9174	10.0.0.0/16	172.31.0.0/16	733004784675	464262061435
<input type="checkbox"/>	New_Peering	pcx-6d55ca04	Active	vpc-b16c90d4 V...	vpc-fc2aa39a De...	172.31.0.0/16	192.168.0.0/16	733004784675	733004784675

Add a route to the route tables in both accounts

- Go to VPC > Subnet > Route table.

VPC > Subnets > subnet-4d315328

subnet-4d315328 / The Subnet created

Details

Subnet ID subnet-4d315328	State Available	VPC vpc-116d9174	IPv4 CIDR 172.31.64.0/20
Available IPv4 addresses 3587	IPv6 CIDR -	Availability Zone us-east-1a	Availability Zone ID use1-az1
Network border group us-east-1	Route table rtb-4da55528	Network ACL acl-c37384a6	Default subnet Yes
Auto-assign public IPv4 address Yes	Auto-assign IPv6 address No	Auto-assign customer-owned IPv4 address No	Customer-owned IPv4 pool -
Outpost ID -	Owner 464262061435	Subnet ARN arn:aws:ec2:us-east-1:464262061435:subnet/subnet-4d315328	

[Flow logs](#)
[Route table](#)
[Network ACL](#)
[Sharing](#)
[Tags](#)

2. Click on the Routes tab.

Route Table ID : rtb-4da55528 Add filter

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
rtb-4da55528	subnet-4d315328	-		Yes	vpc-116d9174	464262061435

Route Table: rtb-4da55528

[Summary](#)
[Routes](#)
[Subnet Associations](#)
[Edge Associations](#)
[Route Propagation](#)
[Tags](#)

[Edit routes](#)

View All routes

Destination	Target	Status	Propagated
172.31.0.0/16	local	active	No
pl-63a5400a	vpce-098587ed33c36408c	active	No

3. Click **Edit routes**.

Edit routes

Destination	Target	Status	Propagated
172.31.0.0/16	local	active	No
10.20.30.0/24	pcx-0791b47f6f9a27d65	active	No
10.129.0.0/20	pcx-0305041f9cc2dfbdb	active	No

[Add route](#)

* Required

[Cancel](#)
[Save routes](#)

4. Click **Add route**, and from the Target drop-down list select **Peering Connection**, and then select the peering connection that you created.

a. In the Destination, enter the other account's subnet CIDR.

Edit routes

Destination	Target	Status	Propagated
172.31.0.0/16	local	active	No
10.20.30.0/24	pcx-0791b47f6f9a27d65	active	No
10.129.0.0/20	pcx-0305041f9cc2dfbdb	active	No
10.0.0.0/24	pcx-		No

Add route

* Required

pcx-05f2d310cb7f49843

pcx-004715531514cb0d8

pcx-049758069d9b7c140 cbs-multi-account

pcx-094f9fdb10a2045ea hill-peer-vadim-vpc

pcx-0791b47f6f9a27d65

pcx-0305041f9cc2dfbdb estycvoconnect

Cancel Save routes

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

[Route Tables](#) > Edit routes

Edit routes

✓ Routes successfully edited

Close

Add the second AWS account credentials in Cloud Manager

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

Credentials

+ Add Credentials

3 Credentials

aws Instance Profile

Credential Type: AWS Keys

464262061435
AWS Account ID

aws-sub-a2
Subscription

CBS-SR-OCCMOCCM1620912870830...
IAM Role

2
Working Environments

aws Saran-XCP-Dev

Credential Type: AWS Keys

733004784675
AWS Account ID

aws-sub-a2
Subscription

AKIA2VKT5MQRZRAWW3HI
AWS Access Key

0
Working Environments

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

Choose an AWS region and then select the working environment that you want to discover.

AWS Region
US East | N. Virginia

aws AWS Credentials

Credential Name

Saran-XCP-Dev | Account ID: 733004784675

Instance Profile | Account ID: 464262061435

To add new AWS credentials, go to the [Credentials settings](#).

Apply Cancel

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

Add an Existing Cloud Volumes ONTAP Region

↑ Previous Step This working environment will be created in Cloud Provider Account: **Saran-XCP-Dev** | Account ID: **733004784675** | [Switch Account](#)

Choose an AWS region and then select the working environment that you want to discover.

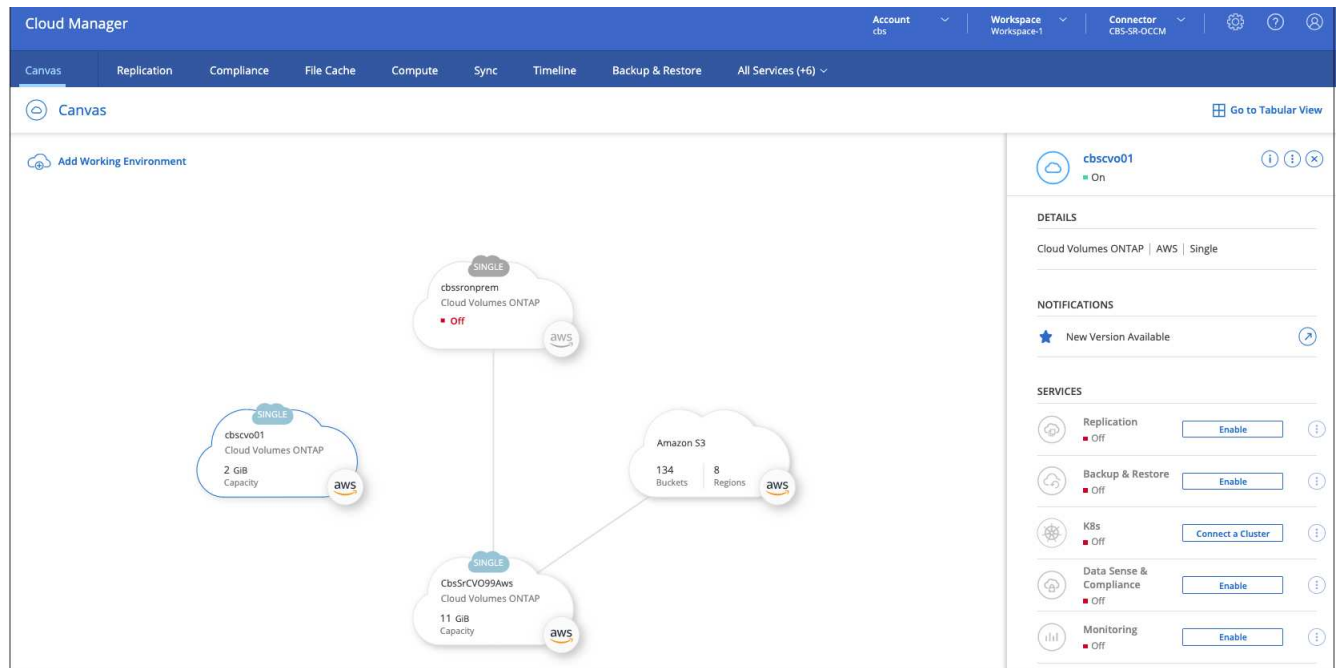
AWS Region
US East | N. Virginia

Cloud Volumes ONTAP instances found

Name	VPC Name	Availability Zone	Subnet Id	Cloud Formation Name	Cluster Address	Type
cbscv001	VPC-NAT	us-east-1f	subnet-68e8d464	cbscv001	10.0.0.80	Cloud Volumes ONTAP
testbyolliraz	VPC for VSA	us-east-1a	subnet-c1d99699	testbyolliraz	172.31.5.142	Cloud Volumes ONTAP
idanAwsHa991001	VPC for VSA	us-east-1a	subnet-c1d99699	idanAwsHa991001	172.31.5.234,172.31.5.110	HA Cloud Volumes ONTAP

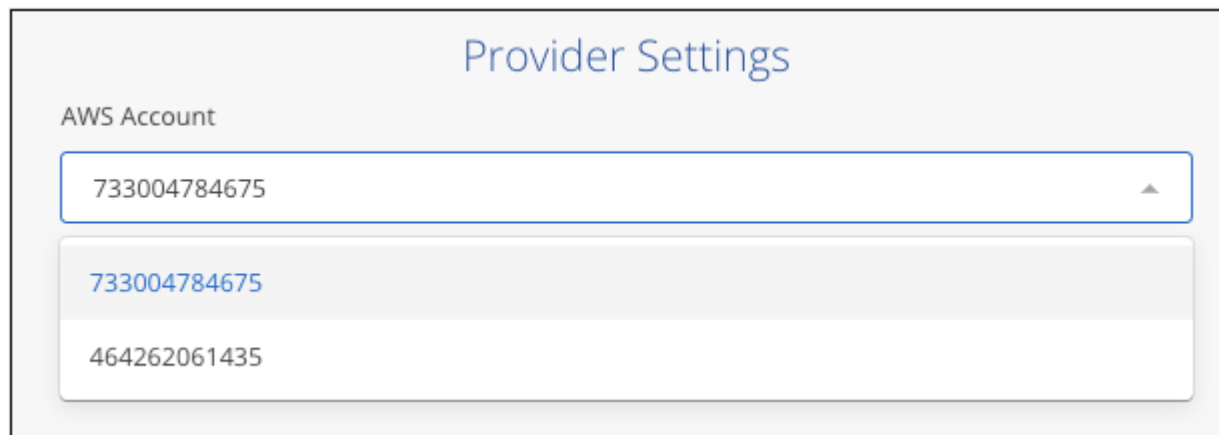
Continue

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



Enable backup in the other AWS account

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



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

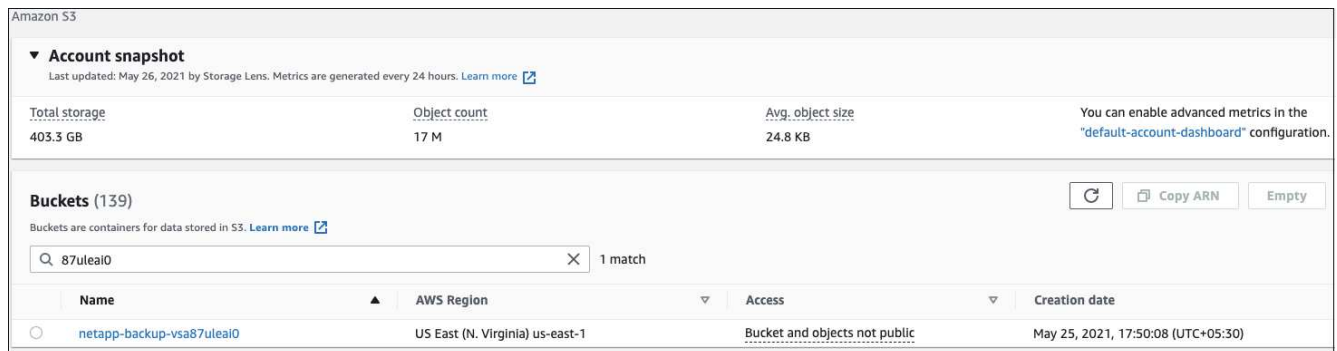
However, adding the bucket to the Cloud Volumes ONTAP system will fail because Cloud Backup uses the instance profile to add the bucket and the Cloud Manager instance profile doesn't have access to the resources in the second account.

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

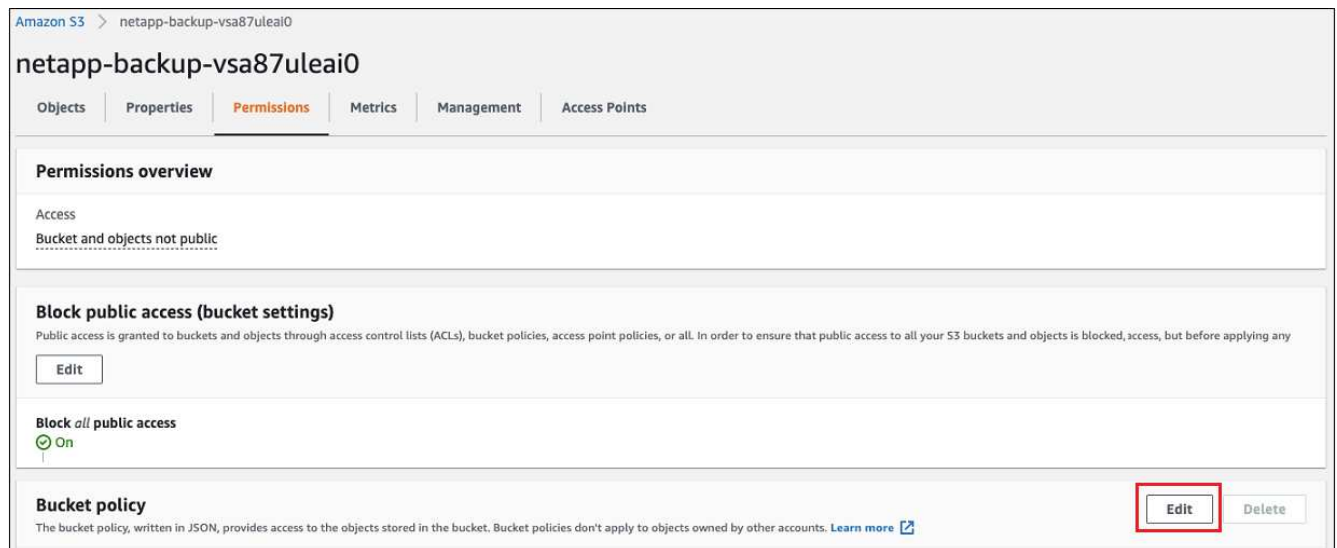


Cloud Backup creates every bucket with the prefix `Netapp-backup-` and will include the working environment ID; for example: `87ULeAI0`

4. In the EC2 portal, go to S3 and search for the bucket with name ending with `87uLeAI0` and you'll see the bucket name displayed as `Netapp-backup-vsa87uLeAI0`.



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



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

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

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

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

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

Configure backup for multi-account access in Azure

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

These steps are required only when you are [backing up Cloud Volumes ONTAP data to Azure Blob storage](#).

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

Set up VNet peering between accounts

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

connectivity.

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

Home > Virtual networks

NetApp HCL (netapphcl.onmicrosoft.com)

+ New Manage view Refresh Export to CSV Open query Assign tags Feedback

Filter for any field... Subscription == OCCM Dev Resource group == all Location == all Add filter

Showing 1 to 60 of 60 records.

<input type="checkbox"/> Name ↑↓	Resource group ↑↓	Location ↑↓
<input type="checkbox"/> cbsnetwork	occm_group_eastasia	East Asia
<input type="checkbox"/> Vnet1	occm_group_australiaeast	Australia East
<input type="checkbox"/> Vnet1	occm_group_australiasoutheast	Australia Southeast

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

Subscription * ⓘ
OCCM Automation

Virtual network *
cbse2evnet

Traffic to remote virtual network ⓘ
☒ Allow (default)
☐ Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ
☒ Allow (default)
☐ Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server ⓘ
☐ Use this virtual network's gateway or Route Server
☐ Use the remote virtual network's gateway or Route Server
☒ None (default)

Add

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

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

cbsnetwork | Peerings

Virtual network

Search (Cmd+/) << + Add Refresh

Filter by name...

Name	Peering status	Peer
cbsnetwork	Connected	cbse2evnet

Settings

- Address space
- Connected devices
- Subnets
- DDoS protection
- Firewall
- Security
- DNS servers
- Peerings**

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

Subscription * ⓘ

OCCM Dev

Virtual network *

cbsnetwork

Traffic to remote virtual network ⓘ

☒ Allow (default)

☐ Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ

☒ Allow (default)

☐ Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server ⓘ

☐ Use this virtual network's gateway or Route Server

☐ Use the remote virtual network's gateway or Route Server

☒ None (default)

Add

The peering settings are added.

cbse2evnet | Peerings ...

Virtual network

Search (Cmd+ /) << + Add ↻ Refresh

Filter by name...

Name	Peering status	Peer
cbsnetworkpeer	Connected	cbsnetwork

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Address space

Connected devices

Subnets

DDoS protection

Firewall

Security

DNS servers

Peerings

Create a private endpoint for the storage account

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



You need network contributor permission to perform the following action.

```
{
  "id": "/subscriptions/d333af45-0d07-4154-943dc25fbbce1b18/providers/Microsoft.Authorization/roleDefinitions/4d97b98b-1d4f-4787-a291-c67834d212e7",
  "properties": {
    "roleName": "Network Contributor",
    "description": "Lets you manage networks, but not access to them.",
    "assignableScopes": [
      "/"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Authorization/*/read",
          "Microsoft.Insights/alertRules/*",
          "Microsoft.Network/*",
          "Microsoft.ResourceHealth/availabilityStatuses/read",
          "Microsoft.Resources/deployments/*",
          "Microsoft.Resources/subscriptions/resourceGroups/read",
          "Microsoft.Support/*"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

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



2. In the Private Endpoint *Basics* page:

- Select subscription 2 (where the Cloud Manager Connector and Cloud Volumes ONTAP system are deployed) and the resource group.
- Enter an endpoint name.
- Select the region.

Create a private endpoint

1 Basics 2 Resource 3 Configuration 4 Tags 5 Review + create

Use private endpoints to privately connect to a service or resource. Your private endpoint must be in the same region as your virtual network, but can be in a different region from the private link resource that you are connecting to. [Learn more](#)

Project details

Subscription * ⓘ OCCM Dev

Resource group * ⓘ cbsoccmdevcvo-rg [Create new](#)

Instance details

Name * cbse2e ✓

Region * (Asia Pacific) East Asia

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

Create a private endpoint ...

✓ Basics **2 Resource** 3 Configuration 4 Tags 5 Review + create

Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. [Learn more](#)

Subscription OCCM Dev (d333af45-0d07-4154-943d-c25fbbce1b18)

Resource type Microsoft.Storage/storageAccounts

Resource test150521

Target sub-resource * ⓘ blob

4. In the Configuration page:

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

Create a private endpoint ...

✓ Basics ✓ Resource **3 Configuration** 4 Tags 5 Review + create

Networking

To deploy the private endpoint, select a virtual network subnet. [Learn more](#)

Virtual network * ⓘ cbsnetwork

Subnet * ⓘ default (10.2.0.0/24)

ⓘ If you have a network security group (NSG) enabled for the subnet above, it will be disabled for private endpoints on this subnet only. Other resources on the subnet will still have NSG enforcement.

Private DNS integration

To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone. You can also utilize your own DNS servers or create DNS records using the host files on your virtual machines. [Learn more](#)

Integrate with private DNS zone ☒ Yes ☐ No

Configuration name	Subscription	Private DNS zone
privatelink-blob-core-...	OCCM Dev	privatelink.blob.core.windows.net

Review + create < Previous Next : Tags >

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

Configuration name	Subscription	Private DNS zone
privatelink-blob-core-...	OCCM Dev	privatelink.blob.core.windows.net
		<input type="text" value="Filter private DNS zones"/> <div> <div>occm_group_centralus</div> <div>privatelink.blob.core.windows.net</div> <div>occm_group_eastus</div> <div>privatelink.blob.core.windows.net</div> <div>occm_group_eastus2</div> <div>privatelink.blob.core.windows.net</div> </div>

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

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

Knowledge and support

Register for support

Before you can open a support case with NetApp technical support, you need to add a NetApp Support Site account to Cloud Manager and then register for support.

Add an NSS account

The Support Dashboard enables you to add and manage all of your NetApp Support Site accounts from a single location.

Steps

1. If you don't have a NetApp Support Site account yet, [register for one](#).
2. In the upper right of the Cloud Manager console, click the Help icon, and select **Support**.



3. Click **NSS Management > Add NSS Account**.
4. When you're prompted, click **Continue** to be redirected to a Microsoft login page.

NetApp uses Microsoft Azure Active Directory as the identity provider for authentication services specific to support and licensing.
5. At the login page, provide your NetApp Support Site registered email address and password to perform the authentication process.

This action enables Cloud Manager to use your NSS account.

Note the account must be a customer-level account (not a guest or temp account).

Register your account for support

Support registration is available from Cloud Manager in the Support Dashboard.

Steps

1. In the upper right of the Cloud Manager console, click the Help icon, and select **Support**.



2. In the **Resources** tab, click **Register for Support**.
3. Select the NSS credentials that you want to register and then click **Register**.

Get help

NetApp provides support for Cloud Manager and its cloud services in a variety of ways. Extensive free self-support options are available 24x7, such as knowledgebase (KB) articles and a community forum. Your support registration includes remote technical support via web ticketing.

Self support

These options are available for free, 24 hours a day, 7 days a week:

- [Knowledge base](#)

Search through the Cloud Manager knowledge base to find helpful articles to troubleshoot issues.

- [Communities](#)

Join the Cloud Manager community to follow ongoing discussions or create new ones.

- [Documentation](#)

The Cloud Manager documentation that you're currently viewing.

- [Feedback email](#)

We value your input. Submit feedback to help us improve Cloud Manager.

NetApp support

In addition to the self-support options above, you can work with a NetApp Support Engineer to resolve any issues after you activate support.

Steps

1. In Cloud Manager, click **Help > Support**.
2. Choose one of the available options under Technical Support:
 - a. Click **Call Us** to find phone numbers for NetApp technical support.
 - b. Click **Open an Issue**, select one the options, and then click **Send**.

A NetApp representative will review your case and get back to you soon.

Legal notices

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

Copyright

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

Trademarks

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

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

Patents

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

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

Privacy policy

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

Open source

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

- [Notice for Cloud Manager 3.9](#)
- [Notice for the Cloud Backup](#)
- [Notice for Single File Restore](#)

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.