



# **Back up data to the cloud**

## **Cloud Manager**

NetApp  
April 22, 2021

# Table of Contents

- Back up data to the cloud . . . . . 1
  - Learn about Cloud Backup . . . . . 1
  - Get started . . . . . 7
- Managing backups for Cloud Volumes ONTAP and on-premises ONTAP systems . . . . . 33
- Restoring data from backup files . . . . . 37

# Back up data to the cloud

## Learn about Cloud Backup

Cloud Backup is an add-on service for Cloud Volumes ONTAP and on-premises ONTAP clusters that delivers backup and restore capabilities for protection, and long-term archive of your cloud data. Backups are automatically generated and stored in an object store in your cloud account, independent of volume Snapshot copies used for near-term recovery or cloning.

A snapshot is an instant record of your system metadata at a given moment in similar storage as the original file, while a data backup is a standalone replica of your data, stored away in a separate system.

There are two services that provide the full suite of backup and restore functionality:

- The **Cloud Backup service** enables you to create backup files from volumes on your Cloud Volumes ONTAP and on-prem ONTAP clusters.
- The **Restore service** enables you to restore an entire *volume*, or one or more *files*, from a backup file to the same or different Cloud Volumes ONTAP or on-premises ONTAP cluster.

[Learn more about the Cloud Backup Service.](#)



You must use Cloud Manager for all backup and restore operations. Any actions taken directly from ONTAP or from your cloud provider results in an unsupported configuration.

## Features

- Back up independent copies of your data volumes to low-cost object storage in the cloud.
- Backup data is secured with AES-256 bit encryption at-rest and TLS 1.2 HTTPS connections in-flight.
- Back up from cloud to cloud, and from on-premises ONTAP systems to cloud.
- Support for up to 1,019 backups of a single volume.
- Restore data from a specific point in time.
- Restore a volume or individual files to the source system or to a different system.
- Browsable file catalog for single file restore.

## Supported working environments and object storage providers

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

Source Working Environment	Backup File Destination
Cloud Volumes ONTAP in AWS	Amazon S3
Cloud Volumes ONTAP in Azure	Azure Blob
Cloud Volumes ONTAP in Google	Google Cloud Storage

Source Working Environment	Backup File Destination
On-premises ONTAP system	Amazon S3 Azure Blob

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

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

## 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 storage and for running a virtual machine/instance in the cloud.

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

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

- For file restore, you pay your cloud provider for compute costs only when the Restore instance is running.

The instance runs only when browsing the backup file to locate the individual files you want to restore. The instance is turned off when not in use to save costs. And it is not deployed at all if you never attempt to restore individual files.

See the [type of virtual machine/instance that is deployed](#) for each supported cloud provider.

- For volume restore there is no cost because no separate instance or virtual machine is required.

### Service charges

Backup 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 target backup capacity *before* ONTAP efficiencies.

There are two ways to pay for the Backup service. The first option is to subscribe from the service provider, which enables you to pay per month based on the amount of backed up data. 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: Bring Your Own License (BYOL) and Pay As You Go (PAYGO). 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.

Backups 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

For PAYGO you'll need to pay your cloud provider for object storage costs (as described earlier) and NetApp for backup licensing costs. The licensing costs are based on target backup capacity (before ONTAP storage efficiencies):

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

### Bring your own license

BYOL is term-based (1YR/2YR/3YR) and capacity-based in 1 TB increments, based on the logical (before ONTAP storage efficiencies) backed up capacity. You pay NetApp to use the service for a period of time, say 1 year, and for a maximum amount backup capacity, say 10 TB, and you'll need to pay your cloud provider for object storage costs (as described earlier).

You'll receive a serial number that you enter in the Cloud Manager Licensing page to enable the service. When either limit is reached you'll need to renew the license. See [Adding and updating your Backup BYOL license](#). The Backup BYOL license applies to all Cloud Volumes ONTAP and on-premises systems associated with your [Cloud Central account](#).

### BYOL license considerations

When using a Cloud Backup BYOL license, Cloud Manager notifies you when backups are nearing the capacity limit or nearing the license expiration date. You receive these notifications:

- 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 receive these notifications.

Two things can happen when your license expires:

- If the account you are using for your ONTAP systems has a marketplace account, the backup service continues to run, but you are shifted over to a PAYGO licensing model. You are charged by your cloud provider for object storage costs, and by NetApp for backup licensing costs, for the capacity that your backups are using.

- If the account you are using for your ONTAP systems does not have a marketplace account, the backup service continues to run, but you will continue to receive the expiration message.

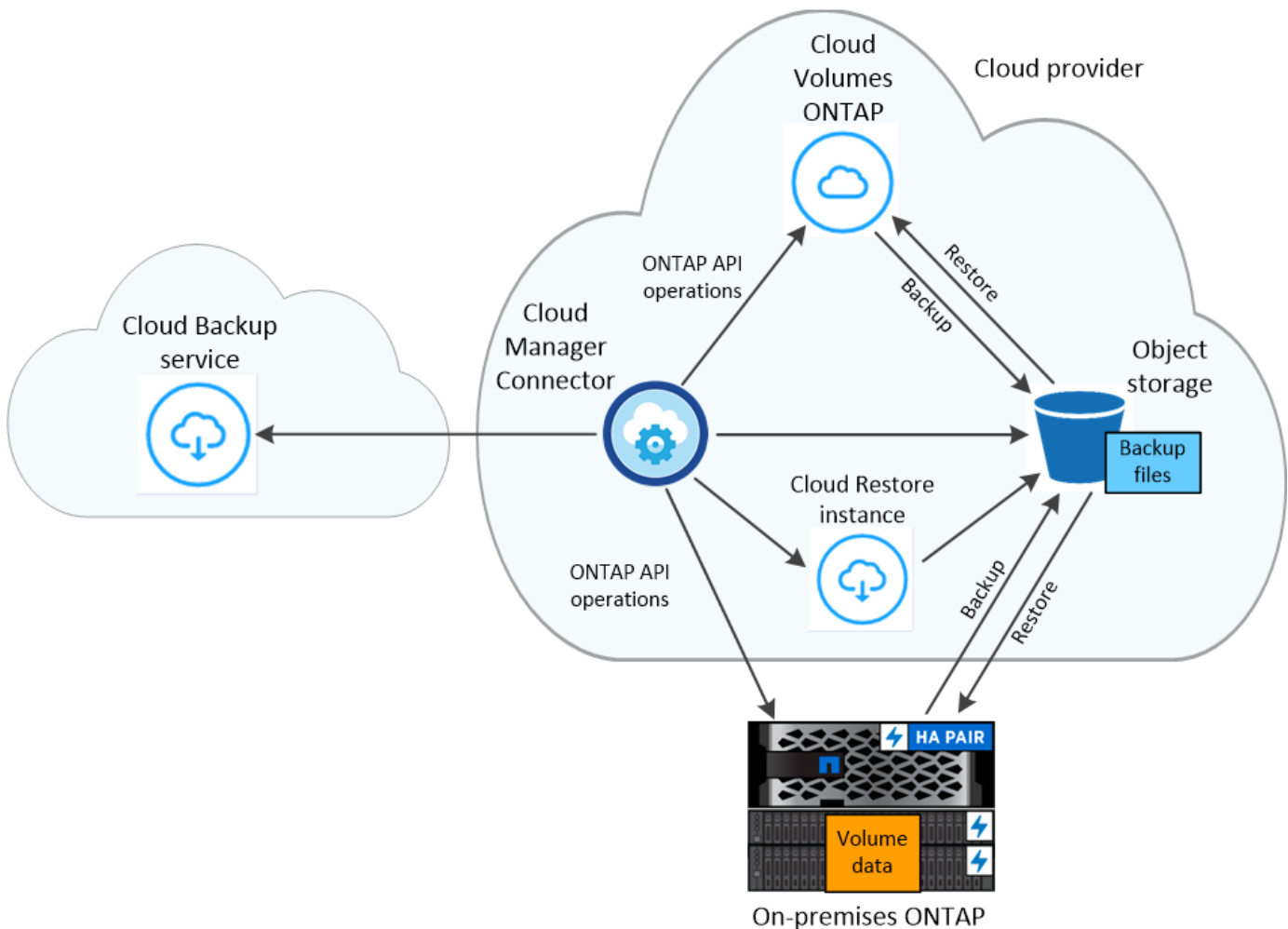
Once you renew your BYOL subscription, Cloud Manager automatically obtains the new license from NetApp and installs it. If Cloud Manager can't access the license file over the secure internet connection, you can obtain the file yourself and manually upload it to Cloud Manager. For instructions, see [Adding and updating your Backup BYOL 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 receiving the warning message and will be charged for backups that occurred while the license was expired.

## 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.

The following image shows the relationship between each component:



## Where backups reside

Backup copies are stored in an S3 bucket, Azure Blob container, or Google Cloud Storage bucket that Cloud

Manager creates in your cloud account. For Cloud Volumes ONTAP systems the object store is created in the same region where the Cloud Volumes ONTAP system is located. For on-premises ONTAP systems you identify the region when you enable the service.

There's one object store per Cloud Volumes ONTAP or on-premises ONTAP system. Cloud Manager names the object store as follows: `netapp-backup-clusteruuid`

Be sure not to delete this object store.

Notes:

- In AWS, Cloud Manager enables the [Amazon S3 Block Public Access feature](#) on the S3 bucket.
- In Azure, Cloud Manager uses a new or existing resource group with a storage account for the Blob container.
- In GCP, Cloud Manager uses a new or existing project with a storage account for the Google Cloud Storage bucket.

### Supported storage classes or access tiers

- In Amazon S3, backups start in the *Standard* storage class and transition to the *Standard-Infrequent Access* storage class after 30 days.
- In Azure, backups are associated with the *cool* access tier.
- In GCP, backups are associated with the *Standard* storage class by default.

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

### Backup settings are system wide

When you enable Cloud Backup, all the volumes you identify on the system are backed up to the cloud.

The schedule and number of backups to retain are defined at the system level. The backup settings affect all volumes on the system.

### The schedule is daily, weekly, monthly, or a combination

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

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

Backup protection policies that you have created on the system using ONTAP System Manager or the ONTAP

CLI are also available as selections.

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

Note that 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.

### Backups are taken at midnight

- 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 of each month.

The start time is based on the time zone set on each source ONTAP system. At this time, you can't schedule backup operations at a user specified time.

### Backup copies are associated with your Cloud Central account

Backup copies are associated with the [Cloud Central account](#) in which Cloud Manager resides.

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

### Supported volumes

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

FlexGroup volumes and SnapLock volumes aren't currently supported.

### 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 retrieval of all local and all tiered data (from the object store). 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.
- A backup operation does not "reheat" the cold data tiered in object storage.

### Limitations

- When making backups from on-premises ONTAP systems, the Connector must be deployed in the cloud.



There is no support for on-premises Connector deployments.

- When backing up data protection (DP) volumes:
  - Only DP volumes that are a destination of a Vault/MirrorAndVault relationship are supported. DP volumes created using the MirrorAllSnapshots policy cannot be backed up and will fail with an error.
  - The rule that is defined for the SnapMirror policy on the source volume must use a label that matches the allowed Cloud Backup policy names of **daily**, **weekly**, or **monthly**. Otherwise the backup will fail for that DP volume.
- In Azure, if you enable Cloud Backup when Cloud Volumes ONTAP is deployed, Cloud Manager creates the resource group for you and you cannot change it. If you want to pick your own resource group when enabling Cloud Backup, **disable** Cloud Backup when deploying Cloud Volumes ONTAP and then enable Cloud Backup and choose the resource group from the Cloud Backup Settings page.
- When backing up volumes from Cloud Volumes ONTAP systems, volumes that you create outside of Cloud Manager aren't automatically backed up. For example, if you create a volume from the ONTAP CLI, ONTAP API, or System Manager, then the volume won't be automatically backed up. If you want to back up these volumes, you would need to disable Cloud Backup and then enable it again.
- ILM (tiering) from the object storage, or direct write to AWS Glacier or similar lower tier object storage, is not supported.
- SVM-DR and SM-BC configurations are not supported.
- MetroCluster (MCC) backup is supported from ONTAP secondary only: MCC → SnapMirror → ONTAP → Cloud Backup Service → object storage.
- WORM/Compliance mode on an object store is not supported.

### Single File Restore limitations

- Single file restore can restore individual files. 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.
- The ONTAP version must be 9.6 or greater in your Cloud Volumes ONTAP or on-premises systems.
- Cross account restore requires manual action in the cloud provider console. See the AWS topic [granting cross-account bucket permissions](#) for details.
- Single file restore is not supported when using the same account with different Cloud Managers in different subnets.
- Restore can browse a single directory with flat files up to a maximum of 30,000 files. Larger directories are currently not supported.

## Get started

### 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

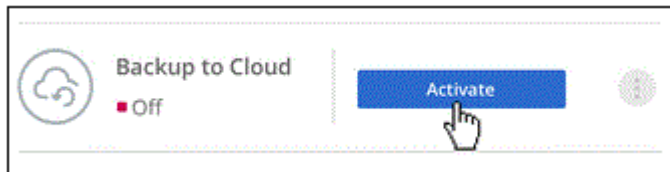
## Verify support for your configuration

- You're running Cloud Volumes ONTAP 9.6 or later in AWS.
- You have subscribed to the [Cloud Manager Marketplace Backup offering](#), or you have purchased **and activated** a Cloud Backup BYOL license from NetApp.
- The IAM role that provides Cloud Manager 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 **Activate** next to the Cloud Backup 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 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 to retain.

### Define Policy

Policy - Retention & Schedule

☒ Create a New Policy
 ☐ Select an Existing Policy

Backup Every

Day

Number of backups to retain

30

DP Volumes

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

Information

Backup\_Bucket\_Name

Bucket Name

## 4

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

Identify which volumes you want to back up in the Select Volumes page.

## 5

### Restore your data, as needed

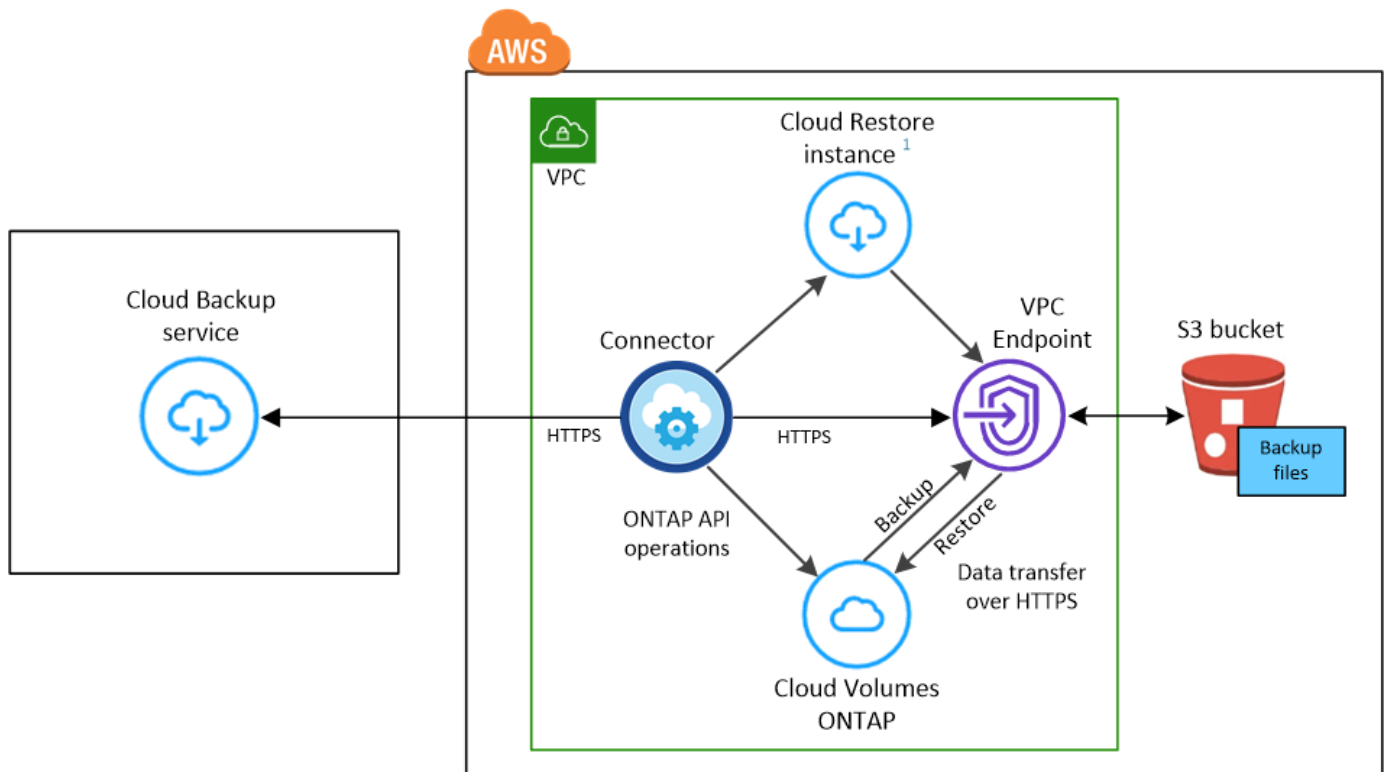
Choose to restore an entire backup to a new volume, or to restore individual files from the backup to an existing volume. You can restore data to a Cloud Volumes ONTAP system in AWS, or to an on-premises ONTAP system.

See [Restoring volume data from backup files](#) for details.

### 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:



<sup>1</sup> Cloud Restore instance is active only during single-file restore operations.

### Supported ONTAP versions

Cloud Volumes ONTAP 9.6 and later.

### Supported AWS regions

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

## License requirements

For Cloud Backup PAYGO licensing, a Cloud Manager subscription is available in the AWS Marketplace that enables deployments of Cloud Volumes ONTAP 9.6 and later (PAYGO) 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 Cloud Backup BYOL licensing, you do not need an AWS Cloud Backup subscription. You need the serial number from NetApp that enables you to use the service for the duration and capacity of the license. See [Adding and updating your Backup BYOL license](#).

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

## 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:

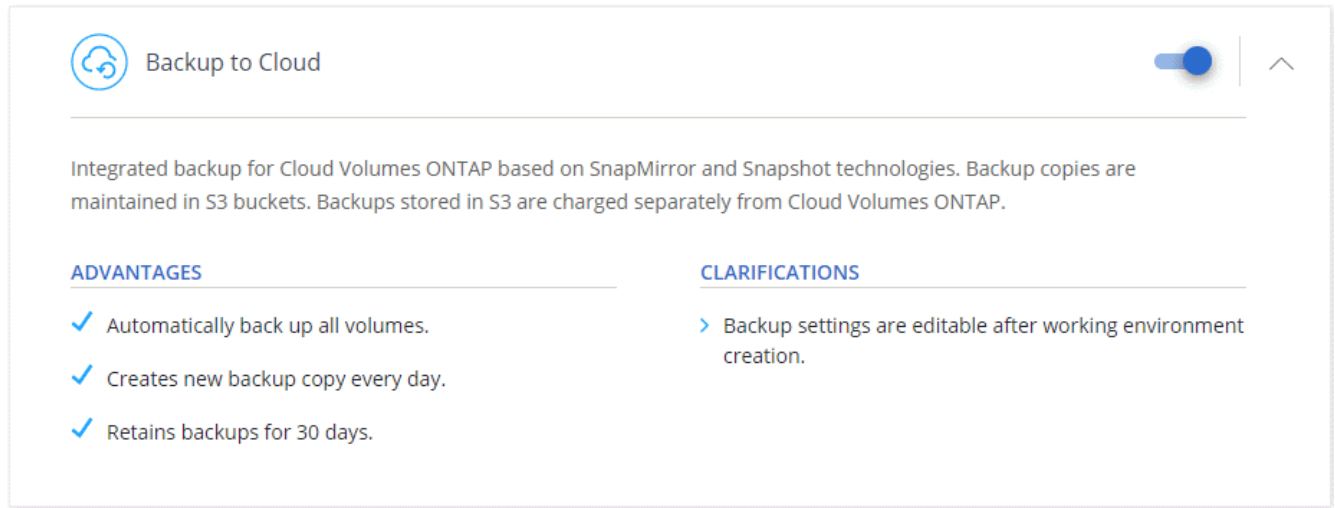
```
{
    "Sid": "backupPolicy",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",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

## Enabling Cloud Backup on a new system

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

### 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](#) and you can [restore entire volumes or individual files from a backup file](#).

## 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 **Activate** next to the Cloud Backup service in the right-panel.



2. Define the backup schedule and retention value and click **Continue**.

### Define Policy

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

Backup Every: 
 Number of backups to retain:

**DP Volumes**

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

**Information**

Backup\_Bucket\_Name  
Bucket Name

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

3. Select the volumes that you want to back up and click **Activate**.

Select Volumes

57 Volumes

<input checked="" type="checkbox"/>	Volume Name	Volume Type	Disk Type	SVM Name	Used Capacity	Allocated Capacity	Volume Status
<input checked="" type="checkbox"/>	Volume_Name_1	RW	GP2	SVM_Name_1	2.25 TB	10 TB	Active
<input checked="" type="checkbox"/>	Volume_Name_2	RW	GP2	SVM_Name_2	2.25 TB	10 TB	Active
<input checked="" type="checkbox"/>	Volume_Name_3	RW	GP2	SVM_Name_3	2.25 TB	10 TB	Active
<input checked="" type="checkbox"/>	Volume_Name_4	DP ⓘ	GP2	SVM_Name_4	2.25 TB	10 TB	Active
<input checked="" type="checkbox"/>	Volume_Name_5	RW	GP2	SVM_Name_5	2.25 TB	10 TB	Active

- 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).

## Result

Cloud Backup starts taking the initial backups of each selected volume.

## What's next?

You can [start and stop backups for volumes](#) or [change the backup schedule](#) and you can [restore entire volumes or individual files from a backup file](#).

## Backing up Cloud Volumes ONTAP data to Azure Blob storage

Complete a few steps to get started backing up data from Cloud Volumes ONTAP to Azure Blob storage.

## Quick start

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

1

### Verify support for your configuration

- You're running Cloud Volumes ONTAP 9.7 or later in Azure.
- You have a valid cloud provider subscription for the storage space where your backups will be located.
- You have subscribed to the [Cloud Manager Marketplace Backup offering](#), or you have purchased [and activated](#) a Cloud Backup BYOL license from NetApp.

2

### Enable Cloud Backup on your new or existing system

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



3

### Enter the provider details

Select the provider subscription and choose whether you want to create a new resource group or use an already existing resource group.

### Provider Settings

Azure Subscription

Azure\_Subscription\_1

Resource Group

☐ Create a new

☒ Use an existing

Select an Existing Resource Group

Resource\_Group\_1

## 4

### 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 weekly or monthly backups, or select one of the system-defined policies that provide more options.

### Define Policy

Policy - Retention & Schedule

☒ Create a New Policy
 ☐ Select an Existing Policy

Backup Every

Day

Number of backups to retain

30

DP Volumes

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

Storage Account

Cloud Manager will create the storage account after you complete the wizard

## 5

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

Identify which volumes you want to back up in the Select Volumes page.

## 6

### Restore your data, as needed

Choose to restore an entire backup to a new volume, or to restore individual files from the backup to an existing volume. You can restore data to a Cloud Volumes ONTAP system in Azure, or to an on-premises ONTAP system.

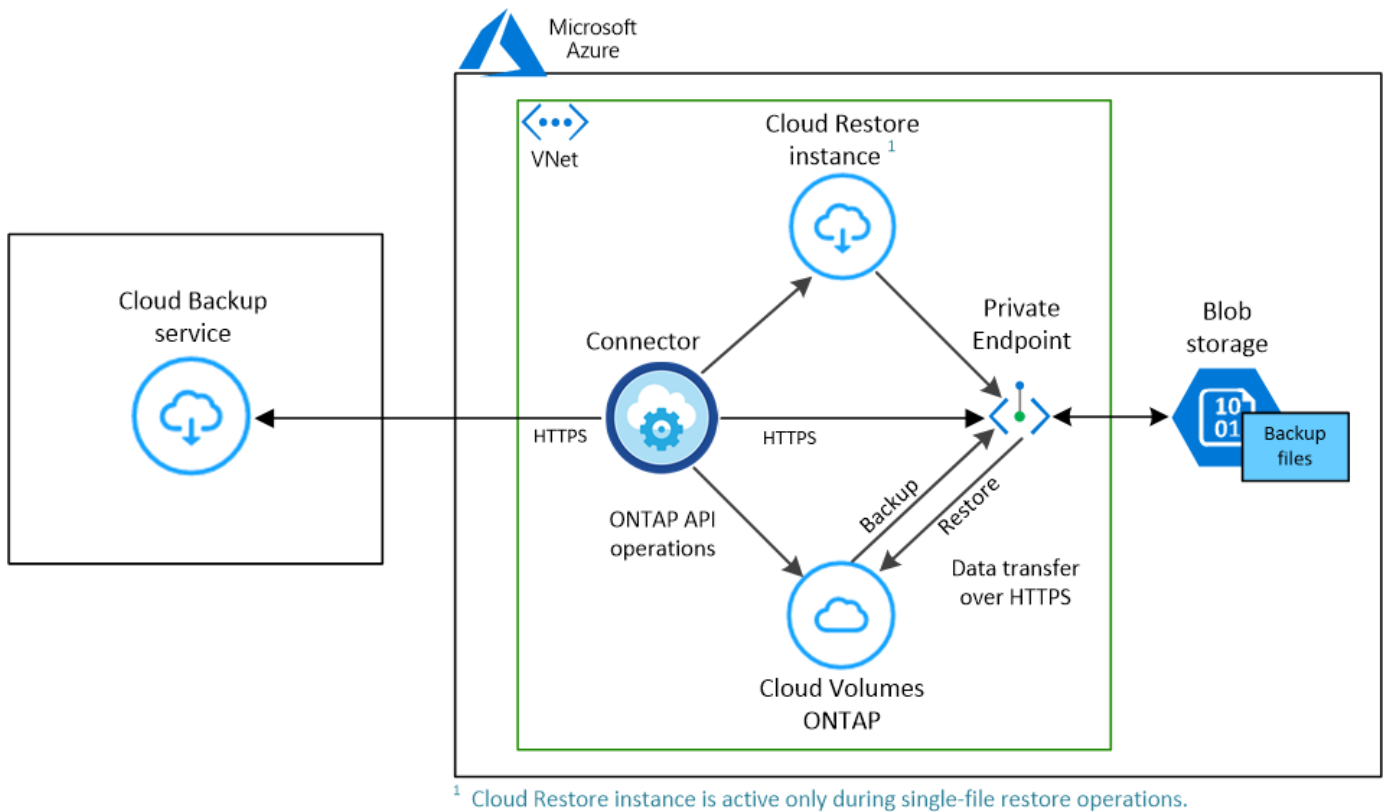
See [Restoring volume data from backup files](#) for details.

### Requirements

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

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





### Supported ONTAP versions

Cloud Volumes ONTAP 9.7 and later.

### Supported Azure regions

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

### License requirements

For Cloud Backup PAYGO licensing, a subscription through the Azure Marketplace is required before you enable Cloud Backup. Billing for Cloud Backup is done through this subscription. [You can subscribe from the Details & Credentials page of the working environment wizard](#).

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

And you need to have a Microsoft Azure subscription for the storage space where your backups will be located.

### 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.

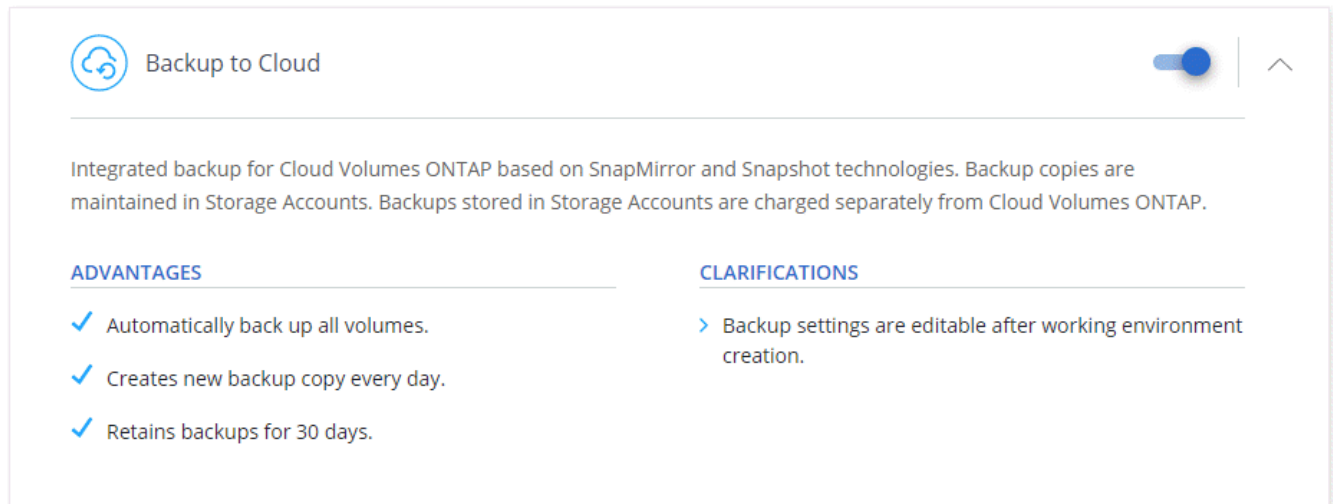


If you want to pick the name of the resource group, **disable** Cloud Backup when deploying Cloud Volumes ONTAP. Follow the steps for [enabling Cloud Backup on an existing system](#) to enable Cloud Backup and choose the resource group.

### Steps

1. Click **Create Cloud Volumes ONTAP**.
2. Select Microsoft Azure as the cloud provider and then choose a single node or HA system.

3. Fill out the Details & Credentials page and be sure that an Azure Marketplace subscription is in place.
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?

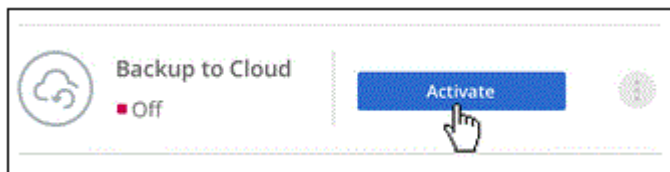
You can [start and stop backups for volumes](#) or [change the backup schedule](#) and you can [restore entire volumes or individual files from a backup file](#).

### 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 **Activate** next to the Cloud Backup service in the right-panel.



2. Select the provider details:
  - a. The Azure subscription used to store the backups.
  - b. The resource group - you can create a new resource group or select an existing resource group.
  - c. And then click **Continue**.

### Provider Settings

**Azure Subscription**

Azure\_Subscription\_1 ▼

**Resource Group**

☐ Create a new ☒ Use an existing

Select an Existing Resource Group

Resource\_Group\_1 ▼

Note that you cannot change the subscription or the resource group after the services has started.

- In the *Define Policy* page, select the backup schedule and retention value and click **Continue**.

### Define Policy

**Policy - Retention & Schedule**

☒ Create a New Policy ☐ Select an Existing Policy

Backup Every: Day ▼

Number of backups to retain: 30

**DP Volumes**

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

**Storage Account**

Cloud Manager will create the storage account after you complete the wizard

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

- Select the volumes that you want to back up and click **Activate**.

### Select Volumes

57 Volumes

<input checked="" type="checkbox"/>	Volume Name	Volume Type	Disk Type	SVM Name	Used Capacity	Allocated Capacity	Volume Status
<input checked="" type="checkbox"/>	Volume_Name_1	RW	GP2	SVM_Name_1	2.25 TB	10 TB	Active
<input checked="" type="checkbox"/>	Volume_Name_2	RW	GP2	SVM_Name_2	2.25 TB	10 TB	Active
<input checked="" type="checkbox"/>	Volume_Name_3	RW	GP2	SVM_Name_3	2.25 TB	10 TB	Active
<input checked="" type="checkbox"/>	Volume_Name_4	DP ⓘ	GP2	SVM_Name_4	2.25 TB	10 TB	Active
<input checked="" type="checkbox"/>	Volume_Name_5	RW	GP2	SVM_Name_5	2.25 TB	10 TB	Active

- 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).

## Result

Cloud Backup starts taking the initial backups of each selected volume.

## What's next?

You can [start and stop backups for volumes](#) or [change the backup schedule](#) and you can [restore entire volumes or individual files from a backup file](#).

## Backing up Cloud Volumes ONTAP data to Google Cloud Storage

Complete a few steps to get started backing up data from Cloud Volumes ONTAP to Google Cloud Storage.

## Quick start

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

### 1

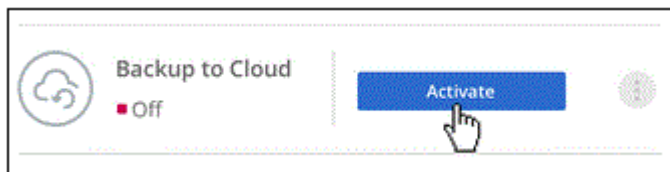
#### Verify support for your configuration

- You're running Cloud Volumes ONTAP 9.7P5 or later in GCP.
- You have a valid GCP subscription for the storage space where your backups will be located.
- You have a service account in your Google Cloud Project that has the predefined Storage Admin role.
- You have subscribed to the [Cloud Manager Marketplace Backup offering](#), or you have purchased [and activated](#) a Cloud Backup BYOL license from NetApp.

### 2

#### Enable Cloud Backup on your new or existing system

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



### 3

#### Enter the provider details

Select the Google Cloud Project where you want the Google Cloud Storage bucket to be created for backups.

Provider Settings

Google Cloud Project

Default Project ▼



#### 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 weekly or monthly backups, or select one of the system-defined policies that provide more options.

Define Policy

**Policy - Retention & Schedule**

☒ Create a New Policy ☐ Select an Existing Policy

Backup Every: Day ▼ Number of backups to retain: 30

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

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



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

Identify which volumes you want to back up in the Select Volumes page.



#### Restore your data, as needed

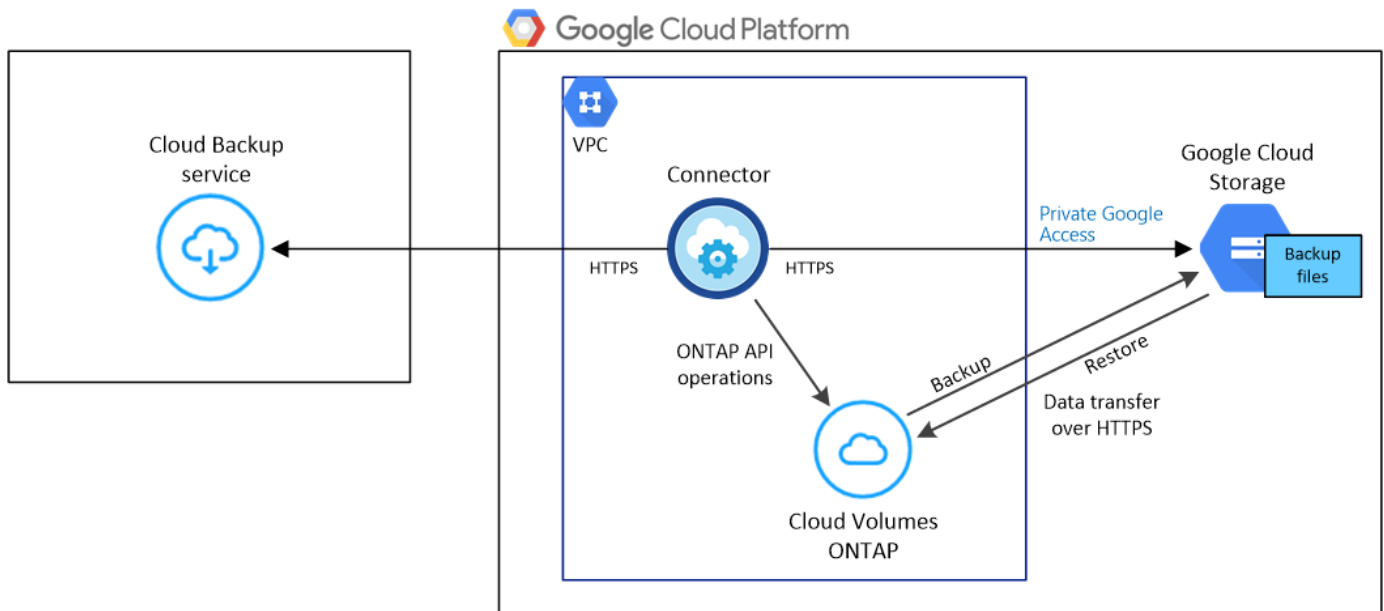
Restore a backup to a new volume. You can restore data to a Cloud Volumes ONTAP system in Google. A Service Account is required on the Cloud Volumes ONTAP system where you are performing the restore.

See [Restoring volume data from backup files](#) for details.

#### Requirements

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

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



### Supported ONTAP versions

Cloud Volumes ONTAP 9.7P5 and later.

### Supported GCP regions

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

### License requirements

For Cloud Backup PAYGO licensing, a subscription through the [GCP Marketplace](#) is required before you enable Cloud Backup. Billing for Cloud Backup is done through this subscription. [You can subscribe from the Details & Credentials page of the working environment wizard](#).

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

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

### GCP Service Account

You need to have a service account in your Google Cloud Project that has the predefined Storage Admin role. [Learn how to create a service account](#).

### Enabling Cloud Backup on a new system

Cloud Backup can be enabled when you complete the working environment wizard to create a new Cloud Volumes ONTAP system.

You must have a Service Account already configured. If you don't select a service account when you create the Cloud Volumes ONTAP system, then you'll need to turn off the system and add the service account to Cloud Volumes ONTAP from the GCP console.

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

### Steps

1. On the Working Environments page, click **Add Working Environment** and follow the prompts.

2. **Choose a Location:** Select **Google Cloud Platform**.
3. **Choose Type:** Select **Cloud Volumes ONTAP** (either single-node or high-availability).
4. **Details & Credentials:** Enter the following information:
  - a. Click **Edit Project** and select a new project if the one you want to use is different than the default Project (where Cloud Manager resides).
  - b. Specify the cluster name.
  - c. Enable the **Service Account** switch and select the Service Account that has the predefined Storage Admin role. This is required to enable backups and tiering.
  - d. Specify the credentials.

Make sure that a GCP Marketplace subscription is in place.

**Details & Credentials**

**Project1** | **MPAWSSubscription1222** Edit Project

Google Cloud Project | Marketplace Subscription

---

**Details**

Working Environment Name (Cluster Name)

TamiVSA

Service Account i ☒

Service Account Name

ServiceAccount1

+ Add Labels Optional Field | Up to four labels

**Credentials**

User Name

admin

Password

\*\*\*\*\*

Confirm Password

\*\*\*\*\*

5. **Services:** Leave the Cloud Backup service enabled and click **Continue**.

**Services**

Backup to Cloud ☒ ▼

6. Complete the pages in the wizard to deploy the system as described in [Launching Cloud Volumes ONTAP in GCP](#).

## Result

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

You can [start and stop backups](#) for additional volumes or [change the backup schedule](#) and you can [restore entire volumes](#) from a backup file.

## Enabling Cloud Backup on an existing system

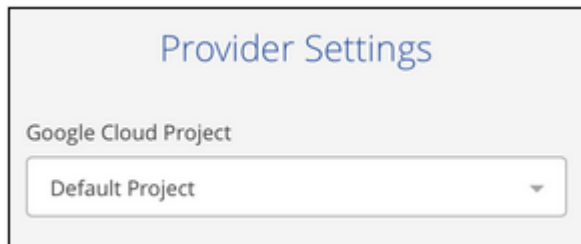
You can enable Cloud Backup at any time directly from the working environment.

### Steps

1. Select the working environment and click **Activate** next to the Cloud Backup service in the right-panel.



2. Select the Google Cloud Project where you want the Google Cloud Storage bucket to be created for backups, and click **Continue**. This can be a different Project than where the Cloud Volumes ONTAP system resides.



Note that the Project must have a Service Account that has the predefined Storage Admin role, and that you cannot change the Project after the service has started.

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

A screenshot of the 'Define Policy' page. The title 'Define Policy' is at the top in blue. Below it, there are two radio buttons: 'Create a New Policy' (selected) and 'Select an Existing Policy'. Under 'Create a New Policy', there are two settings: 'Backup Every' with a dropdown menu showing 'Day', and 'Number of backups to retain' with a text input field showing '30'. Below these are three sections: 'DP Volumes' with a description about retention periods, and 'Storage Account' with a note that Cloud Manager will create the Google Cloud Storage Bucket.

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

4. Select the volumes that you want to back up and click **Activate**.



Select Volumes							
57 Volumes							
<input checked="" type="checkbox"/>	Volume Name	Volume Type	Disk Type	SVM Name	Used Capacity	Allocated Capacity	Volume Status
<input checked="" type="checkbox"/>	Volume_Name_1	RW	GP2	SVM_Name_1	2.25 TB	10 TB	Active
<input checked="" type="checkbox"/>	Volume_Name_2	RW	GP2	SVM_Name_2	2.25 TB	10 TB	Active
<input checked="" type="checkbox"/>	Volume_Name_3	RW	GP2	SVM_Name_3	2.25 TB	10 TB	Active
<input checked="" type="checkbox"/>	Volume_Name_4	DP	GP2	SVM_Name_4	2.25 TB	10 TB	Active
<input checked="" type="checkbox"/>	Volume_Name_5	RW	GP2	SVM_Name_5	2.25 TB	10 TB	Active

- 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).

## Result

Cloud Backup starts taking the initial backups of each selected volume.

## What's next?

You can [start and stop backups for volumes](#) or [change the backup schedule](#) and you can [restore entire volumes from a backup file](#).

## Backing up on-premises ONTAP data to the public cloud

Complete a few steps to get started backing up data from your on-premises ONTAP systems to low-cost object storage in the public cloud. This includes creating backup files on Amazon S3 and Azure Blob.

A Beta feature released in January 2021 allows you to run Compliance scans on the backed up volumes from your on-premises systems. Typically, compliance scans are free up to 1 TB of data, and then a cost for the service is applied for data over 1 TB. When combining Backup and Compliance for your on-prem volumes, the cost for scans on those on-prem volumes is free. Learn more about how [Cloud Compliance](#) can get your business applications and cloud environments privacy ready.

## Quick start

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



### Verify support for your configuration

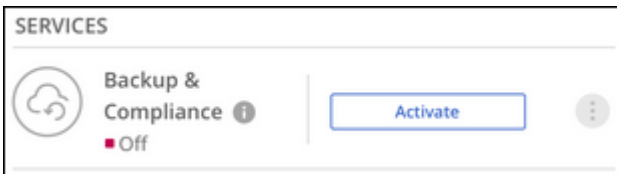
- You have discovered the on-premises cluster and added it to a working environment in Cloud Manager. See [Discovering ONTAP clusters](#) for details.
  - The cluster is running ONTAP 9.7P5 or later.
  - The cluster has a SnapMirror license—which is included as part of the PREM or Data Protection bundle.
- You have subscribed to the [Azure](#) or the [AWS](#) Cloud Manager Marketplace Backup offering, or you have purchased [and activated](#) a Cloud Backup BYOL license from NetApp.

- You have a valid cloud provider subscription for the object storage space where your backups will be located.
- For AWS, you need to have an account that has an access key and the required permissions so the ONTAP cluster can back up data to S3.

## 2

### Enable Cloud Backup on the system

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



## 3

### Select the cloud provider and enter provider details

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

**Note:** Backup to Google Cloud Storage from on-prem ONTAP systems is not currently supported from the UI.

## 4

### 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 weekly or monthly backups, or select one of the system-defined policies that provide more options.

### Define Policy

Policy - Retention & Schedule

☒ Create a New Policy
 ☐ Select an Existing Policy

Backup Every

Day

Number of backups to retain

30

DP Volumes

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

Storage Account

Cloud Manager will create the storage account after you complete the wizard

## 5

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

Identify which volumes you want to back up from the cluster.

## 6

### Activate Compliance scans on the backed up volumes (optional)

Choose whether you want to have Cloud Compliance scan the volumes that are backed up in the cloud.

## 7

### Restore your data, as needed

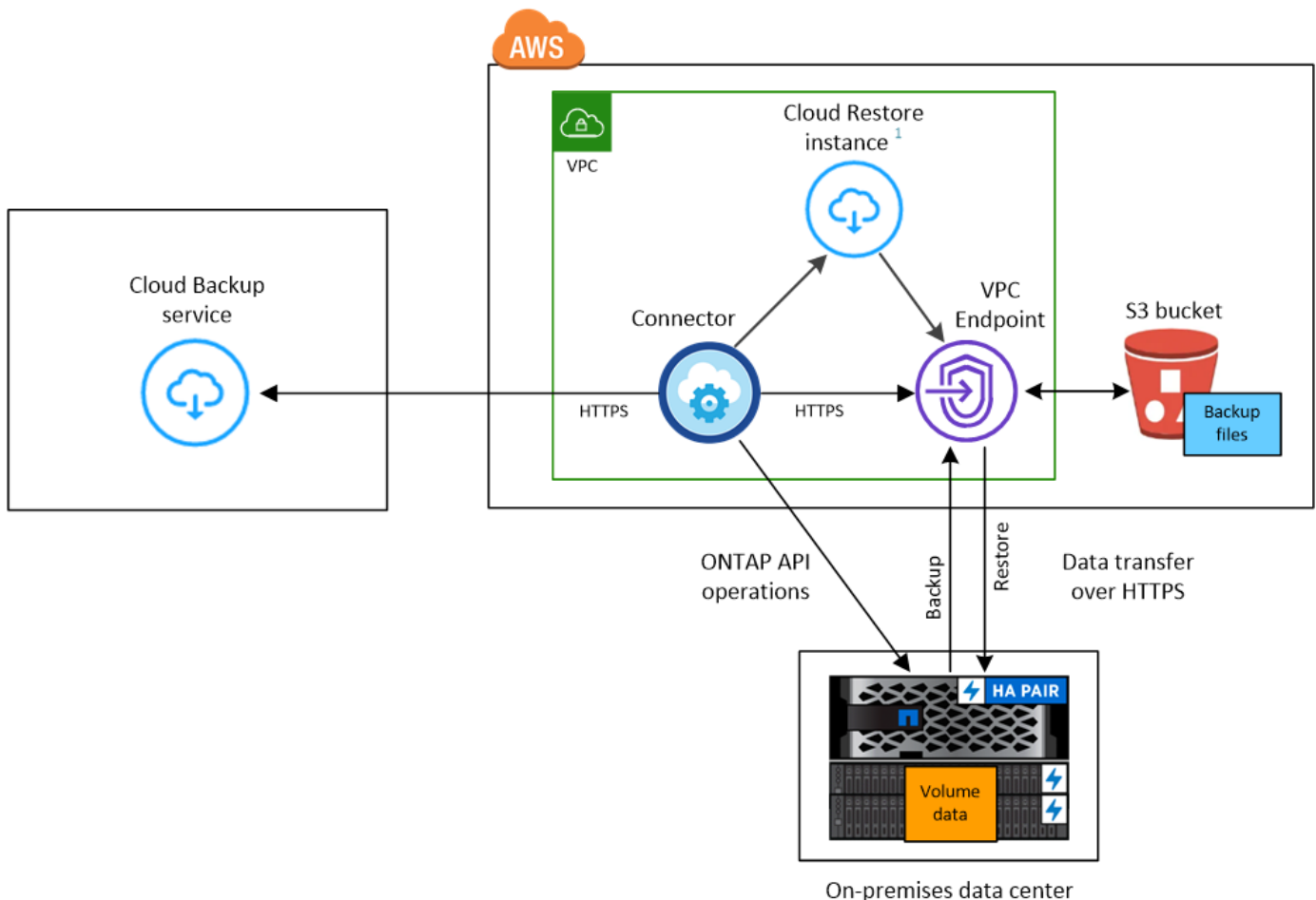
Choose to restore an entire backup to a new volume, or to restore individual files from the backup to an existing volume. You can restore data to a Cloud Volumes ONTAP system that is using the same cloud provider, or to an on-premises ONTAP system.

See [Restoring volume data from backup files](#) for details.

### Requirements

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

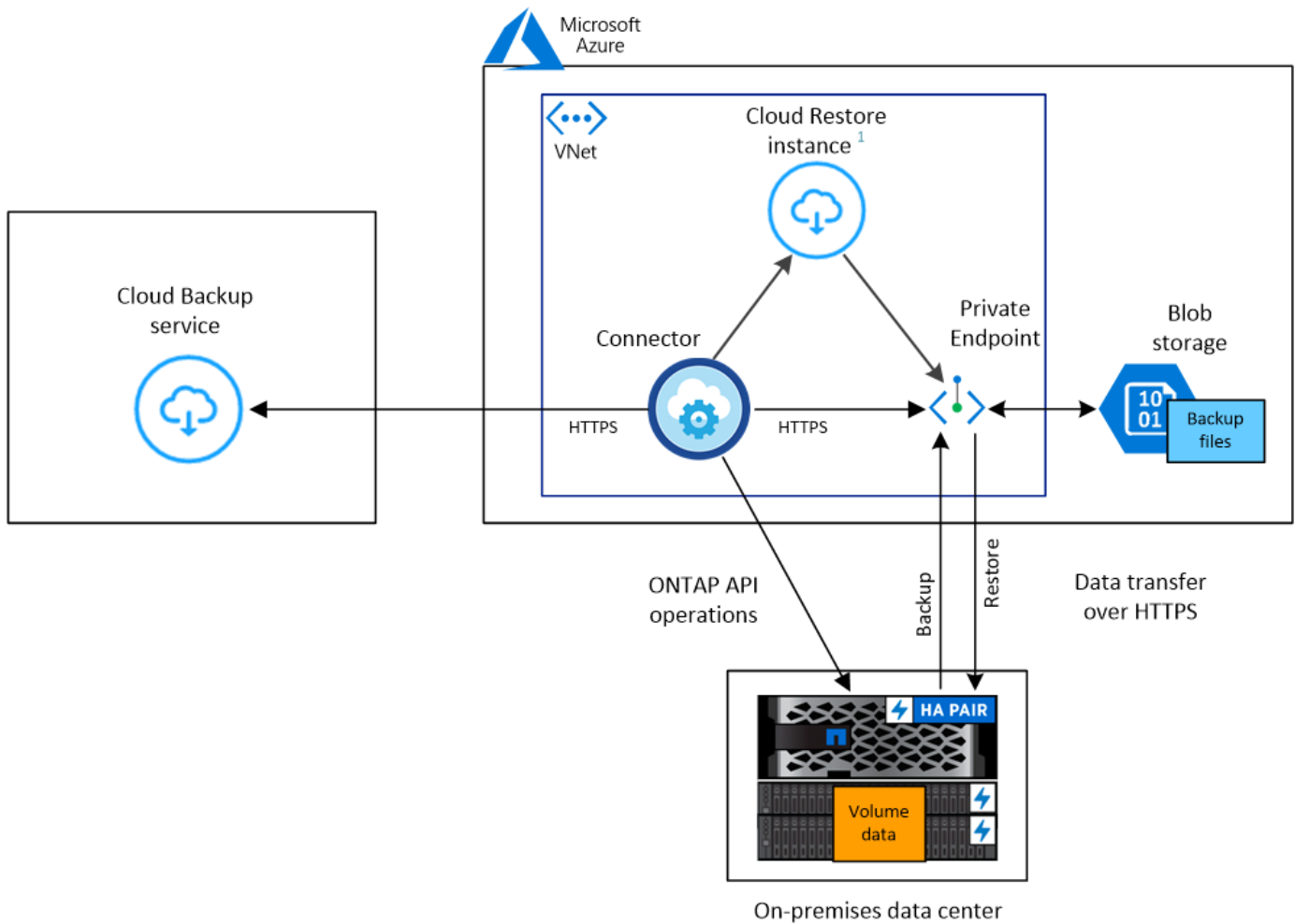
The following image shows each component when backing up an on-prem ONTAP system to Amazon S3 and the connections that you need to prepare between them:



<sup>1</sup> Cloud Restore instance is active only during single-file restore operations.

The following image shows each component when backing up an on-prem ONTAP system to Azure Blob and

the connections that you need to prepare between them:



<sup>1</sup> Cloud Restore instance is active only during single-file restore operations.

### Preparing your ONTAP clusters

Your ONTAP clusters must meet the following requirements when backing up data to cloud storage.

#### ONTAP requirements

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

See how to [manage your cluster licenses](#).

- Time and time zone are set correctly.

See how to [configure your cluster time](#).

#### Cluster networking requirements

- The ONTAP cluster initiates an HTTPS connection over port 443 to the cloud object storage.

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

- An inbound connection is required from the Connector, which can reside in an AWS VPC or Azure

VNet; depending on the object storage provider you are using.

A connection between the cluster and the Cloud Backup service is not required.

- 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.

- Node and intercluster LIFs are able to access the internet.
- DNS servers 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 service connections from ONTAP to object storage through port 443 and name resolution traffic from the storage VM to the DNS server over port 53 (TCP/UDP).

### Discovering an ONTAP cluster

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](#).

### Creating or switching Connectors

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

- [Learn about Connectors](#)
- [Creating a Connector in AWS](#)
- [Creating a Connector in Azure](#)
- [Switching between Connectors](#)

### Preparing networking for the Connector

Ensure that the Connector has the required networking connections.

#### Steps

1. Ensure that the network where the Connector is installed enables the following connections:
  - An outbound internet connection to the Cloud Backup service over port 443 (HTTPS)
  - An HTTPS connection over port 443 to your object storage (S3 or Blob)
  - An HTTPS connection over port 443 to your ONTAP clusters
2. Enable an endpoint to your object storage:
  - For AWS: Enable a VPC Endpoint to S3. This is needed if you have a Direct Connect or VPN

connection from your ONTAP cluster to the VPC and you want communication between the Connector and S3 to stay in your AWS internal network.

- For Azure: Enable a VNet Private Endpoint to Azure storage. This is needed if you have an ExpressRoute or VPN connection from your ONTAP cluster to the VNet and you want communication between the Connector and Blob storage to stay in your virtual private network.

### Supported regions

You can create backups from on-premises systems to the public cloud in all regions [where Cloud Volumes ONTAP is supported](#).

- For Azure, you specify the region where the backups will be stored when you set up the service.
- For AWS, backups are stored in the region where Cloud Manager is installed.

**Note:** Backup to Google Cloud Storage from on-prem ONTAP systems is not currently supported from the UI.

### License requirements

For Cloud Backup PAYGO licensing, you'll need a subscription to the [Azure](#) or the [AWS](#) Cloud Manager Marketplace Backup offering before you enable Cloud Backup. Billing for Cloud Backup is done through this subscription.

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. See [Adding and updating your Backup BYOL license](#).

And you need to have a subscription from your cloud provider for the object storage space where your backups will be located.

### Preparing Amazon S3 for backups

When you are using Amazon S3, you must configure permissions for Cloud Manager to access the S3 bucket, and you must configure permissions so the on-premises ONTAP cluster can access the S3 bucket.

### Steps

1. Provide the following S3 permissions (from the latest [Cloud Manager policy](#)) to the IAM role that provides Cloud Manager with permissions:

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

2. Provide the following permissions to the IAM user so that the ONTAP cluster can back up data to S3.

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

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

3. Create or locate an access key.

Cloud Backup passes the access key on to the ONTAP cluster. The credentials are not stored in the Cloud Backup service.

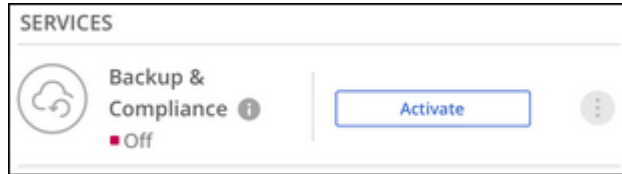
See the [AWS Documentation: Managing Access Keys for IAM Users](#) for details.

## Enabling Cloud Backup

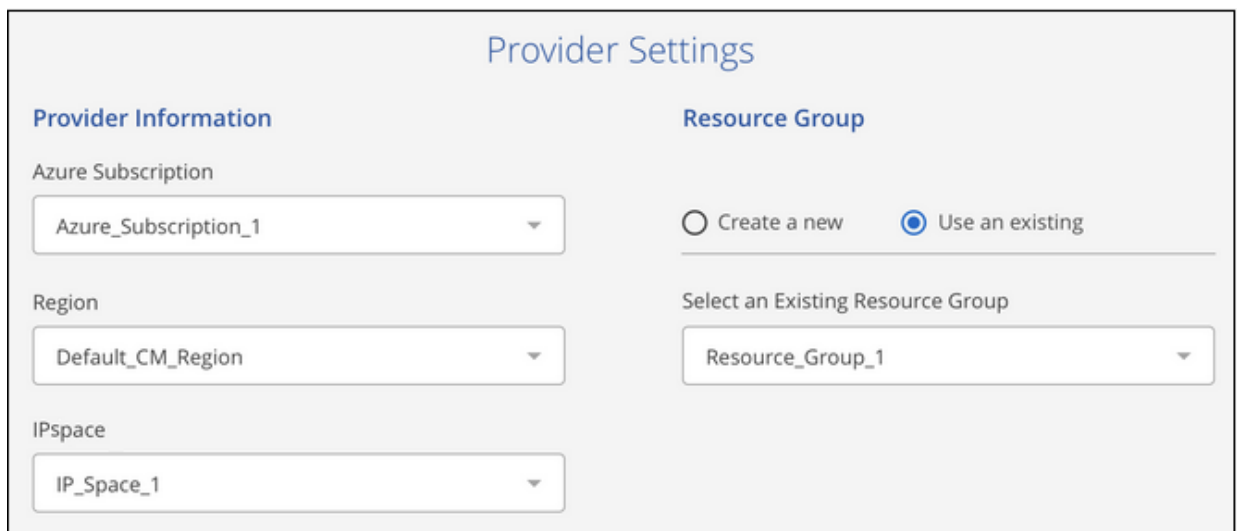
Enable Cloud Backup at any time directly from the on-premises working environment.

### Steps

1. From the Canvas, select the working environment and click **Activate** next to the Backup & Compliance service in the right-panel.



2. Select the provider, and then enter the provider details:
  - For Azure, enter:
    - a. The Azure subscription used for backups and the Azure region where the backups will be stored.
    - b. The resource group - you can create a new resource group or select an existing resource group.
    - c. The IPspace in the ONTAP cluster where the volumes you want to back up reside.

A screenshot of a 'Provider Settings' form. It is divided into two columns. The left column, titled 'Provider Information', contains three dropdown menus: 'Azure Subscription' (selected: Azure\_Subscription\_1), 'Region' (selected: Default\_CM\_Region), and 'IPspace' (selected: IP\_Space\_1). The right column, titled 'Resource Group', contains two radio buttons: 'Create a new' (unselected) and 'Use an existing' (selected). Below the radio buttons is a dropdown menu labeled 'Select an Existing Resource Group' (selected: Resource\_Group\_1).

- For AWS, enter:
  - a. The AWS Access Key and Secret Key used to store the backups.
  - b. The IPspace in the ONTAP cluster where the volumes you want to back up reside.



### Provider Settings

#### AWS Credentials

AWS Access Key

AWS Secret Key

#### Connectivity

IPspace ?

IP\_Space\_1
▼

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

3. Then click **Continue**.
4. In the *Define Policy* page, select the backup schedule and retention value and click **Continue**.

### Define Policy

#### Policy - Retention & Schedule

☒ Create a New Policy    ☐ Select an Existing Policy

Backup Every

Day
▼

Number of backups to retain

30

#### DP Volumes

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

#### Storage Account

Cloud Manager will create the storage account after you complete the wizard

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

5. Select the 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).

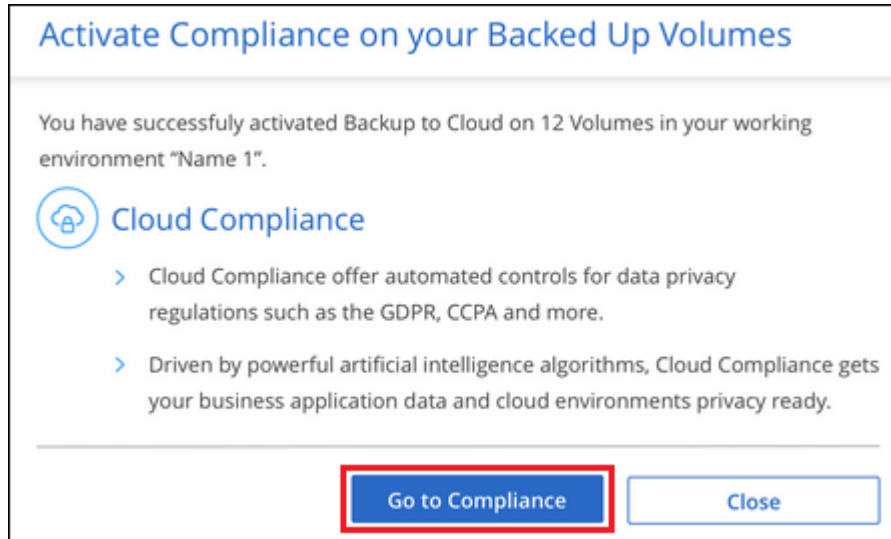
### Select Volumes

57 Volumes 🔍

<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Volume Status
<input checked="" type="checkbox"/>	Volume_Name_1	RW	SVM_Name_1	2.25 TB	10 TB	Active
<input checked="" type="checkbox"/>	Volume_Name_2	RW	SVM_Name_2	2.25 TB	10 TB	Active
<input checked="" type="checkbox"/>	Volume_Name_3	RW	SVM_Name_3	2.25 TB	10 TB	Active

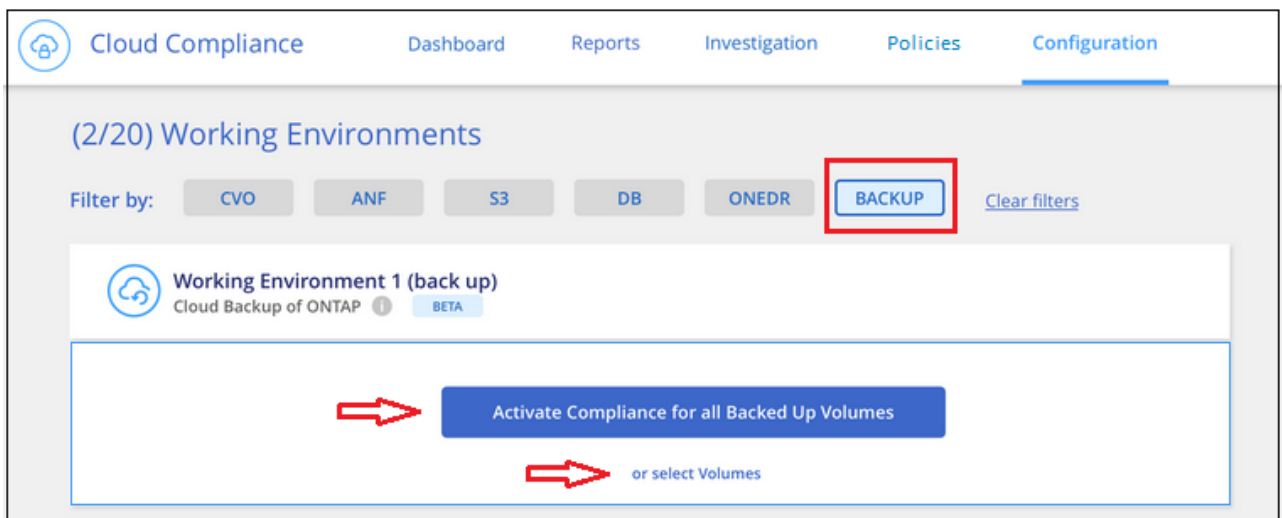
6. Click **Activate** and Cloud Backup starts taking the initial backups of your volumes.

You are prompted whether you want to run compliance scans on the backed up volumes. Cloud Compliance scans are free when you run them on the backed up volumes (except for the [cost of the deployed Cloud Compliance instance](#)).



7. Click **Go to Compliance** to activate compliance scans on the volumes. (If you choose **Close** and not to scan these backed up volumes, you can always [enable this functionality](#) later from Cloud Compliance.)

- If an instance of Cloud Compliance is already deployed in your environment, you are directed to the Configuration page to select the volumes you want to scan in each on-premises working environment that has backups. See [how to choose the volumes](#).



- If Cloud Compliance has not been deployed, you are directed to the Compliance page where you can choose to deploy Compliance in the cloud or in your premises. We strongly recommend deploying it in the cloud. Go [here](#) for installation requirements and instructions.

The screenshot shows the 'Cloud Compliance' interface. At the top, there's a header with a house icon and the text 'Cloud Compliance'. Below it, a link 'How does it work?' is visible. The main heading is 'Always-on Privacy & Compliance Controls'. A subtext explains: 'Automated controls for data privacy regulations such as the GDPR, CCPA and more. Driven by powerful artificial intelligence algorithms, Cloud Compliance gets your business application data and cloud environments privacy ready.' Below this, there are two buttons: 'Deploy Compliance in the Cloud' and 'Deploy Compliance On-Premises'. A link below the buttons says 'Learn about the differences between cloud deployment and on-premises deployment'. On the right, a 'Compliance Status' dashboard is shown. It includes a 'Data Distribution' section with a donut chart showing 75% Non-Sensitive, 20% Personal, and 5% Sensitive Personal. Below this, it shows '28,000 Personal Files' and '7,000 Sensitive Personal Files'. Further down, it lists 'Email Address' (2,700 Files) and 'Credit Card' (2,700 Files) on the left, and 'Health' (2,700 Files) and 'Ethnicity' (2,700 Files) on the right. Each item has a 'View All' link.

After you have deployed Compliance you can choose the volumes you want to scan as described above.

## Result

Cloud Backup backs up your volumes from the on-premises ONTAP system, and optionally, Cloud Compliance runs compliance scans on the backed up volumes.

## What's next?

You can [start and stop backups for volumes](#) or [change the backup schedule](#) and you can [restore entire volumes or individual files from a backup file](#).

You can also [view the results of the compliance scans](#) and review other features of Cloud Compliance that can help you understand data context and identify sensitive data in your organization.



The scan results are not available immediately because Cloud Backup has to finish creating the backups before Cloud Compliance can start compliance scans.

# Managing backups for Cloud Volumes ONTAP and on-premises ONTAP systems

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

## Changing the schedule and backup retention


The default policy backs up volumes every day and retains the most recent 30 backup copies of each volume. You can change to weekly or monthly backups and you can change the number of backup copies to retain. You can also select one of the system-defined policies that provide scheduled backups for 3 months, 1 year, and 7 years.

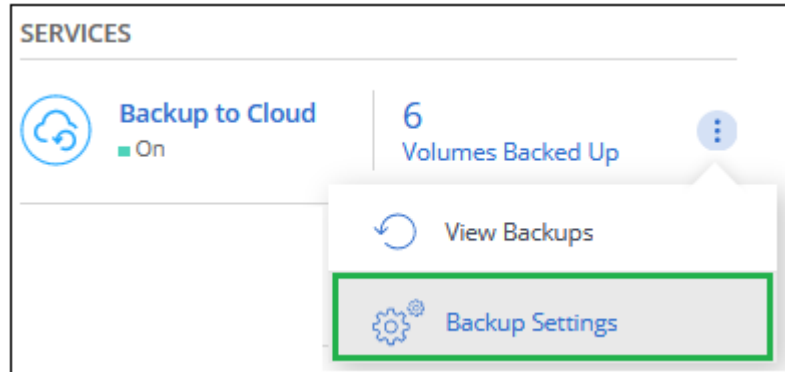



Changing the backup policy affects only new volumes created after you change the schedule. It doesn't affect the schedule for any existing volumes.

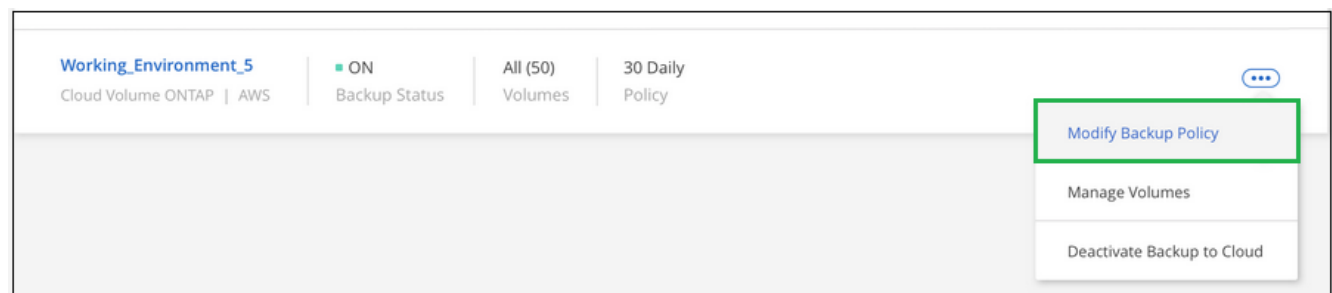
## Steps

1. Select the working environment.

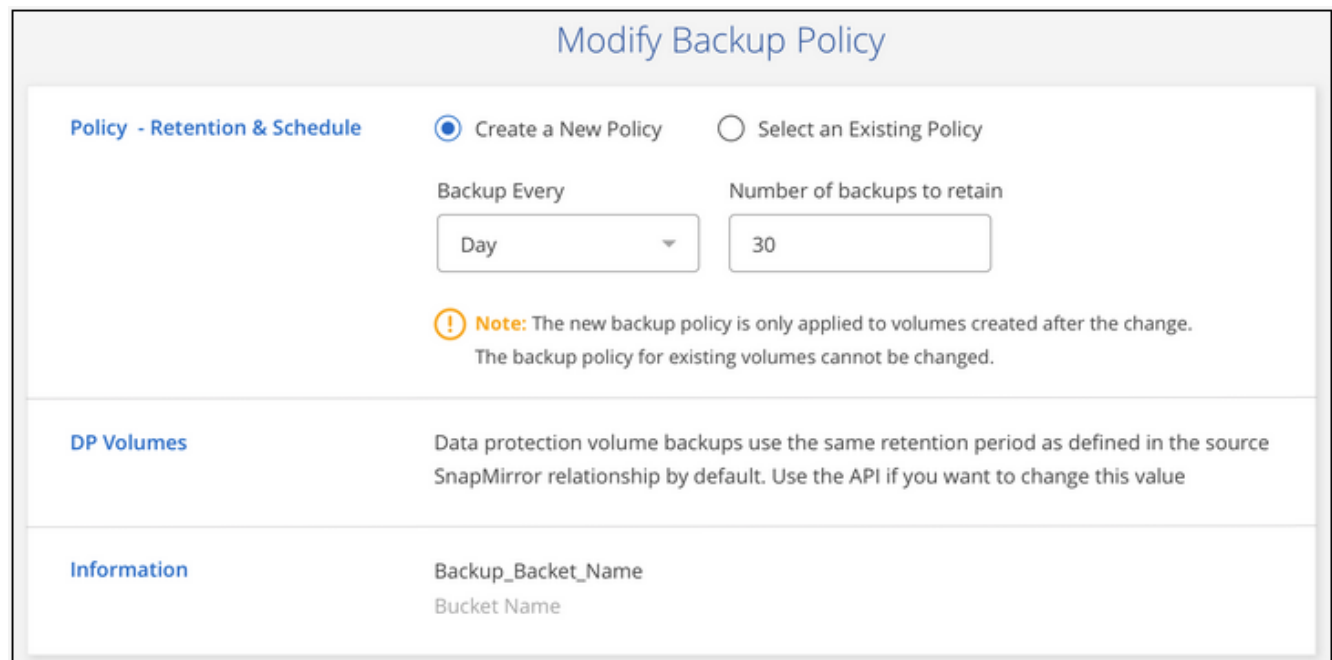
- Click  and select **Backup Settings**.



- From the *Backup Settings* page, click  for the working environment and select **Modify Backup Policy**.



- From the *Modify Backup Policy* page, change the schedule and backup retention and then click **Save**.




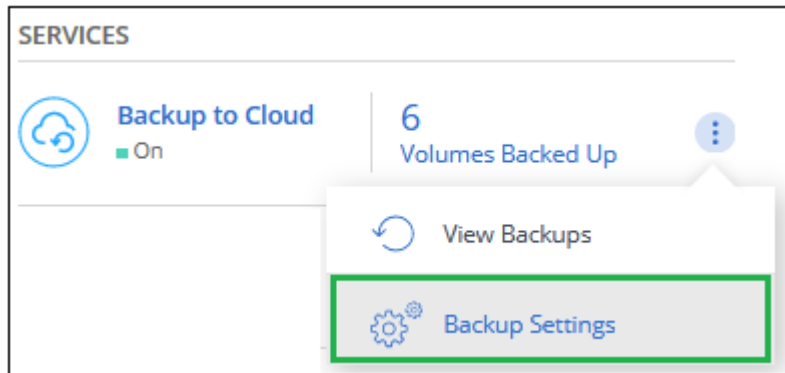
The screenshot shows the 'Modify Backup Policy' page. It has a title 'Modify Backup Policy' at the top. Below the title, there are two radio buttons: 'Create a New Policy' (selected) and 'Select an Existing Policy'. Under 'Create a New Policy', there are two fields: 'Backup Every' with a dropdown menu set to 'Day', and 'Number of backups to retain' with a text input set to '30'. Below these fields, there is a note: 'Note: The new backup policy is only applied to volumes created after the change. The backup policy for existing volumes cannot be changed.' At the bottom, there are two sections: 'DP Volumes' with the text 'Data protection volume backups use the same retention period as defined in the source SnapMirror relationship by default. Use the API if you want to change this value' and 'Information' with the text 'Backup\_Bucket\_Name' and 'Bucket Name'.


## Starting and stopping backups of volumes

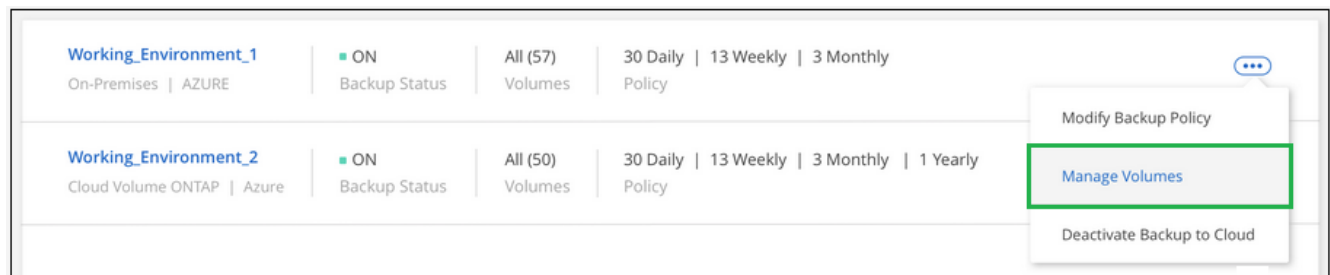
You can stop backing up a volume if you do not need backup copies of that volume and you do not want to pay for the cost to store the backups. You can also add a new volume to the backup list if it is not currently being backed up.

## Steps


1. Select the working environment.
2. Click  and select **Backup Settings**.



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



4. Select the checkbox for volumes that you want to start backing up, and deselect the checkbox for volumes that you want to stop backing up.

Manage Volumes						
57 Volumes   25 Selected Volumes						
<input type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Volume Status
<input type="checkbox"/>	Volume_Name_1	RW	SVM_Name_1	2.25 TB	10 TB	Active
<input type="checkbox"/>	Volume_Name_2	RW	SVM_Name_2	2.25 TB	10 TB	Active
<input checked="" type="checkbox"/>	Volume_Name_3	RW	SVM_Name_3	2.25 TB	10 TB	Active
<input type="checkbox"/>	Volume_Name_4	DP 	SVM_Name_4	2.25 TB	10 TB	Active

**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](#).

## Deleting backups

Cloud Backup enables you to delete *all* backups of a specific volume. You can't delete *individual* backups. You might do this if you no longer need the backups or if you deleted the source volume and want to remove all backups.

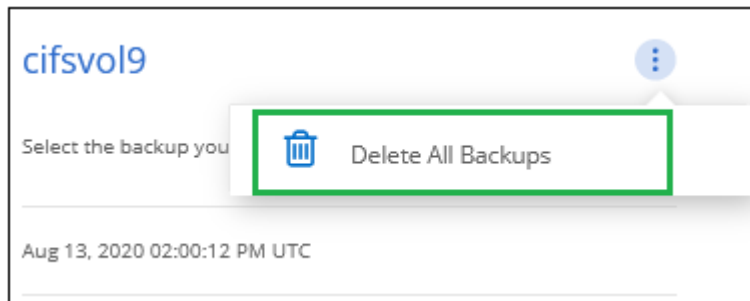
Note that deleting all backups also disables any further backups of this volume. If you later want to start creating backups of that volume, you can re-enable backups [as described here](#).



If you plan to delete a Cloud Volumes ONTAP or on-premises ONTAP system 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.

### Steps

1. At the top of Cloud Manager, click **Backup**.
2. From the volume list, find the volume and click **View Backup List**.
3. Click **...** and select **Delete All Backups**.



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

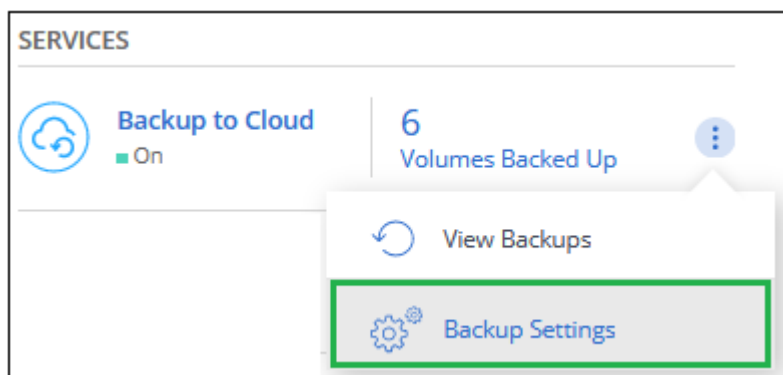
## Disabling Cloud Backup

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.

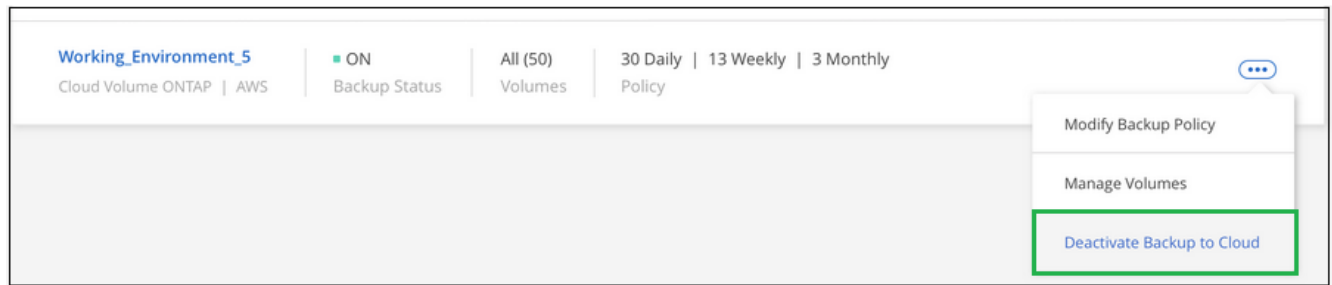
Note that you'll continue to be charged by your cloud provider for object storage costs for the capacity that your backups use unless you delete the backups.

### Steps

1. Select the working environment.
2. Click **...** and select **Backup Settings**.



3. From the *Backup Settings* page, click **...** for the working environment and select **Deactivate Cloud Backup**.



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

## Restoring data from backup files

Backups are stored in an object store in your cloud account so that you can restore data from a specific point in time. You can restore an entire volume from a saved backup file, or if you only need to restore a few files, you can restore up to 8 individual files (at one time) from a saved backup file.

You can restore an entire volume to the same working environment, to a different working environment that's using the same cloud account, or to an on-premises ONTAP system. See [Restoring a volume from a backup](#).

You can restore files to a volume in the same working environment, to a volume in a different working environment that's using the same cloud account, or to a volume on an on-premises ONTAP system. See [Restoring files from a backup](#).

## Supported working environments and object storage providers

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

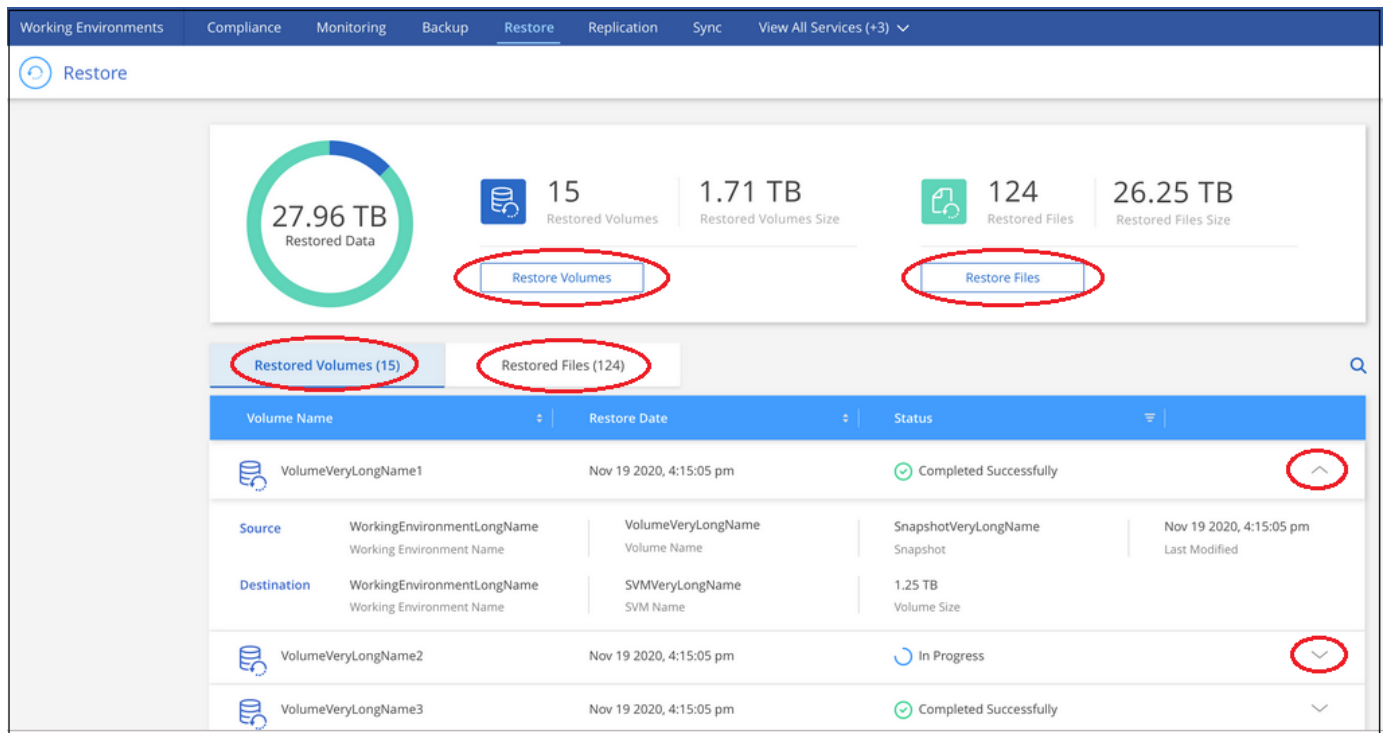
Backup File Location	Destination Working Environment	
	Volume Restore	File Restore
Amazon S3	Cloud Volumes ONTAP in AWS On-premises ONTAP system	Cloud Volumes ONTAP in AWS On-premises ONTAP system
Azure Blob	Cloud Volumes ONTAP in Azure On-premises ONTAP system	Cloud Volumes ONTAP in Azure On-premises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

## The Restore Dashboard

You access the Restore Dashboard by clicking the **Restore** tab from the top of Cloud Manager, or you can click the **Activate** or **Enable** button for the Restore service from the Services panel.



The Cloud Backup service must already be activated for at least one working environment.



The Restore Dashboard provides buttons for you to restore volumes and files. Clicking the *Restore Volumes* or *Restore Files* buttons starts a wizard that walks you through the steps to restore that data.

The dashboard also provides a list of all the volumes and all the files you have restored in case you need a history of previous restore actions. You can expand the row for each restored volume or file to view the details about the source and destination locations for the volume or file.

## Restoring a volume from a backup file

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

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.

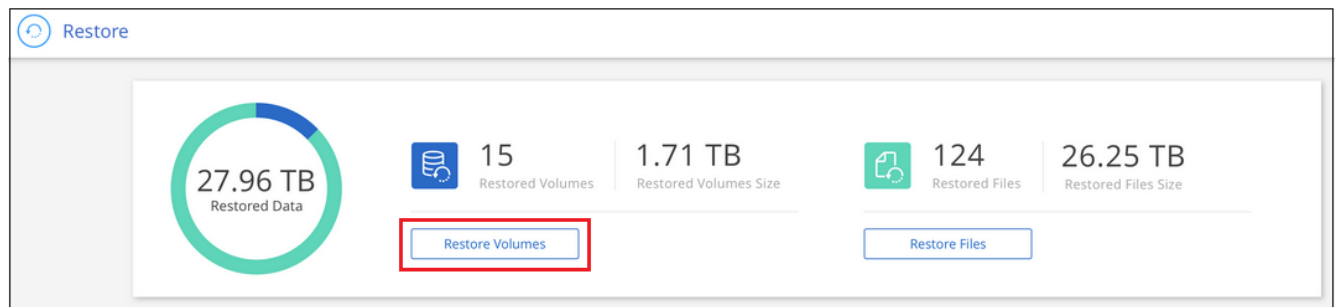
### Steps

1. Select the **Restore** tab.

The Restore Dashboard appears.

2. Click **Restore Volumes**.





- In the *Select Source* page, navigate to the backup file (snapshot) for the volume you want to restore. Select the **Working Environment**, the **Volume**, and the **Snapshot** that has the date/time stamp that you want to restore.

**Select Source**

656 Snapshots

Snapshot Name	Date	Snapshot Policy
Snapshot Very Long Name	Nov 19 2020, 4:15:05 pm	Daily
<b>Snapshot Very Long Name</b>	Nov 19 2020, 4:15:05 pm	Weekly
Snapshot Very Long Name	Nov 19 2020, 4:15:05 pm	Monthly
Snapshot Very Long Name	Nov 19 2020, 4:15:05 pm	Yearly

Selected Working Environment: **Working Environment Name 3**

Selected Volume: **Volume Very Long Name**

Selected Snapshot: **Snapshot Very Long Name**

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

**Select Destination**

5 Working Environments

Working Environment Name	Type	Provider
Working Environment 3 On <a href="#">Source Working Environment</a>	Cloud Volumes ONTAP	Azure
<b>Working Environment 2</b> On	Cloud Volumes ONTAP	AWS

Select Working Environment >

Destination Volume

- 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, enter the IPspace in the ONTAP cluster where the destination volumes reside, and the AWS Access Key and Secret Key needed to access the object storage.

- When restoring from Azure Blob, enter the IPspace in the ONTAP cluster where the destination volumes reside.
  - When restoring from Google Cloud Storage, enter the IPspace in the ONTAP cluster where the destination volumes reside, and the Access Key and Secret Key needed to access the object storage.
7. Select the Storage VM where the volume will reside and enter the name you want to use for the restored volume. By default, **<source\_volume\_name>\_Restore** is used as the volume name.

Select Destination															
<p>Selected Working Environment</p> <p>Working Environment Name 2</p> <p>Destination Volume &gt;</p> <p>Source_Volume_Name_Restore</p>	<p>A new volume will be created in the working environment based on the backup snapshot you selected</p> <p>Storage VM</p> <p>Storage VM 1</p> <p>Aggregate</p> <p>Aggregate 1</p> <p>Volume Name</p> <p>Source_Volume_Name_Restore</p> <table border="1"> <thead> <tr> <th colspan="2">Volume Information</th> </tr> </thead> <tbody> <tr> <td>Volume Size:</td> <td>100 GB</td> </tr> <tr> <td>Snapshot Policy:</td> <td>Default</td> </tr> <tr> <td>NFS Protocol:</td> <td>Custom export policy, 10.20.0.0/16</td> </tr> <tr> <td>Storage Efficiency:</td> <td>ON</td> </tr> <tr> <td>Disk Type:</td> <td>GP2</td> </tr> <tr> <td>Tiering:</td> <td>all</td> </tr> </tbody> </table>	Volume Information		Volume Size:	100 GB	Snapshot Policy:	Default	NFS Protocol:	Custom export policy, 10.20.0.0/16	Storage Efficiency:	ON	Disk Type:	GP2	Tiering:	all
Volume Information															
Volume Size:	100 GB														
Snapshot Policy:	Default														
NFS Protocol:	Custom export policy, 10.20.0.0/16														
Storage Efficiency:	ON														
Disk Type:	GP2														
Tiering:	all														

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

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

## Result

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

## Restoring files from a backup

If you only need to restore a few files from a volume, you can choose to restore individual files instead of restoring the entire volume. You can restore files to a 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 an on-premises ONTAP system.

You can restore up to 8 files at a time from a volume in a backup file. All the files are restored to the same destination volume that you choose. If you need to restore more than 8 files you can run the restore process a second time.



Restoring individual files from a backup file uses a separate Restore instance/virtual machine.

## File Restore process

The process goes like this:

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

2. The Restore instance starts up and displays the folders and files that exist within the backup file.

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

3. Choose the file (or files) that you want to restore from that backup.

4. Select the location where you want the file(s) to be restored (the working environment, volume, and folder), and click **Restore**.

5. The file(s) are restored, and then the Restore instance is shut down to save costs after a period of inactivity.

## Details

### Costs

See [this topic](#) for the cost of the Cloud Backup service and the Restore instance.

### Instance type

- In AWS, the Restore instance runs on an [m5n.xlarge instance](#) with 4 CPUs, 16 GiB Memory, and EBS Only instance storage. In regions where m5n.xlarge instance isn't available, Restore runs on an m5.xlarge instance instead.
- In Azure, the Restore virtual machine runs on a [Standard\\_D4s\\_v3 VM](#) with 4 CPUs, 16 GiB Memory, and a 32 GB disk.

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

## Reviewing prerequisites

Review the following prerequisites to make sure that you have a supported configuration before Cloud Restore is deployed.

### AWS permissions required

When using file Restore with AWS, the IAM role that provides Cloud Manager with permissions must include S3 permissions from the latest [Cloud Manager policy](#) as described in [AWS requirements](#).

Additionally, the following permissions are needed in the policy for file restore:

```
"Action": [  
    "ec2:DescribeInstanceTypeOfferings",  
    "ec2:startInstances",  
    "ec2:stopInstances",  
    "ec2:terminateInstances"  
],
```

### Enable outbound internet access

Cloud Restore requires outbound internet access. If your virtual or physical network uses a proxy server for internet access, ensure that the instance has outbound internet access to contact the following endpoints. When you deploy Cloud Restore in the cloud, it is located in the same subnet as the Connector.

Review the appropriate table depending on whether you are deploying Cloud Restore in AWS or Azure.

#### Required endpoints for AWS deployments:

Endpoints	Purpose
<a href="http://amazonlinux.us-east-1.amazonaws.com/2/extras/docker/stable/x86_64/4bf88ee77c395ffe1e0c3ca68530dfb3a683ec65a4a1ce9c0ff394be50e922b2/">http://amazonlinux.us-east-1.amazonaws.com/2/extras/docker/stable/x86_64/4bf88ee77c395ffe1e0c3ca68530dfb3a683ec65a4a1ce9c0ff394be50e922b2/</a>	CentOS package for the Cloud Restore Instance AMI.
<a href="http://cloudmanagerinfraprod.azurecr.io">http://cloudmanagerinfraprod.azurecr.io</a> <a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a>	Cloud Restore Instance image repository.

#### Required endpoints for Azure deployments:

Endpoints	Purpose
<a href="http://olcentgbl.trafficmanager.net">http://olcentgbl.trafficmanager.net</a> <a href="https://olcentgbl.trafficmanager.net">https://olcentgbl.trafficmanager.net</a>	Provides CentOS packages for the Cloud Restore virtual machine.
<a href="http://cloudmanagerinfraprod.azurecr.io">http://cloudmanagerinfraprod.azurecr.io</a> <a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a>	Cloud Restore Instance image repository.

#### Restoring a single file from a backup file

Follow these steps to restore up to 8 files from a volume backup to a volume. 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 the backup file.

Note that the wording in the UI calls each backup file a "snapshot" because backup files are created using NetApp Snapshot technology.

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

 | <https://img.youtube.com/vi/ROAY6gPL9N0/maxresdefault.jpg>



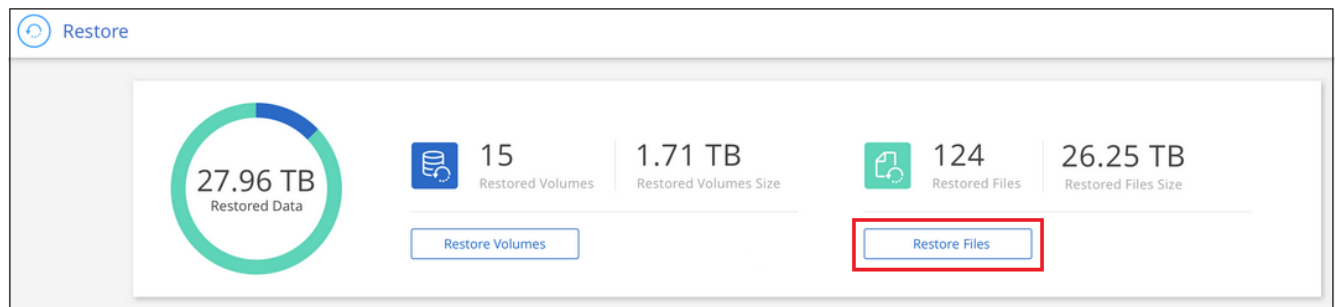
The ONTAP version must be 9.6 or greater in your source and destination ONTAP systems.

#### Steps

1. Click the **Restore** tab.

The Restore Dashboard appears.

2. Click the **Restore Files** button.



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

**Select Source**

1 Select Source 2 Select Files 3 Select Destination

Selected Working Environment: **Working Environment Name 3**

Selected Volume: **Volume Very Long Name**

Select Snapshot > Snapshot Very Long Name

656 Snapshots

Snapshot Name	Date	Time Zone
Snapshot Very Long Name	September 30 2020 00:00:00	NY, USA (GMT-4)
Snapshot Very Long Name	September 30 2020 00:00:00	NY, USA (GMT-4)
<b>Snapshot Very Long Name</b>	September 30 2020 00:00:00	NY, USA (GMT-4)
Snapshot Very Long Name	September 30 2020 00:00:00	NY, USA (GMT-4)

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

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

**Select Files**

Select Files

You can select up to 8 files

1 File D Very Long Name x

Last Modified: September 30 2020 00:00:00

Size: 1.25 MB

Folders & Files

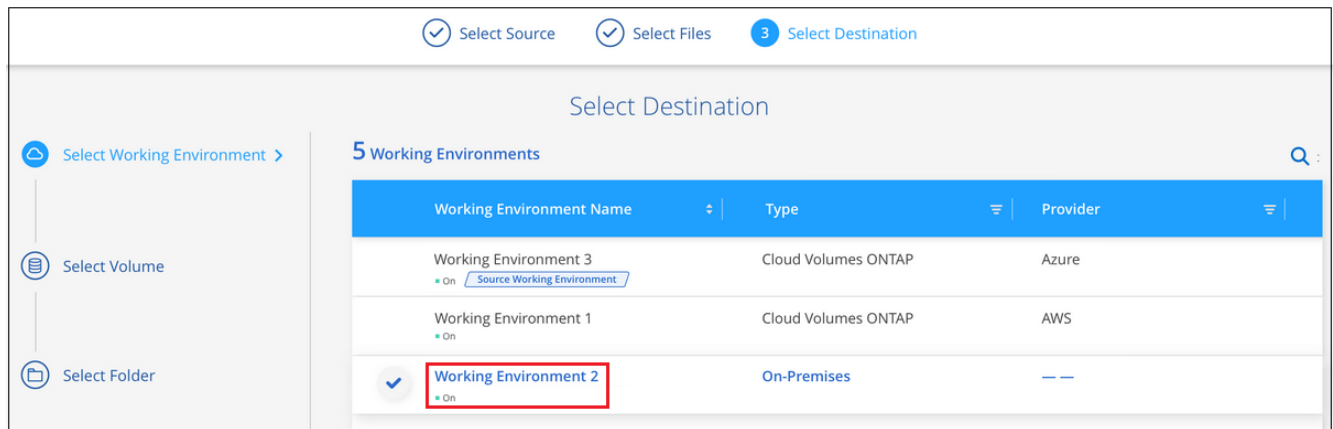
All Folders & Files > Folder A Very Long Name

Name	Last Modified	Size
<b>File D Very Long Name</b>	September 30 2020 00:00:00	1.25 MB
File E Very Long Name	September 30 2020 00:00:00	1.25 MB

- In the **Select Files** page, select the file or files that you want to restore and click **Continue**.
  - You can click the search icon and enter the name of the file to navigate directly to the file.
  - You can click the file name if you see it.
  - 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.

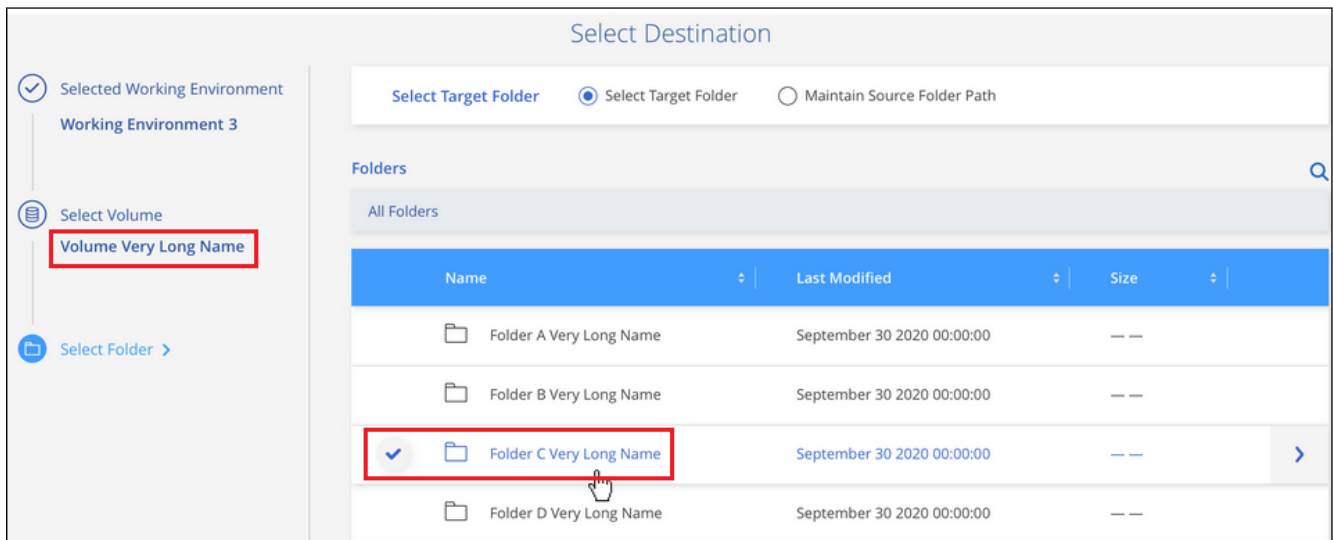
6. In the *Select Destination* page, select the **Working Environment** where you want to restore the files.




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

7. 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.

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

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

## Copyright Information

Copyright © 2021 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.