



Back up to the cloud

Cloud Manager

NetApp

November 10, 2020

This PDF was generated from https://docs.netapp.com/us-en/occm/concept_backup_to_cloud.html on November 10, 2020. Always check docs.netapp.com for the latest.



Table of Contents

- Back up to the cloud..... 1
 - Learn about Backup to Cloud 1
 - Get started 5
 - Managing backups for Cloud Volumes ONTAP and on-premises ONTAP systems 22

Back up to the cloud

Learn about Backup to Cloud

Backup to Cloud 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 stored in an object store in your cloud account, independent of volume Snapshot copies used for near-term recovery or cloning.

Backup to Cloud is powered by 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 the data to a volume on the source system or to a different system.

Supported working environments and object storage providers

Backup to Cloud is supported with the following types of working environments:

- Cloud Volumes ONTAP in AWS
- Cloud Volumes ONTAP in Azure
- On-premises ONTAP clusters

Cost

Backup to Cloud is available in two pricing options: Bring Your Own License (BYOL) and Pay As You Go (PAYGO).

For BYOL you'll pay NetApp to use the service for a period of time, say 6 months, and for a maximum amount backup capacity, say 10 GB (before storage efficiencies), and you'll need to pay your cloud

provider for object storage costs. 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 systems associated with your [Cloud Central account](#).

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

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

Free trial

A 30-day free trial is available. When using the trial version, 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.

How Backup to Cloud works

When you enable Backup to Cloud 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.

Where backups reside

Backup copies are stored in an S3 bucket or Azure Blob container 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.

Supported S3 storage classes

In Amazon S3, backups start in the *Standard* storage class and transition to the *Standard-Infrequent Access* storage class after 30 days.

Supported Azure Blob access tiers

In Azure, each backup is associated with the *cold* access tier.

Backup settings are system wide

When you enable Backup to Cloud, 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:

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

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.

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.

BYOL license considerations

When using a Backup to Cloud 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.

Supported volumes

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

FlexGroup volumes aren't currently supported.

Limitations

- WORM storage (SnapLock) is not supported on a Cloud Volumes ONTAP or on-premises system when Backup to Cloud is enabled.

- Backup to Cloud restrictions when making backups from on-premises ONTAP systems:
 - The on-prem cluster must be running ONTAP 9.7P5 or later.
 - Cloud Manager must be deployed in the cloud (Azure or AWS). There is no support for on-premises Cloud Manager deployments.
 - Backups can be restored only to Cloud Volumes ONTAP systems deployed on the same cloud provider. You cannot restore a backup to an on-premises ONTAP system or to a Cloud Volumes ONTAP system that is using a different cloud provider.

Note that Restoring a backup is not currently supported using the Cloud Manager UI. You can use the API if you need to restore a backup at this time. Restore using the UI will be addressed shortly.

- When backing up data protection (DP) volumes, the rule that is defined for the SnapMirror policy on the source volume must use a label that matches the allowed Backup to Cloud policy names of **daily**, **weekly**, or **monthly**. Otherwise the backup will fail for that DP volume.
- In Azure, if you enable Backup to Cloud 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 Backup to Cloud, **disable** Backup to Cloud when deploying Cloud Volumes ONTAP and then enable Backup to Cloud and choose the resource group from the Backup to Cloud 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 Backup to Cloud and then enable it again.

Get started

Backing up 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.



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 Backup to Cloud BYOL license from NetApp.

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

2

Enable Backup to Cloud on your new or existing system

- New systems: Backup to Cloud 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 Backup to Cloud 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

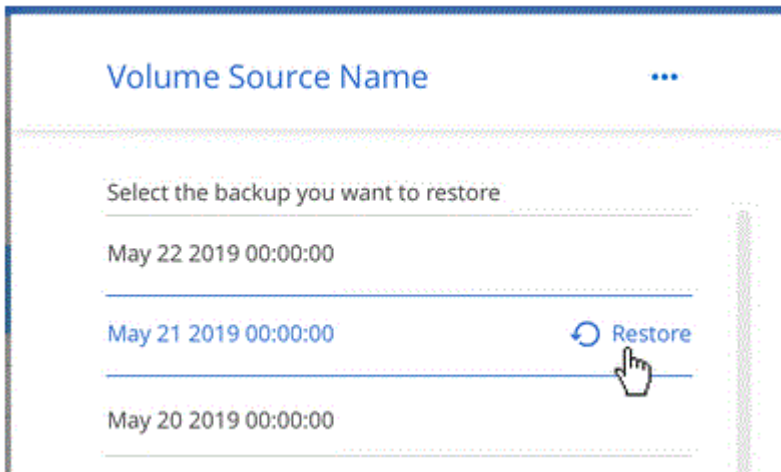
Select the volumes that you want to back up

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

5

Restore your data, as needed

From the Backup List, select a volume, select a backup, and then restore data from the backup to a new volume.



Requirements

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

Supported ONTAP versions

Cloud Volumes ONTAP 9.6 and later.

Supported AWS regions

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

License requirements

For Backup to Cloud 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 Backup to Cloud. You need to [subscribe to this Cloud Manager subscription](#) before you enable Backup to Cloud. Billing for Backup to Cloud is done through this subscription.

For Backup to Cloud BYOL licensing, you do not need an AWS Backup to Cloud 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:

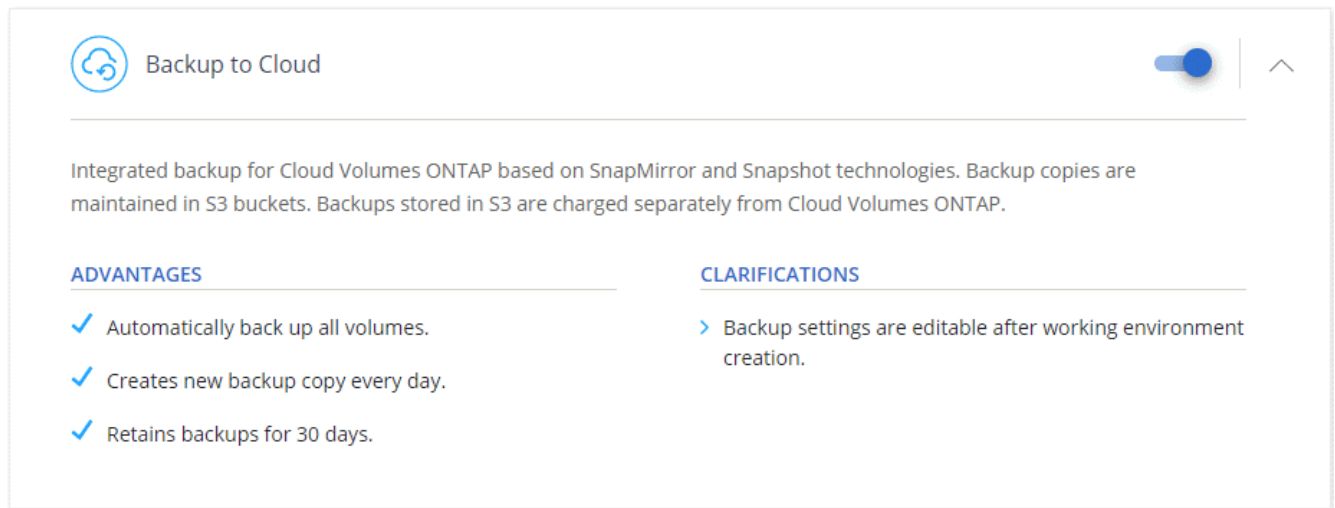
```
{
  "Sid": "backupPolicy",
  "Effect": "Allow",
  "Action": [
    "s3:DeleteBucket",
    "s3:GetLifecycleConfiguration",
    "s3:PutLifecycleConfiguration",
    "s3:PutBucketTagging",
    "s3:ListBucketVersions",
    "s3:GetObject",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "s3:GetBucketTagging",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

Enabling Backup to Cloud on a new system

Backup to Cloud 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

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

What's next?

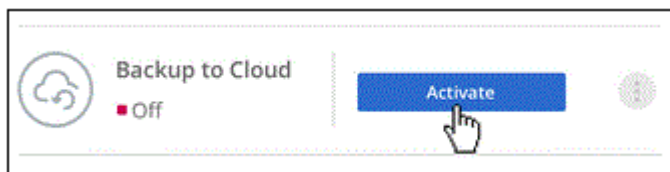
[You can manage backups by changing the backup schedule, restoring volumes, and more.](#)

Enabling Backup to Cloud on an existing system

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

Steps

1. Select the working environment and click **Activate** next to the Backup to Cloud 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

Day ▼

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

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

Result

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

What's next?

[You can manage backups by changing the backup schedule, restoring volumes, and more.](#)

Backing up 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 Backup to Cloud BYOL license from NetApp.

2

Enable Backup to Cloud on your new or existing system

- New systems: Backup to Cloud 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 Backup to Cloud 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

From the Backup List, select a volume, select a backup, and then restore data from the backup to a new volume.

Volume Source Name

...

Select the backup you want to restore

May 22 2019 00:00:00

May 21 2019 00:00:00

May 20 2019 00:00:00

Restore

Requirements

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

Supported ONTAP versions

Cloud Volumes ONTAP 9.7 and later.

Supported Azure regions

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

License requirements

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

For Backup to Cloud 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 Backup to Cloud on a new system

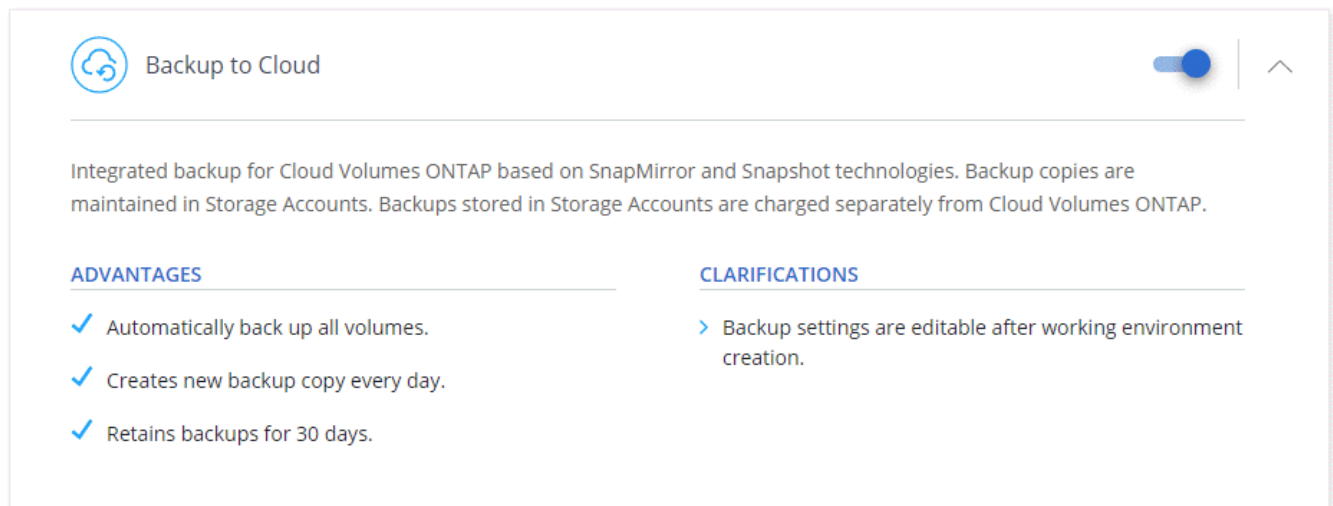
Backup to Cloud is enabled by default in the working environment wizard. Be sure to keep the option enabled.



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

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

What's next?

[You can manage backups by changing the backup schedule, restoring volumes, and more.](#)

Enabling Backup to Cloud on an existing system

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

Steps

1. Select the working environment and click **Activate** next to the Backup to Cloud 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

Result

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

What's next?

You can manage backups by changing the backup schedule, restoring volumes, and more.

Backing up data from an on-premises ONTAP system to the cloud

Complete a few steps to get started backing up data from your on-premises ONTAP system to low-cost object storage in the cloud.

Quick start

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



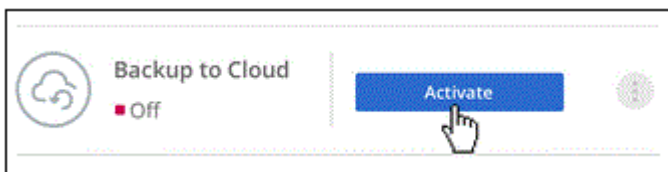
Verify support for your configuration

- 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 NetApp Cloud Manager Marketplace offering](#), the [AWS Cloud Manager Marketplace offering](#), or you have purchased [and activated](#) a Backup to Cloud BYOL license from NetApp.
- You have a valid cloud provider subscription for the 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.



Enable Backup to Cloud on the system

Select the working environment and click **Activate** next to the Backup to Cloud 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.

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.

Requirements

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

ONTAP requirements

ONTAP 9.7P5 and later.

A SnapMirror license (included as part of the PREM or Data Protection bundle).

Cluster networking requirements

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. The Admin SVM must reside on the IPspace. [Learn more about IPspaces.](#)

When you set up backup to cloud, 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.

Supported regions

Backups from on-prem systems are supported 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.

License requirements

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

For Backup to Cloud 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 or Amazon AWS subscription for the storage space where your backups will be located.

Preparing Amazon S3

When using Amazon S3, you must configure permissions for Cloud Manager to access the S3 bucket, and you must configure permissions so the on-prem 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.

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

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

Enabling Backup to Cloud

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

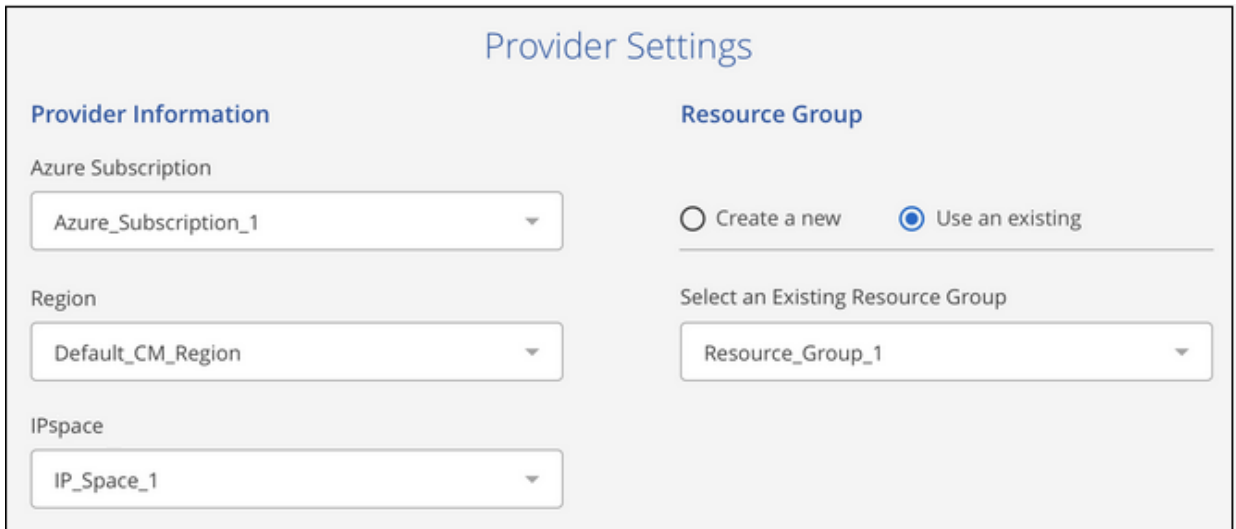
Steps

1. Select the working environment and click **Activate** next to the Backup to Cloud 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. The form is divided into two main sections: 'Provider Information' and 'Resource Group'. Under 'Provider Information', there are three dropdown menus: 'Azure Subscription' with the value 'Azure_Subscription_1', 'Region' with the value 'Default_CM_Region', and 'IPspace' with the value 'IP_Space_1'. Under 'Resource Group', there are 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' with the value '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 and click **Save**.

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

Result

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

What's next?

You can manage backups by changing the backup schedule, restoring volumes, and more.

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

Manage backups for Cloud Volumes ONTAP and on-premises ONTAP systems by changing the backup schedule, restoring volumes, deleting backups, and more.


Changing the schedule and backup retention

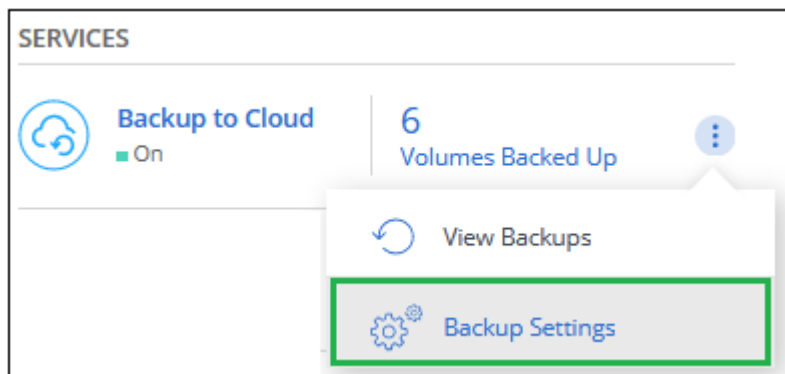
The default policy backs up volumes every day and retains the most recent 30 backup copies of each volume. You can change to weekly or monthly backups and you can change the number of backup copies to retain. You can also select one of the system-defined policies that provide scheduled backups for 3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




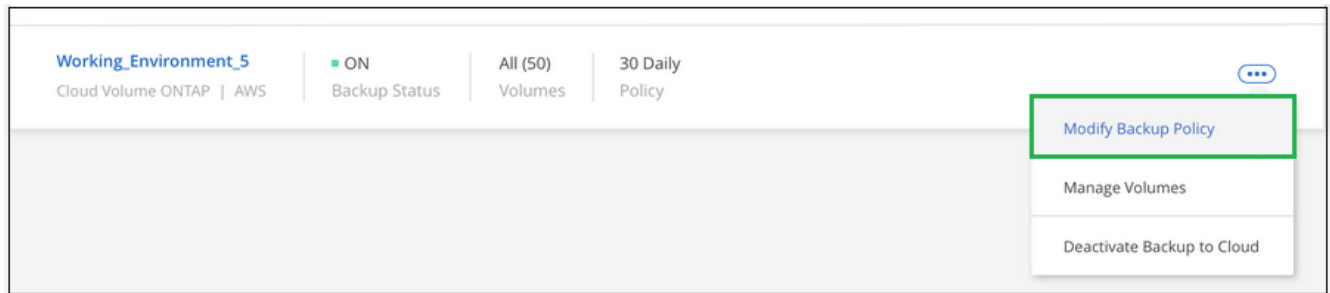
Changing the backup policy affects only new volumes created after you change the schedule. It doesn't affect the schedule for any existing volumes.

Steps

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



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




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

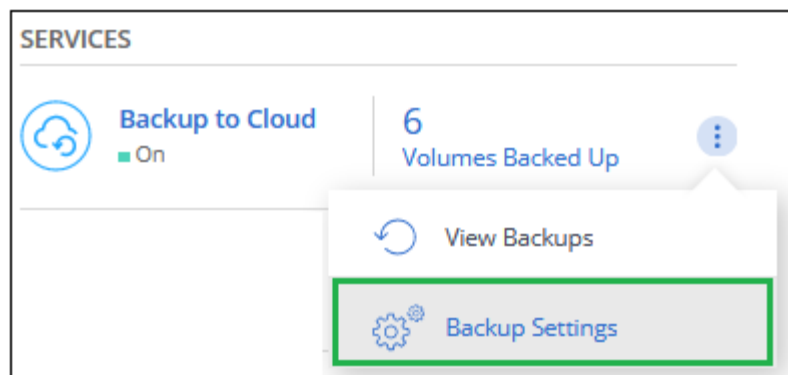
The screenshot shows the 'Modify Backup Policy' page. The title 'Modify Backup Policy' is at the top. Below it, there are two radio buttons: 'Create a New Policy' (selected) and 'Select an Existing Policy'. Under 'Create a New Policy', there are two input fields: 'Backup Every' with a dropdown menu showing 'Day' and 'Number of backups to retain' with a text input showing '30'. Below these fields 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

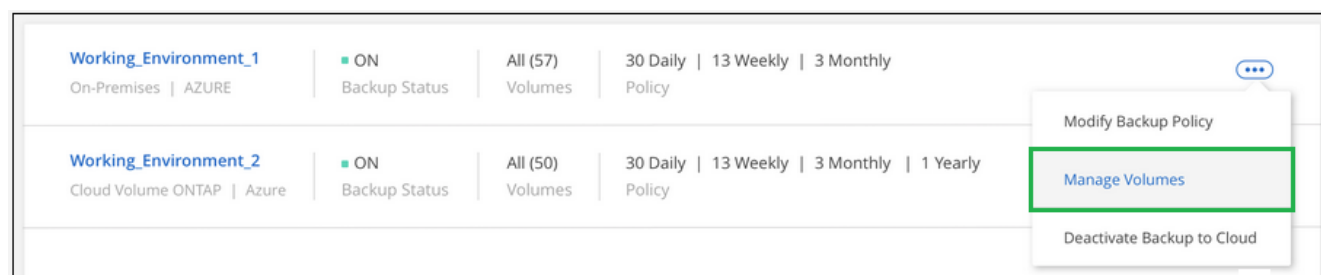
You can stop backing up a volume if you do not need backup copies of that volume and you do not want to pay for the cost to store the backups. You can also add a new volume to the backup list if it is not currently being backed up.

Steps

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



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



- 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.

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](#).


Restoring a volume from a backup

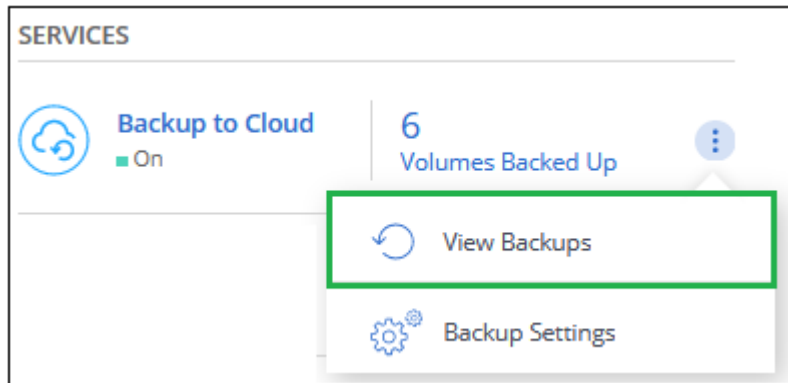
When you restore data from a backup, Cloud Manager creates a *new* volume using the data from the backup. You can restore the data to a volume in the same working environment or to a different working environment that's located in the same cloud account as the source working environment. Because the backup does not contain any snapshots, the newly restored volume does not either.



Backups created from on-premises ONTAP systems can be restored only to Cloud Volumes ONTAP systems that use the same cloud provider as where the backup resides. Restoring a backup is not currently supported using the Cloud Manager UI. You can use the API if you need to restore a backup at this time. Restore using the UI will be addressed shortly.

Steps

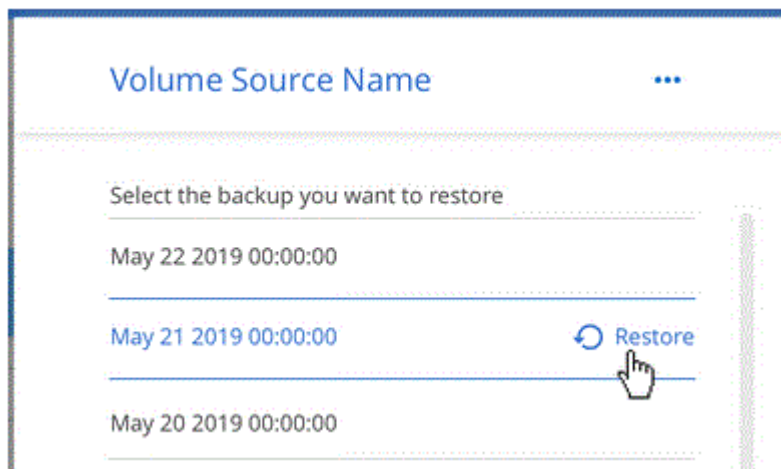
1. Select the working environment.
2. Click  and select **View Backups**.



3. Select the row for the volume that you want to restore and click **View Backup List**.

6 of 16 Volumes						
Working Environment	Source Volume	Last Backup	Policy & Retention	Relationship Status		
gfcDevQaSaCvo (On)	cifsvol9 (Available)	Aug 13, 2020 02:00:12 PM UTC	30 Daily	Active (Idle)		View Backup List
gfcDevQaSaCvo (On)	smbvol (Available)	Aug 13, 2020 02:00:33 PM UTC	30 Daily	Active (Idle)		View Backup List

4. Find the backup that you want to restore and click the **Restore** icon.



5. Fill out the *Restore Backup to new volume* page:

- a. Select the working environment to which you want to restore the volume.
- b. Enter a name for the volume.
- c. Click **Restore**.

Result

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

Deleting backups

Backup to Cloud enables you to delete *all* backups of a specific volume. You can't delete *individual* backups.

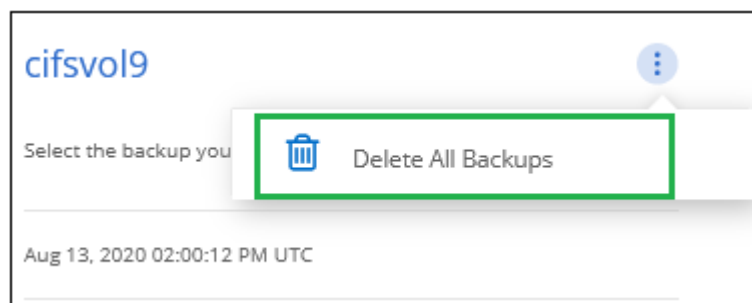
You might do this if you no longer need the backups or if you deleted the source volume and want to remove all backups.



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. Backup to Cloud 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**.

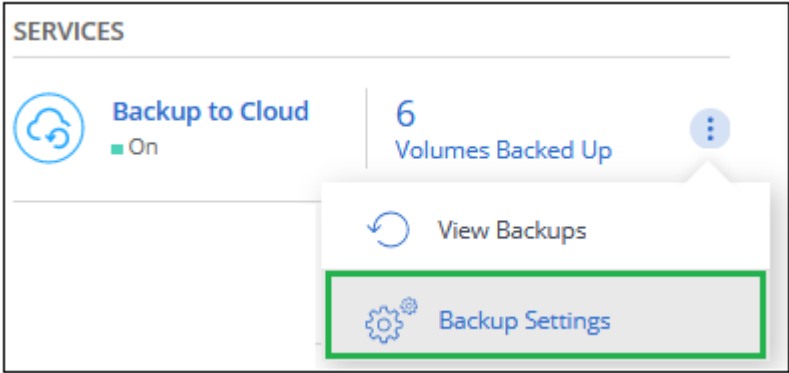
Disabling Backup to Cloud


Disabling Backup to Cloud 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.

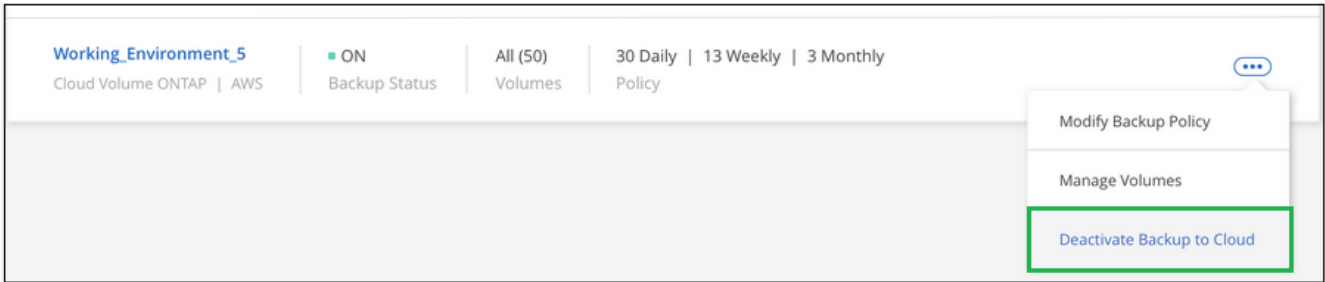
Note that you'll continue to be charged by your cloud provider for object storage costs for the capacity that your backups use unless you delete the backups.

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 Backup to Cloud**.



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

Copyright Information

Copyright © 2020 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.