



Learn about Cloud Backup

Cloud Manager

Tom Onacki, Ben Cammett
August 24, 2021

This PDF was generated from https://docs.netapp.com/us-en/occm/concept_backup_to_cloud.html on October 11, 2021. Always check docs.netapp.com for the latest.

Table of Contents

- Learn about Cloud Backup 1
 - Features 1
 - Supported working environments and object storage providers 1
 - Cost 2
 - Licensing 3
 - How Cloud Backup works 5
 - Supported volumes 7
 - FabricPool tiering policy considerations 7
 - Limitations 7

Learn about Cloud Backup

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

When necessary, you can restore an entire *volume*, or one or more *files*, from a backup to the same or different Cloud Volumes ONTAP or on-premises ONTAP cluster.

[Learn more about Cloud Backup.](#)

Features

- Back up independent copies of your data volumes to low-cost object storage.
- Back up from cloud to cloud, and from on-premises ONTAP systems to public or private cloud.
- Backups can reside on a different subscription/account or different region than your Cloud Volumes ONTAP system.
- Backup data is secured with AES-256 bit encryption at-rest and TLS 1.2 HTTPS connections in-flight.
- Support for up to 4,000 backups of a single volume.
- Restore data from a specific point in time.
- Restore a volume, or individual files, to the source system or to a different system.
- Restore data to a working environment using a different subscription/account or that is in a different region.
- Restores data on a block level, placing the data directly in the location you specify, all while preserving the original ACLs.
- Browsable file catalog for selecting individual files for single file restore.

Supported 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
On-premises ONTAP system	Amazon S3 Azure Blob Google Cloud Storage NetApp StorageGRID

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	
NetApp StorageGRID	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. (There are no storage costs when creating backups on your StorageGRID systems.)

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

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

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

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

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

- For Volume Restore 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 three ways to pay for the Backup service. The first option is to subscribe from your cloud provider,

which enables you to pay per month based on the amount of backed up data. The second option is to get an annual contract - this is only available through AWS. The third option is to purchase licenses directly from NetApp. Read the [Licensing](#) section for details.

Licensing

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

Free trial

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

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

Cloud Backup offers consumption-based licensing in a pay-as-you-go model. The licensing costs are based on target backup capacity (before ONTAP storage efficiencies). After subscribing through your cloud provider's marketplace, you pay per GB for data that's backed up—there's no up-front payment. You are billed by your cloud provider through your monthly bill.

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

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

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

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

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

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

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

Annual contract (AWS only)

Two annual contracts are available from the AWS Marketplace:

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

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

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

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

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

Bring your own license

BYOL is term-based (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).



Backup to StorageGRID does require a BYOL license, but there is no cost for cloud provider storage space in this case.

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

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

BYOL license considerations

When using a Cloud Backup BYOL license, Cloud Manager displays a warning in the user interface when backups are nearing the capacity limit or nearing the license expiration date. You receive these warnings:

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

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

Two things can happen when your license expires:

- If the account you are using 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 see the warnings.

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 [how to update a Cloud Backup license](#).

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

How Cloud Backup works

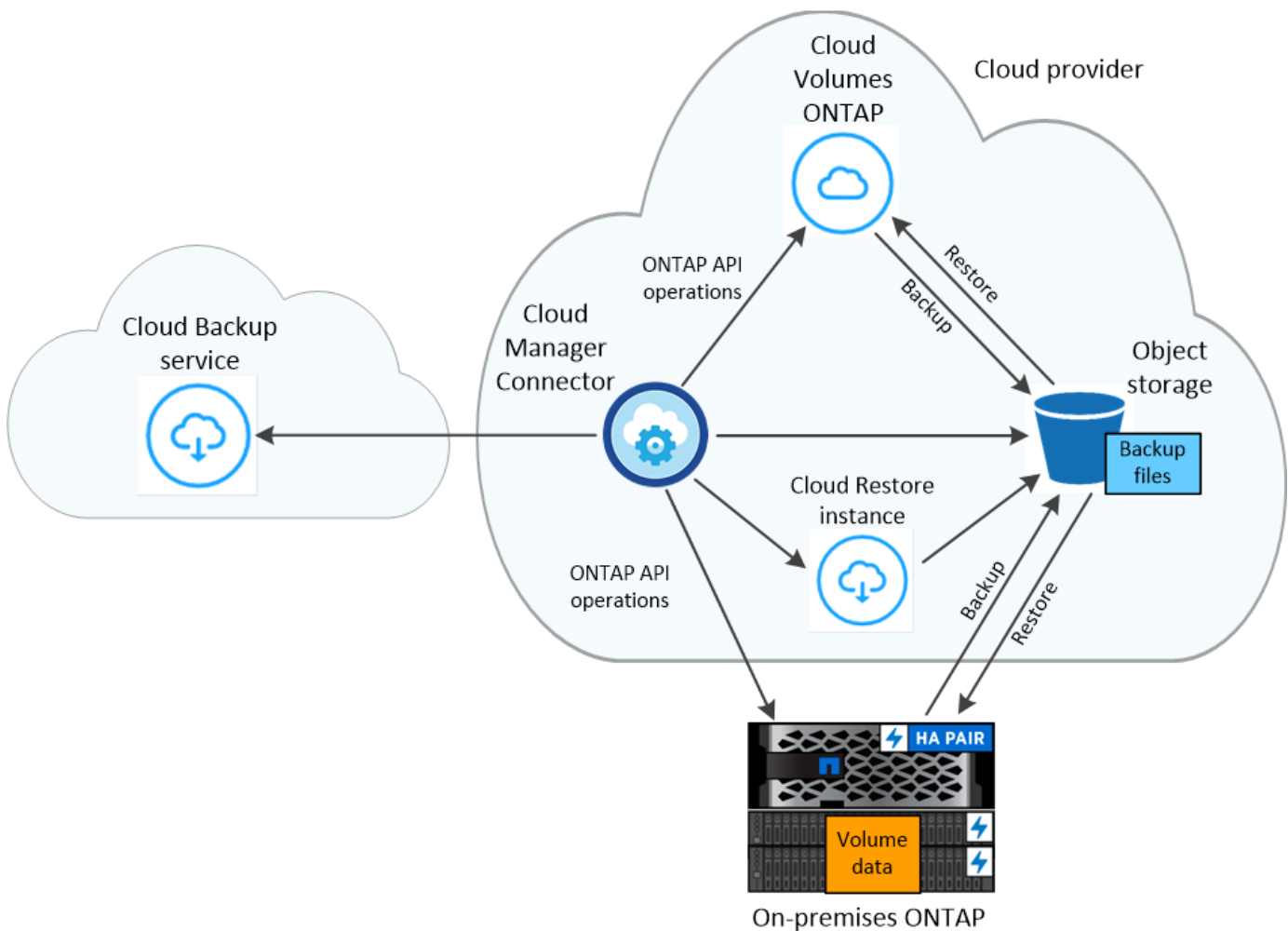
When you enable Cloud Backup on a Cloud Volumes ONTAP or on-premises ONTAP system, the service performs a full backup of your data. Volume snapshots are not included in the backup image. After the initial backup, all additional backups are incremental, which means that only changed blocks and new blocks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

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



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

The following image shows the relationship between each component:



Where backups reside

Backup copies are stored in an object store that Cloud Manager creates in your cloud account. 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.

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

Supported storage classes or access tiers

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

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

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

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 hourly, daily, weekly, monthly, or a combination

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

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

Backup protection policies that you have created on the system using ONTAP System Manager or the ONTAP CLI are also available as selections.

You can also [create an on-demand backup of a volume](#) from the Backup Dashboard in addition to those backup files created from the scheduled backups.

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

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

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

Backup copies are associated with your 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 to public cloud storage, the Connector must be

deployed in the cloud.

- When making backups from on-premises ONTAP systems to StorageGRID (private cloud), the Connector must be deployed on premises.
- When backing up data protection (DP) volumes, relationships with the following SnapMirror labels will not be backed up to cloud:
 - app_consistent
 - all_source_snapshot
- 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 up to 100 individual files at a time. There is currently no support for restoring folders/directories.
- The file being restored must be using the same language as the language on the destination volume. You will receive an error message if the languages are not the same.
- Single file restore is not supported when using the same account with different Cloud Managers in different subnets.

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.