



Backing up Cloud Volumes ONTAP data to Amazon S3

Cloud Manager

Tom Onacki, Ben Cammett
September 14, 2021

Table of Contents

- Backing up Cloud Volumes ONTAP data to Amazon S3 1
 - Quick start 1
 - Requirements 3
 - Enabling Cloud Backup on a new system 5
 - Enabling Cloud Backup on an existing system 6

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.



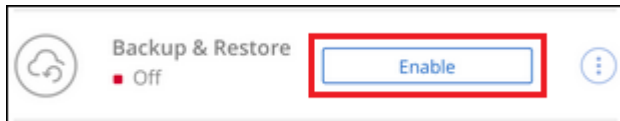
Verify support for your configuration

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



Enable Cloud Backup on your new or existing system

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



Enter the provider details

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

Provider Settings

Provider Information	Location & Connectivity
AWS Account <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;">AWS_Account_1</div>	Region <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;">us-east-2</div>
AWS Access Key <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;">Enter AWS Access Key</div>	Encryption ⓘ <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;">Encryption Key Type: AWS SSE-S3 Change Key</div>
AWS Secret Key <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;">Enter AWS Secret Key</div>	

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

Define Policy

Policy - Retention & Schedule

☒ Create a New Policy
 ☐ Select an Existing Policy

<input type="checkbox"/> Hourly	Number of backups to retain	<div style="border: 1px solid #ccc; padding: 2px 10px; text-align: center;">24</div>
<input checked="" type="checkbox"/> Daily	Number of backups to retain	<div style="border: 1px solid #ccc; padding: 2px 10px; text-align: center;">30</div>
<input type="checkbox"/> Weekly	Number of backups to retain	<div style="border: 1px solid #ccc; padding: 2px 10px; text-align: center;">52</div>
<input type="checkbox"/> Monthly	Number of backups to retain	<div style="border: 1px solid #ccc; padding: 2px 10px; text-align: center;">12</div>

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

S3 Bucket

Cloud Manager will create the S3 bucket 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

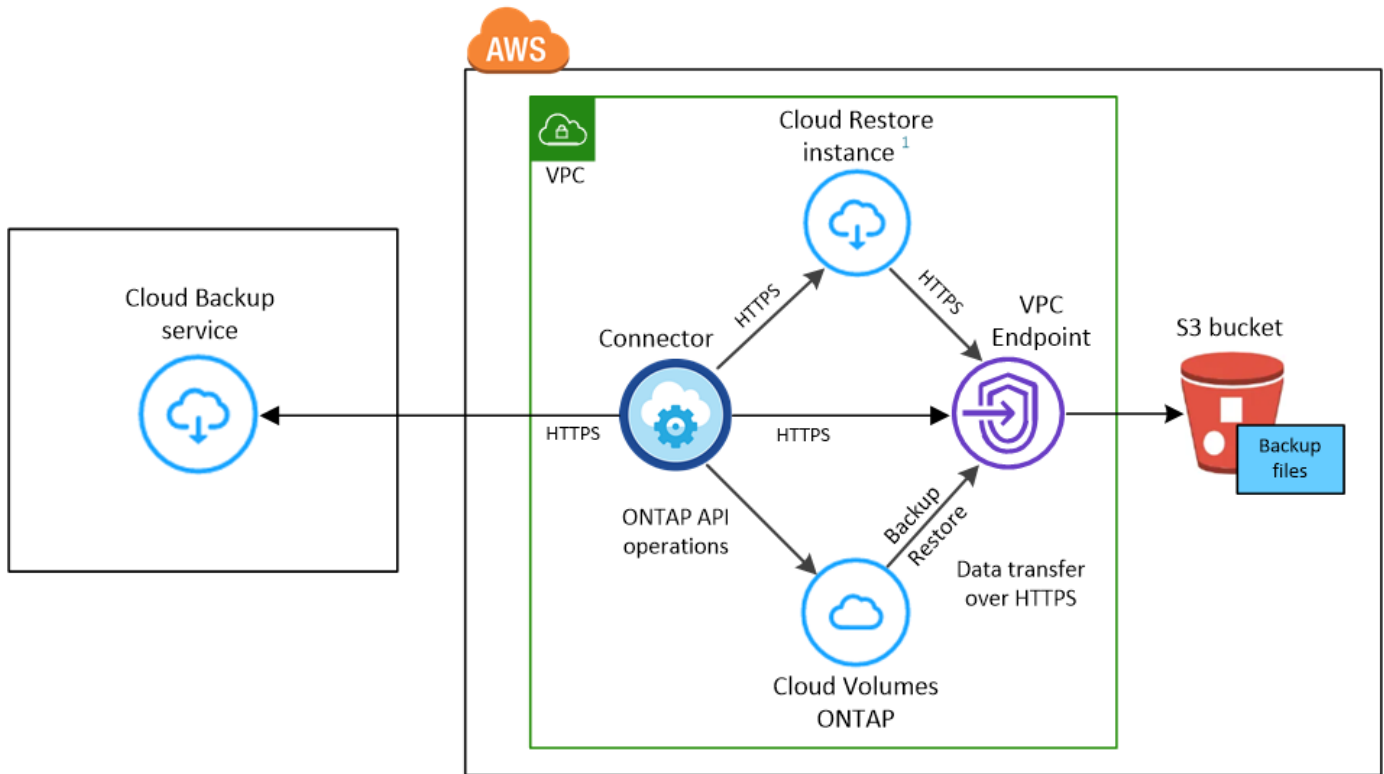
Choose to restore an entire backup to a new volume, or to restore individual files from the backup to an existing volume. You can restore data to a Cloud Volumes ONTAP system in AWS, or to an on-premises ONTAP system.

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:



¹ Cloud Restore instance is active only during single-file restore operations.

When the Cloud Restore instance is deployed in the cloud, it is located in the same subnet as the Connector.

Supported ONTAP versions

Cloud Volumes ONTAP 9.6 and later.

License requirements

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

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

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

For Cloud Backup BYOL licensing, you need the serial number from NetApp that enables you to use the

service for the duration and capacity of the license. [Learn how to manage your BYOL licenses.](#)

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

Supported AWS regions

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

Required setup for creating backups in a different AWS account

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

Required information for using customer-managed keys for data encryption

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

AWS Backup permissions required

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

Here are the specific permissions from the policy:

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

AWS Restore permissions required

The following EC2 permissions are needed for the IAM role that provides Cloud Manager with permissions so that it can start, stop, and terminate the Cloud Restore instance:

```
"Action": [  
    "ec2:DescribeInstanceTypeOfferings",  
    "ec2:StartInstances",  
    "ec2:StopInstances",  
    "ec2:TerminateInstances"  
]
```

Required outbound internet access for AWS deployments

The Cloud Restore instance 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.

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



Enabling Cloud Backup on a new system

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

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

Steps

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

 Backup to Cloud 

Integrated backup for Cloud Volumes ONTAP based on SnapMirror and Snapshot technologies. Backup copies are maintained in S3 buckets. Backups stored in S3 are charged separately from Cloud Volumes ONTAP.

ADVANTAGES

- ✓ Automatically back up all volumes.
- ✓ Creates new backup copy every day.
- ✓ Retains backups for 30 days.

CLARIFICATIONS

- > Backup settings are editable after working environment creation.

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 **Enable** next to the Backup & Restore service in the right-panel.



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

If you want to use a different AWS account for your backups, you must [log in to the AWS portal and link the two accounts](#).
 - b. The region where the backups will be stored. This can be a different region than where the Cloud Volumes ONTAP system resides.
 - c. Whether you'll use the default Amazon S3 encryption keys or choose your own customer-managed keys from your AWS account to manage encryption of your data. ([See how to use your own keys](#)).

Provider Settings

Provider Information

AWS Account

AWS Access Key

AWS Secret Key

Location & Connectivity

Region

Encryption

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

3. Define the backup schedule and retention value and click **Next**.

Define Policy

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

☐ Hourly
☒ Daily
☐ Weekly
☐ Monthly

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

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

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

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

Select Volumes

57 Volumes 🔍

<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Volume_Name_1	RW	SVM_Name_1	0.25 TB	10 TB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume_Name_2	RW	SVM_Name_2	0.25 TB	10 TB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume_Name_3	RW	SVM_Name_3	0.25 TB	10 TB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume_Name_4	DP	SVM_Name_4	0.25 TB	10 TB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume_Name_5	RW	SVM_Name_5	0.25 TB	10 TB	⊖ Not 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 and the Backup Dashboard is displayed so you can monitor the state of the backups.

What's next?

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

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.