



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

Cloud Manager

Tom Onacki
January 28, 2021

This PDF was generated from https://docs.netapp.com/us-en/occm/task_backup_from_onprem.html on February 28, 2021. Always check docs.netapp.com for the latest.

Table of Contents

- Backing up data from an on-premises ONTAP system to the cloud 1
 - Quick start 1
 - Requirements 2
 - Enabling Cloud Backup 5

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.

A Beta feature released in January 2021 allows you to run Compliance scans on the backed up volumes from your on-prem 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.



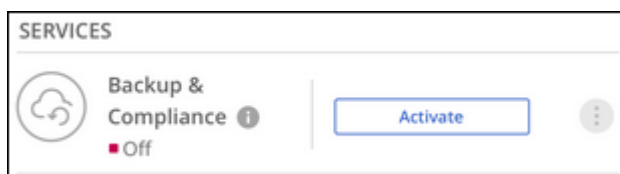
Verify support for your configuration

- 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.



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.



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.



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



Select the volumes that you want to back up

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



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.



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-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. [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.

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.

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

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-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.

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

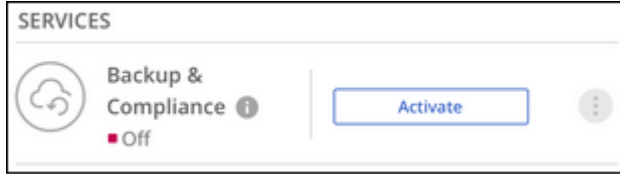
See the [AWS Documentation: Managing Access Keys for IAM Users](#) for details.

Enabling Cloud Backup

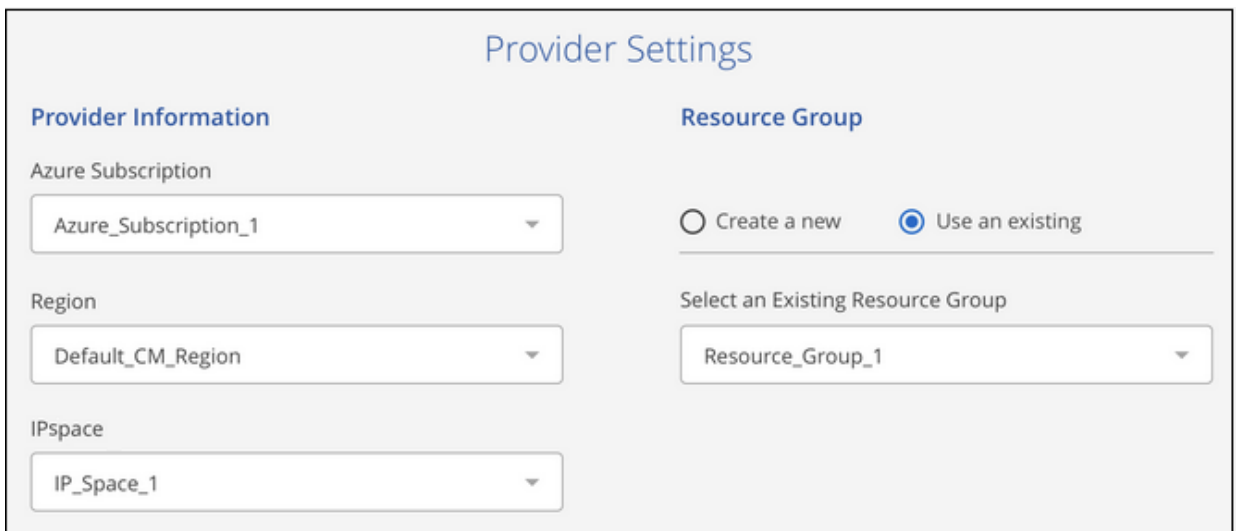
Enable Cloud Backup at any time directly from the on-premises working environment.

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 main sections: 'Provider Information' and 'Resource Group'. Under 'Provider Information', there are three dropdown menus: 'Azure Subscription' (selected: Azure_Subscription_1), 'Region' (selected: Default_CM_Region), and 'IPspace' (selected: 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 '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).

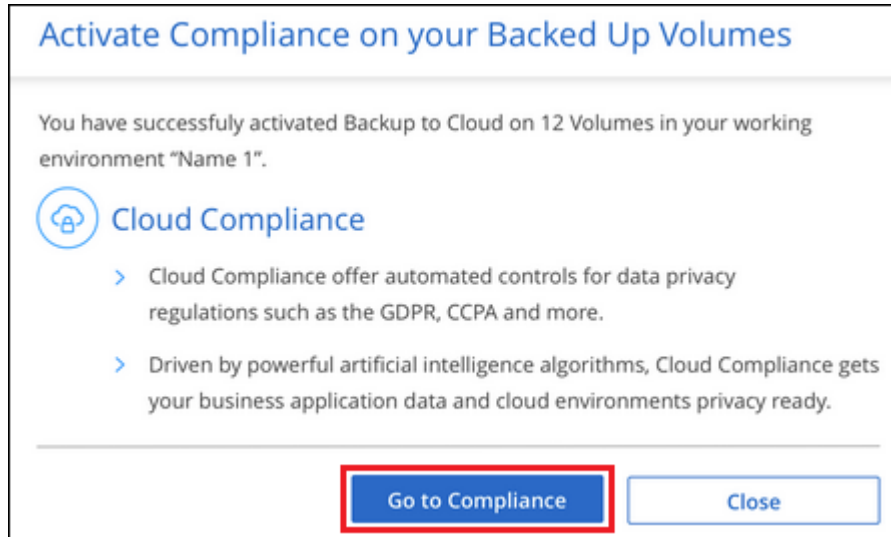
Select Volumes

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

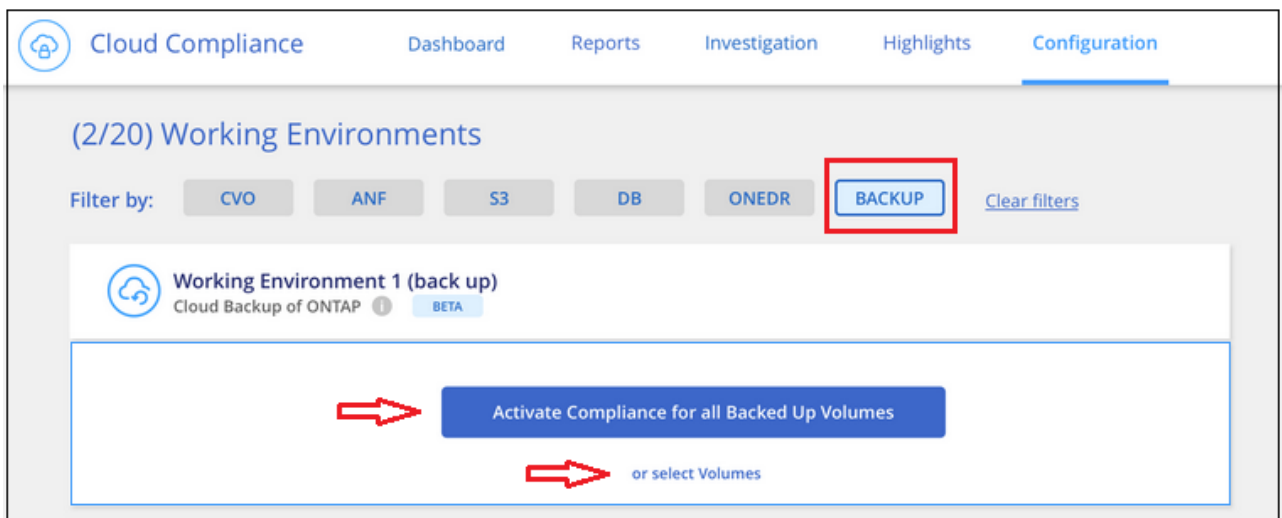
6. Click **Activate** and Cloud Backup starts taking the initial backups of your volumes.

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 displays the 'Cloud Compliance' interface. At the top, there's a header with a cloud icon and the text 'Cloud Compliance'. Below this, a link 'How does it work?' is visible. The main heading is 'Always-on Privacy & Compliance Controls', followed by a description: '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 the text are two buttons: 'Deploy Compliance in the Cloud' and 'Deploy Compliance On-Premises', both highlighted with a red border. At the bottom left, there's a link 'Learn about the differences between cloud deployment and on-premises deployment'. On the right, a 'Compliance Status' dashboard is shown, featuring a circular progress indicator, a 'Data Distribution' chart, and various file counts and categories.

Category	Percentage
Non-Sensitive	75%
Personal	20%
Sensitive Personal	5%

Category	Count
Personal Files	28,000
Email Address	2,700 Files
Credit Card	2,700 Files

Category	Count
Sensitive Personal Files	7,000
Health	2,700 Files
Ethnicity	2,700 Files

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-prem 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.

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.