



Back up to the cloud

ONTAP 9

NetApp
August 21, 2024

Table of Contents

- Back up to the cloud 1
 - Back up data to the cloud using SnapMirror 1
 - Back up data using Cloud Backup 3

Back up to the cloud

Back up data to the cloud using SnapMirror

Beginning with ONTAP 9.9.1, you can back up your data to the cloud and to restore your data from cloud storage to a different volume by using System Manager. You can use either StorageGRID or ONTAP S3 as your cloud object store.

Before using the SnapMirror Cloud feature, you should request a SnapMirror Cloud API license key from the NetApp Support Site: [Request SnapMirror Cloud API license key](#).

Following the instructions, you should provide a simple description of your business opportunity and request the API key by sending an email to the provided email address. You should receive an email response within 24 hours with further instructions on how to acquire the API key.

Add a cloud object store

Before you configure SnapMirror Cloud backups, you need to add a StorageGRID or ONTAP S3 cloud object store.

Steps

1. Click **Protection > Overview > Cloud Object Stores**.
2. Click [Add icon].

Back up using the default policy

You can quickly configure a SnapMirror Cloud backup for an existing volume using the default cloud protection policy, DailyBackup.

Steps

1. Click **Protection > Overview** and select **Back Up Volumes to Cloud**.
2. If this is your first time backing up to the cloud, enter your SnapMirror Cloud API license key in the license field as indicated.
3. Click **Authenticate and Continue**.
4. Select a source volume.
5. Select a cloud object store.
6. Click **Save**.

Create a custom cloud backup policy

If you do not want to use the default DailyBackup cloud policy for your SnapMirror Cloud backups, you can create your own policy.

Steps

1. Click **Protection > Overview > Local Policy Settings** and select **Protection Policies**.
2. Click **Add** and enter the new policy details.
3. In the **Policy Type** section, select **Back up to Cloud** to indicate that you are creating a cloud policy.
4. Click **Save**.

Create a backup from the Volumes page

You can use the System Manager **Volumes** page to when you want to select and create cloud backups for multiple volumes at one time or when you want to use a custom protection policy.

Steps

1. Click **Storage > Volumes**.
2. Select the volumes you want to back up to the cloud, and click **Protect**.
3. In the **Protect Volume** window, click **More Options**.
4. Select a policy.

You can select the default policy, DailyBackup, or a custom cloud policy you created.

5. Select a cloud object store.
6. Click **Save**.

Restore from the cloud

You can use System Manager to restore backed up data from cloud storage to a different volume on the source cluster.

Steps

1. From the source Cluster of a SnapMirror-to-Cloud relationship, click **Storage > Volumes**.
2. Select the volume you want to restore.
3. Select the **Back Up to Cloud** tab.
4. Click [Menu options icon] next to the source volume you want to restore to display the menu, and select **Restore**.
5. Under **Source**, select a storage VM and then enter the name of the volume to which you want the data restored.
6. Under **Destination**, select the Snapshot copy you want to restore.
7. Click **Save**.

Delete a SnapMirror Cloud relationship

You can use System Manager to delete a cloud relationship.

Steps

1. Click **Storage > Volumes** and select the volume you want to delete.
2. Click [Menu options icon] next to the source volume and select **Delete**.
3. Select **Delete the cloud object store endpoint (optional)** if you want to delete the cloud object store endpoint.
4. Click **Delete**.

Remove a cloud object store

You can use System Manager to remove a cloud object store if it is not part of a cloud backup relationship. When a cloud object store is part of a cloud backup relationship, it cannot be deleted.

Steps

1. Click **Protection > Overview > Cloud Object Stores**.
2. Select the object store you want to delete, click [Menu options icon] and select **Delete**.

Back up data using Cloud Backup

Beginning with ONTAP 9.9.1, you can use System Manager to back up data in the cloud using Cloud Backup.



Cloud Backup supports FlexVol read-write volumes and data-protection (DP) volumes. FlexGroup volumes and SnapLock volumes are not supported.

Before you begin

You should perform the following procedures to establish an account in BlueXP. For the service account, you need to create the role as "Account Admin". (Other service account roles do not have the required privileges needed to establish a connection from System Manager.)

1. [Create an account in BlueXP](#).
2. [Create a connector in BlueXP](#) with one of the following cloud providers:
 - Microsoft Azure
 - Amazon Web Services (AWS)
 - Google Cloud Platform (GCP)
 - StorageGrid (ONTAP 9.10.1)



Beginning with ONTAP 9.10.1, you can select StorageGrid as a cloud backup provider, but only if BlueXP is deployed on premises. The BlueXP connector must be installed on premises and available through the BlueXP software-as-a-service (SaaS) application.

3. [Subscribe to Cloud Backup Service in BlueXP](#) (requires the appropriate license).
4. [Generate an access key and a secret key using BlueXP](#).

Register the cluster with BlueXP

You can register the cluster with BlueXP by using either BlueXP or System Manager.

Steps

1. In System Manager, go to **Protection Overview**.
2. Under **Cloud Backup Service**, provide the following details:
 - Client ID
 - Client secret key
3. Select **Register and Continue**.

Enable Cloud Backup

After the cluster is registered with BlueXP, you need to enable the Cloud Backup and initiate the first backup to the cloud.

Steps

1. In System Manager, click **Protection > Overview**, then scroll to the **Cloud Backup Service** section.
2. Enter the **Client ID** and **Client Secret**.



Beginning with ONTAP 9.10.1, you can learn about the cost of using the cloud by clicking [Learn more about the cost of using the cloud](#).

3. Click **Connect and Enable Cloud Backup Service**.
4. On the **Enable Cloud Backup Service** page, provide the following details, depending on the provider you selected.

For this cloud provider...	Enter the following data...
Azure	<ul style="list-style-type: none">• Azure Subscription ID• Region• Resource group name (existing or new)
AWS	<ul style="list-style-type: none">• AWS Account ID• Access key• Secret key• Region
Google Cloud Project (GCP)	<ul style="list-style-type: none">• Google Cloud Project name• Google Cloud Access key• Google Cloud Secret key• Region
StorageGrid (ONTAP 9.10.1 and later, and only for on-premises deployment of BlueXP)	<ul style="list-style-type: none">• Server• SG Access Key• SG Secret Key

5. Select a **Protection policy**:
 - **Existing policy**: Choose an existing policy.
 - **New Policy**: Specify a name and set up a transfer schedule.



Beginning with ONTAP 9.10.1, you can specify whether you want to enable archiving with Azure or AWS.



If you enable archiving for a volume with Azure or AWS, you cannot disable the archiving.

If you enable archiving for Azure or AWS, specify the following:

- The number of days after which the volume is archived.

- The number of backups to retain in the archive. Specify “0” (zero) to archive up to the latest backup.
- For AWS, select the archive storage class.

6. Select the volumes you want to back up.

7. Select **Save**.

Edit the protection policy used for Cloud Backup

You can change which protection policy is used with Cloud Backup.

Steps

1. In System Manager, click **Protection > Overview**, then scroll to the **Cloud Backup Service** section.
2. Click [Menu options icon], then **Edit**.
3. Select a **Protection policy**:
 - **Existing policy**: Choose an existing policy.
 - **New Policy**: Specify a name and set up a transfer schedule.



Beginning with ONTAP 9.10.1, you can specify whether you want to enable archiving with Azure or AWS.



If you enable archiving for a volume with Azure or AWS, you cannot disable the archiving.

If you enable archiving for Azure or AWS, specify the following:

- The number of days after which the volume is archived.
- The number of backups to retain in the archive. Specify “0” (zero) to archive up to the latest backup.
- For AWS, select the archive storage class.

4. Select **Save**.

Protect new volumes or LUNs on the cloud

When you create a new volume or LUN, you can establish a SnapMirror protection relationship that enables backing up to the cloud for the volume or LUN.

Before you begin

- You should have a SnapMirror license.
- Intercluster LIFs should be configured.
- NTP should be configured.
- Cluster must be running ONTAP 9.9.1.

About this task

You cannot protect new volumes or LUNs on the cloud for the following cluster configurations:

- The cluster cannot be in a MetroCluster environment.

- SVM-DR is not supported.
- FlexGroups cannot be backed up using Cloud Backup.

Steps

1. When provisioning a volume or LUN, on the **Protection** page in System Manager, select the checkbox labeled **Enable SnapMirror (Local or Remote)**.
2. Select the Cloud Backup policy type.
3. If the Cloud Backup is not enabled, select **Enable Cloud Backup Service**.

Protect existing volumes or LUNs on the cloud

You can establish a SnapMirror protection relationship for existing volumes and LUNs.

Steps

1. Select an existing volume or LUN, and click **Protect**.
2. On the **Protect Volumes** page, specify **Backup using Cloud Backup Service** for the protection policy.
3. Click **Protect**.
4. On the **Protection** page, select the checkbox labeled **Enable SnapMirror (Local or Remote)**.
5. Select **Enable Cloud Backup Service**.

Restore data from backup files

You can perform backup management operations, such as restoring data, updating relationships, and deleting relationships, only when using the BlueXP interface. Refer to [Restoring data from backup files](#) for more information.

Copyright information

Copyright © 2024 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

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.