



Use replication

Amazon FSx for NetApp ONTAP

NetApp

February 02, 2026

Table of Contents

Use replication	1
Create a replication relationship in NetApp Workload Factory	1
Initialize a replication relationship in NetApp Workload Factory	4

Use replication

Create a replication relationship in NetApp Workload Factory

Create a replication relationship for an FSx for ONTAP file system in NetApp Workload Factory to avoid data loss in case of an unforeseen disaster. Replication is supported between two FSx for ONTAP file systems, and between Cloud Volumes ONTAP or an on-premises ONTAP system and an FSx for ONTAP file system.

About this task

Replication adds protection against data loss if the region where your data resides experiences a disaster.

This operation creates a replication relationship for source volumes in an FSx for ONTAP file system, on-premises ONTAP system, or Cloud Volumes ONTAP system.

Replicated volumes in the target file system are data protection (DP) volumes and follow the naming format: {OriginalVolumeName}_copy.

When you replicate a source volume with immutable files, the target volume and file system stay locked until the retention period of the immutable files in the source volume ends. The immutable files feature is available when you [create a volume](#) for an FSx for ONTAP file system.

- Replication isn't supported for block volumes using iSCSI or NVMe protocols.
- You can replicate one source (read/write) volume or one data protection (DP) volume. Cascading replication is supported, but a third hop isn't. Learn more about [cascading replication](#).

Before you begin

Consider the following before you begin.

- You must have one FSx for ONTAP file system to use for the target in the replication relationship.
- The FSx for ONTAP file system you use for the replication relationship must have an associated link. [Learn how to associate an existing link or to create and associate a new link](#). After you associate the link, return to this operation.
- For replication from an on-premises ONTAP system to an FSx for ONTAP file system, make sure you have discovered the on-premises ONTAP system.

Follow these steps to replicate specific or all volumes in a file system.

Steps

1. Log in using one of the [console experiences](#).
2. Select the menu and then select **Storage**.
3. From the Storage menu, select **FSx for ONTAP**.
4. From **FSx for ONTAP**, select the actions menu of the file system that contains the volume(s) to replicate and then select **Manage**.
5. Either replicate all volumes in a file system or replicate select volumes.

- To replicate all volumes in a file system: From the file system overview, select **Replicate data**.
- To replicate select volumes: From the file system overview, select the **Volumes** tab.

In the Volumes table, select one or more volumes and then select **Replicate data**.

6. On the Replicate data page, under Replication target, provide the following:

- Use case:** Select one of the following use cases for the replication. Depending on the selected use case, Workload Factory fills in the form with recommended values in accordance with best practices. You can accept the recommended values or make changes as you complete the form.
 - Migration: transfers your data to the target FSx for ONTAP file system
 - Hot disaster recovery: ensures high availability and rapid disaster recovery for critical workloads
 - Cold or archive disaster recovery:
 - Cold disaster recovery: uses longer recovery time objectives (RTO) and recovery point objects (RPO) to lower costs
 - Archive: replicates data for long-term storage and compliance
 - Other

Additionally, the use case selection determines the replication policy, or SnapMirror policy (ONTAP). The terms used to describe replication policies come from [ONTAP 9 documentation](#).

- For migration and other, the replication policy is called *MirrorAll/Snapshots*. *MirrorAll/Snapshots* is an asynchronous policy for mirroring all snapshots and the latest active file system.
- For hot, cold, or archive disaster recovery, the replication policy is called *MirrorAndVault*. *MirrorAndVault* is an asynchronous and vault policy for mirroring the latest active file system and daily and weekly snapshots.

For all use cases, if you enable snapshots for long-term retention, the default replication policy is *MirrorAndVault*.

- FSx for ONTAP file system:** Select credentials, region, and FSx for ONTAP file system name for the target FSx for ONTAP file system.
- Storage VM name:** Select the storage VM from the dropdown menu. The storage VM you select is the target for all selected volumes in this replication relationship.
- Volume name:** The target volume name is generated automatically with the following format {OriginalVolumeName}_copy. You can use the auto-generated volume name or enter another volume name.
- Tiering policy:** Select the tiering policy for the data stored in the target volume. The tiering policy defaults to the recommended tiering policy for the use case you selected.

Balanced (Auto) is the default tiering policy when creating a volume using the Workload Factory console. For more information about volume tiering policies, refer to [Volume storage capacity](#) in AWS FSx for NetApp ONTAP documentation. Note that Workload factory uses use-case based names in the Workload Factory console for tiering policies and includes FSx for ONTAP tiering policy names in parentheses.

If you selected the migration use case, Workload Factory automatically selects to copy the tiering policy of source volume to the target volume. You can deselect to copy the tiering policy and select a tiering policy which applies to the volume selected for replication.

f. **Max transfer rate:** Select **Limited** and enter the max transfer limit in MB/s. Alternatively, select **Unlimited**.

Without a limit, network and application performance may decline. Alternatively, we recommend an unlimited transfer rate for FSx for ONTAP file systems for critical workloads, for example, those that are used primarily for disaster recovery.

7. Under Replication settings, provide the following:

- Replication interval:** Select the frequency that snapshots are transferred from the source volume to the target volume.
- Long-term retention:** Optionally, enable snapshots for long-term retention. Long-term retention enables business services to continue operating even through a complete site failure, supporting applications to fail over transparently using a secondary copy.

Replications without long-term retention use the *MirrorAllSnapshots* policy. Enabling long-term retention assigns the *MirrorAndVault* policy to the replication.

If you enable long-term retention, then select an existing policy or create a new policy to define the snapshots to replicate and the number to retain.



Matching source and target labels are required for long-term retention. If desired, Workload factory can create missing labels for you.

- **Choose an existing policy:** select an existing policy from the dropdown menu.
- **Create a new policy:** enter a **policy name**.

- Immutable snapshots:** Optional. Select **Enable immutable snapshots** to prevent snapshots taken in this policy from being deleted during the retention period.
 - Set the **Retention period** in number of hours, days, months, or years.
 - **Snapshot policies:** In the table, select the snapshot policy frequency and the number of copies to retain. You can select more than one snapshot policy.
- S3 access point:** Optionally, attach an S3 access point to access FSx for ONTAP file system data residing on NFS or SMB/CIFS volumes via AWS S3 APIs. Only the file access type is supported. Providing the following details:
 - **S3 access point name:** Enter the name of the S3 access point.
 - **User:** Select an existing user with access to the volume or create a new user.
 - **User type:** Select **UNIX** or **Windows** as the user type.
 - **Network configuration:** Select **Internet** or **Virtual private cloud (VPC)**. The type of network you choose determines whether the access point is accessible from the internet or restricted to a specific VPC.
 - **Enable metadata:** Enabling metadata creates an S3 table containing all objects accessible by the S3 access point, which you can use for auditing, governance, automatic, analysis, and optimization. Enabling metadata incurs additional AWS costs. Refer to [Amazon S3 pricing documentation](#) for more information.
- S3 access point tags:** Optionally, you can add up to 50 tags.

8. Select **Create**.

Result

The replication relationship appears in the **Replication relationships** tab in the target FSx for ONTAP file system.

Initialize a replication relationship in NetApp Workload Factory

Initialize a replication relationship between source and target volumes to transfer the snapshot and all data blocks in NetApp Workload Factory.

About this task

Initialization performs a *baseline* transfer: it makes a snapshot of the source volume, then transfers the snapshot and all the data blocks it references to the target volume.

Before you begin

Consider when you choose to complete this operation. Initialization can be time-consuming. You might want to run the baseline transfer in off-peak hours.

Steps

1. Log in using one of the [console experiences](#).
2. Select the menu and then select **Storage**.
3. From the Storage menu, select **FSx for ONTAP**.
4. From **FSx for ONTAP**, select the actions menu of the file system to update and then select **Manage**.
5. From the file system overview, select the **Replication relationships** tab.
6. In the Replication relationships tab, select the actions menu of the replication relationship to initialize.
7. Select **Initialize**.
8. In the Initialize relationship dialog, select **Initialize**.

Copyright information

Copyright © 2026 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—with 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.