



# Protect data

## ONTAP System Manager

NetApp

April 21, 2020

This PDF was generated from [https://docs.netapp.com/us-en/ontap/concept\\_dp\\_overview.html](https://docs.netapp.com/us-en/ontap/concept_dp_overview.html) on April 21, 2020.  
Always check docs.netapp.com for the latest.



# Table of Contents

Protect data ..... 1

    Data protection overview..... 1

# Protect data

## Data protection overview

Protect your data by creating and managing Snapshot copies, mirrors, vaults, and mirror-and-vault relationships.

*SnapMirror* is disaster recovery technology, designed for failover from primary storage to secondary storage at a geographically remote site. As its name implies, SnapMirror creates a replica, or mirror, of your working data in secondary storage from which you can continue to serve data in the event of a catastrophe at the primary site.

A *vault* is designed for disk-to-disk Snapshot copy replication for standards compliance and other governance-related purposes. In contrast to a SnapMirror relationship, in which the destination usually contains only the Snapshot copies currently in the source volume, a vault destination typically retains point-in-time Snapshot copies created over a much longer period.

= Configure Snapshot copies

:toc: macro

:toclevels: 1

:hardbreaks:

:nofooter:

:icons: font




:linkattrs:

:imagesdir: ./media/

You can create Snapshot copy policies to specify the maximum number of Snapshot copies that are automatically created and how frequently they are created. The policy specifies when to create Snapshot copies, how many copies to retain, and how to name them.

This procedure creates a Snapshot copy policy on the local cluster only.

### Steps

1. Click **Protection > Overview > Local Policy Settings**.
2. Under **Snapshot Policies**, click , and then click  **Add**.
3. Type the policy name, select the policy scope, and under **Schedules**, click  **Add** to enter the schedule details.

= Recover from Snapshot copies

:toc: macro

:toclevels: 1

:hardbreaks:

:nofooter:

:icons: font


:linkattrs:

:imagesdir: ./media/

You can recover a volume to an earlier point in time by restoring from a Snapshot copy.

This procedure restores a volume from a Snapshot copy.

#### Steps

1. Click **Storage** and select a volume.
2. Under **Snapshot Copies**, click  next to the Snapshot copy you want to restore, and select **Restore**.

= Prepare for mirroring and vaulting

:toc: macro

:toclevels: 1

:hardbreaks:

:nofooter:

:icons: font

:linkattrs:

:imagesdir: ./media/

You can protect your data by replicating it to a remote cluster for data backup and disaster recovery purposes.



Several default protection policies are available. You must have created your protection policies if you want to use custom policies.




#### Steps

1. In the local cluster, click **Protection > Overview**.
2. Expand **Intercluster Settings**. Click **Add Network Interfaces** and add intercluster network interfaces for the cluster.

Repeat this step on the remote cluster.

3. In the remote cluster, click **Protection > Overview**. Click  in the Cluster Peers section and click **Generate Passphrase**.
4. Copy the generated passphrase and paste it in the local cluster.
5. In the local cluster, under Cluster Peers, click **Peer Clusters** and peer the local and remote clusters.
6. Optionally, under Storage VM Peers, click  and then **Peer Storage VMs** to peer the storage VMs.

7. Click **Protect Volumes** to protect your volumes. To protect your LUNs, click **Storage > LUNs**, select a LUN to protect, and then click  **Protect**.

Select the protection policy based on the type of data protection you need.

8. To verify the volumes and LUNs are successfully protected from the local cluster, click **Storage > Volumes** or **Storage > LUNs** and, expand the volume/LUN view.

= Configure mirrors and vaults

:toc: macro

:toclevels: 1

:hardbreaks:

:nofooter:

:icons: font

:linkattrs:


:imagesdir: ./media/

Create a mirror and vault of a volume to protect data in case of a disaster and to have multiple archived versions of data to which you can roll back. Only the combined mirror-and-vault policy is supported. You cannot specify separate mirror and vault policies.

This procedure creates a mirror-and-vault policy on a remote cluster. The source cluster and destination cluster use intercluster network interfaces for exchanging data. The procedure assumes the [intercluster network interfaces are created and the clusters containing the volumes are peered](#) (paired). You can also peer storage VMs for data protection; however, if storage VMs are not peered, but permissions are enabled, storage VMs are automatically peered when the protection relationship is created.



#### Steps

1. Select the volume or LUN to protect: click **Storage > Volumes** or **Storage > LUNs**, and then click the desired volume or LUN name.
2. Click  **Protect**.
3. Select the destination cluster and storage VM.
4. The asynchronous policy is selected by default. To select a synchronous policy, click **More Options**.
5. Click **Protect**.
6. Click the **SnapMirror (Local or Remote)** tab for the selected volume or LUN to verify that protection is set up correctly.

= Serve data from a SnapMirror destination

:toc: macro

:toclevels: 1

:hardbreaks:

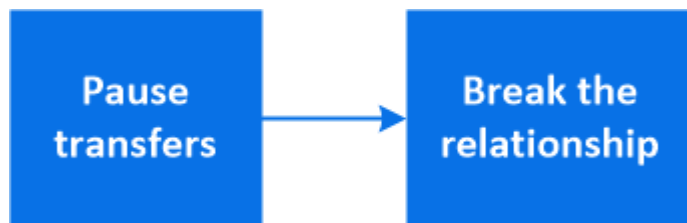
:nofooter:

:icons: font


:linkattrs:

:imagesdir: ./media/

To serve data from a mirror destination when a source becomes unavailable, stop scheduled transfers to the destination, and then break the SnapMirror relationship to make the destination writable.



#### *Steps*

1. Select the desired protection relationship: click **Protection** > **Relationships**, and then click the desired volume name.
2. Click .
3. Stop scheduled transfers : click **Pause**.
4. Make the destination writable: click **Break**.
5. Go to the main **Relationships** page to verify that the relationship state displays as "broken off".

#### *Next steps:*

When the disabled source volume is available again, you should resynchronize the relationship to copy the current data to the original source volume. This process replaces the data on the original source volume.

= Restore from a SnapMirror destination to original source

:toc: macro

:toclevels: 1

:hardbreaks:

:nofooter:

:icons: font

:linkattrs:


:imagesdir: ./media/

When your original source volume is available again after a disaster, you can

resynchronize data from the destination volume and reestablish the protection relationship.

This procedure replaces the data in the original source volume in an asynchronous relationship so that you can start serving data from the original source volume again and resume the original protection relationship.

#### *Steps*

1. Click **Protection** > **Relationships** and then click the broken off relationship you want to resynchronize.
2. Click  and then select **Resync**.
3. Under **Relationships**, monitor the resynchronization progress by checking the relationship state. The state changes to "Mirrored" when resynchronization is complete.

= Roll back data to an earlier version from a vault

:toc: macro

:toclevels: 1

:hardbreaks:

:nofooter:

:icons: font


:linkattrs:

:imagesdir: ./media/

When data in a volume is lost or corrupted, you can roll back your data by restoring from an earlier Snapshot copy.

This procedure replaces the current data on the source volume with data from an earlier Snapshot copy version. You should perform this task on the destination cluster.

#### *Steps*

1. Click **Protection** > **Relationships**, and then click the source volume name.
2. Click  and then select **Restore**.
3. Under **Source**, the source volume is selected by default. Click **Other Volume** if you want to choose a different volume.
4. Under **Destination**, choose the Snapshot copy you want to restore.
5. If your source and destination are located on different clusters, on the remote cluster, click **Protection** > **Relationships** to monitor the restore progress.



## Copyright Information

Copyright © 2019–2020 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.