



Customize a SnapMirror replication policy

ONTAP 9

NetApp
January 23, 2026

This PDF was generated from <https://docs.netapp.com/us-en/ontap/data-protection/create-custom-replication-policy-concept.html> on January 23, 2026. Always check docs.netapp.com for the latest.

Table of Contents

Customize a SnapMirror replication policy	1
Create a custom ONTAP SnapMirror replication policy	1
Define a rule for an ONTAP SnapMirror policy	3
Define an ONTAP SnapMirror schedule to create a local copy on the destination	5

Customize a SnapMirror replication policy

Create a custom ONTAP SnapMirror replication policy

You can create a custom replication policy if the default policy for a relationship is not suitable. You might want to compress data in a network transfer, for example, or modify the number of attempts SnapMirror makes to transfer snapshots.

You can use a default or custom policy when you create a replication relationship. For a custom archive (formerly SnapVault) or unified replication policy, you must define one or more *rules* that determine which snapshots are transferred during initialization and update. You might also want to define a schedule for creating local snapshots on the destination.

The *policy type* of the replication policy determines the type of relationship it supports. The table below shows the available policy types.

Policy type	Relationship type
async-mirror	SnapMirror DR
vault	SnapVault
mirror-vault	Unified replication
strict-sync-mirror	SnapMirror synchronous in the StrictSync mode (supported beginning with ONTAP 9.5)
sync-mirror	SnapMirror synchronous in the Sync mode (supported beginning with ONTAP 9.5)



When you create a custom replication policy, it is a good idea to model the policy after a default policy.

Steps

You can create custom data protection policies with System Manager or the ONTAP CLI. Beginning with ONTAP 9.11.1, you can use System Manager to create custom mirror and vault policies, and to display and select legacy policies. This capability is also available in ONTAP 9.8P12 and later patches of ONTAP 9.8.

Create custom protection policies on both the source and destination cluster.

System Manager

1. Click **Protection > Overview > Local Policy Settings**.
2. Under **Protection Policies**, click .
3. In the **Protection Policies** pane, click  **Add**.
4. Enter the new policy name, and select the policy scope.
5. Choose a policy type. To add a vault-only or mirror-only policy, choose **Asynchronous**, and click **Use a legacy policy type**.
6. Complete the required fields.
7. Click **Save**.
8. Repeat these steps on the other cluster.

CLI

1. Create a custom replication policy:

```
snapmirror policy create -vserver <SVM> -policy _policy_ -type  
<async-mirror|vault|mirror-vault|strict-sync-mirror|sync-mirror>  
-comment <comment> -tries <transfer_tries> -transfer-priority  
<low|normal> -is-network-compression-enabled <true|false>
```

Beginning with ONTAP 9.5, you can specify the schedule for creating a common snapshot schedule for SnapMirror synchronous relationships by using the **-common-snapshot-schedule** parameter. By default, the common snapshot schedule for SnapMirror synchronous relationships is one hour. You can specify a value from 30 minutes to two hours for the snapshot schedule for SnapMirror synchronous relationships.

The following example creates a custom replication policy for SnapMirror DR that enables network compression for data transfers:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy  
DR_compressed -type async-mirror -comment "DR with network  
compression enabled" -is-network-compression-enabled true
```

The following example creates a custom replication policy for SnapVault:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy  
my_snapvault -type vault
```

The following example creates a custom replication policy for unified replication:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy  
my_unified -type mirror-vault
```

The following example creates a custom replication policy for SnapMirror synchronous relationship in the StrictSync mode:

```
cluster_dst::> snapmirror policy create -vserver svml -policy
my_strictsync -type strict-sync-mirror -common-snapshot-schedule
my_sync_schedule
```

Learn more about `snapmirror policy create` in the [ONTAP command reference](#).

After you finish

For “vault” and “mirror-vault” policy types, you must define rules that determine which snapshots are transferred during initialization and update.

Use the `snapmirror policy show` command to verify that the SnapMirror policy was created.

Learn more about `snapmirror policy show` in the [ONTAP command reference](#).

Define a rule for an ONTAP SnapMirror policy

For custom policies with the `vault` or `mirror-vault` policy type, you must define at least one rule that determines which snapshots are transferred during initialization and update. You can also define rules for default policies with the `vault` or `mirror-vault` policy type.

About this task

Every policy with the `vault` or `mirror-vault` policy type must have a rule that specifies which snapshots to replicate. The rule `bi-monthly`, for example, indicates that only snapshots assigned the SnapMirror label `bi-monthly` should be replicated. You specify the SnapMirror label when you configure the snapshot policy on the source.

Each policy type is associated with one or more system-defined rules. These rules are automatically assigned to a policy when you specify its policy type. The table below shows the system-defined rules.

System-defined rule	Used in policy types	Result
<code>sm_created</code>	<code>async-mirror</code> , <code>mirror-vault</code> , <code>Sync</code> , <code>StrictSync</code>	A snapshot created by SnapMirror is transferred on initialization and update.
<code>all_source_snapshots</code>	<code>async-mirror</code>	New snapshots on the source are transferred on initialization and update.
<code>daily</code>	<code>vault</code> , <code>mirror-vault</code>	New snapshots on the source with the SnapMirror label <code>daily</code> are transferred on initialization and update.

weekly	vault,mirror-vault	New snapshots on the source with the SnapMirror label <code>weekly</code> are transferred on initialization and update.
monthly	mirror-vault	New snapshots on the source with the SnapMirror label <code>monthly</code> are transferred on initialization and update.
app_consistent	Sync, StrictSync	Snapshots with the SnapMirror label <code>app_consistent</code> on source are synchronously replicated to the destination. Supported beginning with ONTAP 9.7.

Except for the “`async-mirror`” policy type, you can specify additional rules as needed, for default or custom policies. For example:

- For the default `MirrorAndVault` policy, you might create a rule called `bi-monthly` to match snapshots on the source with the `bi-monthly` SnapMirror label.
- For a custom policy with the `mirror-vault` policy type, you might create a rule called `bi-weekly` to match snapshots on the source with the `bi-weekly` SnapMirror label.

Step

1. Define a rule for a policy:

```
snapmirror policy add-rule -vserver SVM -policy policy_for_rule -snapmirror
-label snapmirror-label -keep retention_count
```

The following example adds a rule with the SnapMirror label `bi-monthly` to the default `MirrorAndVault` policy:

```
cluster_dst::> snapmirror policy add-rule -vserver svml -policy
MirrorAndVault -snapmirror-label bi-monthly -keep 6
```

The following example adds a rule with the SnapMirror label `bi-weekly` to the custom `my_snapvault` policy:

```
cluster_dst::> snapmirror policy add-rule -vserver svml -policy
my_snapvault -snapmirror-label bi-weekly -keep 26
```

The following example adds a rule with the SnapMirror label `app_consistent` to the custom `Sync` policy:

```
cluster_dst::> snapmirror policy add-rule -vserver svml -policy Sync  
-snapmirror-label app_consistent -keep 1
```

Learn more about `snapmirror policy add-rule` in the [ONTAP command reference](#).

You can then replicate snapshots from the source cluster that match this SnapMirror label:

```
cluster_src::> snapshot create -vserver vs1 -volume voll -snapshot  
snapshot1 -snapmirror-label app_consistent
```

Define an ONTAP SnapMirror schedule to create a local copy on the destination

For SnapVault and unified replication relationships, you can protect against the possibility that an updated snapshot is corrupted by creating a copy of the last transferred snapshot on the destination. This "local copy" is retained regardless of the retention rules on the source, so that even if the snapshot originally transferred by SnapMirror is no longer available on the source, a copy of it will be available on the destination.

About this task

You specify the schedule for creating a local copy in the `-schedule` option of the `snapmirror policy add-rule` command.

Step

1. Define a schedule for creating a local copy on the destination:

```
snapmirror policy add-rule -vserver SVM -policy policy_for_rule -snapmirror  
-label snapmirror-label -schedule schedule
```

For an example of how to create a job schedule, see [Creating a replication job schedule](#).

The following example adds a schedule for creating a local copy to the default `MirrorAndVault` policy:

```
cluster_dst::> snapmirror policy add-rule -vserver svml -policy  
MirrorAndVault -snapmirror-label my_monthly -schedule my_monthly
```

The following example adds a schedule for creating a local copy to the custom `my_unified` policy:

```
cluster_dst::> snapmirror policy add-rule -vserver svml -policy  
my_unified -snapmirror-label my_monthly -schedule my_monthly
```

Learn more about `snapmirror policy add-rule` in the [ONTAP command reference](#).

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—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.