Replication between NetApp Element Software and ONTAP

November 2018 | 215-12645_E0
doccomments@netapp.com
Updated for ONTAP 9.5
# Contents

Deciding whether to use the Replication between NetApp Element software and ONTAP guide ................................................................. 4  
Understanding replication between Element and ONTAP ............................. 5  
Workflow for replication between Element and ONTAP ................................. 8  
Enabling SnapMirror in Element software .................................................. 10  
  Enabling SnapMirror on the Element cluster .............................................. 10  
  Enabling SnapMirror on the Element source volume ................................. 10  
  Creating a SnapMirror endpoint ................................................................. 11  
Configuring a replication relationship ......................................................... 12  
  Creating a replication job schedule ............................................................. 12  
  Customizing a replication policy ................................................................. 12  
    Creating a custom replication policy ....................................................... 13  
    Defining a rule for a policy ................................................................. 14  
  Creating a replication relationship ............................................................. 15  
    Creating a relationship from an Element source to an ONTAP destination ................................................................. 15  
    Creating a relationship from an ONTAP source to an Element destination ................................................................. 16  
  Initializing a replication relationship .......................................................... 17  
Serving data from a SnapMirror DR destination volume .............................. 19  
  Making the destination volume writeable .................................................. 19  
  Configuring the destination volume for data access .................................... 20  
  Reactivating the original source volume .................................................... 20  
Updating a replication relationship manually .............................................. 24  
Resynchronizing a replication relationship .................................................. 25  
Where to find additional information ........................................................... 26  
Copyright information ............................................................................. 27  
Trademark information ............................................................................ 28  
How to send comments about documentation and receive update notifications .............................................................................. 29  
Index ....................................................................................................... 30
Deciding whether to use the Replication between NetApp Element software and ONTAP guide

This guide describes how to ensure business continuity on an Element system by using SnapMirror to replicate Snapshot copies of an Element volume to an ONTAP destination. In the event of a disaster at the Element site, you can serve data to clients from the ONTAP system, and then reactivate the Element system when service is restored.

Starting with ONTAP 9.4, you can replicate Snapshot copies of a LUN created on an ONTAP node back to an Element system. You might have created a LUN during an outage at the Element site, or you might be using a LUN to migrate data from ONTAP to Element software.

You should use this guide if you want to work with Element to ONTAP backup in the following way:

• You want to use best practices, not explore every available option.
• You do not want to read a lot of conceptual background.
• You want to use the ONTAP command-line interface (CLI), not OnCommand System Manager or an automated scripting tool.
• You are using iSCSI to serve data to clients.

If you require additional configuration or conceptual information, you should choose among the following documentation:

• Element configuration
  NetApp Element software documentation
• SnapMirror concepts and configuration
  Data protection
• ONTAP conceptual background
  ONTAP concepts
• Command reference
  ONTAP 9 commands
• Automation of management tasks
  NetApp Documentation: OnCommand Workflow Automation (current releases)
Understanding replication between Element and ONTAP

Starting with ONTAP 9.3, you can use SnapMirror to replicate Snapshot copies of an Element volume to an ONTAP destination. In the event of a disaster at the Element site, you can serve data to clients from the ONTAP system, then reactivate the Element source volume when service is restored.

Starting with ONTAP 9.4, you can replicate Snapshot copies of a LUN created on an ONTAP node back to an Element system. You might have created a LUN during an outage at the Element site, or you might be using a LUN to migrate data from ONTAP to Element software.

Types of data protection relationship

SnapMirror offers two types of data protection relationship. For each type, SnapMirror creates a Snapshot copy of the Element source volume before initializing or updating the relationship:

- In a disaster recovery (DR) data protection relationship, the destination volume contains only the Snapshot copy created by SnapMirror, from which you can continue to serve data in the event of a catastrophe at the primary site.
- In a long-term retention data protection relationship, the destination volume contains point-in-time Snapshot copies created by Element software, as well as the Snapshot copy created by SnapMirror. You might want to retain monthly Snapshot copies created over a 20-year span, for example.

Default policies

The first time you invoke SnapMirror, it performs a baseline transfer from the source volume to the destination volume. The SnapMirror policy defines the contents of the baseline and any updates.

You can use a default or custom policy when you create a data protection relationship. The policy type determines which Snapshot copies to include and how many copies to retain.

The table below shows the default policies. Use the MirrorLatest policy to create a traditional DR relationship. Use the MirrorAndVault or Unified7year policy to create a unified replication relationship, in which DR and long-term retention are configured on the same destination volume.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Policy Type</th>
<th>Update behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>MirrorLatest</td>
<td>async-mirror</td>
<td>Transfer the Snapshot copy created by SnapMirror.</td>
</tr>
<tr>
<td>MirrorAndVault</td>
<td>mirror-vault</td>
<td>Transfer the Snapshot copy created by SnapMirror and any less recent Snapshot copies made since the last update, provided they have SnapMirror labels “daily” or “weekly”.</td>
</tr>
<tr>
<td>Unified7year</td>
<td>mirror-vault</td>
<td>Transfer the Snapshot copy created by SnapMirror and any less recent Snapshot copies made since the last update, provided they have SnapMirror labels “daily”, “weekly”, or “monthly”.</td>
</tr>
</tbody>
</table>

Note: For complete background information on SnapMirror policies, including guidance on which policy to use, see the ONTAP Data Protection Power Guide.

Understanding SnapMirror labels

Every policy with the “mirror-vault” policy type must have a rule that specifies which Snapshot copies to replicate. The rule “daily”, for example, indicates that only Snapshot copies assigned the
SnapMirror label “daily” should be replicated. You assign the SnapMirror label when you configure Element Snapshot copies.

**Replication from an Element source cluster to an ONTAP destination cluster**

You can use SnapMirror to replicate Snapshot copies of an Element volume to an ONTAP destination system. In the event of a disaster at the Element site, you can serve data to clients from the ONTAP system, then reactivate the Element source volume when service is restored.

An Element volume is roughly equivalent to an ONTAP LUN. SnapMirror creates a LUN with the name of the Element volume when a data protection relationship between Element software and ONTAP is initialized. SnapMirror replicates data to an existing LUN if the LUN meets the requirements for Element to ONTAP replication.

Replication rules are as follows:

- An ONTAP volume can contain data from one Element volume only.
- You cannot replicate data from an ONTAP volume to multiple Element volumes.

**Replication from an ONTAP source cluster to an Element destination cluster**

Starting with ONTAP 9.4, you can replicate Snapshot copies of a LUN created on an ONTAP system back to an Element volume:

- If a SnapMirror relationship already exists between an Element source and an ONTAP destination, a LUN created while you are serving data from the destination is automatically replicated when the source is reactivated.
- Otherwise, you must create and initialize a SnapMirror relationship between the ONTAP source cluster and the Element destination cluster.

Replication rules are as follows:

- The replication relationship must have a policy of type “async-mirror”.
  Policies of type “mirror-vault” are not supported.
- Only iSCSI LUNs are supported.
- You cannot replicate more than one LUN from an ONTAP volume to an Element volume.
- You cannot replicate a LUN from an ONTAP volume to multiple Element volumes.

**Prerequisites**

You must have completed the following tasks before configuring a data protection relationship between Element and ONTAP:

- The Element cluster must be running NetApp Element software version 10.1 or later.
- The ONTAP cluster must be running ONTAP 9.3 or later.
- SnapMirror must have been licensed on the ONTAP cluster.
- You must have configured volumes on the Element and ONTAP clusters that are large enough to handle anticipated data transfers.
- If you are using the “mirror-vault” policy type, a SnapMirror label must have been configured for the Element Snapshot copies to be replicated.

**Note:** You can perform this task in the Element software web UI only. For more information, see the *NetApp Element Software User Guide*.

*NetApp Element software documentation*

- You must have ensured that port 5010 is available.
- If you foresee that you might need to move a destination volume, you must have ensured that full-mesh connectivity exists between the source and destination. Every node on the Element source cluster must be able to communicate with every node on the ONTAP destination cluster.
## Support details

The following table shows support details for Element to ONTAP backup.

<table>
<thead>
<tr>
<th>Resource or feature</th>
<th>Support details</th>
</tr>
</thead>
</table>
| **SnapMirror**      | • The SnapMirror restore feature is not supported.  
                     • The MirrorAllSnapshots and XDPDefault policies are not supported.  
                     • The “vault” policy type is not supported.  
                     • The system-defined rule “all_source_snapshots” is not supported.  
                     • The “mirror-vault” policy type is supported only for replication from Element software to ONTAP. Use “async-mirror” for replication from ONTAP to Element software.  
                     • The `-schedule` and `-prefix` options for snapmirror policy add-rule are not supported.  
                     • The `-preserve` and `-quick-resync` options for snapmirror resync are not supported.  
                     • Storage efficiency is not preserved.  
                     • Fan-out and cascade data protection deployments are not supported. |
| **ONTAP**           | • Cloud Volumes ONTAP is not supported.  
                     • ONTAP Select is not supported. |
| **Element**         | • Volume size limit is 8 TiB.  
                     • Volume block size must be 512 bytes. A 4K byte block size is not supported.  
                     • Volume size must be a multiple of 1 MiB.  
                     • Volume attributes are not preserved.  
                     • Maximum number of Snapshot copies to be replicated is 30. |
| **Network**         | • A single TCP connection is allowed per transfer.  
                     • The Element node must be specified as an IP address. DNS hostname lookup is not supported.  
                     • IPspaces are not supported. |
| **SnapLock**        | SnapLock volumes are not supported. |
| **FlexGroup**       | FlexGroup volumes are not supported. |
| **SVM DR**          | ONTAP volumes in an SVM DR configuration are not supported. |
| **MetroCluster**    | ONTAP volumes in a MetroCluster configuration are not supported. |
| **NetApp Cloud Backup** | Element software-to-ONTAP-to-Cloud Backup cascade relationships are not supported. |

**Related information**

*Data protection*
Workflow for replication between Element and ONTAP

Whether you are replicating data from Element to ONTAP or from ONTAP to Element, you need to configure a job schedule, specify a policy, and create and initialize the relationship. You can use a default or custom policy.

The workflow assumes that you have completed the prerequisite tasks listed in Prerequisites. For complete background information on SnapMirror policies, including guidance on which policy to use, see the ONTAP Data Protection Power Guide.
Related information

Data protection
Enabling SnapMirror in Element software

You must perform several tasks in the Element software web UI before you can create replication relationships.

Steps
1. Enabling SnapMirror on the Element cluster on page 10
2. Enabling SnapMirror on the Element source volume on page 10
3. Creating a SnapMirror endpoint on page 11

Enabling SnapMirror on the Element cluster

You must enable SnapMirror on the Element cluster before you can create a replication relationship. You can perform this task in the Element software web UI only.

Before you begin

- The Element cluster must be running NetApp Element software version 10.1 or later.
- SnapMirror can only be enabled for Element clusters used with NetApp ONTAP volumes.

About this task

The Element system comes with SnapMirror disabled by default. SnapMirror is not automatically enabled as part of a new installation or upgrade.

Note: Once enabled, SnapMirror cannot be disabled. You can only disable the SnapMirror feature and restore the default settings by returning the cluster to the factory image.

Steps
1. Click Clusters > Settings.
2. Find the cluster-specific settings for SnapMirror.
3. Click Enable SnapMirror.

Enabling SnapMirror on the Element source volume

You must enable SnapMirror on the Element source volume before you can create a replication relationship. You can perform this task in the Element software web UI only.

Before you begin

- You must have enabled SnapMirror on the Element cluster.
- The volume block size must be 512 bytes.
- The volume must not be participating in Element remote replication.
- The volume access type must not be “Replication Target”.

About this task

The procedure below assumes the volume already exists. You can also enable SnapMirror when you create or clone a volume.
Steps
1. Click Management > Volumes.
2. Click the button for the volume.
3. In the drop-down menu, select Edit.
4. In the Edit Volume dialog, select Enable SnapMirror.
5. Click Save Changes.

Creating a SnapMirror endpoint

You must create a SnapMirror endpoint before you can create a replication relationship. You can perform this task in the Element software web UI only.

Before you begin

You must have enabled SnapMirror on the Element cluster.

Steps
1. Click Data Protection > SnapMirror Endpoints.
2. Click Create Endpoint.
3. In the Create a New Endpoint dialog, enter the ONTAP cluster management IP address.
4. Enter the user ID and password of the ONTAP cluster administrator.
5. Click Create Endpoint.
Configuring a replication relationship

Whether you are replicating data from Element to ONTAP or from ONTAP to Element, you need to configure a job schedule, specify a policy, and create and initialize the relationship. You can use a default or custom policy.

Steps
1. Creating a replication job schedule on page 12
2. Customizing a replication policy on page 12
3. Creating a replication relationship on page 15
4. Initializing a replication relationship on page 17

Creating a replication job schedule

You can use the `job schedule cron create` command to create a replication job schedule. The job schedule determines when SnapMirror automatically updates the data protection relationship to which the schedule is assigned.

About this task
You assign a job schedule when you create a data protection relationship. If you do not assign a job schedule, you must update the relationship manually.

Step
1. Create a job schedule:

   `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

   For `-month`, `-dayofweek`, and `-hour`, you can specify `all` to run the job every month, day of the week, and hour, respectively.

Example

The following example creates a job schedule named `my_weekly` that runs on Saturdays at 3:00 a.m.:

```
cluster_dst:> job schedule cron create -name my_weekly -dayofweek "Saturday" -hour 3 -minute 0
```

Customizing a replication policy

You can use a default or custom policy when you create a replication relationship. For a custom unified replication policy, you must define one or more rules that determine which Snapshot copies are transferred during initialization and update.

Related tasks
- Creating a custom replication policy on page 13
- Defining a rule for a policy on page 14
Creating a custom 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 Snapshot copies.

About this task

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

<table>
<thead>
<tr>
<th>Policy type</th>
<th>Relationship type</th>
</tr>
</thead>
<tbody>
<tr>
<td>async-mirror</td>
<td>SnapMirror DR</td>
</tr>
<tr>
<td>mirror-vault</td>
<td>Unified replication</td>
</tr>
</tbody>
</table>

Step

1. Create a custom replication policy:

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

For complete command syntax, see the man page.

Example

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
```

Example

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

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

After you finish

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

Use the `snapmirror policy show` command to verify that the SnapMirror policy was created. For complete command syntax, see the man page.
Defining a rule for a policy

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

About this task

Every policy with the “mirror-vault” policy type must have a rule that specifies which Snapshot copies to replicate. The rule “bi-monthly”, for example, indicates that only Snapshot copies assigned the SnapMirror label “bi-monthly” should be replicated. You assign the SnapMirror label when you configure Element Snapshot copies.

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.

<table>
<thead>
<tr>
<th>System-defined rule</th>
<th>Used in policy types</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>sm_created</td>
<td>async-mirror, mirror-vault</td>
<td>A Snapshot copy created by SnapMirror is transferred on initialization and update.</td>
</tr>
<tr>
<td>daily</td>
<td>mirror-vault</td>
<td>New Snapshot copies on the source with the SnapMirror label “daily” are transferred on initialization and update.</td>
</tr>
<tr>
<td>weekly</td>
<td>mirror-vault</td>
<td>New Snapshot copies on the source with the SnapMirror label “weekly” are transferred on initialization and update.</td>
</tr>
<tr>
<td>monthly</td>
<td>mirror-vault</td>
<td>New Snapshot copies on the source with the SnapMirror label “monthly” are transferred on initialization and update.</td>
</tr>
</tbody>
</table>

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 Snapshot copies 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 Snapshot copies 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

   For complete command syntax, see the man page.

Example

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

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy MirrorAndVault -snapmirror-label bi-monthly -keep 6
```
Example

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

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy my_snapvault -snapmirror-label bi-weekly -keep 26
```

Creating a replication relationship

The relationship between the source volume in primary storage and the destination volume in secondary storage is called a **data protection relationship**. You can use the `snapmirror create` command to create a data protection relationship from an Element source to an ONTAP destination, or from an ONTAP source to an Element destination.

Creating a relationship from an Element source to an ONTAP destination

You can use SnapMirror to replicate Snapshot copies of an Element volume to an ONTAP destination system. In the event of a disaster at the Element site, you can serve data to clients from the ONTAP system, then reactivate the Element source volume when service is restored.

Before you begin

- The Element node containing the volume to be replicated must have been made accessible to ONTAP.
- The Element volume must have been enabled for SnapMirror replication.
- If you are using the “mirror-vault” policy type, a SnapMirror label must have been configured for the Element Snapshot copies to be replicated.

**Note:** You can perform this task in the Element software web UI only. For more information, see the *NetApp Element Software User Guide*.

Element documentation

About this task

You must specify the Element source path in the form `hostip:/lun/name`, where “lun” is the actual string “lun” and `name` is the name of the Element volume.

An Element volume is roughly equivalent to an ONTAP LUN. SnapMirror creates a LUN with the name of the Element volume when a data protection relationship between Element software and ONTAP is initialized. SnapMirror replicates data to an existing LUN if the LUN meets the requirements for replicating from Element software to ONTAP.

Replication rules are as follows:

- An ONTAP volume can contain data from one Element volume only.
- You cannot replicate data from an ONTAP volume to multiple Element volumes.

In ONTAP 9.3 and earlier, a destination volume can contain up to 251 Snapshot copies. In ONTAP 9.4 and later, a destination volume can contain up to 1019 Snapshot copies.

**Step**

1. Create a replication relationship from an Element source to an ONTAP destination:

```
  snapmirror create -source-path hostip:/lun/name -destination-path SVM:volume|cluster://SVM/volume -type XDP -schedule schedule -policy policy
```
For complete command syntax, see the man page.

**Example**
The following example creates a SnapMirror DR relationship using the default *MirrorLatest* policy:

```
cluster_dst::> snapmirror create -source-path 10.0.0.11:/lun/0005 -destination-path svm_backup:volA_dst -type XDP -schedule my_daily -policy MirrorLatest
```

**Example**
The following example creates a unified replication relationship using the default *MirrorAndVault* policy:

```
cluster_dst::> snapmirror create -source-path 10.0.0.11:/lun/0005 -destination-path svm_backup:volA_dst -type XDP -schedule my_daily -policy MirrorAndVault
```

**Example**
The following example creates a unified replication relationship using the *Unified7year* policy:

```
cluster_dst::> snapmirror create -source-path 10.0.0.11:/lun/0005 -destination-path svm_backup:volA_dst -type XDP -schedule my_daily -policy Unified7year
```

**Example**
The following example creates a unified replication relationship using the custom *my_unified* policy:

```
cluster_dst::> snapmirror create -source-path 10.0.0.11:/lun/0005 -destination-path svm_backup:volA_dst -type XDP -schedule my_daily -policy my_unified
```

**After you finish**
Use the `snapmirror show` command to verify that the SnapMirror relationship was created. For complete command syntax, see the man page.

### Creating a relationship from an ONTAP source to an Element destination

Starting with ONTAP 9.4, you can use SnapMirror to replicate Snapshot copies of a LUN created on an ONTAP source back to an Element destination. You might be using the LUN to migrate data from ONTAP to Element software.

**Before you begin**
- The Element destination node must have been made accessible to ONTAP.
- The Element volume must have been enabled for SnapMirror replication.

**About this task**
You must specify the Element destination path in the form `hostip:/lun/name`, where “lun” is the actual string “lun” and *name* is the name of the Element volume.

Replication rules are as follows:
• The replication relationship must have a policy of type “async-mirror”.
  You can use a default or custom policy.
• Only iSCSI LUNs are supported.
• You cannot replicate more than one LUN from an ONTAP volume to an Element volume.
• You cannot replicate a LUN from an ONTAP volume to multiple Element volumes.

Step
1. Create a replication relationship from an ONTAP source to an Element destination:

```
snapmirror create -source-path SVM:volume|cluster://SVM/volume -destination-path hostip:/lun/name -type XDP -schedule schedule -policy policy
```

For complete command syntax, see the man page.

Example
The following example creates a SnapMirror DR relationship using the default MirrorLatest policy:

```
cluster_dst::> snapmirror create -source-path svm_1:volA_dst -destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily -policy MirrorLatest
```

Example
The following example creates a SnapMirror DR relationship using the custom my_mirror policy:

```
cluster_dst::> snapmirror create -source-path svm_1:volA_dst -destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily -policy my_mirror
```

After you finish
Use the `snapmirror show` command to verify that the SnapMirror relationship was created. For complete command syntax, see the man page.

Initializing a replication relationship
For all relationship types, initialization performs a baseline transfer: it makes a Snapshot copy of the source volume, then transfers that copy and all the data blocks it references to the destination volume.

Before you begin
• The Element node containing the volume to be replicated must have been made accessible to ONTAP.
• The Element volume must have been enabled for SnapMirror replication.
• If you are using the “mirror-vault” policy type, a SnapMirror label must have been configured for the Element Snapshot copies to be replicated.

About this task
You must specify the Element source path in the form `hostip:/lun/name`, where “lun” is the actual string “lun” and `name` is the name of the Element volume.

Initialization can be time-consuming. You might want to run the baseline transfer in off-peak hours.
**Important:** If initialization of a relationship from an ONTAP source to an Element destination fails for any reason, it will continue to fail even after you have corrected the problem (an invalid LUN name, for example). The workaround is as follows:

1. Delete the relationship.
2. Delete the Element destination volume.
3. Create a new Element destination volume.
4. Create and initialize a new relationship from the ONTAP source to the Element destination volume.

**Step**

1. Initialize a replication relationship:

   ```
   snapmirror initialize -source-path hostip:/lun/name -destination-path SVM:volume|cluster://SVM/volume
   ```

   For complete command syntax, see the man page.

**Example**

The following example initializes the relationship between the source volume 0005 at IP address 10.0.0.11 and the destination volume volA_dst on svm_backup:

```bash
cluster_dst::> snapmirror initialize -source-path 10.0.0.11:/lun/0005 -destination-path svm_backup:volA_dst
```
Serving data from a SnapMirror DR destination volume

When disaster disables the primary site for a SnapMirror DR relationship, you can serve data from the destination volume with minimal disruption. You can reactivate the source volume when service is restored at the primary site.

Steps
1. Making the destination volume writeable on page 19
2. Configuring the destination volume for data access on page 20
3. Reactivating the original source volume on page 20

Making the destination volume writeable

You need to make the destination volume writeable before you can serve data from the volume to clients. You can use the `snapmirror quiesce` command to stop scheduled transfers to the destination, the `snapmirror abort` command to stop ongoing transfers, and the `snapmirror break` command to make the destination writeable.

About this task

You must specify the Element source path in the form `hostip:/lun/name`, where “lun” is the actual string “lun” and `name` is the name of the Element volume.

Steps
1. Stop scheduled transfers to the destination:
   `snapmirror quiesce -source-path hostip:/lun/name -destination-path SVM:volume|cluster://SVM/volume`

   For complete command syntax, see the man page.

   Example
   The following example stops scheduled transfers between the source volume 0005 at IP address 10.0.0.11 and the destination volume `volA_dst` on `svm_backup`:

   ```
   cluster_dst:~> snapmirror quiesce -source-path 10.0.0.11:/lun/0005 -destination-path svm_backup:volA_dst
   ```

2. Stop ongoing transfers to the destination:
   `snapmirror abort -source-path hostip:/lun/name -destination-path SVM:volume|cluster://SVM/volume`

   For complete command syntax, see the man page.

   Example
   The following example stops ongoing transfers between the source volume 0005 at IP address 10.0.0.11 and the destination volume `volA_dst` on `svm_backup`:

   ```
   cluster_dst:~> snapmirror abort -source-path 10.0.0.11:/lun/0005 -destination-path svm_backup:volA_dst
   ```
3. Break the SnapMirror DR relationship:

   `snapmirror break -source-path hostip:/lun/name -destination-path
   SVM:volume|cluster://SVM/volume`

   For complete command syntax, see the man page.

   **Example**

   The following example breaks the relationship between the source volume **0005** at IP address
   10.0.0.11 and the destination volume **volA_dst** on **svm_backup** and the destination volume
   **volA_dst** on **svm_backup**:

   ```bash
   cluster_dst::> snapmirror break -source-path 10.0.0.11:/lun/0005 -
   destination-path svm_backup:volA_dst
   ```

**Configuring the destination volume for data access**

After making the destination volume writeable, you must configure the volume for data access. SAN hosts can access the data from the destination volume until the source volume is reactivated.

1. Map the Element LUN to the appropriate initiator group.
2. Create iSCSI sessions from the SAN host initiators to the SAN LIFs.
3. On the SAN client, perform a storage re-scan to detect the connected LUN.

**Related information**

*SAN administration*

**Reactivating the original source volume**

You can reestablish the original data protection relationship between the source and destination volumes when you no longer need to serve data from the destination.

**About this task**

The procedure below assumes that the baseline in the original source volume is intact. If the baseline is not intact, you must create and initialize the relationship between the volume you are serving data from and the original source volume before performing the procedure.

You must specify the Element source path in the form `hostip:/lun/name`, where “lun” is the actual string “lun” and `name` is the name of the Element volume.

Starting with ONTAP 9.4, Snapshot copies of a LUN created while you are serving data from the ONTAP destination are automatically replicated when the Element source is reactivated.

Replication rules are as follows:

- Only iSCSI LUNs are supported.
- You cannot replicate more than one LUN from an ONTAP volume to an Element volume.
- You cannot replicate a LUN from an ONTAP volume to multiple Element volumes.

**Steps**

1. Delete the original data protection relationship:

   `snapmirror delete -source-path SVM:volume|cluster://SVM/volume -
   destination-path hostip:/lun/name -policy policy`
For complete command syntax, see the man page.

**Example**

The following example deletes the relationship between the original source volume, `0005` at IP address `10.0.0.11`, and the volume you are serving data from, `volA_dst` on `svm_backup`:

```bash
cluster_src::> snapmirror delete -source-path 10.0.0.11:/lun/0005 -policy MirrorLatest -destination-path svm_backup:volA_dst
```

2. Reverse the original data protection relationship:

```bash
snapmirror resync -source-path SVM:volume|cluster://SVM/volume -destination-path hostip:/lun/name -policy policy
```

For complete command syntax, see the man page.

Although resync does not require a baseline transfer, it can be time-consuming. You might want to run the resync in off-peak hours.

**Example**

The following example reverses the relationship between the original source volume, `0005` at IP address `10.0.0.11`, and the volume you are serving data from, `volA_dst` on `svm_backup`:

```bash
cluster_src::> snapmirror resync -source-path svm_backup:volA_dst -destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
```

3. Update the reversed relationship:

```bash
snapmirror update -source-path SVM:volume|cluster://SVM/volume -destination-path hostip:/lun/name
```

For complete command syntax, see the man page.

**Note:** The command fails if a common Snapshot copy does not exist on the source and destination. Use `snapmirror initialize` to re-initialize the relationship.

**Example**

The following example updates the relationship between the volume you are serving data from, `volA_dst` on `svm_backup`, and the original source volume, `0005` at IP address `10.0.0.11`:

```bash
cluster_src::> snapmirror update -source-path svm_backup:volA_dst -destination-path 10.0.0.11:/lun/0005
```

4. Stop scheduled transfers for the reversed relationship:

```bash
snapmirror quiesce -source-path SVM:volume|cluster://SVM/volume -destination-path hostip:/lun/name
```

For complete command syntax, see the man page.

**Example**

The following example stops scheduled transfers between the volume you are serving data from, `volA_dst` on `svm_backup`, and the original source volume, `0005` at IP address `10.0.0.11`:

```bash
cluster_src::> snapmirror quiesce -source-path svm_backup:volA_dst -destination-path 10.0.0.11:/lun/0005
```

5. Stop ongoing transfers for the reversed relationship:
snapmirror abort -source-path SVM:volume|cluster://SVM/volume -destination-path hostip:/lun/name

For complete command syntax, see the man page.

Example

The following example stops ongoing transfers between the volume you are serving data from, volA_dst on svm_backup, and the original source volume, 0005 at IP address 10.0.0.11:

```
cluster_src::> snapmirror abort -source-path svm_backup:volA_dst -destination-path 10.0.0.11:/lun/0005
```

6. Break the reversed relationship:

snapmirror break -source-path SVM:volume|cluster://SVM/volume -destination-path hostip:/lun/name

For complete command syntax, see the man page.

Example

The following example breaks the relationship between the volume you are serving data from, volA_dst on svm_backup, and the original source volume, 0005 at IP address 10.0.0.11:

```
cluster_src::> snapmirror break -source-path svm_backup:volA_dst -destination-path 10.0.0.11:/lun/0005
```

7. Delete the reversed data protection relationship:

snapmirror delete -source-path SVM:volume|cluster://SVM/volume -destination-path hostip:/lun/name -policy policy

For complete command syntax, see the man page.

Example

The following example deletes the reversed relationship between the original source volume, 0005 at IP address 10.0.0.11, and the volume you are serving data from, volA_dst on svm_backup:

```
cluster_src::> snapmirror delete -source-path svm_backup:volA_dst -destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
```

8. Reestablish the original data protection relationship:

snapmirror resync -source-path hostip:/lun/name -destination-path SVM:volume|cluster://SVM/volume

For complete command syntax, see the man page.

Example

The following example reestablishes the relationship between the original source volume, 0005 at IP address 10.0.0.11, and the original destination volume, volA_dst on svm_backup:

```
cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005 -destination-path svm_backup:volA_dst
```
After you finish

Use the `snapmirror show` command to verify that the SnapMirror relationship was created. For complete command syntax, see the man page.
**Updating a replication relationship manually**

You might need to update a replication relationship manually when you no longer need to serve data from a destination volume, or after an update fails because of a network error.

**About this task**

You must specify the Element source path in the form `hostip:/lun/name`, where “lun” is the actual string “lun” and `name` is the name of the Element volume.

**Step**

1. Update a replication relationship manually:

   ```
   snapmirror update -source-path hostip:/lun/name -destination-path SVM:volume|cluster://SVM/volume
   ```

   For complete command syntax, see the man page.

   **Note:** The command fails if a common Snapshot copy does not exist on the source and destination. Use `snapmirror initialize` to re-initialize the relationship.

**Example**

The following example updates the relationship between the source volume `0005` at IP address 10.0.0.11 and the destination volume `volA_dst` on `svm_backup`:

```
cluster_src::> snapmirror update -source-path 10.0.0.11:/lun/0005 -destination-path svm_backup:volA_dst
```
Resynchronizing a replication relationship

You need to resynchronize a replication relationship after you make a destination volume writeable, after an update fails because a common Snapshot copy does not exist on the source and destination volumes, or if you want to change the replication policy for the relationship.

About this task
Although resync does not require a baseline transfer, it can be time-consuming. You might want to run the resync in off-peak hours.

You must specify the Element source path in the form `hostip:/lun/name`, where “lun” is the actual string “lun” and `name` is the name of the Element volume.

Step

1. Resync the source and destination volumes:

   ```
   snapmirror resync -source-path hostip:/lun/name -destination-path SVM:volume|cluster://SVM/volume -type XDP -schedule schedule -policy policy
   ```

   For complete command syntax, see the man page.

Example
The following example resyncs the relationship between the source volume `0005` at IP address 10.0.0.11 and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005 -policy MirrorLatest -destination-path svm_backup:volA_dst
```
Where to find additional information

You can learn more about tasks related to SnapMirror replication in NetApp’s extensive documentation library.

- **SAN administration**
  Describes how to configure and manage the iSCSI, FCoE, and FC protocols, including configuration of LUNs, igroups, and targets.

- **Cluster management using System Manager**
  Describes how to configure, manage, and monitor storage objects and storage systems in System Manager.
Copyright information

Copyright © 2018 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.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, 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).
Trademark information

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

doccomments@netapp.com

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

• NetApp, Inc., 1395 Crossman Ave., Sunnyvale, CA 94089 U.S.
• Telephone: +1 (408) 822-6000
• Fax: +1 (408) 822-4501
• Support telephone: +1 (888) 463-8277
Index

B
baseline transfer
description of 17

C
comments
how to send feedback about documentation 29

D
Data Backup between NetApp Element software and ONTAP Guide
deciding whether to use 4
data protection relationships
creating between source and destination volumes 15, 16
Element Snapshot copies replicated to ONTAP volume if disaster occurs 5
reestablishing original relationships between source and destination 20
destination volumes configuring data access to 20
making writeable before serving data 19
reestablishing original data protection relationship to source volume 20
resynchronizing relationships after destination volume made writeable 25
documentation
how to receive automatic notification of changes to 29
how to send feedback about 29
DR relationships workflow illustrated 8

E
Element cluster enabling SnapMirror 10
Element clusters
SnapMirror endpoint 11
Element Snapshot copies replicated to ONTAP destination volume if disaster occurs 5
Element volume enabling SnapMirror 10

F
feedback
how to send comments about documentation 29

I
information
how to send feedback about improving documentation 29

J
job schedules
creating for SnapMirror replication 12

N
NAS clients
accessing data from destination volumes 20

R
replication policies
creating custom for SnapMirror 13
defining a rule for transfer of vault or mirror-vault types 14
replication relationships initializing to transfer Snapshot copy from source to destination 17
resynchronizing after making destination volume writeable 25
updating manually 24

S
SAN hosts
accessing data from destination volumes 20
SnapMirror DR relationships
creating data protection relationships between source and destination volumes 15, 16
SnapMirror replication
creating job schedules 12
Snapshot copies
creating custom replication policies for SnapMirror 13
defining a rule for transfer of vault or mirror-vault policy types 14
source volumes
reestablishing original data protection relationship to destination volume 20
suggestions
how to send feedback about documentation 29

T
Twitter
how to receive automatic notification of documentation changes 29

U
unified replication relationships
creating data protection relationships between source and destination volumes 15, 16
workflow illustrated 8
update failures can occur when source volume is moved 24
common Snapshot copy missing between source and destination volumes 25