Replication between NetApp Element software and ONTAP

ONTAP 9

NetApp
November 16, 2022

Table of Contents

Replication between NetApp Element software and ONTAP

Replication between NetApp Element software and ONTAP overview

You can 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.

Beginning 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 work with Element to ONTAP backup if the following apply:

- You want to use best practices, not explore every available option.
- You want to use the ONTAP command-line interface (CLI), not System Manager or an automated scripting tool.
- You are using iSCSI to serve data to clients.

If you require additional configuration or conceptual information, see the following documentation:

- Element configuration

  NetApp Element software documentation

- SnapMirror concepts and configuration

  Data protection overview

About replication between Element and ONTAP

Beginning 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.

Beginning 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.

Policy	Policy Type	Update behavior
MirrorLatest	async-mirror	Transfer the Snapshot copy created by SnapMirror.
MirrorAndVault	mirror-vault	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”.
Unified7year	mirror-vault	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”.

For complete background information on SnapMirror policies, including guidance on which policy to use, see Data Protection.

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

Beginning 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.

  You can perform this task in the Element software web UI only. For more information, see the 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.

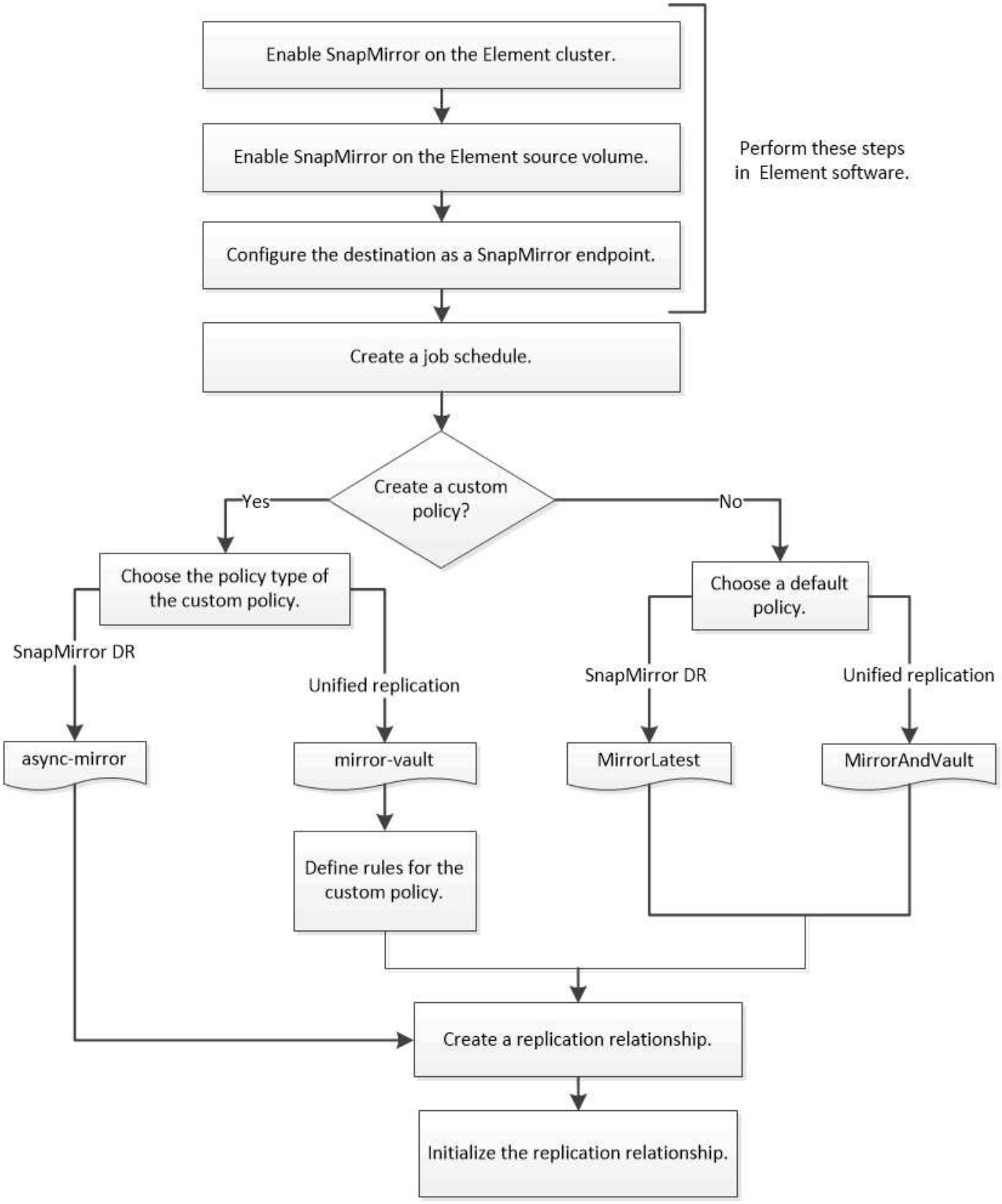
Resource or feature	Support details
SnapMirror	• The SnapMirror restore feature is not supported. • The `MirrorAllSnapshots` and `XDPDefault` policies are not supported. • The “vault” policy type is not supported. • The system-defined rule “all_source_snapshots” is not supported. • The “mirror-vault” 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	• ONTAP Select is supported beginning with ONTAP 9.4 and Element 10.3. • Cloud Volumes ONTAP is supported beginning with ONTAP 9.5 and Element 11.0.
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.

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 Data protection.



Enable SnapMirror in Element software

Enable 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.

> 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**.

Enable 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**.

Create 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**.

Configure a replication relationship

Create a replication job schedule

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.

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.

   Beginning with ONTAP 9.10.1, you can include the Vserver for your job schedule:

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

   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
```

Customize a replication policy

Create a custom 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.

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.

Policy type	Relationship type
async-mirror	SnapMirror DR
mirror-vault	Unified replication

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.

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

Define 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.

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

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.

   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
   ```

   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 svm1 -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 svm1 -policy Sync
   -snapmirror-label app_consistent -keep 1
   ```

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

   ```
   cluster_src::> snapshot create -vserver vs1 -volume vol1 -snapshot
   snapshot1 -snapmirror-label app_consistent
   ```

Create a replication relationship

Create a relationship from an Element source to an ONTAP destination

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.

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.

> ⓘ You can perform this task in the Element software web UI only. For more information, see the 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. From the destination cluster, 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.

   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
   ```

   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
```

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
```

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.

Create a relationship from an ONTAP source to an Element destination

Beginning 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.

   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
   ```

   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.

Initialize 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.

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.

   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`:

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

Serve data from a SnapMirror DR destination volume

Make the destination volume writeable

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.

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.

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.

   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.

   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`:

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

Configure 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.

Reactivate 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.

Beginning 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.

   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`:

   ```
   cluster_dst::> 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:

   `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.

   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`:

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

3. Update the reversed relationship:

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

   For complete command syntax, see the man page.

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

   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:

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

4. Stop scheduled transfers for the reversed relationship:

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

   For complete command syntax, see the man page.

   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:

   ```
   cluster_dst::> 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.

   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_dst::> 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.

   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_dst::> 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.

   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.

   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.

Update a replication relationship manually

You might need to update a replication relationship manually if 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.

Steps

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.

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

   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
   ```

Resynchronize 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.

   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
```

Copyright information

Trademark information