Consistency Groups management

ONTAP 9

NetApp
August 11, 2022

This PDF was generated from https://docs.netapp.com/us-en/ontap/consistency-groups/index.html on August 11, 2022. Always check docs.netapp.com for the latest.

Table of Contents

Consistency Groups management

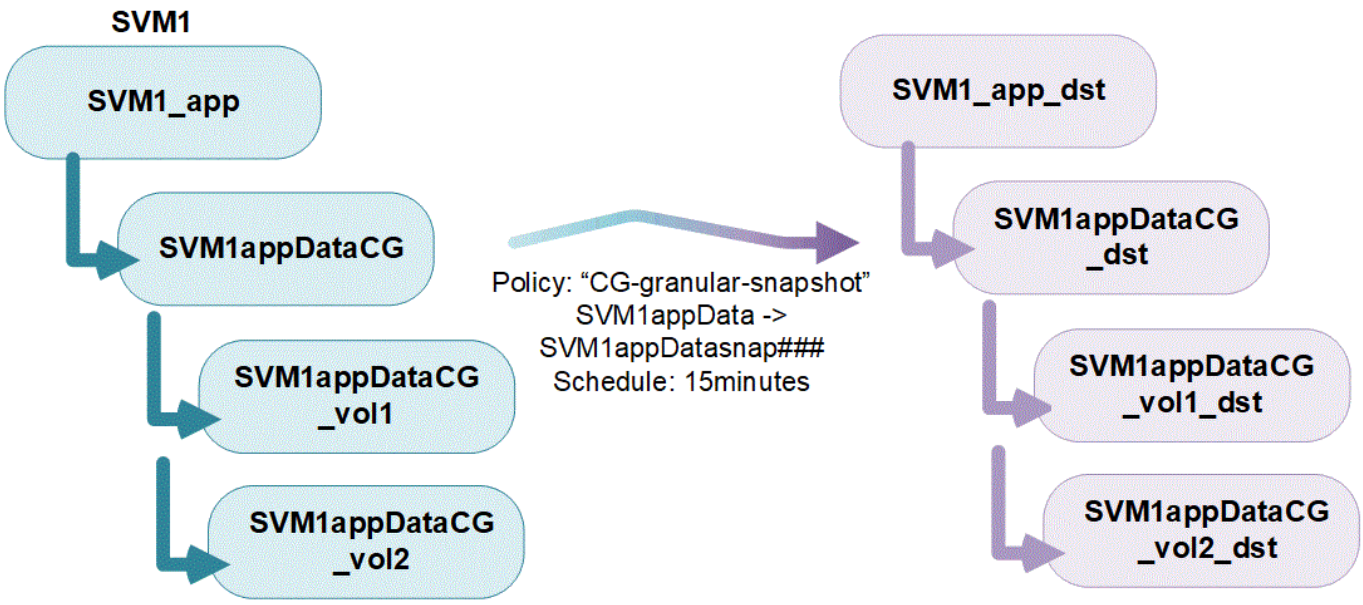
Consistency groups overview

A consistency group is a collection of volumes that provides a write-order consistency guarantee for an application workload spanning multiple volumes.

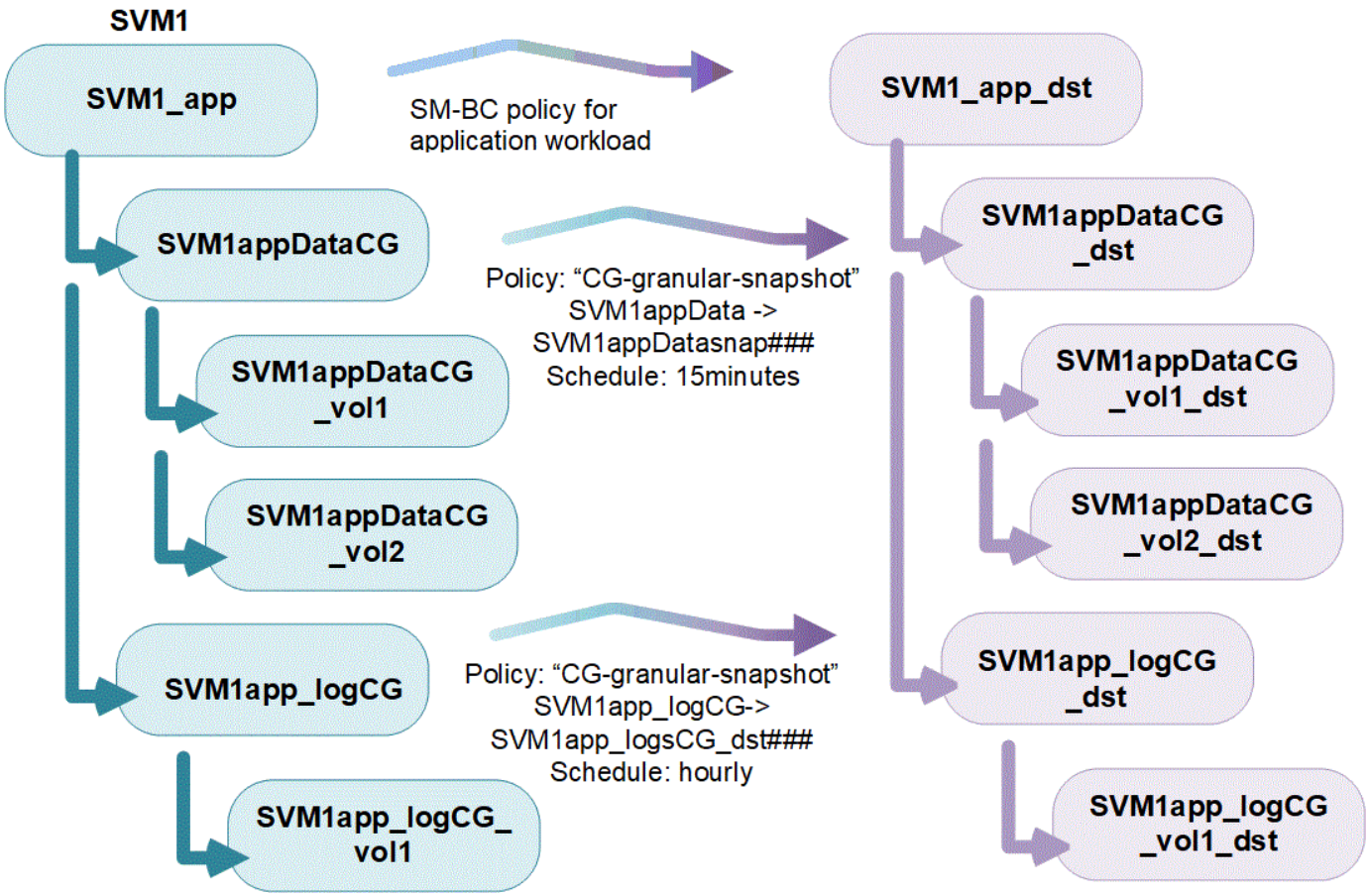
Consistency groups facilitate application workload management, providing easy management of local and remote protection policies and providing simultaneous crash-consistent or application-consistent Snapshot copies of a collection of volumes at a point in time. Snapshots in consistency groups enable an entire application workload to be restored.

Consistency groups support any FlexVol volume regardless of protocol (NAS, SAN, or NVMe) and can be managed through the ONTAP REST APIs or in System Manager under the **Storage > Consistency Groups** menu item.

Consistency groups can exist on their own or in a hierarchical relationship. An individual consistency group is a collection of volumes. Volumes can have their own volume-granular snapshot policy. In addition, the consistency group the volume is associated with can have its own snapshot policy. The consistency group can only have one SM-BC relationship and shared SM-BC policy, which can be used to recover the entire consistency group.



Larger application workloads might require multiple consistency groups. In these situations, multiple consistency groups can be placed together in a hierarchical relationship. In this configuration, single consistency groups become the child components of a parent consistency group. The parent consistency group can include up to five child consistency groups. Like in individual consistency groups, a remote SM-BC protection policy can be applied to the entire configuration of consistency groups (parent and children) to recover the application workload.



Protection

Consistency groups offer remote protection through SnapMirror Business Continuity (SM-BC) and local protection through Snapshot policies. In order to utilize remote protection, you must meet the requirements for SnapMirror Business Continuity deployments. By default, consistency groups do not have a protection policy set and will not protect your data unless a policy is selected. See “Protect a consistency group” for more information.

SM-BC relationships cannot be established on volumes mounted for NAS access.

Beginning in ONTAP 9.11.1, there is additional support for consistency groups with two-phase consistency group snapshot creation.

Consistency groups in MetroCluster configurations

Beginning with ONTAP 9.11.1, you can provision consistency groups with new volumes on a cluster within a MetroCluster configuration. These volumes are provisioned on mirrored aggregates.

After they are provisioned, you can move volumes associated with consistency groups between mirrored and unmirrored aggregates. Therefore, they can be located on mirrored aggregates, unmirrored aggregates, or both. You can modify mirrored aggregates containing volumes associated with consistency groups to become unmirrored. Similarly, you can modify unmirrored aggregates containing volumes associated with consistency groups to enable mirroring.

Volumes associated with consistency groups placed on mirrored aggregates and their Snapshots, including any consistency group Snapshots, are replicated to the remote site (site B). The contents of the volumes on

site B are consistency group semantics-compliant. You can access replicated consistency group Snapshots using consistency group Snapshot REST APIs and System Manager on clusters running ONTAP 9.11.1 or later.

If some or all of the volumes associated with a consistency group are located on unmirrored aggregates that are not currently accessible, GET or DELETE operations on the consistency group behave as if the local volumes or hosting aggregates are offline.

Consistency group configuration replication

If site B is running ONTAP 9.10.1 or earlier, only the volumes associated with the consistency groups located on mirrored aggregates are replicated to site B. The consistency group configurations are only replicated to site B, if both sites are running ONTAP 9.11.1 or later.After site B is upgraded to ONTAP 9.11.1, data for consistency groups on site A that have all their associated volumes placed on mirrored aggregates are replicated to site B.

Upgrade considerations

Consistency groups created with SM-BC in ONTAP 9.8 and 9.9.1 will automatically be upgraded and become manageable under **Storage > Consistency Groups** in System Manager or the ONTAP REST API when upgrading to ONTAP 9.10.1. For more information about upgrading, see SM-BC upgrade and revert considerations.

Consistency group snapshots created with the ONTAP REST API can be managed through System Manager's Consistency Group interface and through consistency group API endpoints.

Snapshots created with the ONTAPI commands `cg-start` and `cg-commit` will not be recognized as consistency group Snapshots and thus cannot be managed through System Manager's Consistency Group interface or the consistency group endpoints in the ONTAP API.

Consistency group object limits

Consistency Groups	Scope	Minimum	Maximum
Number of consistency groups	Cluster	0	Same as maximum volume count in cluster
Number of parent consistency groups	Cluster	0	Same as maximum volume count in cluster
Number of individual and parent consistency groups	Cluster	0	Same as maximum volume count in cluster
Consistency group	Same as maximum volume count in cluster	1	80
Number of volumes in the child of a parent consistency group	Parent consistency group	1	80
Number of volumes in a child consistency group	Child consistency group	1	80
Number of child consistency groups in a parent consistency group	Parent consistency group	1	5

If you are using SM-BC, refer to SM-BC restrictions and limitations for limits.

Learn more about consistency groups

Configure a single consistency group

Consistency groups can be created with existing volumes or with new volumes. Once a volume is added to a consistency group, it cannot be added to another consistency group. A volume can be removed from a consistency group by deleting the volume or deleting the consistency group.

Create a consistency group with new volumes

Steps

1. Select **Storage > Consistency groups**.
2. Select **+Add.** then **Using New LUNs**.
3. Name the consistency group. Designate the number of LUNs and capacity per LUN.
4. Select the host operating system and LUN format. Enter the host initiator information.
5. To configure protection policies, add a child consistency group, or show more options about host initiators, select **More options**
6. Select **Save**.
7. Confirm your consistency group has been created by returning to the main consistency group menu where it will appear once the ONTAP job completes. If you set a protection policy, look under the appropriate policy, remote or local, which should display a green shield with a checkmark.

Create a consistency group with existing volumes

Steps

1. Select **Storage > Consistency groups**.
2. Select **+Add.** then **Using existing volumes**.
3. Name the consistency group and select the storage VM.
4. Select the existing volumes to include. Only volumes that are not already part of a consistency group will be available for selection.

   If creating a consistency group with new volumes, the consistency group supports FlexVol volumes. Volumes with Asynchronous or Synchronous SnapMirror relationships can be added to consistency groups, but they are not consistency group-aware. Consistency groups do not support S3 buckets, MCC, or SVMs with SVMDR relationships.

5. Select **Save**.
6. Confirm your consistency group has been created by returning to the main consistency group menu where it will appear once the ONTAP job completes. If you have chosen a protection policy, confirm it was properly set by selecting your consistency group from the menu. If you set a protection policy, look under the appropriate policy, remote or local, which should display a green shield with a checkmark.

Configure a hierarchical consistency group

If your application workload consists of more than one subset of volumes, where each subset is consistent across its own associated volumes, ONTAP allows you to create a hierarchical consistency group. Hierarchical consistency groups have a parent that can include up to five individual consistency groups. Hierarchical consistency groups can support different local Snapshot policies across consistency groups or individual volumes. If you use a remote SM-BC policy, that will apply for the entire consistency group.

For object limits on consistency groups, see Object limits for consistency groups.

Create a hierarchical consistency group with new volumes

Steps

1. Select **Storage > Consistency groups**.
2. Select **+Add.** then **Using New LUNs**.
3. Name the consistency group. Designate the number of LUNs and capacity per LUN.
4. Select the host operating system and LUN format. Enter the host initiator information.
5. To configure protection policies, add a child consistency group, or show more options about host initiators, select **More options**.
6. To add a child consistency group, select **+Add child consistency group**.
7. Select the performance level, the number of LUNs, and capacity per LUN. Designate the host operating system, LUN format, and select a new or existing host initiator group.
8. **Optional**: select a local snapshot policy.
9. Repeat for up to five child consistency groups.

10. Select **Save**.
11. Confirm your consistency group has been created by returning to the main consistency group menu where it will appear once the ONTAP job completes. If you set a protection policy, look under the appropriate policy, remote or local, which should display a green shield with a checkmark in it.

Create a hierarchical consistency group with existing volumes

Steps

1. Select **Storage > Consistency groups**.
2. Select **+Add.** then **Using existing volumes**.
3. Select the storage VM.
4. Select the existing volumes to include. Only volumes that are not already part of a consistency group will be available for selection.
5. To add a child consistency group, select **+Add Child Consistency Group**. Create the necessary consistency groups, which will be named automatically.
6. Assign existing volumes to each consistency group.
7. **Optional**: select a local Snapshot policy.
8. Repeat for up to five child consistency groups.
9. Select **Save**.
10. Confirm your consistency group has been created by returning to the main consistency group menu where it will appear once the ONTAP job completes. If you have chosen a protection policy, confirm it was properly set by selecting your consistency group from the menu. If you set a protection policy, look under the appropriate policy, remote or local, which should display a green shield with a checkmark in it.

Protect a consistency group

Consistency groups offer easily managed local and remote protection for SAN, NAS, and NVMe applications that span multiple volumes.

Creating a consistency group does not automatically enable protection. Local and/or remote protection policies can be set at the time of creation or after creating your consistency group. Protection policies can include local Snapshot copies or remote SnapMirror protection with SnapMirror Business Continuity (SM-BC). If you are utilizing nested consistency groups, you can set different protection policies for individual volumes. Beginning in ONTAP 9.11.1, consistency groups offer two-phase consistency group Snapshot creation.

If you are utilizing remote SM-BC protection, to ensure Snapshot copies of consistency groups created on your consistency group are copied to the destination, the policy labels in the source and destination cluster must match. SM-BC will not replicate Snapshot copies by default unless a rule with a SnapMirror label is added to the predefined AutomatedFailOver policy and the Snapshot copies are created with that label. To learn more about this process, refer to Configure protection for business continuity.

Recovery can occur for an entire consistency group, a single consistency group in a hierarchical configuration, or for individual volumes within the consistency group. Recovery can be achieved by selecting the consistency group you want to recover from, selecting the Snapshot copy type, and then identifying the particular Snapshot copy to base the restoration on. For more information about this process, see Restore a volume from an earlier Snapshot copy.

Beginning with ONTAP 9.10.1, System Manager visualizes LUN maps under the **Protection > Relationships**

menu. When you select a source relationship, System Manager displays a visualization of the source relationships. By selecting a volume, you can delve deeper into these relationships to see a list of the contained LUNs and the initiator group relationships. This information can be downloaded as an Excel workbook from the individual volume view. The task will run in the background.

Set a local Snapshot protection policy

Steps

1. Select the consistency group you have created from the Consistency group menu.
2. At the top right of the overview page for the consistency group, select **Edit**.
3. Check the box next to **Schedule Snapshot copies (local)**.
4. Select a Snapshot policy. To configure a new, custom policy, refer to Create a custom data protection policy.
5. Select **Save**.
6. Return to the consistency group overview menu. In the left column under **Snapshot Copies (Local)**, the status should say protected next to  .

Set a remote SM-BC policy

Steps

1. Ensure you have met the prerequisites for using SM-BC. See SM-BC prerequisites

SM-BC relationships cannot be established on volumes mounted for NAS access.

1. Select the consistency group you have created from the Consistency group menu.
2. At the top right of the overview page, select **More** then **Protect**.
3. The source-side information should be autofilled on the left-hand side of the page.
4. Select the appropriate cluster and storage VM for the destination. Select a protection policy. Ensure that **Initialize relationship** is checked.
5. Click **Save**.
6. The consistency group will have to initialize and synchronize. When this is complete, under **SnapMirror (Remote)** the status should say “Protected” next to  .

Two-phase CG Snapshot creation

Beginning in ONTAP 9.11.1, consistency groups support two-phase commits for consistency group (CG) Snapshot creation. This feature is only available with the ONTAP REST API. Two-phase CG Snapshot creation is only available for Snapshot creation, not provisioning consistency groups or restoring consistency groups.

A two-phase CG Snapshot creation breaks the Snapshot creation process invoked with a POST request to the `/application/consistency-groups/{consistency_group_uuid}/snapshots` endpoint into a sequence of two phases. In the first phase initiated with a POST request, the API executes prechecks, triggers Snapshot creation, and starts a timer for designated interval. If the POST request in phase one completes with a 201 status code, you can invoke the second phase within the designated interval from the first phase, committing the Snapshot to the appropriate endpoint.

To use two-phase CG Snapshot creation, all nodes in the cluster must be running ONTAP 9.11.1. The two-

phase CG Snapshot creation can be invoked with the `action=start` parameter. You can additionally use the `action_timeout` parameter that specifies the maximum number of seconds that the Snapshot creation process can take. The `action_timeout` parameter can be set equal to an integer between 5 and 120. The default value of `action_timeout` is 7.

Only one active invocation of a consistency group Snapshot creation operation is supported on a consistency group instance at a time, whether it be a one-phase or two-phase. Attempting to invoke a Snapshot creation while another one is in progress will result in a failure.

For more information about the ONTAP REST API, refer to the API reference or visit the ONTAP REST API page at the NetApp Developer Network for a complete list of API endpoints.

Create a two-phase commit

1. Invoke the Snapshot creation with a POST request to the consistency group endpoint using the `action=start` parameter.

```
curl -k -X POST 'https://<IP_address>/application/consistency-
groups/<cg-uuid>/snapshots?action=start&action_timeout=7' -H "accept:
application/hal+json" -H "content-type: application/json" -d '
{
  "name": "name_of_this_snapshot",
  "consistency_type": "crash",
  "comment": "<comment>",
  "snapmirror_label": "<snap_mirror label>"
}'
```

2. If the POST request succeeds, your output will include a snapshot uuid. Using that information, submit a PATCH request to commit the Snapshot.

```
curl -k -X PATCH 'https://<IP_address>/application/consistency-
groups/<cg_uuid>/snapshots/<snapshot_id>?action=commit' -H "accept:
application/hal+json" -H "content-type: application/json"
```

Next Steps

Configure Snapshot copies
Create custom data protection policies
Recover from Snapshot copies
Restore a volume from an earlier Snapshot copy

Delete a consistency group

If you decide that you no longer need a consistency group, it can be deleted.

Deleting a consistency group deletes the instance of the consistency group and does **not** impact the constituent volumes or LUNs. Deleting a consistency group does not result in deletion of the Snapshots present on each volume, but they will no longer be accessible as consistency group Snapshots. They can, however, continue to be managed as ordinary volume granular snapshots.

Consistency groups will also be deleted if all of the volumes in a consistency group are deleted. Volumes can only be removed from a consistency group if the volume itself is deleted, in which case the volume is automatically removed from the consistency group.

Steps

1. In the consistency group menu under **Storage > Consistency groups**, select the consistency group you would like to delete.
2. Next to the name of the consistency group, select ⋮ and then **Delete**.

SnapMirror Business Continuity

Overview

Beginning with ONTAP 9.8, you can use SnapMirror Business Continuity (SM-BC) to protect applications with LUNs, enabling applications to fail over transparently, ensuring business continuity in case of a disaster. SM-BC is supported on AFF clusters or All SAN Array (ASA) clusters, where the primary and secondary clusters can be either AFF or ASA. SM-BC protects applications with iSCSI or FCP LUNs.

Benefits

SnapMirror Business Continuity provides the following benefits:

- Provides continuous availability for business-critical applications
- Ability to host critical applications alternately from primary and secondary site
- Simplified application management using consistency groups for dependent write-order consistency
- The ability to test failover for each application
- Instantaneous creation of mirror clones without impacting application availability
- Beginning in ONTAP 9.11.1, SM-BC supports single-file SnapRestore.

Typical use cases

Application deployment for zero RTO or Transparent Application Failover

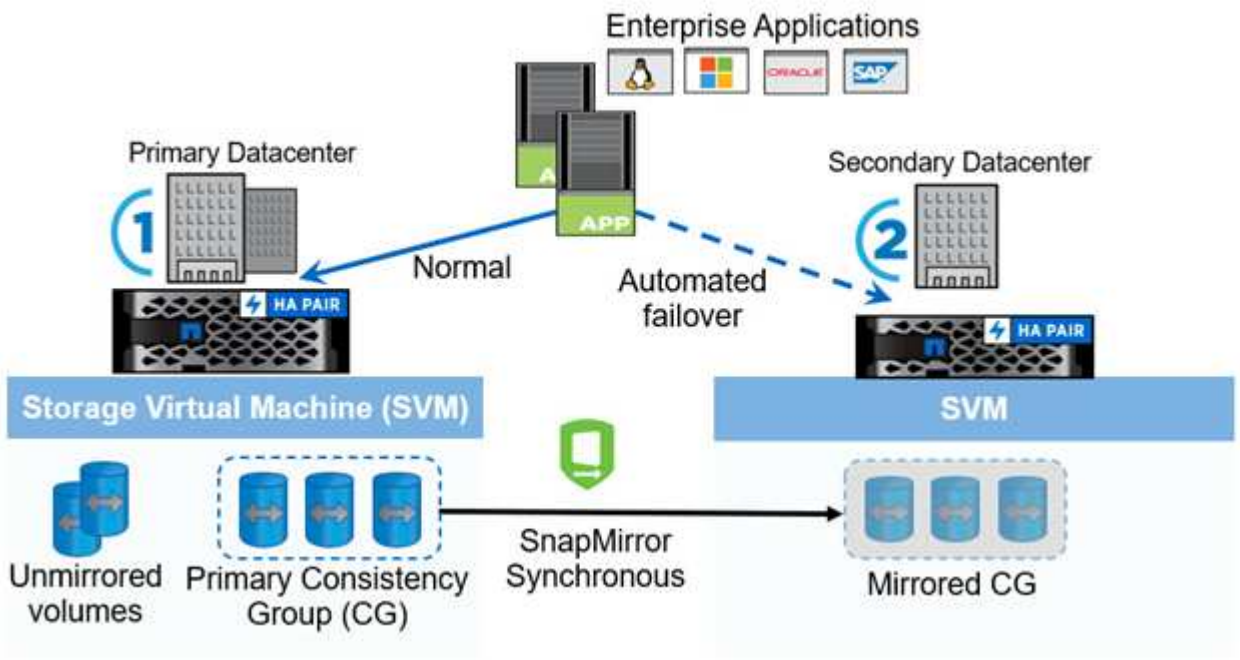
Transparent Application Failover is based on host multipath I/O (MPIO) software-based path failover to achieve non-disruptive access to the storage. Both LUN copies, for example, primary(L1P) and mirror copy(L1S), have the same identity (serial number) and are reported as read-writable to the host. However, reads and writes are serviced only by the primary volume. I/Os issued to the mirror copy are proxied to the primary copy. The host's preferred path to L1 is VS1:N1 based on Asymmetric Logical Unit Access (ALUA) access state Active Optimized (A/O). Mediator is recommended as part of the deployment, primarily to perform failover in case of a storage outage on the primary.

Disaster scenario

The site hosting the primary cluster experiences a disaster. Host multipathing software marks all paths through the cluster as down and uses paths from the secondary cluster. The result is a non-disruptive failover to the mirror copy for LUN L1. L1S is converted from a mirror copy to an active copy of LUN L1. The failover happens automatically when an external Mediator is configured. The host's preferred path to L1 becomes VS2:N1.

Architecture

The following figure illustrates the operation of the SnapMirror Business Continuity feature at a high level.



Additional information

For more information about data protection using SnapMirror Synchronous, see the SnapMirror Synchronous disaster recovery documentation.

Key concepts

As you begin to explore the ONTAP SnapMirror Business Continuity and plan a deployment, it is helpful to become familiar with the key terminology and concepts.

SM-BC

Acronym for the SnapMirror Business Continuity (SM-BC) solution available with ONTAP 9.8 and later.

Consistency group

Beginning with ONTAP 9.10.1, consistency groups have become a first-order management unit. To learn more about consistency groups, refer to Consistency groups overview.

A consistency group (CG) is a collection of FlexVol volumes that provide a write order consistency guarantee for the application workload which needs to be protected for business continuity. The purpose of a consistency group is to take simultaneous crash-consistent Snapshot copies of a collection of volumes at a point in time. In regular deployment, the group of volumes picked to be part of a CG are mapped to an application instance. SnapMirror relationships, also known as a CG relationship, is established between a source CG and a destination CG. The source and destination CGs must contain the same number and type of volumes.

Constituent

The individual FlexVol volumes that are part of a consistency group.

Mediator

ONTAP Mediator provides an alternate health path to the peer cluster, with the intercluster LIFs providing the other health path. With the Mediator's health information, clusters can differentiate between intercluster LIF failure and site failure. When the site goes down, Mediator passes on the health information to the peer cluster on demand, facilitating the peer cluster to fail over. With the Mediator-provided information and the intercluster LIF health check information, ONTAP determines whether to perform an auto failover, if it is failover incapable, continue or stop.

Mediator is one of three parties in the SM-BC quorum, working with the primary cluster and the secondary cluster to reach a consensus. A consensus requires at least two parties in the quorum to agree to an operation.

Out of Sync (OOS)

The application I/O is not replicating to the secondary storage system. The destination volume is not in sync with the source volume because SnapMirror replication is not occuring. If the mirror state is Snapmirrored, this indicates a transfer failure or failure due to an unsupported operation.

Zero RPO

Zero recovery point objective. This is the acceptable amount of data loss from downtime.

Zero RTO

Zero recovery time objective or Transparent Application Failover is achieved by using host multipath I/O (MPIO) software-based path failover to provide non-disruptive access to the storage.

Planned failover

A manual operation to change the roles of copies in a SM-BC relationship. The primary becomes the secondary and the secondary becomes the primary. ALUA reporting also changes.

Automatic unplanned failover (AUFO)

An automatic operation to perform a failover to the mirror copy. The operation requires assistance from Mediator to detect that the primary copy is unavailable.

Planning

Prerequisites

There are several prerequisites that you should consider as part of planning a SnapMirror Business Continuity solution deployment.

Hardware

- Only two-node HA clusters are supported
- Both clusters must be either AFF or ASA (no mixing)

Software

- ONTAP 9.8 or later
- ONTAP Mediator 1.2 or later
- A Linux server or virtual machine for the ONTAP Mediator running one of the following:

Mediator version	Supported Linux versions

1.4	• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5 • CentOS: 7.6, 7.7, 7.8, 7.9
1.3	• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3 • CentOS: 7.6, 7.7, 7.8, 7.9
1.2	• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 8.1 • CentOS: 7.6, 7.7, 7.8

Licensing

- SnapMirror synchronous (SM-S) license must be applied on both clusters
- SnapMirror license must be applied on both clusters

> If your ONTAP storage systems were purchased before June 2019, click NetApp ONTAP Master License Keys to get the required SM-S license.

Networking environment

- Inter-cluster latency round trip time (RTT) must be less than 10 milliseconds
- SCSI-3 persistent reservations are **not** supported with SM-BC

Supported protocols

- Only SAN protocols are supported (not NFS/SMB)
- Only Fibre Channel and iSCSI protocols are supported
- The default IPspace is required by SM-BC for cluster peer relationships. Custom IPspace is not supported.

ONTAP Mediator

- Must be provisioned externally and attached to ONTAP for transparent application failover.
- For more information about the ONTAP Mediator, see Prepare to install the ONTAP Mediator service.

Read-write destination volumes

- SM-BC relationships are not supported on read-write destination volumes. Before you can use a read-write volume, you must convert it to a DP volume by creating a volume-level SnapMirror relationship and then deleting the relationship. For details, see Converting existing relationships to SM-BC relationships

Large LUNs and large volumes

- Large LUNs and large volumes greater than 100TB are supported only on All SAN Arrays

> You must ensure that both the primary and secondary cluster are All SAN Arrays, and that they both have ONTAP 9.8 installed. If the secondary cluster is running a version earlier than ONTAP 9.8 or if it is not an All SAN Array, the synchronous relationship can go out of sync if the primary volume grows larger than 100 TB.

Additional restrictions and limitations

There are several additional restrictions and limitations when using the SnapMirror Business Continuity solution.

Consistency groups in a cluster

Consistency group limits for a cluster with SM-BC are calculated based on relationships and depend on the version of ONTAP used. Limits are platform-independent.

ONTAP version	Maximum number of relationships
ONTAP 9.8-9.9.1	5
ONTAP 9.10.1	20
ONTAP 9.11.1	50

Volumes per consistency group

From ONTAP 9.8 to 9.9.1, the maximum number of volumes supported per SM-BC consistency group relationship is twelve, a limit which is platform-independent. Beginning with ONTAP 9.10.1, the maximum number of volumes supported per SM-BC relationship is sixteen.

Volumes

Limits in SM-BC are calculated based on the number of endpoints, not the number of relationships. A consistency group with 12 volumes contributes 12 endpoints on both the source and destination. Both SM-BC and SnapMirror Synchronous relationships contribute to the total number of endpoints.

The maximum endpoints per platform are included in the following table.

S. No	Platform	Endpoints per HA for SM-BC			Overall sync and SM-BC endpoints per HA		
		ONTAP 9.8-9.9.1	ONTAP 9.10.1	ONTAP 9.11.1	ONTAP 9.8-9.9.1	ONTAP 9.10.1	ONTAP 9.11.1
1	AFF	60	200	400	80	200	400
2	ASA	60	200	400	80	200	400

SAN object limits

The following SAN object limits are included in the following table and apply regardless of the platform.

Limits of objects in an SM-BC relationship	Count
LUNs per volume	256
LUN maps per node	2048
LUN maps per cluster	4096
LIFs per VServer (with at least one volume in an SM-BC relationship)	256
Inter-cluster LIFs per node	4

Limits of objects in an SM-BC relationship	Count
Inter-cluster LIFs per cluster	8

NTFS Security Style

NTFS security style is not supported on SM-BC volumes.

Fan-out configurations

SM-BC supports fan-out configurations with the `MirrorAllSnapshots` policy and, beginning in ONTAP 9.11.1, the the `MirrorAndVault` policy. Fan-out configurations are not supported with `XDPDefault` policy.

If you experience a failover on the SM-BC destination in a fan-out configuration, you will have to manually resume protection in the fan-out configuration.

AIX

Beginning with ONTAP 9.11.1, AIX is supported with SM-BC. With an AIX configuration, the primary cluster is the "active" cluster.

In an AIX configuration, failovers are disruptive. With each failover, you will need to perform a re-scan on the host for I/O operations to resume.

To configure for AIX host with SM-BC, refer to the Knowledge Base article How to configure an AIX host for SnapMirror Business Continuity (SM-BC).

Solaris Host setting recommendation for SM-BC configuration

Beginning with ONTAP 9.10.1, SM-BC supports Solaris 11.4. To ensure the Solaris client applications are nondisruptive when an unplanned site failover switchover occurs in an SM-BC environment, the following setting must be configured on Solaris 11.4 Host. This setting overrides failover module – `f_tpgs` to prevent the code path that detects the contradiction from being executed.

Follow these steps to configure the override parameter:

1. Create configuration file `/etc/driver/drv/scsi_vhci.conf` with an entry similar to the following for the NetApp storage type connected to the host:

```
scsi-vhci-failover-override =
"NETAPP  LUN","f_tpgs"
```

2. Use `devprop` and `mdb` commands to verify the override has been successfully applied:

```
root@host-A:~# devprop -v -n /scsi_vhci scsi-vhci-failover-override
scsi-vhci-failover-override=NETAPP  LUN + f_tpgs
root@host-A:~# echo "*scsi_vhci_dip::print -x struct dev_info devi_child
| ::list struct dev_info devi_sibling| ::print struct dev_info
devi_mdi_client| ::print mdi_client_t ct_vprivate| ::print struct
scsi_vhci_lun svl_lun_wwn svl_fops_name"| mdb -k`
```

```
svl_lun_wwn = 0xa002a1c8960 "600a0980383134775543f524539787938"
svl_fops_name = 0xa00298d69e0 "conf f_tpgs"
```

`conf` will be added to the `svl_fops_name` when a `scsi-vhci-failover-override` has been applied.
For additional information and recommended changes to default settings, refer to NetApp KB article Solaris Host support recommended settings in SnapMirror Business Continuity (SM-BC) configuration.

HP-UX Known issues and limitations for SM-BC configuration

Beginning in ONTAP 9.10.1, SM-BC for HP-UX is supported. If an automatic unplanned failover (AUFO) event occurs on the isolated master cluster in the SM-BC configuration, it might take more than 120 seconds for I/O to resume on the HP-UX host. Depending on the applications that are running, this might not lead to any I/O disruption or error messages. If an AUFO event on the isolated master cluster occurs, you must restart applications on the HP-UX host that have a disruption tolerance of less than 120 seconds.

An AUFO event on the isolated master cluster might cause dual event failure when the connection between the primary and the secondary cluster is lost and the connection between the primary cluster and the mediator is also lost. This is considered a rare event, unlike other AUFO events.

ONTAP access options

You have several access options available when configuring the ONTAP nodes participating in an SM- BC deployment. You should select the option that best matches your specific environment and deployment goals.

In all cases, you must sign in using the administrator account with a valid password.

Command line interface

The text-based command line interface is available through the ONTAP management shell. You can access the CLI using secure shell (SSH).

System Manager

You can connect to the System Manager using a modern web browser. The web GUI provides an intuitive and easy-to-use interface when accessing the SnapMirror Business Continuity functionality. For more information about using System Manager, see System Manager documentation.

REST API

The ONTAP REST API exposed to external clients provides another option when connecting to the ONTAP. You can access the API using any mainstream programming language or tool that supports REST web services. Popular choices include:

- Python (including the ONTAP Python client library)
- Java
- Curl

Using a programming or scripting language provides an opportunity to automate the deployment and management of a SnapMirror Business Continuity deployment. For more information, see the ONTAP online

documentation page at your ONTAP storage system.

Prepare to use the ONTAP CLI

You should be familiar with the following commands when deploying the SnapMirror Business Continuity solution using the ONTAP command line interface.

> SM-BC does not support the `snapmirror quiesce` and `snapmirror resume` commands for relationships with active
> sync policy.

For more information about the following ONTAP commands, see NetApp Documentation: ONTAP 9.

Command	Description
lun igroup create	Create an igroup on a cluster
lun map	Map a LUN to an igroup
lun show	Display a list of LUNs
snapmirror create	Create a new SnapMirror relationship
snapmirror initialize	Initialize an SM-BC consistency group
snapmirror update	Initiates a common snapshot creation operation
snapmirror show	Display a list of SnapMirror relationships
snapmirror failover	Start a planned failover operation
snapmirror resync	Start a resynchronization operation
snapmirror delete	Delete a SnapMirror relationship
snapmirror release	Remove source information for a SnapMirror relationship
volume snapshot restore-file	Available with SM-BC beginning in ONTAP 9.11.1, restore a single file or LUN

Prepare to use the ONTAP Mediator

The ONTAP Mediator establishes a quorum for the ONTAP clusters in an SM-BC relationship. It coordinates automated failover when a failure is detected and helps to avoid split-brain scenarios when each cluster simultaneously tries to establish control as the primary cluster.

Prerequisites for the ONTAP Mediator

The ONTAP Mediator includes its own set of prerequisites. You must meet these prerequisites before installing the mediator. For more information, see Prepare to install the ONTAP Mediator service.

Network configuration

By default, the ONTAP Mediator provides service through TCP port 31784. You should make sure that port 31784 is open and available between the ONTAP clusters and the mediator.

Summary of deployment best practices

There are several best practices that you should consider as part of planning an SnapMirror Business Continuity deployment.

SAN

The SnapMirror Business Continuity solution supports only SAN workloads. You should follow the SAN best practices in all cases.

In addition:

- Replicated LUNs in the secondary cluster must be mapped to the host and the I/O paths to the LUNs from both the primary and secondary cluster must be discovered at the time of host configuration.
- After an out of sync (OOS) event exceeds 80 seconds, or after an automatic unplanned failover, it is important to rescan the host LUN I/O path to ensure that there is no I/O path loss. For more information, see the respective host OS vendor's documentation on rescan of LUN I/O paths.

Mediator

To be fully functional and to enable automatic unplanned failover, the external ONTAP mediator should be provisioned and configured with ONTAP clusters.

When installing the mediator, you should replace the self-signed certificate with a valid certificate signed by a mainstream reliable CA.

SnapMirror

You should terminate an SnapMirror relationship in the following order:

1. Perform `snapmirror delete` at the destination cluster
2. Perform `snapmirror release` at the source cluster

Manage SnapMirror for Business Continuity using System Manager

Configure Mediator

Use System Manager to configure the Mediator server to be used for automated failover. You can also replace the self-signed SSL and CA with the third party validated SSL Certificate and CA if you have not already done so.

Steps

1. Navigate to **Protection > Overview > Mediator > Configure**.
2. Click **Add**, and enter the following Mediator server information:
    - IPv4 address
    - Username
    - Password
    - Certificate

Configure protection for business continuity

Configuring protection for business continuity involves selecting LUNs on the ONTAP source cluster and adding them to a consistency group. Open System Manager from a browser on the source cluster to begin configuring protection for business continuity.

This workflow is designed for ONTAP 9.8 and 9.9. Beginning with ONTAP 9.10.1, it is recommended that you begin by creating a consistency group and then use SM-BC as a remote protection.

About this task

- LUNs must reside on the same storage VM.
- LUNs can reside on different volumes.
- The source and destination cluster cannot be the same.
- The default IPspace is required by SM-BC for cluster peer relationships. Custom IPspace is not supported.

Steps

1. Choose the LUNs you want to protect and add them to a protection group: **Protection > Overview > Protect for Business Continuity > Protect LUNs**.
2. Select one or more LUNs to protect on the source cluster.
3. Select the destination cluster and SVM.
4. **Initialize relationship** is selected by default. Click **Save** to begin protection.
5. Go to **Dashboard > Performance** to verify IOPS activity for the LUNs.
6. On the destination cluster, use System Manager to verify that the protection for business continuity relationship is in sync: **Protection > Relationships**.

Reestablish the original protection relationship after an unplanned failover

ONTAP uses the ONTAP Mediator to detect when a failure occurs on the primary storage system and executes automatic unplanned failover to the secondary storage system. You can use System Manager to reverse the relationship and reestablish the original protection relationship when original source cluster is back online.

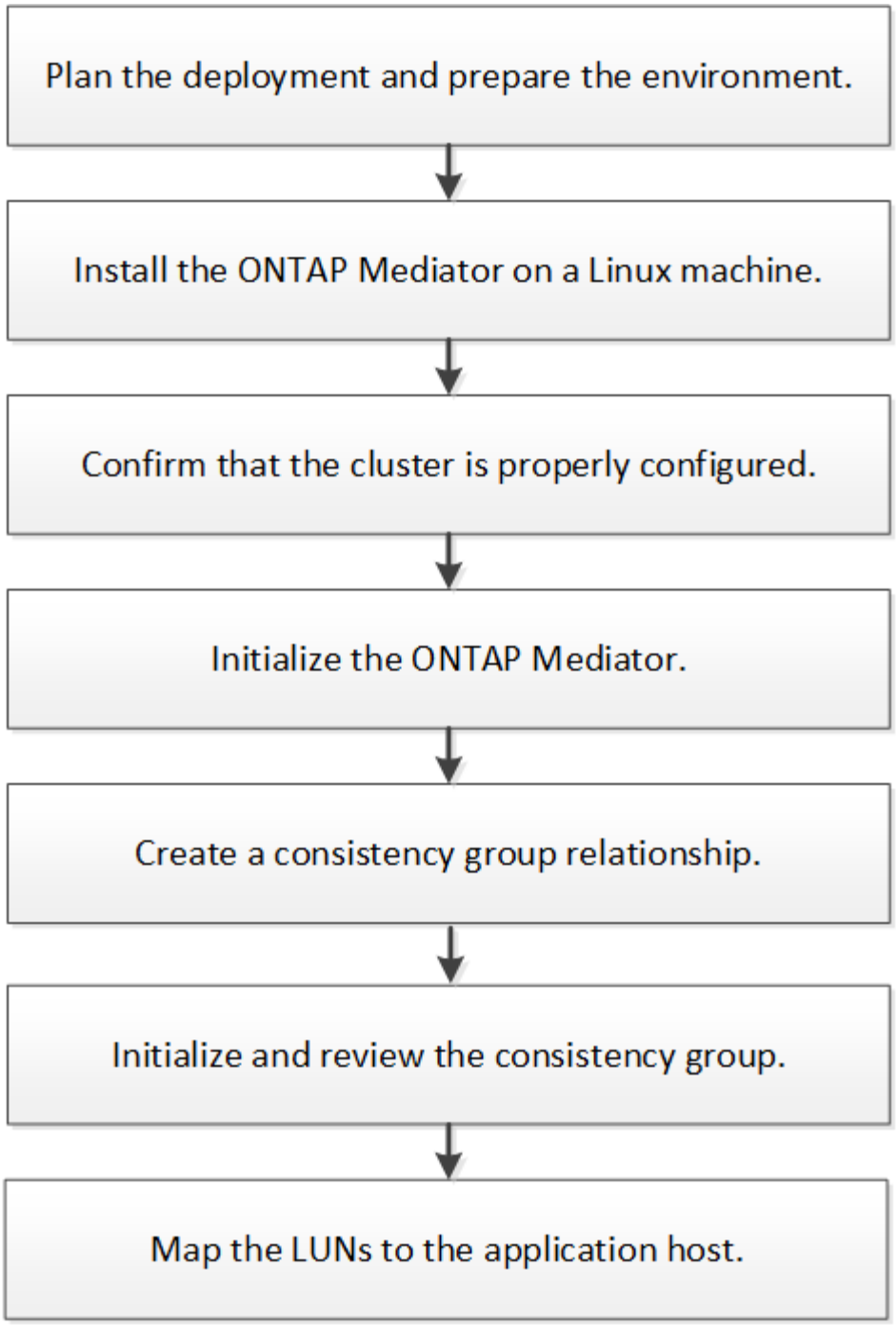
Steps

1. Navigate to **Protection > Relationships** and wait for the relationship state to show “InSync.”
2. To resume operations on the original source cluster, click ⋮ and select **Failover**.

Installation and setup using the ONTAP CLI

High level deployment workflow

You can use the following workflow to install and implement the SnapMirror Business Continuity solution.



Install ONTAP Mediator Service and confirm the ONTAP cluster configuration

You should make sure that your source and destination clusters are configured properly.

About this task

Proceed through each of the following steps. For each step, you should confirm that the specific configuration has been performed. Use the link included after each step to get more information as needed.

Steps

1. Install the ONTAP Mediator service before you ensure that your source and destination clusters are configured properly.

ONTAP Mediator service

2. Confirm that a cluster peering relationship exists between the clusters.

   The default IPspace is required by SM-BC for cluster peer relationships. Custom IPspace is not supported.

   Configure peer relationships

3. Confirm that the Storage VMs are created on each cluster.

   Creating an SVM

4. Confirm that a peer relationship exists between the Storage VMs on each cluster.

   Creating an SVM peering relationship

5. Confirm that the volumes exist for your LUNs.

   Creating a volume

6. Confirm that at least one SAN LIF is created on each node in the cluster.

   Considerations for LIFs in a cluster SAN environment

   Creating a LIF

7. Confirm that the necessary LUNs are created and mapped to igroup, which is used to map LUNs to the initiator on the application host.

   Create LUNs and map igroups

8. Rescan the application host to discover any new LUNs.

Initialize the ONTAP Mediator

You must initialize Mediator on one of your cluster peers before SM-BC can perform planned and automatic unplanned failover operations.

About this task

You can initialize Mediator from either cluster. When you issue the `mediator add` command on one cluster, Mediator is automatically added on the other cluster.

Steps

1. Initialize Mediator on one of the clusters:

   ```
   snapmirror mediator add -mediator-address IP_Address -peer-cluster
   cluster_name -username user_name
   ```

   Example

```
cluster1::> snapmirror mediator add -mediator-address 192.168.10.1 -peer
-cluster cluster2 -username mediatoradmin
Notice: Enter the mediator password.

Enter the password: ******
Enter the password again: ******
```

2. Check the status of the Mediator configuration:

   `snapmirror mediator show`

```
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
192.168.10.1     cluster-2        connected         true
```

   `-quorum-status` indicates whether the SnapMirror consistency group relationships are synchronized with Mediator.

Create a consistency group relationship

You must create a SM-BC consistency group which also establishes the synchronous consistency group relationship.

> This workflow applies to users in ONTAP 9.8 and 9.9.1. If using these ONTAP CLI commands beginning with ONTAP 9.10.1, they will still work to create a consistency group, however, it is recommended that you manage consistency groups with System Manager or the ONTAP REST API.

Before you begin

The following prerequisites and restrictions apply:

- You must be a cluster or storage VM administrator
- You must have a SnapMirror Synchronous license
- The destination volumes must be type DP
- The primary and the secondary storage VM must be in a peered relationship
- All constituent volumes in a consistency group must be in a single Storage VM
- You cannot establish SM-BC consistency group relationships across ASA clusters and non-ASA clusters
- The name of the consistency group must be unique

About this task

You must create the consistency group relationship from the destination cluster. You can map up to 12 constituents using the `cg-item-mappings` parameter on the `snapmirror create` command.

Steps

1. Create a consistency group and constituent relationship. This example creates two consistency groups: cg_src with constituent volumes vol1 and vol2, and cg_dist with constituent volumes vol1_dr and vol2_dr.

```
destination::> snapmirror create -source-path vs1_src:/cg/cg_src -destination
-path vs1_dst:/cg/cg_dst -cg-item-mappings
vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy AutomatedFailOver
```

Initialize a consistency group

After creating a consistency group, you must initialize it.

This workflow applies to users in ONTAP 9.8 and 9.9.1. If using these ONTAP CLI commands beginning with ONTAP 9.10.1, they will still work to initialize a consistency group, however, is recommended that you manage consistency groups with System Manager or the ONTAP REST API.

Before you begin

You must be a cluster or storage VM administrator.

About this task

You initialize the consistency group from the destination cluster.

Steps

1. Sign in to the ONTAP CLI at the destination cluster and initialize the consistency group:

```
destination::>snapmirror initialize -destination-path vs1_dst:/cg/cg_dst
```

2. Confirm that the initialization operation completed successfully. The status should be `InSync`.

```
snapmirror show
```

Mapping LUNs to the application hosts

You must create an igroup on each cluster so you can map LUNs to the initiator on the application host.

About this task

You should perform this configuration on both the source and destination clusters.

Steps

1. Create an igroup on each cluster:

```
lun igroup create -igroup name -protocol fcp|iscsi -ostype os -initiator
initiator_name
```

Example

```
lun igroup create -igroup ig1 -protocol iscsi -ostype linux -initiator
-initiator iqn.2001-04.com.example:abc123
```

2. Map LUNs to the igroup:

   ```
   lun map -path path_name -igroup igroup_name
   ```

   Example:

   ```
   lun map -path /vol/src1/11 -group ig1
   ```

3. Verify the LUNs are mapped:

   ```
   lun show
   ```

4. On the application host, discover the new LUNs.

Administration

Create a common Snapshot copy

In addition to the regularly scheduled Snapshot copy operations, you can manually create a common Snapshot copy between the volumes in the primary SnapMirror consistency group and the volumes in the secondary SnapMirror consistency group.

In ONTAP 9.8, the scheduled snapshot creation interval is one hour. Beginning with ONTAP 9.9.1, that interval is 12 hours.

Before you begin

The SnapMirror group relationship must be in sync.

Steps

1. Create a common Snapshot copy:

   ```
   destination::>snapmirror update -destination-path vs1_dst:/cg/cg_dst
   ```

2. Monitor the progress of the update:

   ```
   destination::>snapmirror show -fields -newest-snapshot
   ```

Perform a planned failover

You can perform a planned failover to test your disaster recovery configuration or to perform maintenance on the primary cluster.

Before you begin

- The relationship must be in sync
- Nondisruptive operations must not be running
- The ONTAP Mediator must be configured, connected, and in quorum

About this task

A planned failover is initiated by the administrator of the secondary cluster. The operation requires switching

the primary and secondary roles so that the secondary cluster takes over from the primary. The new primary cluster can then begin processing input and output requests locally without disrupting client operations.

Steps

1. Start the failover operation:

   ```
   destination::>snapmirror failover start -destination-path vs1_dst:/cg/cg_dst
   ```

2. Monitor the progress of the failover:

   ```
   destination::>snapmirror failover show
   ```

3. When the failover operation is complete, you can monitor the Synchronous SnapMirror protection relationship status from the destination:

   ```
   destination::>snapmirror show
   ```

Automatic unplanned failover operations

An automatic unplanned failover (AUFO) operation occurs when the primary cluster is down or isolated. When this occurs, the secondary cluster is converted to the primary and begins serving clients. This operation is performed only with assistance from the ONTAP Mediator.

After the automatic unplanned failover, it is important to rescan the host LUN I/O paths so that there is no loss of I/O paths.

You can monitor the status of the automatic unplanned failover by using the `snapmirror failover show` command.

Basic monitoring

There are several SM-BC components and operations you can monitor.

ONTAP mediator

During normal operation, the Mediator state should be connected. If it is in any other state, this might indicate an error condition. You can review the Event Management System (EMS) messages to determine the error and appropriate corrective actions.

EMS Name	Description
sm.mediator.added	Mediator is added successfully
sm.mediator.removed	Mediator is removed successfully
sm.mediator.unusable	Mediator is unusable due to a corrupted Mediator server
sm.mediator.misconfigured	Mediator is repurposed or the Mediator package is no longer installed on the Mediator server
sm.mediator.unreachable	Mediator is unreachable

EMS Name	Description
sm.mediator.removed.force	Mediator is removed from the cluster using the "force" option
sm.mediator.cacert.expiring	Mediator certificate authority (CA) certificate is due to expire in 30 days or less
sm.mediator.serverc.expiring	Mediator server certificate is due to expire in 30 days or less
sm.mediator.clientc.expiring	Mediator client certificate is due to expire in 30 days or less
sm.mediator.cacert.expired	Mediator certificate authority (CA) certificate has expired
sm.mediator.serverc.expired	Mediator server certificate has expired
sm.mediator.clientc.expired	Mediator client certificate has expired
sm.mediator.in.quorum	All the SM-BC records are resynchronized with Mediator

Planned failover operations

You can monitor status and progress of a planned failover operation using the `snapmirror failover show` command. For example:

```
ClusterB::> snapmirror failover start -destination-path vs1:/cg/dcg1
```

Once the failover operation is complete, you can monitor the Synchronous SnapMirror protection status from the new destination cluster. For example:

```
ClusterA::> snapmirror show
```

You can also review the following messages to determine if there is an error and take the appropriate corrective actions.

EMS Name	Description
smbc.pfo.failed	SMBC planned failover operation failed. Destination path:
smbc.pfo.start. Destination path:	SMBC planned failover operation started

Automatic unplanned failover operations

During an unplanned automatic failover, you can monitor the status of the operation using the `snapmirror failover show` command. For example:

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
         Source Path: vs1:/cg/scg3
    Destination Path: vs3:/cg/dcg3
     Failover Status: completed
        Error Reason:
            End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
       Failover Type: unplanned
  Error Reason codes: -
```

You can also review the following messages to determine if there is an error and take the appropriate corrective actions.

EMS Name	Description
smbc.aufo.failed	SnapMirror automatic planned failover operation failed. Destination path:
smbc.aufo.start	SMBC planned failover operation started. Destination path:
smbc.aufo.completed:	SnapMirror automatic planned failover operation completed. Destination path:
smbc.aufo.failover.incapable	block.giveback.during.aufo

SM-BC availability

You can check the availability of the SM-BC relationship using a series of commands, either on the primary cluster, the secondary cluster, or both.

Commands you use include the `snapmirror mediator show` command on both the primary and secondary cluster to check the connection and quorum status, the `snapmirror show` command, and the `volume show` command. For example:

```
SMBC_A::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_B           connected         true

SMBC_B::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_A           connected         true

SMBC_B::*> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/cg1 XDP  vs1:/cg/cg1_dp Snapmirrored InSync  -         true    -
vs0:vol1    XDP  vs1:vol1_dp  Snapmirrored InSync    -         true    -
2 entries were displayed.

SMBC_A::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------ -------------- ------------------------ --------------
vs0     vol1   true           false                      Consensus

SMBC_B::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1_dp
vserver volume  is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------- -------------- ------------------------ --------------
vs1     vol1_dp false          true                       No-consensus
```

Add and remove volumes in a consistency group

If you want to change the composition of the consistency group by adding or removing a volume, you must first delete the original relationship and then create the consistency group again with the new composition.

> This workflow applies to ONTAP 9.8 and 9.9.1. Beginning with ONTAP 9.10.1, it is recommended that you manage consistency groups through System Manager or with the ONTAP REST API.

About this task

- The composition change is not allowed when the consistency group is in the “InSync” state.
- The destination volume should be of type DP.

> The new volume you add to expand the consistency group must have a pair of common Snapshot copies between the source and destination volumes.

Steps

This procedure assumes that there are two volume mappings: vol_src1 ←→ vol_dst1 and vol_src2 ←→ vol_dst2, in a consistency group relationship between the end points vs1_src:/cg/cg_src and vs1_dst:/cg/cg_dst.

1. Verify that a common Snapshot copy exists between the source and destination volumes on both the source and destination cluster:

   ```
   source::>snapshot show -vserver vs1_src -volume vol_src3 -snapshot snapmirror*

   destination::>snapshot show -vserver vs1_dst -volume vol_dst3 -snapshot
   snapmirror*
   ```

2. If no common Snapshot copy exists, create and initialize a FlexVol SnapMirror relationship:

   ```
   destination::>snapmirror initialize -source-path vs1_src:vol_src3 -destination
   -path vs1_dst:vol_dst3
   ```

3. Delete the zero RTO consistency group relationship:

   ```
   destination::>snapmirror delete -destination-path vs1_dst:vol_dst3
   ```

4. Release the source SnapMirror relationship and retain the common Snapshot copies:

   ```
   source::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol_dst3
   ```

5. Unmap the LUNs and delete the existing consistency group relationship:

   ```
   destination::>lun mapping delete -vserver vs1_dst -path <lun_path> -igroup
   <igroup_name>
   ```

   > The destination LUNs are unmapped, while the LUNs on the primary copy continue to serve the host I/O.

   ```
   destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst

   source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst -relationship
   -info-only true
   ```

6. Create the new consistency group with the new composition:

   ```
   destination::>snapmirror create -source-path vs1_src:/cg/cg_src -destination
   -path vs1_dst:/cg/cg_dst -cg-item-mappings vol_src1:@vol_dst1,
   vol_src2:@vol_dst2, vol_src3:@vol_dst3
   ```

7. Resynchronize the zero RTO consistency group relationship to ensure it is in sync:

```
destination::>snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

8. Remap the LUNs that you unmapped in Step 5:

```
destination::> lun map -vserver vs1_dst -path <lun_path> -igroup <igroup_name>
```

9. Rescan host LUN I/O paths to restore all paths to the LUNs.

Resume protection in a fan-out configuration with SM-BC

SM-BC supports fan-out configurations. Your source volume can be mirrored to an SM-BC destination endpoint and to one or more asynchronous SnapMirror relationships.

Fan-out configurations are supported with the `MirrorAllSnapshots` policy, and, beginning with ONTAP 9.11.1, the `MirrorAndVault` policy. Beginning in ONTAP 9.11.1, fan-out configurations in SM-BC are not supported with the `XDPDefault` policy.

If you experience a failover on the SM-BC destination, the asynchronous SnapMirror destination will become unhealthy, and you must manually restore protection by deleting and recreating the relationship with the asynchronous SnapMirror endpoint.

Resume protection in a fan-out configuration

1. Verify the failover has completed successfully:
   `snapmirror failover show`
2. On the asynchronous Snapmirror endpoint, delete the fan-out endpoint:
   `snapmirror delete -destination-path` *`destination_path`*
3. On the third site, create an asynchronous SnapMirror relationships between the new SM-BC primary volume and the async fan-out destination volume:
   `snapmirror create -source-path` *`source_path`* `-destination-path` *`destination_path`* `-policy MirrorAllSnapshots -schedule` *`schedule`*
4. Resynchronize the relationship:
   `SnapMirror resync -destination-path` *`destination_path`*
5. Verify the relationship status and heath:
   `snapmirror show`

Convert existing relationships to SM-BC relationships

You can convert an existing zero recovery point protection (zero RPO) Synchronous SnapMirror relationship to an SM-BC zero RTO Synchronous SnapMirror consistency group relationship.

Before you begin

- A zero RPO Synchronous SnapMirror relationship exists between the primary and secondary.
- All LUNs on the destination volume are unmapped before the zero RTO SnapMirror relationship is created.
- SM-BC only supports SAN protocols (not NFS/CIFS). Ensure no constituent of the consistency group is mounted for NAS access.

About this task

- You must be a cluster and SVM administrator on the source and destination.
- You cannot convert zero RPO to zero RTO sync by changing the SnapMirror policy.
- If existing LUNs on the secondary volume are mapped, `snapmirror create` with AutomatedFailover policy triggers an error.
  You must ensure the LUNs are unmapped before issuing the `snapmirror create` command.

Steps

1. Perform a SnapMirror update operation on the existing relationship:

   ```
   destination::>snapmirror update -destination-path vs1_dst:vol1
   ```

2. Verify that the SnapMirror update completed successfully:

   ```
   destination::>snapmirror show
   ```

3. Quiesce each of the zero RPO synchronous relationships:

   ```
   destination::>snapmirror quiesce -destination-path vs1_dst:vol1

   destination::>snapmirror quiesce -destination-path vs1_dst:vol2
   ```

4. Delete each of the zero RPO synchronous relationships:

   ```
   destination::>snapmirror delete -destination-path vs1_dst:vol1

   destination::>snapmirror delete -destination-path vs1_dst:vol2
   ```

5. Release the source SnapMirror relationship but retain the common Snapshot copies:

   ```
   source::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol1

   source::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol2
   ```

6. Create a group zero RTO Synchronous Snapmirror relationship:

   ```
   destination::> snapmirror create -source-path vs1_src:/cg/cg_src -destination
   -path vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy
   AutomatedFailover
   ```

7. Resynchronize the zero RTO consistency group:

   ```
   destination::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
   ```

8. Rescan host LUN I/O paths to restore all paths to the LUNs.

SM-BC upgrade and revert considerations

You should be aware of the requirements for upgrading and reverting an SM-BC configuration.

Upgrade

Before you can configure and use SM-BC, you must upgrade all nodes on the source and destination clusters to ONTAP 9.8 or later.
xref:./smbc/Upgating software on ONTAP clusters

> SM-BC is not supported with mixed ONTAP 9.7 and ONTAP 9.8 clusters.

Upgrading clusters from 9.8 or 9.9.1 to 9.10.1 creates new consistency groups on both source and destination for SM-BC relationships.

Reverting to ONTAP 9.9.1 from ONTAP 9.10.1

To revert relationships from 9.10.1 to 9.9.1, SM-BC relationships must be deleted, followed by the 9.10.1 consistency group instance. Consistency groups cannot be deleted with an active SMBC relationship. Any FlexVol volumes that were upgraded to 9.10.1 previously associated with another Smart Container or Enterprise App in 9.9.1 or earlier will no longer be associated on revert. Deleting consistency groups does not delete the constituent volumes or volume granular snapshots. Refer to Delete a consistency group for more information on this task.

Reverting to ONTAP 9.7 from ONTAP 9.8

When you revert from ONTAP 9.8 to ONTAP 9.7, you must be aware of the following:

- If the cluster is hosting an SM-BC destination, reverting to ONTAP 9.7 is not allowed until the relationship is broken and deleted.
- If the cluster is hosting an SM-BC source, reverting to ONTAP 9.7 is not allowed until the relationship is released.
- All user-created custom SM-BC SnapMirror policies must be deleted before reverting to ONTAP 9.7.

Steps

1. Perform a revert check from one of the clusters in the SM-BC relationship:

   ```
   cluster::*> system node revert-to -version 9.7 -check-only
   ```

   Example:

   ```
   cluster::*> system node revert-to -version 9.7 -check-only
   Error: command failed: The revert check phase failed. The following
   issues must be resolved before revert can be completed. Bring the data
   LIFs down on running vservers. Command to list the running vservers:
   vserver show -admin-state running Command to list the data LIFs that are
   up: network interface show -role data -status-admin up Command to bring
   all data LIFs down: network interface modify {-role data} -status-admin
   down
   Disable snapshot policies.
       Command to list snapshot policies: "snapshot policy show".
       Command to disable snapshot policies: "snapshot policy modify
   -vserver
      * -enabled false"
   ```

```
   Break off the initialized online data-protection (DP) volumes and
delete
   Uninitialized online data-protection (DP) volumes present on the
local
   node.
    Command to list all online data-protection volumes on the local
node:
   volume show -type DP -state online -node <local-node-name>
    Before breaking off the initialized online data-protection volumes,
   quiesce and abort transfers on associated SnapMirror relationships
and
   wait for the Relationship Status to be Quiesced.
    Command to quiesce a SnapMirror relationship: snapmirror quiesce
    Command to abort transfers on a SnapMirror relationship: snapmirror
   abort
    Command to see if the Relationship Status of a SnapMirror
relationship
   is Quiesced: snapmirror show
    Command to break off a data-protection volume: snapmirror break
    Command to break off a data-protection volume which is the
destination
   of a SnapMirror relationship with a policy of type "vault":
snapmirror
   break -delete-snapshots
    Uninitialized data-protection volumes are reported by the
"snapmirror
   break" command when applied on a DP volume.
    Command to delete volume: volume delete

   Delete current version snapshots in advanced privilege level.
    Command to list snapshots: "snapshot show -fs-version 9.8"
    Command to delete snapshots: "snapshot prepare-for-revert -node
   <nodename>"

   Delete all user-created policies of the type active-strict-sync-
mirror
   and active-sync-mirror.
   The command to see all active-strict-sync-mirror and active-sync-
mirror
   type policies is:
    snapmirror policy show -type
   active-strict-sync-mirror,active-sync-mirror
   The command to delete a policy is :
    snapmirror policy delete -vserver <SVM-name> -policy <policy-name>
```

For information on reverting clusters, see Revert ONTAP.

Remove an SM-BC configuration

You can remove zero RTO Synchronous SnapMirror protection and delete the SM-BC relationship configuration.

About this task

Before you delete the SM-BC relationship, all LUNs in the destination cluster must be unmapped.
After the LUNs are unmapped and the host is rescanned, the SCSI target notifies the hosts that the LUN inventory has changed. The existing LUNs on the zero RTO secondary volumes change to reflect a new identity after the zero RTO relationship is deleted. Hosts discover the secondary volume LUNs as new LUNs that have no relationship to the source volume LUNs.
The secondary volumes remain DP volumes after the relationship is deleted. You can issue the snapmirror break command to convert them to read/write.
Deleting the relationship is not allowed in the failed-over state when the relationship is not reversed.

Steps

1. Delete the SM-BC consistency group relationship between the source endpoint and destination endpoint:

   ```
   Destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
   ```

2. From the source cluster, release the consistency group relationship and the Snapshot copies created for the relationship:

   ```
   Source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
   ```

3. Perform a host rescan to update the LUN inventory.
4. Beginning with ONTAP 9.10.1, deleting the SnapMirror relationship does not delete the consistency group. If you want to delete the consistency group, you must use System Manager or the ONTAP REST API. See Delete a consistency group for more information.

Remove ONTAP Mediator

If you want to remove an existing ONTAP Mediator configuration from your ONTAP clusters, you can do so by using the `snapmirror mediator remove` command.

Steps

1. Remove ONTAP Mediator:

   ```
   snapmirror mediator remove -mediator-address 12.345.678.90 -peer-cluster
   cluster_xyz
   ```

Troubleshooting

SnapMirror delete operation fails in takover state

Issue:

When ONTAP 9.9.1 is installed on a cluster, executing the `snapmirror delete` command fails when an SM-BC consistency group relationship is in takeover state.

Example:

```
C2_cluster::> snapmirror delete  vs1:/cg/dd

Error: command failed: RPC: Couldn't make connection
```

Solution

When the nodes in an SM-BC relationship are in takeover state, perform the SnapMirror delete and release operation with the "-force" option set to true.

Example:

```
C2_cluster::> snapmirror delete  vs1:/cg/dd -force true

Warning: The relationship between source "vs0:/cg/ss" and destination
         "vs1:/cg/dd" will be deleted, however the items of the
destination
         Consistency Group might not be made writable, deletable, or
modifiable
         after the operation. Manual recovery might be required.
Do you want to continue? {y|n}: y
Operation succeeded: snapmirror delete for the relationship with
destination "vs1:/cg/dd".
```

Failure creating a SnapMirror relationship and initializing consistency group

Issue:

Creation of SnapMirror relationship and consistency group initialization fails.

Solution:

Ensure that you have not exceeded the limit of consistency groups per cluster. Consistency group limits in SM-BC are platform independent and differ based on the version of ONTAP. See Additional restrictions and limitations for limitations based on ONTAP version.

Error:

If the consistency group is stuck initializing, check the status of your consistency group initializations with the ONTAP REST API, System Manager or the command `sn show -expand`.

Solution:

If consistency groups fail to initialize, remove the SM-BC relationship, delete the consistency group, then recreate the relationship and initialize it. This workflow differs depending on the version of ONTAP you are using.

If you are using ONTAP 9.8-9.9.1	If you are using ONTAP 9.10.1 or later

1. Remove the SM-BC configuration 2. Create a consistency group relationship 3. Initialize the consistency group relationship	1. Under **Protection > Relationships**, find the SM-BC relationship on the consistency group. Select ⋮, then **Delete** to remove the SM-BC relationship. 2. Delete the consistency group 3. Configure the consistency group

Planned failover unsuccessful

Issue:

After executing the `snapmirror failover start` command, the output for the `snapmirror failover show` command displays a message indicates that a nondisruptive operation is in progress.

Example:

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-------- ----------- -------- --------- ---------- ---------- ----------
vs1:/cg/cg vs0:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
Failover cannot start because a volume move is running. Retry the command
once volume move has finished.
                                                              08:35:04
08:35:04
```

Cause:

Planned failover cannot begin when a nondisruptive operation is in progress, including volume move, aggregate relocation, and storage failover.

Solution:

Wait for the nondisruptive operation to complete and try the failover operation again.

Mediator not reachable or Mediator quorum status is false

Issue:

After executing the `snapmirror failover start` command, the output for the `snapmirror failover show` command displays a message indicating that Mediator is not configured.

See Initialize the ONTAP Mediator.

Example:

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-------- ---------- -------- --------- ---------- ---------- ----------
vs0:/cg/cg vs1:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
failover cannot start because the source-side precheck failed. reason:
Mediator not configured.
05:50:42 05:50:43
```

Cause:

Mediator is not configured or there are network connectivity issues.

Solution:

If Mediator is not configured, you must configure Mediator before you can establish an SM-BC relationship. Fix any network connectivity issues. Make sure Mediator is connected and quorum status is true on both the source and destination site using the snapmirror mediator show command.

Example:

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.234.10.143    cluster2         connected         true
```

Automatic unplanned failover not triggered on Site B

Issue:

A failure on Site A does not trigger an unplanned failover on Site B.

Possible cause #1:

Mediator is not configured. To determine if this is the cause, issue the `snapmirror mediator show` command on the Site B cluster.

Example:

```
Cluster2::*> snapmirror mediator show
This table is currently empty.
```

This example indicates that Mediator is not configured on Site B.

Solution:

Ensure that Mediator is configured on both clusters, that the status is connected, and quorum is set to True.

Possible cause #2:

SnapMirror consistency group is out of sync. To determine if this is the cause, view the event log to view if the consistency group was in sync during the time at which the Site A failure occurred.

Example:

```
cluster::*> event log show -event *out.of.sync*

Time                Node             Severity      Event
------------------- ---------------- -------------
---------------------------
10/1/2020 23:26:12  sti42-vsim-ucs511w ERROR       sms.status.out.of.sync:
Source volume "vs0:zrto_cg_556844_511u_RW1" and destination volume
"vs1:zrto_cg_556881_511w_DP1" with relationship UUID "55ab7942-03e5-11eb-
ba5a-005056a7dc14" is in "out-of-sync" status due to the following reason:
"Transfer failed."
```

Solution:

Complete the following steps to perform a forced failover on Site B.

1. Unmap all LUNs belonging to the consistency group from Site B.
2. Delete the SnapMirror consistency group relationship using the `force` option.
3. Enter the `snapmirror break` command on the consistency group constituent volumes to convert volumes from DP to R/W, to enable I/O from Site B.
4. Boot up the Site A nodes to create a zero RTO relationship from Site B to Site A.
5. Release the consistency group with `relationship-info-only` on Site A to retain common Snapshot copy and unmap the LUNs belonging to the consistency group.
6. Convert volumes on Site A from R/W to DP by setting up a volume level relationship using either the Sync policy or Async policy.
7. Issue the `snapmirror resync` to synchronize the relationships.
8. Delete the SnapMirror relationships with the Sync policy on Site A.
9. Release the SnapMirror relationships with Sync policy using `relationship-info-only true` on Site B.
10. Create a consistency group relationship from Site B to Site A.
11. Perform a consistency group resync from Site A, and then verify that the consistency group is in sync.
12. Rescan host LUN I/O paths to restore all paths to the LUNs.

Link between Site B and Mediator down and Site A down

To check on the connection of the Mediator, use the `snapmirror mediator show` command. If the connection status is unreachable and Site B is unable to reach Site B, you will have an output similar to the one below. Follow the steps in the solution to restore connection

Example:

```
cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.237.86.17     C1_cluster       unreachable       true
SnapMirror consistency group relationship status is out of sync.

C2_cluster::*> snapmirror show -expand
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/src_cg_1 XDP vs1:/cg/dst_cg_1 Snapmirrored OutOfSync - false   -
vs0:zrto_cg_655724_188a_RW1 XDP vs1:zrto_cg_655755_188c_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655733_188a_RW2 XDP vs1:zrto_cg_655762_188c_DP2 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655739_188b_RW1 XDP vs1:zrto_cg_655768_188d_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655748_188b_RW2 XDP vs1:zrto_cg_655776_188d_DP2 Snapmirrored
OutOfSync - false -
5 entries were displayed.

Site B cluster is unable to reach Site A.
C2_cluster::*> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
C1_cluster            1-80-000011           Unavailable    ok
```

Solution

Force a failover to enable I/O from Site B and then establish a zero RTO relationship from Site B to Site A.

Complete the following steps to perform a forced failover on Site B.

1. Unmap all LUNs belonging to the consistency group from Site B.
2. Delete the SnapMirror consistency group relationship using the force option.
3. Enter the snapmirror break command on the consistency group constituent volumes to convert volumes from DP to RW, to enable I/O from Site B.
4. Boot up the Site A nodes to create a zero RTO relationship from Site B to Site A.
5. Release the consistency group with relationship-info-only on Site A to retain common Snapshot copy and unmap the LUNs belonging to the consistency group.

6. Convert volumes on Site A from RW to DP by setting up a volume level relationship using either Sync policy or Async policy.
7. Issue the snapmirror resync to synchronize the relationships.
8. Delete the SnapMirror relationships with Sync policy on Site A.
9. Release the SnapMirror relationships with Sync policy using relationship-info-only true on Site B.
10. Create a consistency group relationship from Site B to Site A.
11. Perform a consistency group resync from Site A, and then verify that the consistency group is in sync.
12. Rescan host LUN I/O paths to restore all paths to the LUNs.

Link between Site A and Mediator down and Site B down

When using SM-BC, you may lose connectivity between the mediator or your peered clusters. You can diagnose the issue by checking the connection, availability, and consensus status of the different parts of the SM-BC relationship and then forcefully resuming connection.

Table 1. Determining the cause

What to check	CLI command	Indicator
Mediator from Site A	`snapmirror mediator show`	The connection status will be `unreachable`
Site B connectivity	`cluster peer show`	Availability will be `unavailable`
Consensus status of the SM-BC volume	`volume show` *`volume_name`* `-fields smbc-consensus`	The `sm-bc consensus` field will read `Awaiting-consensus`

For additional information about diagnosing and resolving this issue, refer to the Knowledge Base article Link between Site A and Mediator down and Site B down when using SM-BC.

SM-BC SnapMirror delete operation fails when fence is set on destination volume

Issue:

SnapMirror delete operation fails when any of the destination volumes have redirection fence set.

Solution

Performing the following operations to retry the redirection and remove the fence from the destination volume.

- SnapMirror resync
- SnapMirror update

Volume move operation stuck when primary is down

Issue:

A volume move operation is stuck indefinitely in cutover deferred state when the primary site is down in an SM-BC relationship.
When the primary site is down, the secondary site performs an automatic unplanned

failover (AUFO). When a volume move operation is in progress when the AUFO is triggered the volume move becomes stuck.

Solution:

Abort the volume move instance that is stuck and restart the volume move operation.

SnapMirror release fails when unable to delete Snapshot copy

Issue:

The SnapMirror release operation fails when the Snapshot copy cannot be deleted.

Solution:

The Snapshot copy contains a transient tag. Use the `snapshot delete` command with the `-ignore -owners` option to remove the transient Snapshot copy.

```
snapshot delete -volume <volume_name> -snapshot <snapshot_name> -ignore-owners true -force true
```

Retry the `snapmirror release` command.

Volume move reference Snapshot copy shows as the newest

Issue:

After performing a volume move operation on a consistency group volume, the volume move reference Snapshot copy might display as the newest for the SnapMirror relationship.

You can view the newest Snapshot copy with the following command:

```
snapmirror show -fields newest-snapshot status -expand
```

Solution:

Manually perform a `snapmirror resync` or wait for the next automatic resync operation after the volume move operation completes.

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.