NetApp

SnapMirror Business Continuity

ONTAP 9

NetApp
August 15, 2023

Table of Contents

SnapMirror Business Continuity

SnapMirror Business Continuity overview

SnapMirror Business Continuity (SM-BC) enables business services to continue operating even through a complete site failure, supporting applications to fail over transparently using a secondary copy. Neither manual intervention nor additional scripting is required to trigger a failover with SM-BC.

SM-BC is available beginning with ONTAP 9.8. 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

SM-BC provides the following benefits:

- 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.

Use cases

Application deployment for zero recovery time object (RTO)

In an SM-BC deployment, you will have a primary and secondary cluster. A LUN in the primary cluster ($1LP$) will have a mirror ($L1s$) on the secondary; both LUNs share the same serial ID and are reported as read-write LUNs to the host. Read and write operations, however, are only serviced to the primary LUN, $1LP$. Any writes to the mirror $L1S$ are served by proxy.

Disaster scenario

With SM-BC, you can synchronously replicate multiple volumes for an application between sites at geographically dispersed locations. You can automatically failover to the secondary copy in case of disruption of the primary, thus enabling business continuity for tier one applications.

Architecture

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

In section one of the diagram, an application is deployed on a SVM in the primary data center. The volumes that have been added to the primary consistency group are protected with SM-BC and are mirrored to secondary consistency group at a secondary data center. The volumes in the primary consistency group will failover to the mirrored consistency group in the event of a disruption. Volumes not in a mirrored consistency group are not served in the event of a failover.

Further information

- TR-4878: SnapMirror Business Continuity

Key concepts

SnapMirror Business Continuity (SM-BC) utilizes features such as consistency groups and the ONTAP Mediator to ensure your data is replicated and served even in the event of a disaster scenario. When planning your SM-BC deployment, it is important to understand the essential concepts in SM-BC and its architecture.

Architecture

The following figure illustrates a high-level overview of an SM-BC deployment.
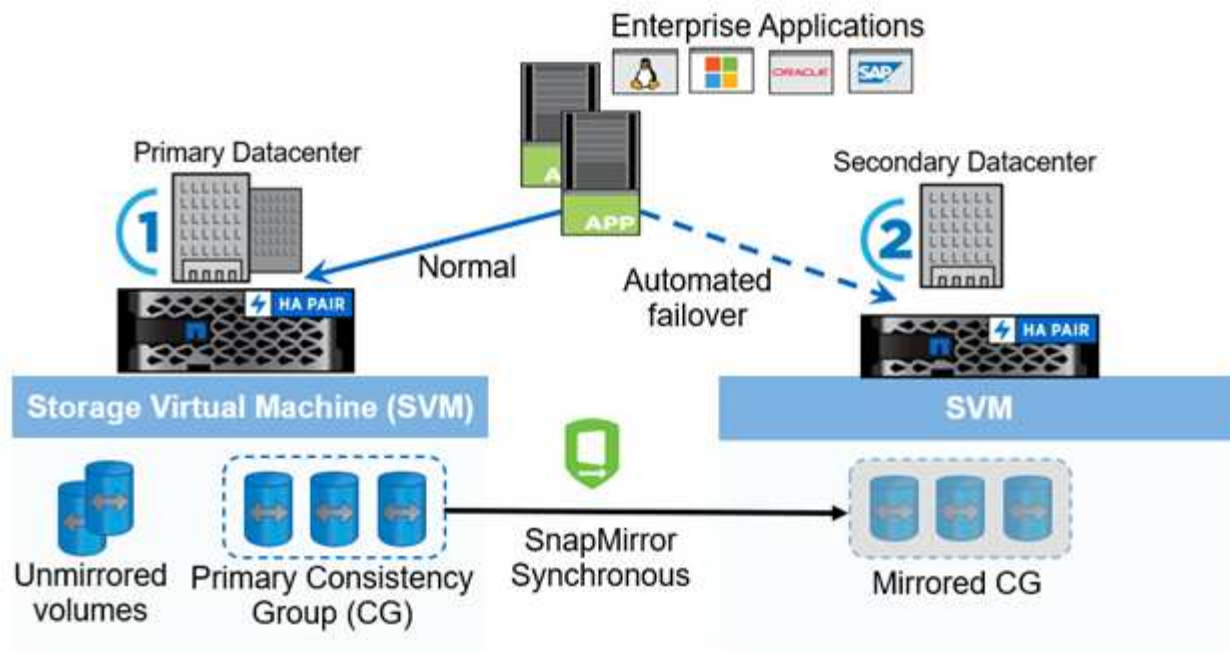
The diagram shows an enterprise application that is hosted on an storage VM (SVM) at the primary data center. The SVM contains five volumes, three of which are part of a consistency group. The three volumes in the consistency group are mirrored to a secondary data center. In normal circumstances, all write operations are performed to the primary data center; in effect, this data center serves as the source for I/O operations, while the secondary data center serves as a destination.

In the event of a disaster scenario at the primary data center, the ONTAP Mediator will direct the secondary data center to act as the primary, serving all I/O operations. Only the volumes that are mirrored in the consistency group will be served. Any operations pertaining to the other two volumes on the SVM will be affected by the disaster event.

Essential concepts

Understanding the following terms will help you deploy SM-BC.

Consistency group

A consistency group is a collection of volumes or LUNs that provide a write-order consistency guarantee for the application workload that needs to be protected for business continuity. A consistency group ensures all volumes of this data set are quiesced and then snapped at the same point in time, providing a data-consistent restore point across volumes for that data set.

In SM-BC, you will create a primary and secondary consistency group for replication and data protection. The secondary consistency group will serve your data in the event of a disruption.

To learn more about consistency groups, see Consistency groups overview.

Constituent

An individual volume or LUN that is part of a consistency group, which is protected by the SM-BC relationship.

ONTAP Mediator

The ONTAP Mediators monitors the two ONTAP clusters and orchestrates failover in case your primary storage system fails. With the ONTAP Mediator, your application automatically reconnects to the resources in the secondary storage system.

With the ONTAP Mediator's health information, clusters can differentiate between intercluster LIF failure and site failure. When the site goes down, ONTAP Mediator passes on the health information to the peer cluster on demand, facilitating the peer cluster to failover.

Learn more about the ONTAP Mediator.

Planned failover

A manual operation to change the roles of copies in a SM-BC relationship. The primary sites becomes the secondary, and the secondary becomes the primary.

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.

Out of Sync (OOS)

When the application I/O is not replicating to the secondary storage system, it will be reported as **out of sync**. An out of sync status means the secondary volumes are not synchronized with the primary (source) and that SnapMirror replication is not occurring.

If the mirror state is `Snapmirrored`, this indicates a transfer failure or failure due to an unsupported operation.

Zero RPO

RPO stands for recovery point objective, which is the amount of data loss deemed acceptable during a given time period. Zero RPO signifies that no data loss is acceptable.

Zero RTO

RTO stands for recovery time objective, which is the amount of time that is deemed acceptable for an application to return to normal operations following an outage, failure, or other data loss event. Zero RTO signifies that no amount of downtime is acceptable.

Plan

Prerequisites

When planning your SnapMirror Business Continuity deployment, ensure you have met the various hardware, software, and system configuration requirements.

Hardware

- Only two-node HA clusters are supported
- Both clusters must be either AFF (including AFF C-Series) 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:

ONTAP Mediator version	Supported Linux versions

1.6	• Red Hat Enterprise Linux: 8.4, 8.5, 8.6, 8.7, 8.8, 9.0, 9.1, 9.2
	• Rocky Linux 8 and 9
1.5	• 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
1.4	• 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, see 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.

NTFS Security Style

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

ONTAP Mediator

- The ONTAP Mediator be provisioned externally and attached to ONTAP for transparent application failover.
- To be fully functional and to enable automatic unplanned failover, the external ONTAP mediator should be provisioned and configured with ONTAP clusters.
- The ONTAP Mediator must be installed in a third failure domain, separate from the two ONTAP clusters.

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

- 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

Support for large LUNs and large volumes (greater than 100 TB) depends on the version of ONTAP you are using and your platform.

ONTAP 9.12.1P2 and later

- For ONTAP 9.12.1 P2 and later, SMBC supports Large LUNs and large volumes greater than 100TB on ASA and AFF (including C-Series).

  ⓘ For ONTAP Releases 9.12.1P2 and later, You must ensure that both the primary and secondary clusters are either All SAN Arrays or All Flash Array, and that they both have ONTAP 9.12.1 P2 or later installed. If the secondary cluster is running a version earlier than ONTAP 9.12.1P2 or if the array type is not the same as primary cluster, the synchronous relationship can go out of sync if the primary volume grows larger than 100 TB.

ONTAP 9.8 - 9.12.1P1

- For ONTAP releases between ONTAP 9.8 and 9.12.1 P1 (inclusive), Large LUNs and large volumes greater than 100TB are supported only on All SAN Arrays.

  ⓘ For ONTAP releases between ONTAP 9.8 and 9.12.1 P2, You must ensure that both the primary and secondary clusters are All SAN Arrays, and that they both have ONTAP 9.8 or later 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.

Further information

- Hardware Universe
- ONTAP Mediator overview

Supported configurations and features

SnapMirror Business Continuity is compatible with numerous operating systems and other features in ONTAP. Learn about details and recommended configurations.

Supported configurations

SM-BC is supported with numerous operating systems, including:

- AIX (beginning ONTAP 9.11.1)
- HP-UX (beginning ONTAP 9.10.1)
- Solaris 11.4 (beginning ONTAP 9.10.1)

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).

HP-UX

Beginning in ONTAP 9.10.1, SM-BC for HP-UX is supported.

Limitations with HP-UX

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.

Solaris Host setting recommendation

Beginning with ONTAP 9.10.1, SM-BC supports Solaris 11.4.

To ensure the Solaris client applications are non-disruptive when an unplanned site failover switchover occurs in an SM-BC environment, modify the default Solaris OS settings. To configure Solaris with the recommended settings, see the Knowledge Base article Solaris Host support recommended settings in SnapMirror Business Continuity (SM-BC) configuration.

ONTAP integrations

SM-BC offers support for other features in ONTAP, including:

- Fan-out configurations
- NDMP copy (beginning ONTAP 9.13.1)
- Partial file restore (beginning ONTAP 9.12.1)

FabricPool

SM-BC supports source and destination volumes on FabricPool aggregates with the tiering policy of None, Snapshot or Auto. SM-S SM-BC does not support FabricPool aggregates using a tiering policy of All.

Fan-out configurations

In a fan-out configurations, your source volume can be mirrored to an SM-BC destination endpoint and to one or more asynchronous SnapMirror relationships.
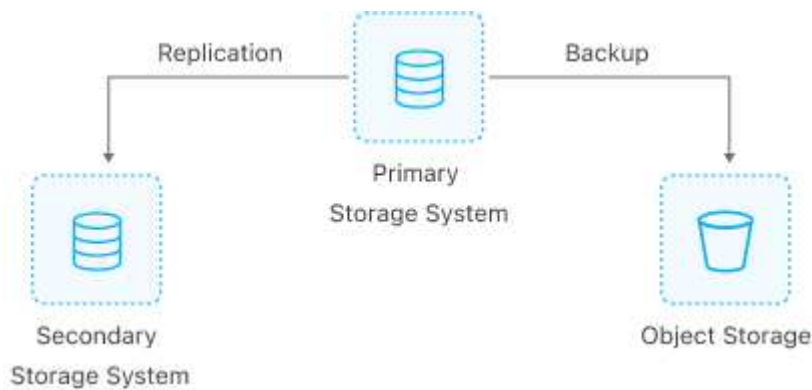
SM-BC supports fan-out configurations with the `MirrorAllSnapshots` policy and, beginning in ONTAP 9.11.1, the `MirrorAndVault` policy. Fan-out configurations are not supported in SM-BC with the `XDPDefault` policy.

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.

NDMP restore

Beginning in ONTAP 9.13.1, you can use NDMP to copy and restore data with SM-BC. Using NDMP allows you to move data onto the SM-BC source to complete a restore without pausing protection. This is particularly useful in fan-out configurations.

To learn more about this process, see Transfer data using ndmp copy.

Partial file restore

Beginning in ONTAP 9.12.1, partial LUN restore is supported for SM-BC volumes. For information on this process, refer to Restore part of a file from a Snapshot copy.

Object limits for SnapMirror Business Continuity

When preparing to use and managing SnapMirror Business Continuity, be aware of the following limitations.

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 and later	50

Volumes per consistency group

The maximum number of volumes per consistency group with SM-BC is platform independent.

ONTAP version	Maximum number of volumes supported in a consistency group relationship
ONTAP 9.8-9.9.1	12
ONTAP 9.10.1 and later	16

Volumes

Volume 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 primary and secondary cluster. 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 and later	ONTAP 9.8-9.9.1	ONTAP 9.10.1	ONTAP 9.11.1 and later
1	AFF	60	200	400	80	200	400
2	ASA	60	200	400	80	200	400

SAN object limits

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

Object in an SM-BC relationship	Count
LUNs per volume	256
LUN maps per node	2048
LUN maps per cluster	4096
LIFs per SVM (with at least one volume in an SM-BC relationship)	256
Inter-cluster LIFs per node	4
Inter-cluster LIFs per cluster	8

Related information

- Hardware Universe
- Consistency group limits

Install and set up

Configure the ONTAP Mediator and clusters for SnapMirror Business Continuity

SnapMirror Business Continuity (SM-BC) utilizes peered clusters to ensure your data is available in the event of a failover scenario. The ONTAP Mediator is a key resource ensuring business continuity, monitoring the health of each cluster. To configure SM-BC, you must first install the ONTAP Mediator and ensure you primary and secondary clusters are configured properly.

Once you have installed the ONTAP Mediator and configured your clusters, you must Initialize the ONTAP mediator for SM-BC the ONTAP Mediator for use with SM-BC. You must then Create, initialize, and map the consistency group for SM-BC

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, determining which cluster acts as the primary and ensuring data is served to and from the correct destination.

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.

- 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.

Install the ONTAP Mediator and confirm cluster configuration

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.

   Prepare to install or upgrade the ONTAP Mediator service

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

   > (i) The default IPspace is required by SM-BC for cluster peer relationships. A 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 an 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 for SM-BC

Once you have installed the ONTAP Mediator and confirmed you cluster configuration, you must initialize the ONTAP Mediator for cluster monitoring. You can initialize the ONTAP Mediator using System Manager or the ONTAP CLI.

System Manager

With System Manager, you can configure the ONTAP Mediator server 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. Select **Add**, and enter the following ONTAP Mediator server information:

   ◦ IPv4 address

   ◦ Username

   ◦ Password

   ◦ Certificate

CLI

You can initialize the ONTAP Mediator from either the primary or secondary cluster using the ONTAP CLI. When you issue the `mediator add` command on one cluster, the ONTAP 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 the mediator; a status of `true` indicates successful synchronization.

Establish protection with SnapMirror Business Continuity

Configuring protection using SnapMirror Business Continuity involves selecting LUNs on the ONTAP source cluster and adding them to a consistency group.

Before you begin

- You must have a SnapMirror Synchronous license.

- You must be a cluster or storage VM administrator.

- All constituent volumes in a consistency group must be in a single storage VM (SVM).

  - LUNs can reside on different volumes.

- The source and destination cluster cannot be the same.

- You cannot establish SM-BC consistency group relationships across ASA clusters and non-ASA clusters.

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

- The name of the consistency group must be unique.

- The volumes on the secondary (destination) cluster must be type DP.

- The primary and the secondary SVMs must be in a peered relationship.

Steps

You can configure a consistency group using the ONTAP CLI or System Manager.

Beginning in ONTAP 9.10.1, ONTAP offers a consistency group endpoint and menu in System Manager, offering additional management utilities. If you are using ONTAP 9.10.1 or later, see Configure a consistency group then configure protection to create an SM-BC relationship.

System Manager

1. On the primary cluster, navigate to **Protection > Overview > Protect for Business Continuity > Protect LUNs**.

2. Select the LUNs you want to protect and add them to a protection group.

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**.

CLI

1. Create a consistency group relationship from the destination cluster.
   `destination::> snapmirror create -source-path *source-path* -destination-path *destination-path* -cg-item -mappings *volume-paths* -policy *policy-name*

   You can map up to 12 constituent volumes using the `cg-item-mappings` parameter on the `snapmirror create` command.

   The following example creates two consistency groups: `cg_src_` on the source with `vol1` and `vol2` and a mirrored destination consistency group, `cg_dst`.

   ```
   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
   ```

2. From the destination cluster, initialize the consistency group.

   ```
   destination::>snapmirror initialize -destination-path destination-
   consistency-group
   ```

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

   ```
   snapmirror show
   ```

4. On each cluster, create an igroup so you can map LUNs to the initiator on the application host.
   `lun igroup create -igroup *name* -protocol *fcp|iscsi* -ostype *os* -initiator *initiator_name*`

5. On each cluster, map LUNs to the igroup:

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

6. Verify the LUN mapping completed successfully with the `lun map` command. Then, you can discover the new LUNs on the application host.

Manage SM-BC and protect data

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.

About this task

- 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

In a planned failover, you switch the roles of the primary and secondary clusters, so that the secondary cluster takes over from the primary cluster. During a failover, what is normally the secondary cluster processes input and output requests locally without disrupting client operations.

You may want to perform a planned failover to test the health of your disaster recovery configuration or to perform maintenance on the primary cluster.

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.

Before you begin

- The SM-BC relationship must be in sync.
- You cannot initiate a planned failover when a nondisruptive operation is in process. Nondisruptive operations include volume moves, aggregate relocations, and storage failovers.
- The ONTAP Mediator must be configured, connected, and in quorum.

Steps

You can perform a planned failover using the ONTAP CLI or System Manager.

ONTAP CLI

1. From the destination cluster, initiate 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
   ```

System Manager

1. In System Manager, select **Protection > Overview > Relationships**.

2. Identify the SM-BC relationship you want to failover. Next to its name, select the … next to the relationship's name, then select **Failover**.

3. To monitor the status of the failover, use the `snapmirror failover show` in the ONTAP CLI.

Recover from automatic unplanned failover operations

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

> (i) 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.

Reestablish the protection relationship after an unplanned failover

You can reestablish the protection relationship using System Manager or the ONTAP CLI.

System Manager

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**.

CLI

You can monitor the status of the automatic unplanned failover 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: -
```

Refer to the EMS reference to learn about event messages and about corrective actions.

Resume protection in a fan-out configuration after failover

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

Steps

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`

Monitor SnapMirror Business Continuity operations

You can monitor the following SnapMirror Business Continuity (SM-BC) operations to ensure the health of your SM-BC configuration:

- ONTAP Mediator
- Planned failover operations
- Automatic unplanned failover operations
- SM-BC availability

ONTAP Mediator

During normal operations, the ONTAP 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.

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
```

Refer to the EMS reference to learn about event messages and corrective actions.

Automatic unplanned failover operations

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

```
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: -
```

Refer to the EMS reference to learn about event messages and about corrective actions.

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 or remove volumes to a consistency group

As your application workload requirements change, you may need to add or remove
volumes from a consistency group to ensure business continuity. The process of adding
and removing volumes in an an active SM-BC relationship depends on the version of
ONTAP you are using.

In most instances, this is a disruptive process requiring you to break the SnapMirror relationship, modify the
consistency group, then resume protection. Beginning with ONTAP 9.13.1, adding volumes to a consistency
group with an active SM-BC relationship is a non-disruptive operation.

About this task

- In ONTAP 9.8 through 9.9.1, you can add or remove volumes to a consistency group using the ONTAP CLI.

- Beginning with ONTAP 9.10.1, it is recommended that you manage consistency groups through System Manager or with the ONTAP REST API.

  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.

- Beginning in ONTAP 9.13.1, you can non-disruptively add volumes to a consistency group with an active SM-BC relationship from the source or destination.

  Removing volumes is a disruptive operation. You must break the SnapMirror relationship before proceeding removing volumes.

ONTAP 9.8-9.13.0

Before you begin

- You cannot begin to modify the consistency group while it 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

The examples shown in 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. On the source and destination clusters, verify there is a common Snapshot between the source and destination clusters with the command `snapshot show -vserver` *svm_name* `-volume` *volume_name* `-snapshot` *snapmirror*

   ```
   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 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. **If you are using ONTAP 9.10.1 through 9.13.0,** delete and recreate and the consistency group on

the source with the correct composition. Follow the steps in Delete a consistency group and then Configure a single consistency group. In ONTAP 9.10.1 and later, you must perform the delete and create operations in System Manager or with the ONTAP REST API; there is no CLI procedure.

If you are using ONTAP 9.8, 9.0, or 9.9.1, skip to the next step.

7. Create the new consistency group on the destination 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
```

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

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

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

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

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

ONTAP 9.13.1 and later

Beginning in ONTAP 9.13.1, you can non-disruptively add volumes to a consistency group with an active SM-BC relationship. SM-BC supports adding volumes from both the source or destination.

For details on adding volumes from the source consistency group, see Modify a consistency group.

Add a volume from the destination cluster

1. On the destination cluster, select **Protection** > **Relationships**.
2. Find the SM-BC relationship you want to add volumes to. Select ⋮ then **Expand**.
3. Select the volume relationships whose volumes are to be added to consistency group
4. Select **Expand**.

Convert existing relationships to SM-BC relationships

If you have an existing Synchronous SnapMirror relationship between a source and destination cluster, you can convert it to an SM-BC relationship. This allows you to associate the mirrored volumes with a consistency group, ensuring zero RPO across a multi-volume workload. Additionally, you can retain existing SnapMirror snapshots if you need to revert to a point in time prior to establishing the SM-BC relationship.

Before you begin

- A zero RPO Synchronous SnapMirror relationship must exist between the primary and secondary cluster.
- All LUNs on the destination volume must be unmapped before the zero RTO SnapMirror relationship can be 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 primary and secondary clusters.
- You cannot convert zero RPO to zero RTO sync by changing the SnapMirror policy.
- You must ensure the LUNs are unmapped before issuing the `snapmirror create` command.

  If existing LUNs on the secondary volume are mapped and the `AutomatedFailover` policy is configured, the `snapmirror create` will trigger an error.

Steps

1. From the secondary cluster, perform a SnapMirror update 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 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.

Upgrade and revert ONTAP with SM-BC

SnapMirror Business Continuity (SM-BC) is supported beginning with ONTAP 9.8.

Upgrading and reverting your ONTAP cluster has implications on your SM-BC relationships depending on the ONTAP version to which you are upgrading or reverting.

Upgrade ONTAP

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/Upgrade software on ONTAP clusters

> ⓘ The `snapmirror quiesce` and `snampirror resume` commands are not supported with SM-BC.

When you upgrade clusters from 9.8 or 9.9.1 to 9.10.1, ONTAP creates new consistency groups on both source and destination for SM-BC relationships. These can be managed in System Manager under the **Consistency Groups** option or using the ONTAP REST API with the consistency groups endpoint.

Revert 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 with an active SM-BC relationship cannot be deleted. 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 in ONTAP 9.10.1 and later.

Revert to ONTAP 9.7 from ONTAP 9.8

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

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

- If the cluster host an SM-BC destination, reverting to ONTAP 9.7 is not allowed until the relationship is broken and deleted.
- If the cluster hosts 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.

To meet these requirements, see Remove an SM-BC configuration.

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

If you no longer require zero RTO Syncronous SnapMirror protection, you can delete your SM-BC relationship.

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. From the secondary cluster, remove 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 primary 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
```

Troubleshoot

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:

A 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.

ONTAP 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 the ONTAP Mediator is not configured, you must configure the ONTAP 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. For more information, see Configure the ONTAP Mediator.

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:

The ONTAP 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 ONTAP Mediator is not configured on Site B.

Solution:

Ensure that ONTAP 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 ONTAP 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.