ONTAP System Manager docs

ONTAP System Manager

NetApp
December 07, 2020

This PDF was generated from https://docs.netapp.com/us-en/ontap/index.html on December 07, 2020. Always
check docs.netapp.com for the latest.

Table of Contents

Documentation for the SnapMirror Business Continuity solution

This site contains the documentation for the NetApp SM-BC solution available with ONTAP 9.8.

Introduction

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

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.
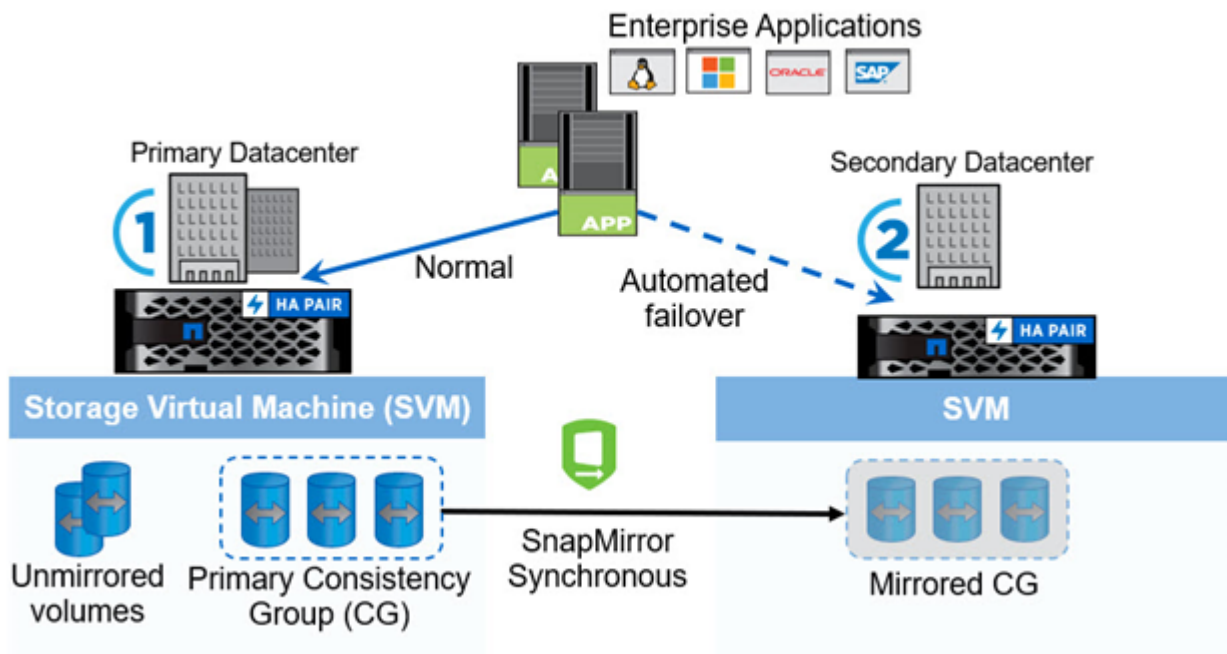
Key terminology

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

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

External software installed in a standalone server or in a VM. It is a monolithic process that is required to complete a quorum for SM-BC deployment. Mediator is used for health checking and to establish a consensus across a 3-party quorum where the other two parties are the two clusters hosting the SM-BC primary CG and mirror CG copies. Both are used interchangeably.

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.

Role of 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.

Basic failover and recovery concepts

It might be helpful to understand some of the basic SM-BC failover and recovery concepts.

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.

Additional information

For more information about data protection using SnapMirror Synchronous, see the following documentation:

[SnapMirror Synchronous disaster recovery basics](#)

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:
  - RedHat Enterprise Linux 7.6 or 7. 7
  - CentOS 8.0 or 8.1

Licensing

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

> ℹ️ 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

Supported protocols

- Only SAN protocols are supported (not NFS/CIFS)
- Only Fibre Channel and iSCSI protocols are supported

ONTAP Mediator

- Must be provisioned externally and attached to ONTAP for transparent application failover

Large LUNs and large volumes

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

  ℹ️ 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.

AppDM Application volumes

Volumes associated with an AppDM Application are not supported with SM-BC. Before creating an SM-BC relationship for a set of volumes, make sure that none of the volumes are associated with an AppDM Application.

  ℹ️ In ONTAP 9.8 RC releases, SM-BC does not automatically check before creating a relationship with a set of AppDM Application volumes.

Additional restrictions and limitations

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

Consistency groups

The maximum number of SnapMirror Synchronous consistency group relationships in a cluster is five, a limit which is platform-independent. If you reach or attempt to exceed this limit, the following message is displayed:

```
The number of SnapMirror Synchronous consistency group relationships in a cluster cannot
exceed 5
```

Volumes per consistency group

The maximum number of volumes supported per SnapMirror Synchronous consistency group relationship is twelve, a limit which is platform-independent. If you reach or attempt to exceed this limit, the following message is displayed:

```
The number of volumes in a SnapMirror Synchronous Consistency Group cannot exceed 12
```

Volumes

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
1	AFF	60	80
2	ASA	60	80

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
Inter-cluster LIFs per cluster	8

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.

ℹ️ 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 ONTAP 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 ONTAP 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 or click NetApp DevNet ONTAP REST API.

Preparing 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.

> ℹ️ 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

Command	Description
snapmirror release	Remove source information for a SnapMirror relationship

Preparing 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 avoids 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 Installing or upgrading 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

Installation and setup

High level deployment workflow

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

Plan the deployment and prepare the environment.

↓

Install the ONTAP Mediator on a Linux machine.

↓

Confirm that the cluster is properly configured.

↓

Initialize the ONTAP Mediator.

↓

Create a consistency group relationship.

↓

Initialize and review the consistency group.

↓

Map the LUNs to the application host.
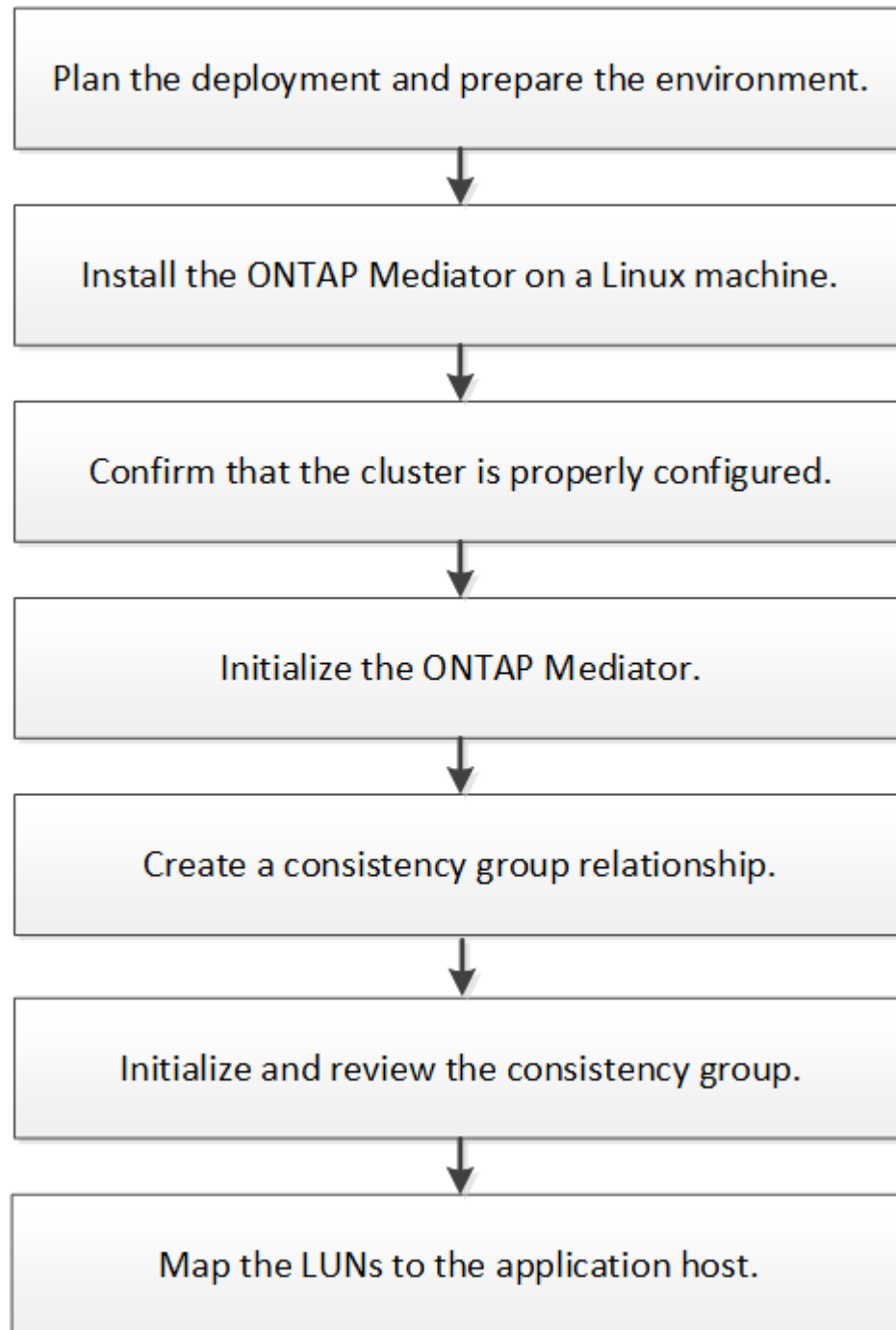
Installing the ONTAP Mediator

You must install the ONTAP Mediator, which includes accepting the licensing agreement, before you can configure and use the SnapMirror Business Continuity solution.

Before you begin

The following software is required:

- ONTAP Mediator 1.2 or later
- One of the following Linux distributions:
    - RHEL 7.6 or 7.7
    - CentOS 8.0 or 8.1

About this task

You should install the ONTAP Mediator at an external site that is physically separated from the two ONTAP clusters.

For complete installation instructions, see Installing or upgrading the ONTAP Mediator service

Steps

1. Sign into the Linux system that will host the ONTAP Mediator.

2. Download the mediator installation package from the ONTAP Mediator page.

   NetApp Downloads: ONTAP Mediator.

3. Install the ONTAP Mediator and respond to all prompts as required:

   `./ontap-mediator_1.2`

4. Optionally replace the self-signed SSL and certificate authority (CA) with the third party validated SSL Certificate and CA. Copy the contents of the ca.crt file from the ONTAP Mediator directory:

   `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`

5. At the ONTAP CLI, install the certificate on both the local and peer cluster:

   `security certificate install -type server-ca -vserver cserverName`

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

   Configure peer relationships

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

   Creating an SVM

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

   Creating an SVM peering relationship

4. Confirm that the volumes exist for your LUNs.

   Creating and managing volumes

5. 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

6. 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

7. 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.

Creating a consistency group relationship

You must create a SnapMirror consistency group which also establishes the synchronous consistency group relationship.

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

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: srccg with constituent volumes vol1 and vol2, and dstcg 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
   ```

Initializing a consistency group

After creating a consistency group, you must initialize it.

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 so you can map LUNs to the initiator on the application host.

About this task

You should perform this configuration at the source cluster.

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

Creating 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.

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
   ```

Performing 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.

> ℹ️ 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
sm.mediator.removed.force	Mediator is removed from the cluster using the "force" option

EMS Name	Description
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. Destination path:	SMBC planned failover operation started
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
```

Adding and removing 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.

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

1. Delete the zero RTO consistency group relationship:

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

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

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

3. 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_src2:@vol_dst2
   ```

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

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

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

Converting 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

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.

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

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 <vserver-name> -policy <policy-name>
```

Removing 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:

    ```
    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.

Removing 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

Failure creating a SnapMirror relationship and initializing consistency group

Issue:

Creation of SnapMirror relationship and consistency group initialization fails.

Error message:

```
command failed: The number of SnapMirror Synchronous Consistency Group
relationships in a cluster cannot exceed 5
```

Solution:

Ensure that the configuration has no more than 5 consistency groups. See Additional restrictions and limitations.

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. (I WILL ADD LINK TO COMMAND ONCE TOPIC IS IN GITHUB)

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

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

Determining the cause:

Check the status of Mediator from Site A.

Example:

```
C1_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster    Connection Status Quorum Status
--------------- --------------- ---------------- -------------
10.237.86.17    C2_cluster      unreachable      true

C1_cluster::*> snapmirror list-destinations
                                         Progress
Source             Destination      Transfer Last       Relationship
Path        Type Path          Status Progress Updated    Id
----------- ----- ----------- ------- --------- ----------- ---------------
vs0:/cg/src_cg_1  XDP   vs1:/cg/dst_cg_1  OutOfSync  -        -          bba7d354-
06f6-11eb-9138-005056acec19
```

Check Site B connectivity:

```
C1_sti78-vsim-ucs188a_cluster::*> cluster peer show
Peer Cluster Name          Cluster Serial Number Availability   Authentication
------------------------   --------------------  -------------- --------------
C2_cluster                 1-80-000011           Unavailable    ok
```

Check the consensus status on SM-BC volume:

```
C1_cluster::*> volume show zrto_cg_894191_188b_RW1 -fields smbc-consensus
vserver volume                  smbc-consensus
------- ----------------------- ------------------
vs0     zrto_cg_894191_188b_RW1 Awaiting-consensus
```

Solution:

Complete the following steps to override SM-BC consensus and forcefully resume I/O on Site A:

1. Unmap the LUNs on Site A.

2. Issue the snapmirror release command using the `-force` and `override-smbc-consensus` option on Site A.

3. Remap the LUNs.

4. First, bring up Mediator, and then bring up the Site B nodes.

5. Resync the consistency group relationship using `snapmirror resync`.

6. After Site B is up, verify that the consistency group relationship is up and is in sync.

7. Perform a LUN rescan on the host to restore all paths to the LUNs.

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.