



ONTAP System Manager docs

ONTAP System Manager

NetApp

November 19, 2020

This PDF was generated from <https://docs.netapp.com/us-en/ontap/index.html> on November 19, 2020. Always check docs.netapp.com for the latest.



Table of Contents

- Documentation for the SnapMirror Business Continuity solution 1
- Planning 2
 - Prerequisites 2
 - Additional restrictions and limitations 3
 - ONTAP access options 4
 - Preparing to use the ONTAP CLI 5
 - Preparing to use the ONTAP Mediator 5
 - Summary of deployment best practices 6
- Installation and setup 7
 - High level deployment workflow 7
 - Installing the ONTAP Mediator 8
 - Confirm the ONTAP cluster configuration 8
 - Initialize the ONTAP Mediator 9
 - Creating a consistency group relationship 10
 - Initializing a consistency group 11
 - Mapping LUNs to the application hosts 11
- Administration 13
 - Creating a common Snapshot copy 13
 - Performing a planned failover 13
 - Automatic unplanned failover operations 14
 - Basic monitoring 14
 - Adding and removing volumes in a consistency group 17
 - Converting existing relationships to SM-BC relationships 18

Documentation for the SnapMirror Business Continuity solution

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

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



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 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

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.



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 limit is on the number of endpoints and not the number of relationships. A consistency group with 12 volumes contributes 12 endpoints on both the source and destination. A SnapMirror Synchronous relationship with both source and destination volumes on the same HA pair contributes 2 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
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.



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.

For more information, see [NetApp Documentation: ONTAP 9](#).

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

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 avoid split-brain scenarios when each cluster simultaneously tries to establish control as the primary cluster.

Prerequisites for the ONTAP Mediator

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

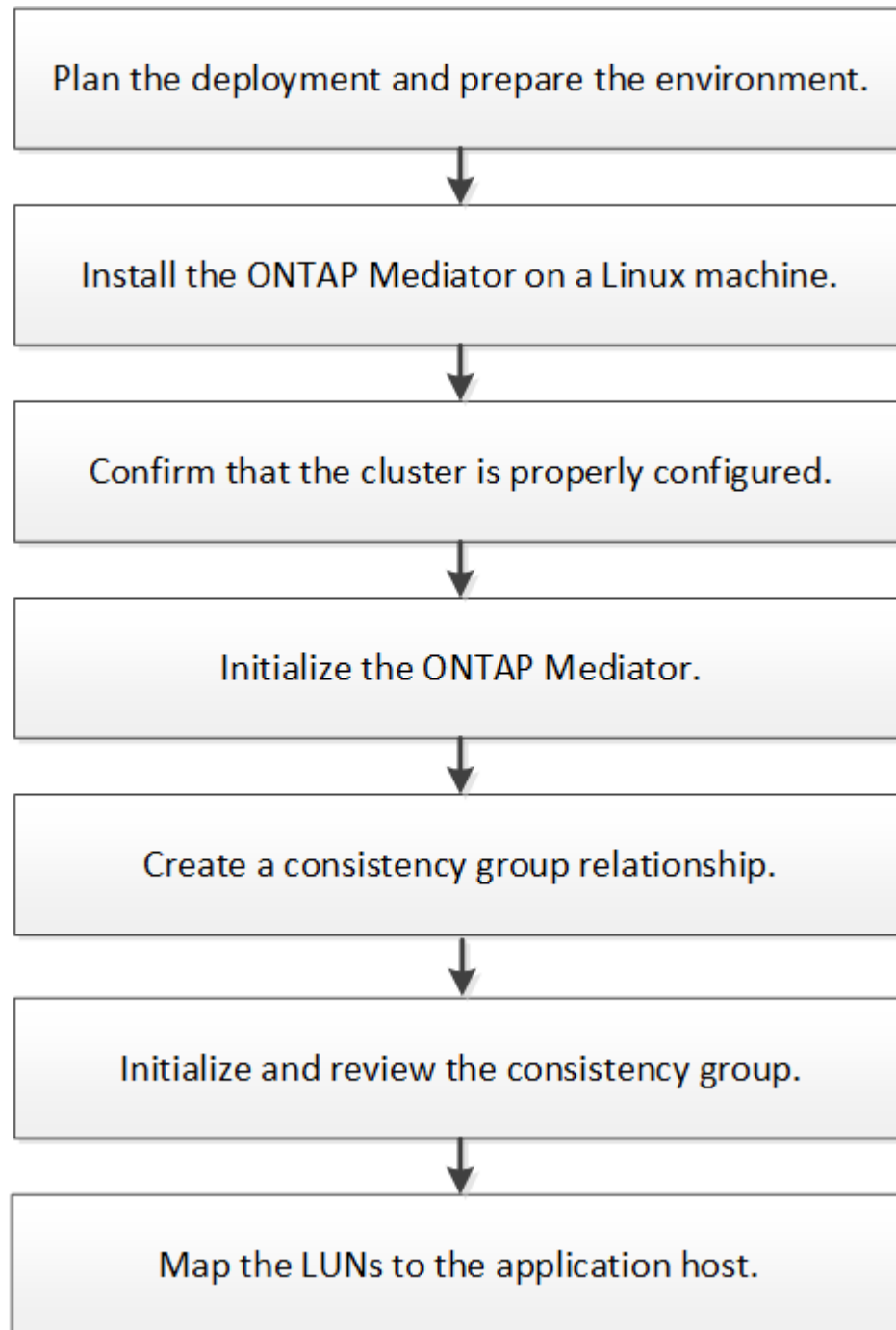
You should terminate an SnapMirror relationship in the following order:

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.



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
```

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

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

Automatic unplanned failover operations

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



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

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

Basic monitoring

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

ONTAP mediator

During normal operation, the Mediator state should be connected. If it is in any other state, this might indicate an error condition. You can review the 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
```

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: -
```

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

Source          Destination Mirror Relationship Total Progress 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
```

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. Quiesce each of the zero RPO synchronous relationships:

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

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

2. Delete each of the zero RPO synchronous relationships:

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

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

3. 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
```

4. 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
```

5. Resynchronize the zero RTO consistency group:

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

Copyright Information

Copyright © 2020 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

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

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

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

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

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

Trademark Information

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