

IBM System Storage N series



Clustered Data ONTAP 8.2 SnapMirror Intercluster Failover and Resync Express Guide

Contents

Preface	v
About this guide	v
Supported features	v
Websites.	v
Getting information, help, and service	vi
Before you call	vi
Using the documentation	vi
Hardware service and support	vi
Firmware updates	vi
How to send your comments	vii
Deciding whether to use this guide	1
Preparing for an intercluster volume SnapMirror failover event	3
Monitoring the status of SnapMirror data transfers	3
SnapMirror intercluster failover and resync workflow	7
How SnapMirror failover and resync works in System Manager	7
Verifying the status of a source volume in a SnapMirror relationship	10
Breaking SnapMirror relationships.	12
Verifying destination volume settings after breaking a SnapMirror relationship	14
Reverse resynchronizing SnapMirror relationships	16
Updating SnapMirror relationships	18
Returning a recovered volume to the source role	20
Where to find additional information	25
Copyright and trademark information	27
Trademark information	28
Notices	29
Index	31

Preface

About this guide

This document applies to IBM N series systems running Data ONTAP, including systems with gateway functionality. If the terms *Cluster-Mode* or *clustered Data ONTAP* are used in this document, they refer to the Data ONTAP features and functionality designed for clusters, which are different from 7-Mode and prior Data ONTAP 7.1, 7.2, and 7.3 release families.

In this document, the term *gateway* describes IBM N series storage systems that have been ordered with gateway functionality. Gateways support various types of storage, and they are used with third-party disk storage systems—for example, disk storage systems from IBM, HP®, Hitachi Data Systems®, and EMC®. In this case, disk storage for customer data and the RAID controller functionality is provided by the back-end disk storage system. A gateway might also be used with disk storage expansion units specifically designed for the IBM N series models.

The term *filer* describes IBM N series storage systems that either contain internal disk storage or attach to disk storage expansion units specifically designed for the IBM N series storage systems. Filer storage systems do not support using third-party disk storage systems.

Supported features

IBM System Storage N series storage systems are driven by NetApp Data ONTAP software. Some features described in the product software documentation are neither offered nor supported by IBM. Please contact your local IBM representative or reseller for further details.

Information about supported features can also be found on the N series support website (accessed and navigated as described in Websites).

Websites

IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. The following web pages provide N series information:

- A listing of currently available N series products and features can be found at the following web page:
www.ibm.com/storage/nas/
- The IBM System Storage N series support website requires users to register in order to obtain access to N series support content on the web. To understand how the N series support web content is organized and navigated, and to access the N series support website, refer to the following publicly accessible web page:
www.ibm.com/storage/support/nseries/
This web page also provides links to AutoSupport information as well as other important N series product resources.
- IBM System Storage N series products attach to a variety of servers and operating systems. To determine the latest supported attachments, go to the IBM N series interoperability matrix at the following web page:

www.ibm.com/systems/storage/network/interophome.html

- For the latest N series hardware product documentation, including planning, installation and setup, and hardware monitoring, service and diagnostics, see the IBM N series Information Center at the following web page:
publib.boulder.ibm.com/infocenter/nasinfo/nseries/index.jsp

Getting information, help, and service

If you need help, service, or technical assistance or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you. This section contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your IBM N series product, and whom to call for service, if it is necessary.

Before you call

Before you call, make sure you have taken these steps to try to solve the problem yourself:

- Check all cables to make sure they are connected.
- Check the power switches to make sure the system is turned on.
- Use the troubleshooting information in your system documentation and use the diagnostic tools that come with your system.
- Refer to the N series support website (accessed and navigated as described in Websites) for information on known problems and limitations.

Using the documentation

The latest versions of N series software documentation, including Data ONTAP and other software products, are available on the N series support website (accessed and navigated as described in Websites).

Current N series hardware product documentation is shipped with your hardware product in printed documents or as PDF files on a documentation CD. For the latest N series hardware product documentation PDFs, go to the N series support website.

Hardware documentation, including planning, installation and setup, and hardware monitoring, service, and diagnostics, is also provided in an IBM N series Information Center at the following web page:

publib.boulder.ibm.com/infocenter/nasinfo/nseries/index.jsp

Hardware service and support

You can receive hardware service through IBM Integrated Technology Services. Visit the following web page for support telephone numbers:

www.ibm.com/planetwide/

Firmware updates

IBM N series product firmware is embedded in Data ONTAP. As with all devices, ensure that you run the latest level of firmware. Any firmware updates are posted to the N series support website (accessed and navigated as described in Websites).

Note: If you do not see new firmware updates on the N series support website, you are running the latest level of firmware.

Verify that the latest level of firmware is installed on your machine before contacting IBM for technical support.

How to send your comments

Your feedback helps us to provide the most accurate and high-quality information. If you have comments or suggestions for improving this document, please send them by email to starpubs@us.ibm.com.

Be sure to include the following:

- Exact publication title
- Publication form number (for example, GC26-1234-02)
- Page, table, or illustration numbers
- A detailed description of any information that should be changed

Deciding whether to use this guide

This guide describes how to quickly fail over an asynchronous disaster recovery (ADR) SnapMirror relationship from a source volume on one cluster to a destination volume on a different cluster, and then return the recovered source volume to read/write status.

You should use this guide if you want to perform a volume-level disaster recovery procedure and do not want a lot of conceptual background for the tasks.

The instructions in this guide are implemented using OnCommand System Manager to perform the disaster recovery actions.

This guide is based on the following assumptions:

- You are a cluster administrator with appropriate privileges.
- You have downloaded and are running System Manager 3.0 or later.
- You have the same versions of clustered Data ONTAP installed on both the source and destination clusters.
- You are using FlexVol volumes and not an Infinite Volume.
- You are operating in a NAS environment.
- You have configured your source and destination volumes in a SnapMirror relationship between peered clusters.
- You have configured your peered clusters and Vservers following the instructions in the *Data ONTAP Cluster and Vserver Peering Express Guide*.
- You have configured your SnapMirror relationships following the instructions in the *SnapMirror Intercluster Configuration Express Guide* and the destination volume is ready to be put into production immediately if the source becomes unavailable.

If these assumptions are not correct for your situation, or if you want more conceptual background information, you should see the following documentation instead, available from the IBM N series support website (accessed and navigated as described in Websites):

- *Clustered Data ONTAP Data Protection Guide*
- *Clustered Data ONTAP Logical Storage Management Guide*
- *SnapMirror Configuration and Best Practices Guide for Clustered Data ONTAP 8.2 (Technical Report-4015)*

Note: This technical report contains information about NetApp products that IBM licenses and in some cases customizes. Technical reports might contain information about models and features that are not supported by IBM.

Related information:

 IBM N series support website: www.ibm.com/storage/support/nseries

Preparing for an intercluster volume SnapMirror failover event

To properly protect your data, you should configure your cluster environment and SnapMirror relationships according to IBM requirements and best practices. You should also regularly monitor your peer relationships and SnapMirror relationships to ensure that they are ready for failover before a disaster recovery event actually occurs.

SnapMirror configuration considerations

For failover and resynchronization of your data to occur properly in case of a disaster, you must ensure that your environment is configured according to IBM requirements and best practices.

Attention: Failure to properly configure your environment or your SnapMirror relationships can result in data loss if a failover occurs.

See the following documentation for more information:

- *Data ONTAP Cluster and Vserver Peering Express Guide*
- *SnapMirror Intercluster Configuration Express Guide*

Maintaining SnapMirror relationships

After your SnapMirror relationships are created and properly configured, you need to ensure that the relationships remain healthy and that the destination volume remains available for read/write access in case the source volume becomes unavailable.

See *Monitoring the status of SnapMirror data transfers* for information about how to monitor peered clusters and volumes and verify the status of SnapMirror relationships.

Monitoring the status of SnapMirror data transfers

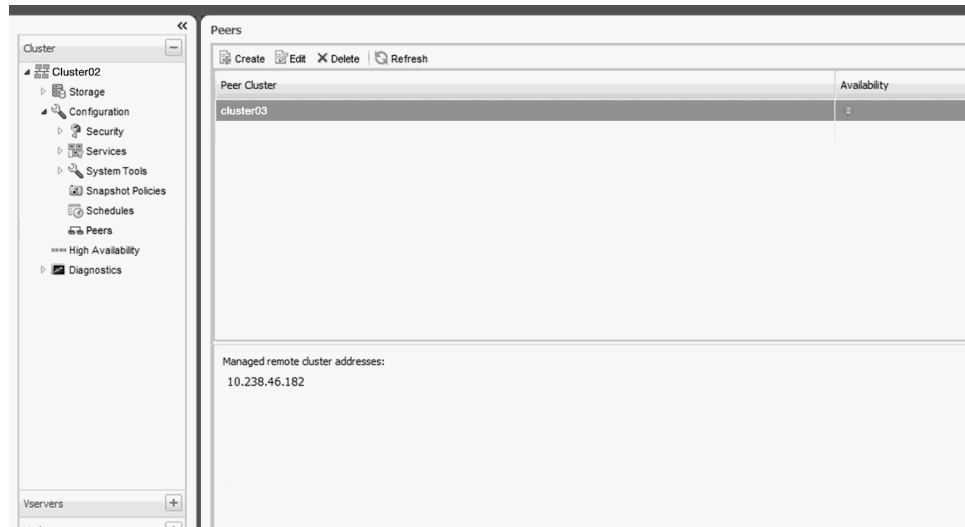
You should periodically monitor the status of SnapMirror relationships, including the status of the cluster peer and Vserver peer relationships, to ensure that the SnapMirror data transfers are occurring per the specified schedule.

About this task

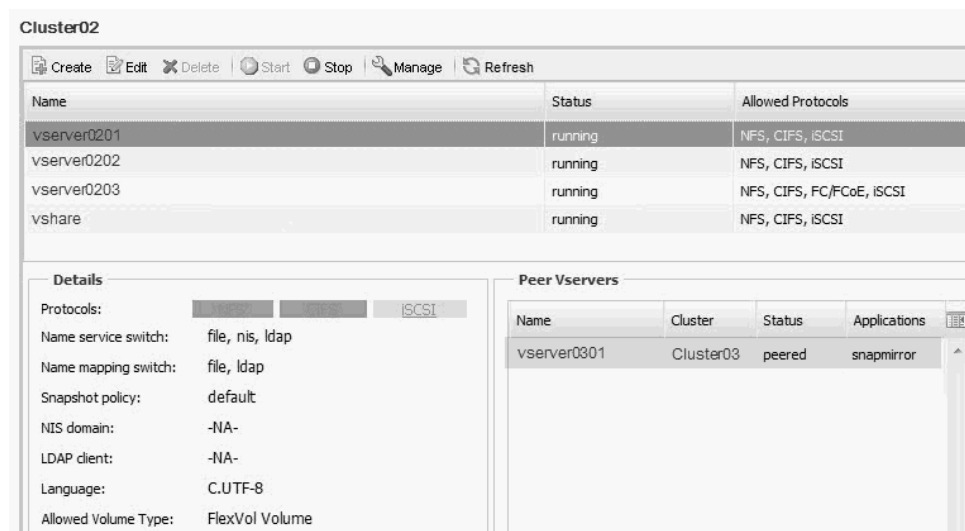
You can perform this task either from the source or destination cluster.

Procedure

1. From the System Manager home page, double-click the appropriate cluster.
2. Expand the **Cluster** hierarchy in the left navigation pane.
3. Click **Configuration > Peers**, and then verify that the peer cluster is available.









4. Expand the **Vservers** hierarchy in the left navigation pane.
5. Select the source Vserver from the “Vservers window,” and then verify that the peer relationship with the destination Vserver is in the peered state.






6. Click **Protection**, and then verify the status of the SnapMirror relationships in the Details section. The Details section displays the health status of the SnapMirror relationship, and also shows the transfer errors and lag time.
 - The **Is Healthy** field must display **Yes**.
For most SnapMirror data transfer failures, the **Is Healthy** field displays **No**. In some failure cases, however, the **Is Healthy** field continues to display **Yes**. You must check the transfer errors in the Details section to be certain that no SnapMirror data transfer failure occurred.
 - The **Relationship State** field must either display **Uninitialized** or **Snapmirrored**.
 - The **Lag Time** must be no more than two times the transfer schedule.
For example, if the SnapMirror relationship is assigned a transfer schedule of **hourly**, the transfer occurs once every day at 05 minutes past the hour. The lag time should be no more than 2 hours since the last transfer.

Protection

 If you have upgraded from Data ONTAP 8.1.x to 8.2, you must upgrade the SnapMirror relationships through the CLI to view the relationships.

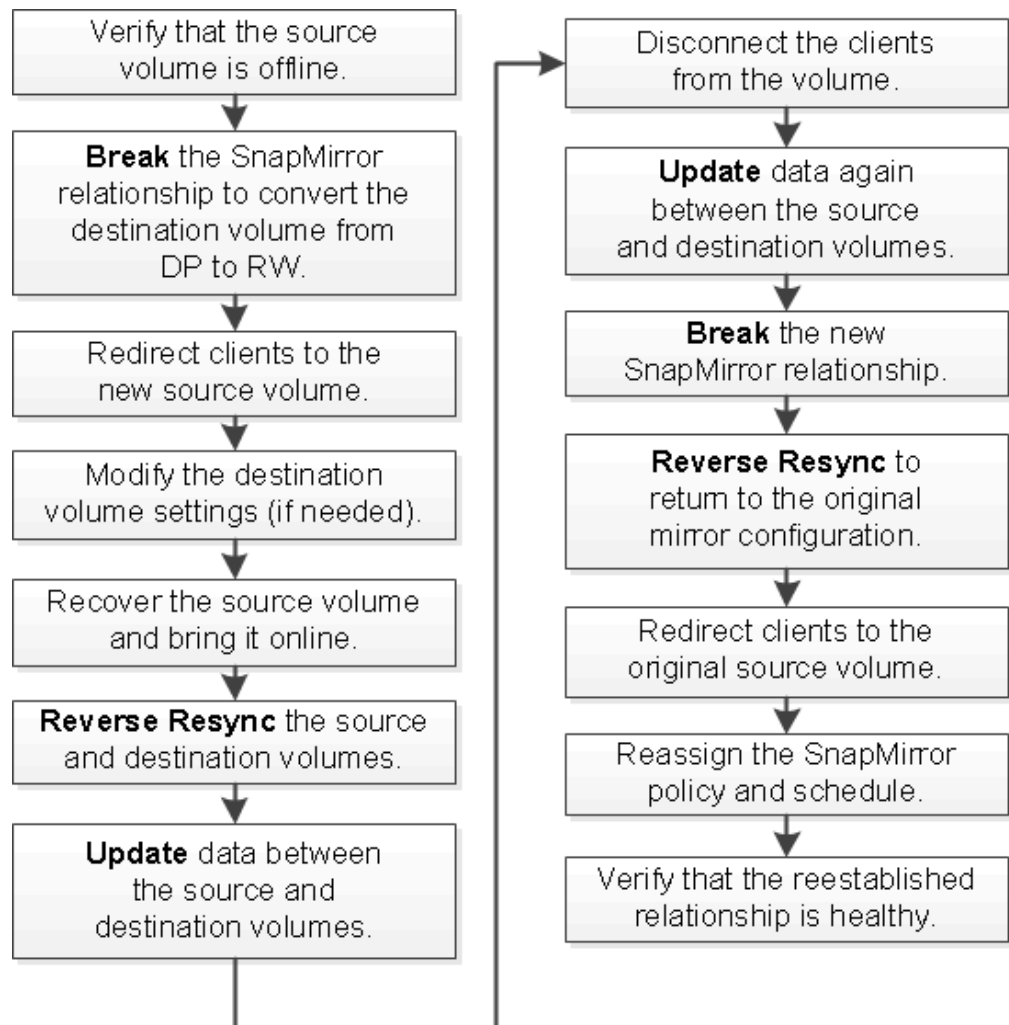
 Create ▾
  Edit
  Delete
  Operations ▾
  Refresh

Source Vserver	Source Volume	Destination Volume	Is Healthy	Relationship State	Transfer Status	Type	Lag Time
vserver0201	vol05src	vol05dest	 Yes	Snapmirrored	Idle	Mirror	0 day(s) 0 hr(s) 33 min(s)
vserver0201	vol06src	vol06dest	 Yes	Snapmirrored	Idle	Mirror	0 day(s) 56 min(s)

Source Location: vserver0201:vol05src Is Healthy:  Yes Transfer Status: Idle
 Destination Location: vserver0301:vol05dest Relationship State: Snapmirrored Current Transfer Type: None
 Source Cluster: Cluster02 Current Transfer Error: None
 Destination Cluster: Cluster03 Last Transfer Error: None
 Transfer Schedule: Hourly Last Transfer Type: Initialize
 Data Transfer Rate: Unlimited Latest Snapshot Timestamp: 08/29/2013 12:43:43
 Lag Time: 0 day(s) 0 hr(s) 33 min(s) Latest Snapshot Copy: snapmirror_1576e897-0e123478563412_2147484

SnapMirror intercluster failover and resync workflow

When a source volume becomes unavailable for read/write access, you can perform a volume-level disaster recovery failover and resynchronization from OnCommand System Manager. This functionality is available from the Protection page of the destination Vserver.

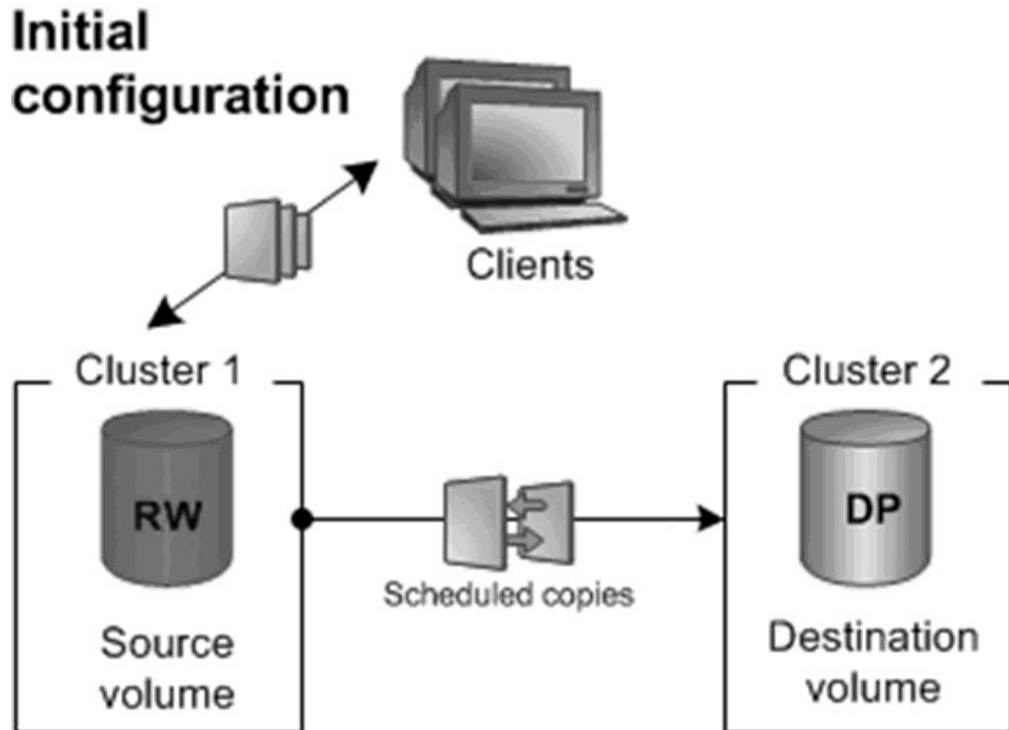


SnapMirror relationships are managed from the destination cluster. Therefore, in System Manager the **Break**, **Reverse Resync**, and **Update** options are accessed from the **Operations** menu on the Protection page of the Vserver that contains the destination volume.

How SnapMirror failover and resync works in System Manager

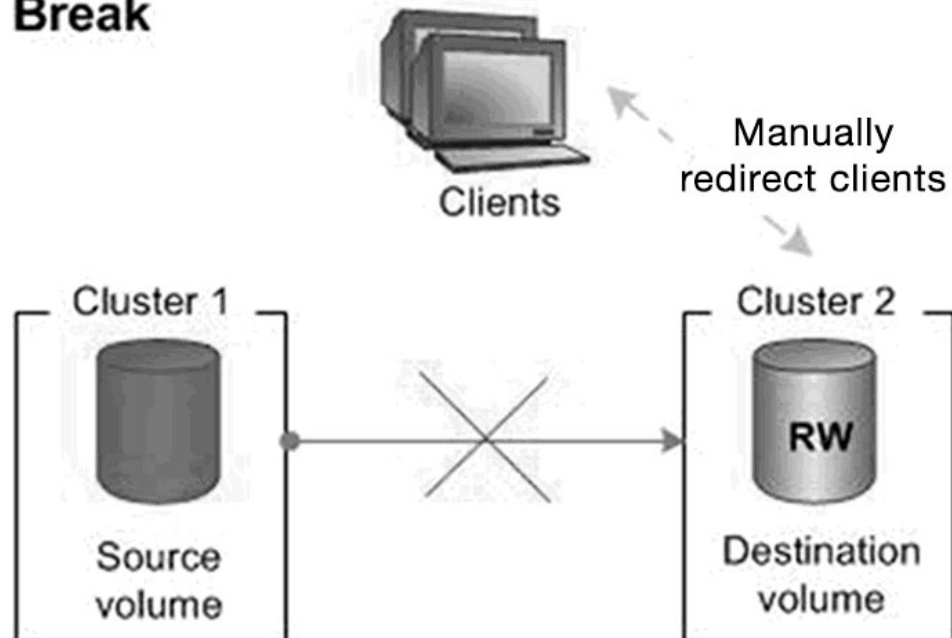
System Manager simplifies the process of failing over and resynchronizing a SnapMirror relationship by grouping the Data ONTAP commands into three options: **Break**, **Reverse Resync**, and **Update**.

In a functioning intercluster SnapMirror relationship, the source volume is located on one cluster and the destination volume is located on another cluster. Client applications perform read/write actions only on the source volume. Data on the source is mirrored to the destination volume. The destination volume is configured for data protection (DP), which makes the volume read-only for clients.



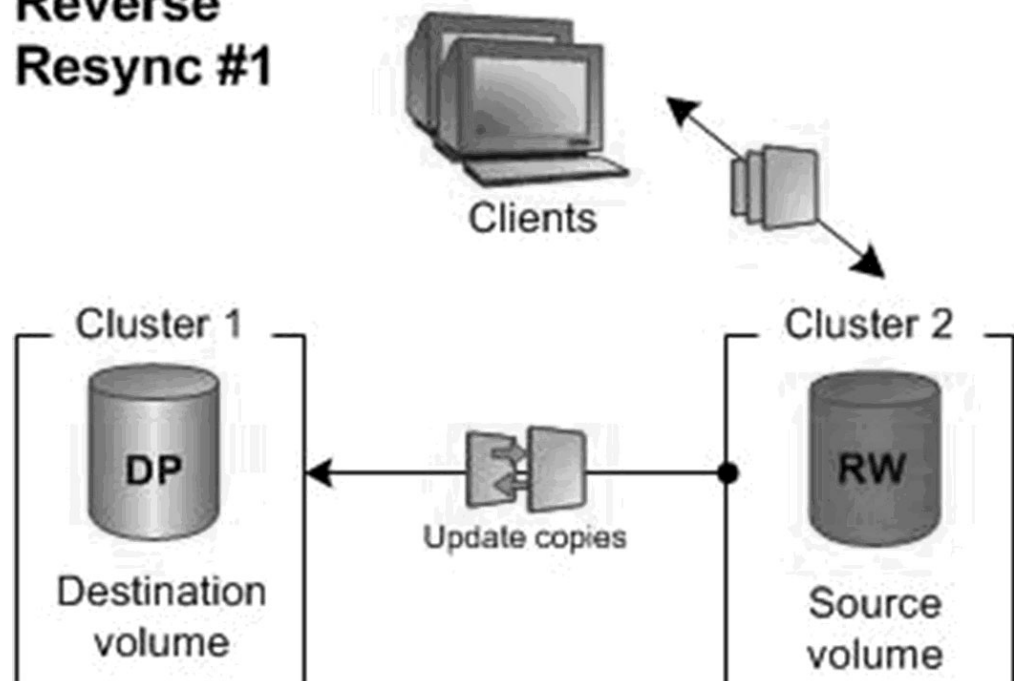
When you use the **Break** option in System Manager, data transfers discontinue between the source and destination volumes, and the destination volume converts to read/write status. Clients that were accessing the original source volume must be manually redirected to read and write data to the destination volume.

Break

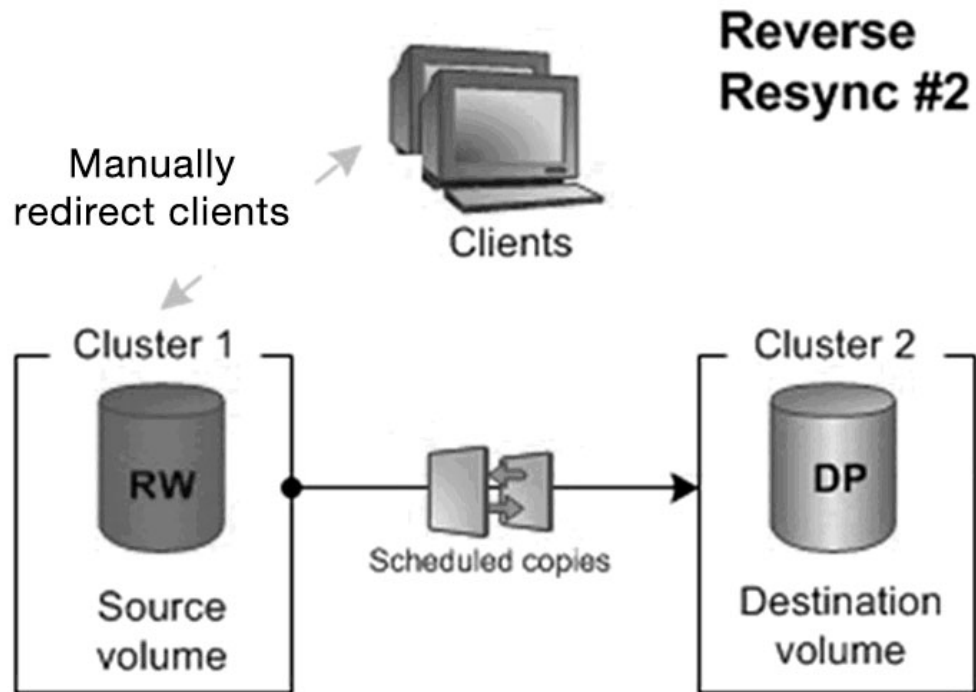


When the problem with the original source volume is resolved and the original source is brought online and put into production, the destination volume must take over the source volume role. The **Reverse Resync** option deletes and releases the old relationship, creates the new relationship by reversing the roles of the original source and destination volumes, and establishes a base Snapshot copy on the new source volume.

Reverse Resync #1



After the relationship is reversed, you can use the **Update** option to copy all new data from the source to the destination volume. Stop client read/write access and select **Update** again to copy any new data written to the source during the previous update. If you want to return the original source volume to its original role, you would again perform a **Break** and **Reverse Resync** on the new SnapMirror relationship. The second **Reverse Resync** returns the original source volume to read/write status and returns the new source volume to the original destination role.



After the new source volume is returned to the original destination role, you must redirect clients to the original source and verify that the reestablished relationship is healthy and that clients can read and write data to the source volume.

Verifying the status of a source volume in a SnapMirror relationship

If you have a problem with a SnapMirror relationship, you can view and modify details about the source volume from the Volumes window. You can also get details about the SnapMirror relationship, such as the names of the destination Vserver and destination volume.

About this task

This task is performed on the cluster that contains the source volume in the SnapMirror relationship.

Procedure

1. From the home page, double-click the appropriate storage system.
2. Expand the **Vservers** hierarchy in the navigation pane.

3. Select the Vserver that contains the source volume, and then click **Storage > Volumes**.



4. Select the source volume in the Volumes list and verify that the source volume is offline.

Volumes

Name	Aggregate	Status	Thin Provisioned	% Used	Available Space	Total Space	Storage Efficiency
root_vol	aggr_3_4_5A...	online	No	5	15.8/MB	20 MB	Disabled
source_vol	aggr_1_2_3A...	offline	-NA-	-NA-	-NA-	-NA-	Enabled
vo1	aggr_1_2_3A...	online	Yes	5	15.85 MB	20 MB	Disabled

5. Click the **Data Protection** bottom tab to display the name of the destination volume in the SnapMirror relationship, and the name of the Vserver that the volume resides on.

Destination Vserver	Destination Volume	Is Healthy	Relationship State	Transfer Status	Type	Lag Time	Policy
dest_vserver	dest_vol	Yes	Broken Off	Idle	Mirror	None	DPDefault

Details Space Allocation Snapshot Copies Storage Efficiency **Data Protection**

What to do next

You must next access the cluster that contains the destination volume and break the SnapMirror relationship so that the destination volume is available for read/write access.

Breaking SnapMirror relationships

If a SnapMirror source volume becomes unavailable and you want to access the data from the SnapMirror destination volume, you must break the SnapMirror relationship. Access to the destination volume is changed from data protection (DP) to read/write (RW).

Before you begin

- The SnapMirror destination volume must be in the quiesced or idle state.
- The destination volume must be premounted into the destination Vserver namespace.
- Protocol access, such as CIFS, NFS, and iSCSI, must be configured on the destination Vserver to enable client access.

About this task

You can use the destination volume to serve data while you repair or replace the source, until you can reestablish the original SnapMirror relationship configuration.

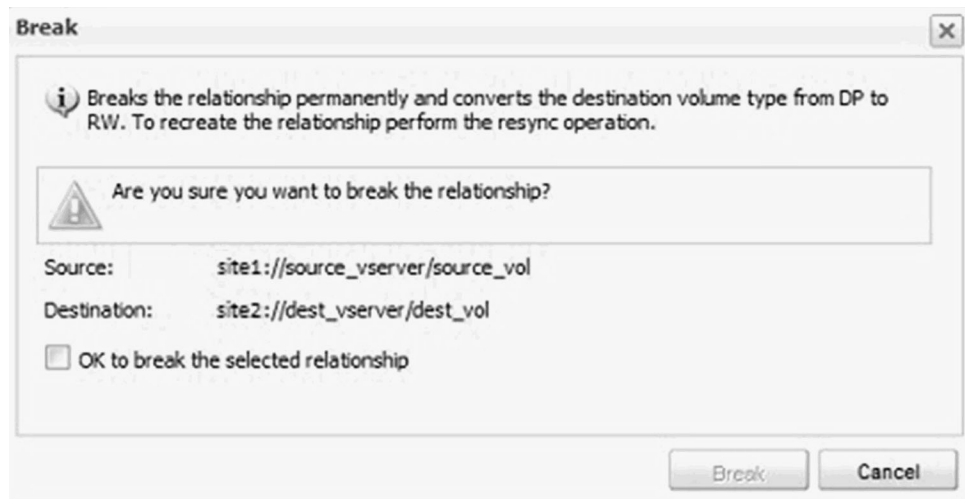
SnapMirror relationships are listed and managed from the Vserver that contains the *destination* volume.

Procedure

1. From the home page, double-click the appropriate storage system.
2. Expand the **Vservers** hierarchy in the left navigation pane.
3. Select the Vserver that contains the destination volume, and then click **Protection**.



4. Select the SnapMirror relationship that you want to break and verify that the Transfer Status column displays either Idle or Quiesced. If the relationship needs to be quiesced, click **Operations > Quiesce**.
5. Click **Operations > Break**.
6. Select the confirmation check box, and then click **Break**.



7. Verify that the Relationship State column displays Broken Off.

Protection

If you have upgraded from Data ONTAP 8.1.x to 8.2, you must upgrade the SnapMirror relationships through the CLI to view the relationships.

Source Vserver	Source Volume	Destination Volume	Is Health	Relationship State	Transfer Status	Type	Lag Time	Policy
source_vserver	source_vol	dest_vol	Yes	Broken Off	Idle	Mirror	None	DPDefault

8. Redirect client applications to the destination volume. The procedures for redirecting clients vary depending on the configuration of your environment. See the Data ONTAP documentation for more information.

Results

The SnapMirror relationship is broken. The destination volume type changes from data protection (DP) read-only to read/write (RW). The system stores the base Snapshot copy for the data protection mirror relationship for later use.

What to do next

The best practice is to pre-mount the destination NAS volumes into the destination Vserver namespace as part of your disaster recovery configuration. If this was not done, you need to mount the volumes after breaking the SnapMirror relationship, to ensure that the volumes are accessible on the destination. You mount them into the namespace using the same junction path that the source volume was mounted to in the source Vserver. For details, see the task for mounting FlexVol volumes in the System Manager online Help.

Related information:

 IBM N series support website: www.ibm.com/storage/support/nseries

Verifying destination volume settings after breaking a SnapMirror relationship

After breaking a SnapMirror relationship, you should verify that the destination type has changed from DP (data protection) to RW (read/write). You should also verify that settings that are enabled on the source, such as storage efficiency and thin provisioning, are enabled on the destination.

About this task

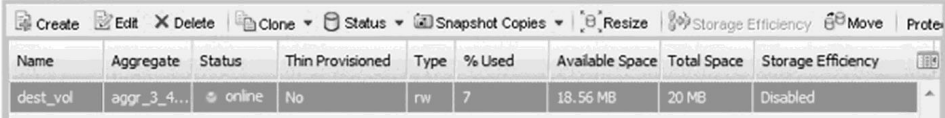
- This task is performed on the cluster that contains the destination volume in the SnapMirror relationship.
- Functionality such as storage efficiency and thin provisioning cannot be enabled on a volume of type DP.

If this functionality is enabled on the source volume but not on the destination, you need to enable it after the destination volume is converted to RW.

Procedure


1. From the home page, double-click the appropriate storage system.
2. Expand the **Vservers** hierarchy in the navigation pane.
3. Select the Vserver that contains the destination volume, and then click **Volumes**.
4. Verify that “rw” is displayed in the Type column for the destination volume. The Type column is not displayed by default. You might need to add the Type column from the column selector drop-down list.

Volumes



Name	Aggregate	Status	Thin Provisioned	Type	% Used	Available Space	Total Space	Storage Efficiency
dest_vol	aggr_3_4...	online	No	rw	7	18.56 MB	20 MB	Disabled

5. Verify that the volume settings on the destination volume match the settings on the source volume. If capabilities such as thin provisioning, deduplication, compression, autogrow, and so forth are enabled on the source volume, they should be enabled on the destination volume. If they are not, modify the settings by doing the following:
 - a. Click **Edit**.
 - b. Modify the General, Storage Efficiency, and Advanced settings as appropriate for your environment.



Edit Volume

General | Storage Efficiency | Advanced

Name: dest_vol

Security style: UNIX

UNIX permissions

	Read	Write	Execute
Owner	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Group	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Others	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Thin Provisioned

Allocate space as it is needed by the volume. Recommended for increasing the capacity utilization of the volume when the volume is unlikely to use all of its allocated space. If unchecked, complete space is allocated immediately.

[Tell me more about Thin Provisioning](#)

Save Save and Close Cancel

- c. Click **Save and Close**.
6. Verify that the columns in the Volumes list have updated to the appropriate values.

What to do next

After verifying that the destination volume is ready for read/write access, you should resolve the problem that led to the source volume being unavailable and bring the source volume back online when possible.

When the source volume is back online, you need to reverse the roles of the source and destination volumes.

Reverse resynchronizing SnapMirror relationships

You can reestablish a SnapMirror relationship that was previously broken. In a reverse resynchronization operation, you reverse the roles of the source and destination volumes, and the source volume is converted to a copy of the original destination volume.

About this task

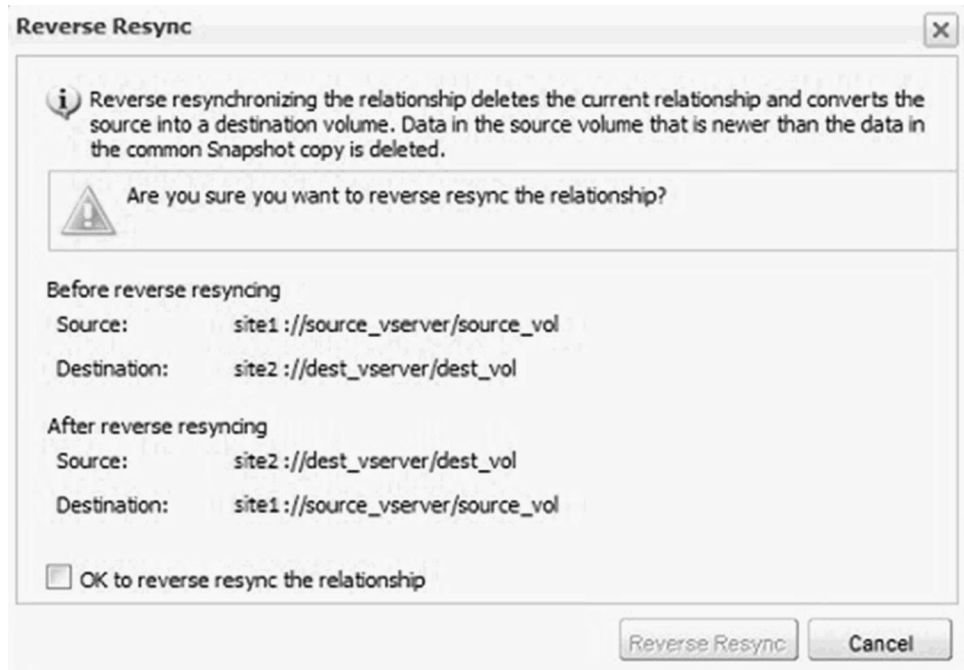
- Reverse resynchronization converts the source volume to a copy of the destination volume, and the contents on the source volume are overwritten by the contents from the destination volume.

Attention: All data from the last scheduled SnapMirror Snapshot copy before the source was disabled and all the data written to the destination volume after it was made writeable is preserved. Any data written to the source volume between the last SnapMirror Snapshot copy and the time that the source volume was disabled is not preserved.

- The destination volume must be launched in System Manager before the source volume is launched, or an error might be generated when you try to reverse resynchronize.

Procedure

1. From the home page, double-click the appropriate storage system.
2. Expand the **Vservers** hierarchy in the left navigation pane.
3. In the navigation pane, select the Vserver that contains the destination volume, and then click **Protection**.
4. Select the SnapMirror relationship that you want to reverse resynchronize.
5. Click **Operations > Reverse Resync**. If System Manager cannot retrieve the cached credentials of the source cluster, you are prompted to enter the credentials.
6. Select the confirmation check box, and then click **Reverse Resync**.



The following occurs:

- The SnapMirror policy of the relationship is set to DPDefault and the SnapMirror schedule is set to None.
No scheduled transfers will occur unless you reassign a schedule to the relationship.
 - The SnapMirror relationship is removed from the Protection list.
Because SnapMirror relationships are always listed by the destination volume, you can view the new relationship from the Protection page of the new destination volume.
7. Optional: Configure a policy and schedule matching the original relationship and apply it to this reversed relationship. You might want to do this if the source volume will be unavailable for a long period of time.
 - a. Select the relationship in the list, and then click **Edit**.
 - b. Select the desired Mirror Policy and Mirror Schedule, and then click **OK**.

Results

The original destination volume is now established as the new source volume, containing the baseline Snapshot copy. Read/write activity continues to the new source volume. The original source volume is now functioning as the destination volume. You can see the new SnapMirror relationship listed on the Protection page of the new destination volume.

What to do next

Next, update the SnapMirror relationships and return the recovered volume to the source role.

Updating SnapMirror relationships

You should initiate an unscheduled mirror update after you perform the initial reverse resync and prior to returning the new destination volume to its original role as source. This ensures that the most recent writes to the new source are transferred to the destination.

Before you begin

- The mirror relationship must be in the Snapmirrored state.
- You must have enabled password caching and saved the storage system credentials.

About this task

The update process is generally performed while clients are still writing to the source volume, and it only replicates the new data and Snapshot copies added since the last update to the destination volume. As a result, under some circumstances you might want to perform multiple updates. For example, if you update a large amount of data that takes a long time to complete and have heavy write traffic to the source volume during the update, you might want to do additional updates to capture all of the newly written data. The time required for each successive update should get progressively shorter. Because the final update must be performed after client access has been disconnected, performing multiple updates minimizes the length of time that clients are disconnected.

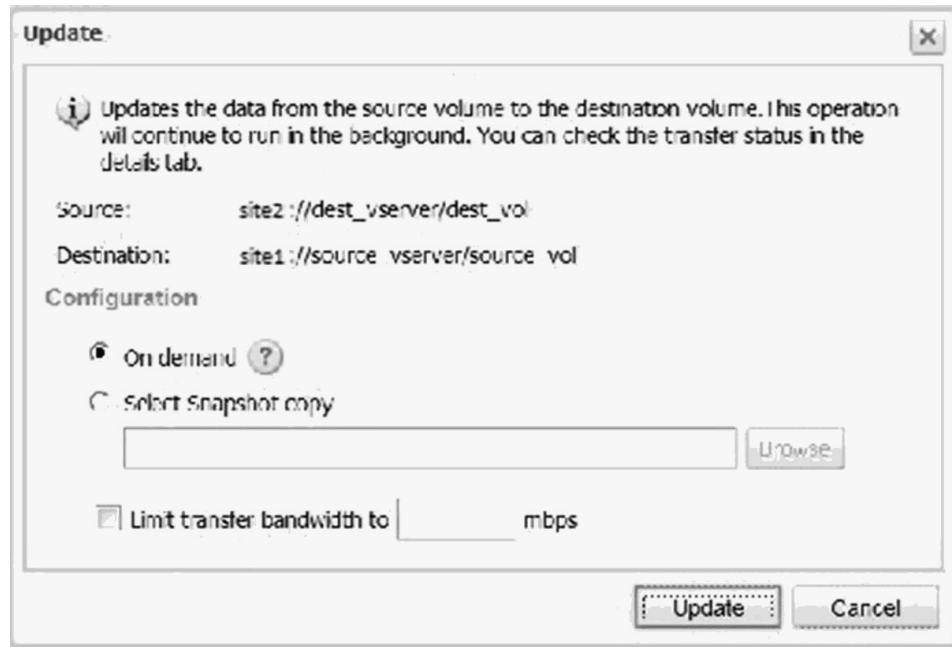
When you update a destination volume, all new and existing Snapshot copies from the source volume are transferred to the destination volume. In addition, any Snapshot copies deleted from the source volume are deleted from the destination volume during the update.

Procedure

1. From the home page, double-click the appropriate storage system.
2. Expand the **Vservers** hierarchy in the left navigation pane.
3. In the navigation pane, select the Vserver that contains the destination volume, and then click **Protection**.



4. Select the SnapMirror relationship that you want to update, and then click **Operations > Update**.
5. Select **On demand** to perform an incremental transfer from the recent common Snapshot copy between the source and destination volumes.



6. Optional: Select **Limit transfer bandwidth to** to limit the network bandwidth used for transfers and specify the maximum transfer speed.
7. Click **Update**.
8. Verify the transfer status in the Details area.
9. Optional: If necessary, repeat the update process to capture new writes that occur during the update process. Because you need to disconnect clients prior to performing the final update, continue performing online updates until you are satisfied with the length of time of the update, which impacts how long your clients need to be disconnected.
10. Disconnect the clients from the source volume. The procedures for disconnecting clients vary depending on the configuration of your environment. See the Data ONTAP documentation for more information.
11. Click **Update** to perform a final update of the data.

What to do next

To minimize the time clients cannot access the data, continue immediately to the next task, Returning a recovered volume to the source role.

Related information:

 IBM N series support website: www.ibm.com/storage/support/nseries

Returning a recovered volume to the source role

After an unavailable source volume has been recovered, and a reverse resync and an update have been performed, you can return the volume to its original role as source volume in the SnapMirror relationship. You must break and reverse resynchronize a second time.

Before you begin

- The SnapMirror destination volume must be in the quiesced or idle state.
- The destination volume must be premounted into the destination Vserver namespace.

About this task

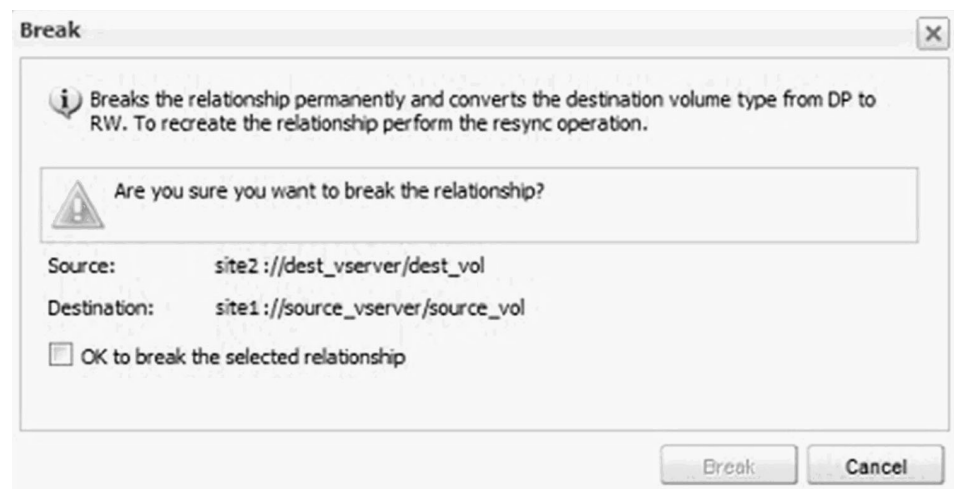
- This task is performed on the cluster that contains the destination volume in the SnapMirror relationship.
- Reverse resynchronization converts the source volume to a copy of the destination volume, and the contents on the source volume are overwritten by the contents from the destination volume.

All data up to the last scheduled or on-demand SnapMirror update is preserved.

- When you perform reverse resynchronization, the mirror policy of the relationship is set to DPDefault and the mirror schedule is set to None.

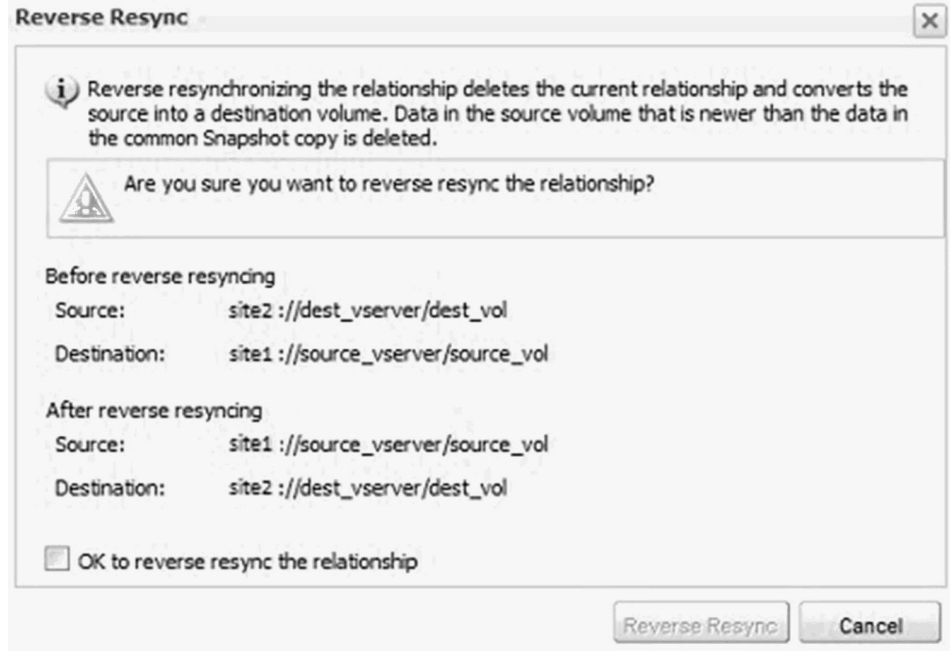
Procedure

1. From the home page, double-click the appropriate storage system.
2. Expand the **Vservers** hierarchy in the navigation pane.
3. Select the Vserver that contains the destination volume, and then click **Protection**.
4. Select the SnapMirror relationship that you want to reverse resynchronize.
5. Click **Operations > Break**.
6. Select the confirmation check box, and then click **Break**.



The following occurs:

- The data protection SnapMirror relationship is broken.
 - The destination volume type changes from read-only data protection (DP) to read/write (RW).
 - The system stores the base Snapshot copy for the data protection mirror relationship for later use.
7. Redirect client applications to the destination volume. The procedures for redirecting clients vary depending on the configuration of your environment. See the Data ONTAP documentation for more information.
 8. Click **Operations > Reverse Resync**. If System Manager cannot retrieve the cached credentials of the source cluster, you are prompted to enter the credentials.
 9. Select the confirmation check box, and then click **Reverse Resync**.



The following occurs:

- The SnapMirror policy of the relationship is set to DPDefault and the SnapMirror schedule is set to None.
No scheduled transfers will occur unless you reassign a schedule to the relationship.
- The SnapMirror relationship is removed from the Protection list.
Because SnapMirror relationships are always listed by the destination volume, you can view the new relationship from the Protection page of the new destination volume.

10. Select the Vserver that contains the new destination volume, and then click **Protection**.



11. Ensure that the relationship is correctly reestablished by doing the following:
 - a. Verify that the correct source Vserver and source volume names are listed.
 - b. Verify that the Is Healthy table column displays a status of Yes.
 - c. Verify that the Relationship State column displays a status of Snapmirrored.

Protection

⚠ If you have upgraded from Data ONTAP 8.1.x to 8.2, you must upgrade the SnapMirror relationships through the CLI to view the relationships.

Create Edit Delete Operations Refresh

Source Vserver	Source Volume	Destination Volume	Is Healthy	Relationship State	Transfer Status	Type	Lag Time	Policy
source_vserver	source_vol	dest_vol	Yes	Snapmirrored	Transferring	Mirror	None	DPDefault

12. Configure a policy and schedule matching the protection configuration of the original SnapMirror relationship and apply it to this reversed relationship:
 - a. Select the relationship in the list, and then click **Edit**.
 - b. Select the desired Mirror Policy and Mirror Schedule, and then click OK.

Results

The original roles are reestablished for the source and destination volumes in the SnapMirror relationship. Read/write activity is directed to the recovered source volume.

Related information:

 IBM N series support website: www.ibm.com/storage/support/nseries

Where to find additional information

There are additional documents to help you learn more about using OnCommand System Manager to complete failover and resynchronization tasks, and to provide other methods of disaster recovery to protect the availability of your data resources.

All of the following documentation is available from the IBM N series support website (accessed and navigated as described in Websites):

Technical Report 4015: SnapMirror Configuration and Best Practices Guide for Clustered Data ONTAP 8.2

Provides information and best practices related to configuring replication in clustered Data ONTAP.

Note: This technical report contains information about NetApp products that IBM licenses and in some cases customizes. Technical reports might contain information about models and features that are not supported by IBM.

Clustered Data ONTAP Data Protection Guide

Describes how to manage your backup and recover data on clustered systems.

Clustered Data ONTAP Logical Storage Management Guide

Describes how to efficiently manage your logical storage resources on systems running clustered Data ONTAP, using volumes, FlexClone volumes, files and LUNs, FlexCache volumes, deduplication, compression, qtrees, and quotas.

Clustered Data ONTAP Network Management Guide

Describes how to connect your cluster to your Ethernet networks and how to manage logical interfaces (LIFs).

Clustered Data ONTAP System Administration Guide for Cluster Administrators

Describes general system administration for IBM N series systems running clustered Data ONTAP.

Related information:

 IBM N series support website: www.ibm.com/storage/support/nseries

Copyright and trademark information

This section includes copyright and trademark information, and important notices.

Copyright information

Copyright ©1994 - 2013 NetApp, Inc. All rights reserved. Printed in the U.S.A.

Portions copyright © 2013 IBM Corporation. All rights reserved.

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

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.

References in this documentation to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM's or NetApp's intellectual property rights may be used instead of the IBM or NetApp product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM and NetApp, are the user's responsibility.

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.A. 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

IBM, the IBM logo, and [ibm.com](http://www.ibm.com) are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. A complete and current list of other IBM trademarks is available on the Web at <http://www.ibm.com/legal/copytrade.shtml>

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

NetApp, the NetApp logo, Network Appliance, the Network Appliance logo, Akorri, ApplianceWatch, ASUP, AutoSupport, BalancePoint, BalancePoint Predictor, Bycast, Campaign Express, ComplianceClock, Cryptainer, CryptoShred, CyberSnap, Data Center Fitness, Data ONTAP, DataFabric, DataFort, Decru, Decru DataFort, DenseStak, Engenio, Engenio logo, E-Stack, ExpressPod, FAServer, FastStak, FilerView, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexSuite, FlexVol, FPolicy, GetSuccessful, gFiler, Go further, faster, Imagine Virtually Anything, Lifetime Key Management, LockVault, Mars, Manage ONTAP, MetroCluster, MultiStore, NearStore, NetCache, NOW (NetApp on the Web), Onaro, OnCommand, ONTAPI, OpenKey, PerformanceStak, RAID-DP, ReplicatorX, SANscreen, SANshare, SANtricity, SecureAdmin, SecureShare, Select, Service Builder, Shadow Tape, Simplicity, Simulate ONTAP, SnapCopy, Snap Creator, SnapDirector, SnapDrive, SnapFilter, SnapIntegrator, SnapLock, SnapManager, SnapMigrator, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapSuite, SnapValidator, SnapVault, StorageGRID, StoreVault, the StoreVault logo, SyncMirror, Tech OnTap, The evolution of storage, Topio, VelocityStak, vFiler, VFM, Virtual File Manager, VPolicy, WAFL, Web Filer, and XBB are trademarks or registered trademarks of NetApp, Inc. in the United States, other countries, or both.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

NetApp is a licensee of the CompactFlash and CF Logo trademarks.

NetApp NetCache is certified RealSystem compatible.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe on any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, N.Y. 10504-1785
U.S.A.

For additional information, visit the web at:
<http://www.ibm.com/ibm/licensing/contact/>

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM web sites are provided for convenience only and do not in any manner serve as an endorsement of those web sites. The materials at those web sites are not part of the materials for this IBM product and use of those web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may

vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

Index

A

- ADR
 - See* asynchronous disaster recovery
- asynchronous disaster recovery
 - requirements for using SnapMirror Intercluster Failover and Resync Express Guide to perform 1

C

- cluster peers
 - monitoring for SnapMirror relationship health 3
- copyright and trademark information 27
- copyright information 27

D

- destination volumes
 - converting to RW role 16
 - verifying settings after breaking SnapMirror relationship 15
 - verifying settings, considerations for 15
- diagrams
 - SnapMirror intercluster failover and resync workflow 7
- disaster recovery
 - requirements for using SnapMirror Intercluster Failover and Resync Express Guide to perform asynchronous 1
 - where to get additional information about 25

E

- express guides
 - requirements for using SnapMirror Intercluster Failover and Resync 1

F

- failover
 - events, preparing for intercluster volume SnapMirror 3
 - requirements for using SnapMirror Intercluster Failover and Resync Express Guide to perform 1
 - where to get additional information about 25
 - workflow diagram for SnapMirror intercluster resync and 7
- failover process
 - SnapMirror, how it works in System Manager 8
- flowcharts
 - SnapMirror intercluster failover and resync workflow diagram 7

G

- guides
 - requirements for using SnapMirror Intercluster Failover and Resync Express 1

I

- intercluster SnapMirror relationships
 - failover and resync workflow diagram for 7
- intercluster volumes
 - preparing for SnapMirror failover event on 3

L

- lag times
 - monitoring for SnapMirror relationship health 3

M

- mirror relationships
 - See* SnapMirror relationships

N

- notices 29
- Notices 29

R

- recovered volumes
 - returning to source role 20
- relationships
 - See* SnapMirror relationships
- resync
 - workflow diagram for SnapMirror intercluster resync and 7
- resync process
 - SnapMirror, how it works in System Manager 8
- resynchronization
 - performing reverse, for SnapMirror relationship 16
 - where to get additional information about 25
- reverse resync
 - returning source volume to RW role 20
- reverse resynchronization
 - performing SnapMirror relationship 16

S

- SnapMirror
 - how failover and resync work in System Manager 8
 - intercluster failover and resync workflow diagram 7
- SnapMirror failover and resync
 - where to get additional information about 25
- SnapMirror relationships
 - breaking 12
 - considerations for reverse resynchronizing 16
 - monitoring health of 3
 - preparing for intercluster volume failover events in 3
 - prerequisites for breaking 12
 - prerequisites for updating 18
 - requirements for using SnapMirror Intercluster Failover and Resync Express Guide for failover and recovery 1
 - returning recovered volume to source role 20
 - reverse resynchronizing 16

- SnapMirror relationships *(continued)*
 - SnapMirror
 - configuration considerations 3
 - updating 18
 - verifying destination volume settings after breaking 15
 - verifying status of source volumes in 10
 - source volumes
 - considerations for recovering 20
 - prerequisites for recovering 20
 - returning RW role to 20
 - verifying status of, in SnapMirror relationship 10
- System Manager
 - how SnapMirror failover and resync work in 8

T

- trademark information 28

U

- updates
 - performing SnapMirror relationship 18

V

- volume-level disaster recovery
 - requirements for using SnapMirror Intercluster Failover and Resync Express Guide to perform 1
- volumes
 - converting destination to RW role 16
 - preparing for SnapMirror failover event on intercluster 3
 - recovered, returning to source role 20
 - verifying destination settings after breaking SnapMirror relationship 15
 - verifying status of source, in SnapMirror relationship 10

W

- workflows
 - SnapMirror intercluster failover and resync diagram 7



NA 210-06360_A0, Printed in USA

SC27-6416-00

