



FluidFS Disaster Recovery Best Practices Guide

Dell EMC FS8600 Network-Attached Storage (NAS)

FluidFS System Engineering
February 2017

Acknowledgements

This white paper was produced by the FluidFS Systems Engineering Team and the Dell EMC Solutions Engineering team.

Authors:	Bryan Lusk, Marek Roll, and the FluidFS Systems Engineering team.
----------	---

Feedback

Please give us feedback on the quality and usefulness of this document by sending an email to:

FluidFS-System-Engineering@Dell.com

Revisions

Revision	Date	Description
A	October 2013	Initial Release
B	January 2015	Updated for FluidFS v4
C	January 2016	Updated for FluidFS v5
D	February 2017	Updated for FluidFS v6

Table of contents

Acknowledgements.....	2
Feedback	2
Revisions.....	2
1 Preface.....	5
1.1 Audience.....	5
1.2 Purpose.....	5
1.3 Disclaimer.....	5
1.4 Customer support.....	5
2 Introduction.....	6
2.1 FluidFS replication.....	7
2.2 FluidFS Replication prerequisites.....	8
2.3 RPO and RTO.....	10
3 Replication topologies.....	11
3.1 Two NAS cluster replication topologies	11
3.2 Multiple NAS cluster replication topologies	12
3.3 One to Many NAS Volume replication	13
3.4 Cascading NAS Volume replication.....	14
3.5 Multiple Disaster Recovery Sites best practices	15
4 Configuring replication.....	16
4.1 Setup prerequisites	16
4.2 Configuring replication – One-to-one configuration	16
4.3 Managing replication policies	28
5 Disaster Recovery Procedure	30
5.1 Failover to secondary site.....	31
5.2 Failback to primary site	41
6 Planned Failover Procedure.....	53
6.1 Full Cluster Planned Failover and Failback	53
7 Single NAS Volume Planned Failover and Failback.....	55
8 Testing Disaster Recovery using Volume Clones	57
A Appendix A: Scripting failover/failback using the FluidFS CLI.....	58
A.1 Replication Setup	58

A.2	Failover CLI Scripting	59
A.3	Failback CLI Scripting	59
B	Appendix B: Additional resources	61

1 Preface

1.1 Audience

The audience for this document is intended to be systems, networking, storage or backup administrators who are responsible for the day-to-day management responsibilities of a Dell Compellent FS8600 FluidFS NAS solution.

Proper management of an FS8600 requires administrators (or teams of administrators) capable of managing and configuring enterprise-class Fibre Channel SAN and Ethernet networks, any enterprise-grade backup software intended to be used, the Dell Compellent Storage Center, as well as general purpose NAS administration

1.2 Purpose

The purpose of this document is to help the storage administrator understand the FS8600 disaster recovery mechanism. This document is not intended to be a primer or Dell Compellent FS8600 introductory resource for any of the subject matters involved, and it assumes at least introductory knowledge of many of the subjects covered in this document.

This document should be used in conjunction with other Dell Compellent resources as listed in [Appendix B – Additional Resources](#).

1.3 Disclaimer

The information contained within this best practices document is intended to provide general recommendations only. Actual configurations in customer environments may need to vary due to individual circumstances, budget constraints, service level agreements, applicable industry-specific regulations, or other factors. Configurations should be tested before implementing them a production environment.

1.4 Customer support

Dell Compellent provides live support at 1-866-EZSTORE (866.397.8673), 24 hours a day, 7 days a week, 365 days a year. For additional support, email Dell Compellent at support@compellent.com. Dell Compellent responds to emails during normal business hours.

2 Introduction

The Dell FS8600 scale-out NAS solution running Fluid File System (FluidFS) has several built-in features that help organizations protect against unplanned outages and data loss. Downtime and loss of data, even if temporary, can be very costly for an organization. Extended downtime can even be fatal to an organization.

The best practice for protecting data against disasters is typically to create and keep copies of important data in a different location so it can always be recovered. FluidFS v5 running on an FS8600 NAS appliance offers powerful, flexible and easy-to-manage asynchronous replication for disaster recovery.

Below is an example of a possible DR solution. This image shows a DR configuration between four production sites and one DR site. All production sites are replicating volumes to one DR site using FluidFS replication. In case of a production site failure, the storage administrator can recover from the DR site.

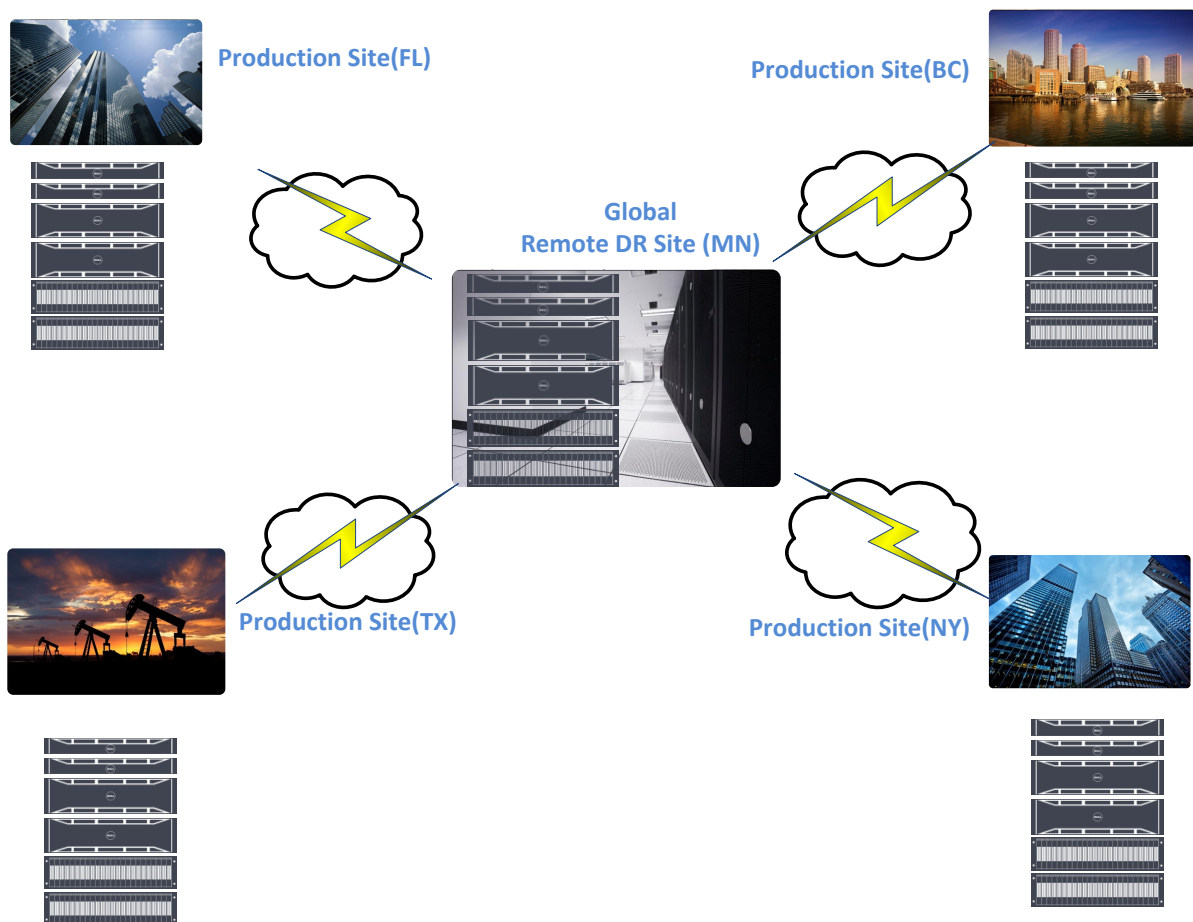


Figure 1 Possible DR solution between four production sites and one centralized DR site.

2.1 FluidFS replication

FS8600 appliances run Dell EMC Fluid File System (FluidFS) to provide file services to clients. Up to four FS8600 NAS appliances can be clustered together to build a single scale-out NAS cluster. FluidFS includes snapshot-based asynchronous replication between two FS8600 NAS clusters. FluidFS does not support utilizing SAN-based snapshots or replication to protect data. While all NAS data is stored on a backing SAN via a FluidFS cluster, all snapshotting and replication of NAS data takes place between FluidFS clusters and not the backing SANs.

FluidFS replication operates at the NAS volume level. A NAS volume may contain one or more SMB shares or NFS exports. An entire volume is replicated to another volume, either on the same NAS cluster or on another remote NAS cluster. The destination volume is an exact replica of the source volumes folders and files, and it can be configured to be an exact replica of the source volumes configuration items, including snapshots, shares, exports, snapshot schedules, and quotas. The exceptions to this rule include data that has been deduplicated and/or the deduplication policy, or if different snapshot retention policies are in use. The destination volume can be configured as a snapshot archive so as to keep snapshots for a time period different than on the primary site. Alternatively, the solution provides flexibility to not keep any snapshots at the DR site at all.

The storage administrator can configure a schedule to run replication, which is independent of any snapshot schedules. When replication runs, it replicates every snapshot consecutively, one after the other, along with the active data, until the destination volume is an exact mirror of the source at the time the replication began. The administrator can also define a QoS node, to throttle replication during peak hours.

When a replication is initiated between FluidFS clusters, a temporary snapshot of the current active data is created. This temporary snapshot is used to maintain a consistent data set throughout the replication process and to encapsulate any active data that is not already managed by a previous snapshot. The replication will leverage the delta changes maintained by any interval snapshots that were taken since the previous replication so that only the data changed between replications is moved. FluidFS optimizes block size for data, as low as 4K, depending on data ingest pattern. This optimizes replication due to being able to track changed blocks on a very granular level, reducing replication time and network overhead. Snapshots on the source volume will be replicated in such a way as to be accessible on the destination volume.

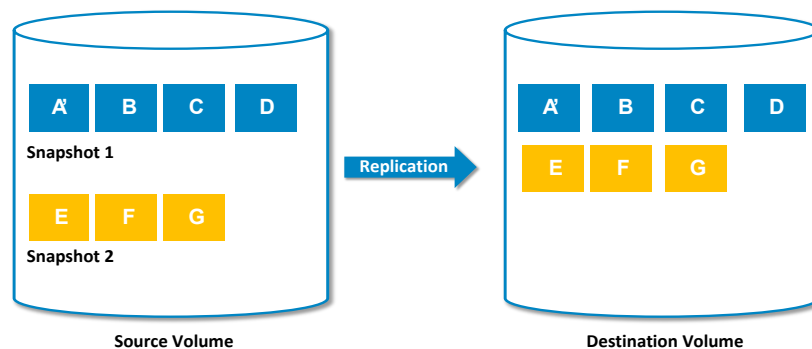


Figure 2 Snapshot based Replication

2.2 FluidFS Replication prerequisites

The following parameters are prerequisites to be used in an FS8600 DR environment. Please make sure that these prerequisites are in place before initiating replication setup.

Firewall ports

FluidFS v4 uses **TCP ports 10550-10551 and 10560-10568** for the replication process.

In **FluidFS v5** and later, a **single, user-defined TCP port** is used for FluidFS replication.

The storage administrator needs to make sure these ports are open, to allow traffic between the primary and secondary clusters in a firewalled environment. Additionally, ICMP echo requests (ping) should be allowed between the two clusters.

Networking Connectivity

In order to improve replication performance, FluidFS replicates using all NAS controllers in parallel. Hence, all NAS controllers need to be able to communicate with one another to be able to start the replication process. When configuring the networking on the local/remote site, if possible, make sure that the NAS clusters can ping to the appropriate FluidFS NAS **controller IP's and Virtual IPs (VIPs)** at the remote site. Replication uses the client-facing physical controller IP addresses, as well as the Virtual IPs. As a troubleshooting step, one can also verify ports are open and network connectivity is established by doing a telnet from one FluidFS NAS cluster to the other, using the ports specified above in the "Firewall ports" section.

FluidFS NAS Cluster Sizing (appliance count and disks)

As long as all NAS clusters are at FluidFS v4 or later, the source and destination cluster can have a different number of appliances. However, if the source NAS clusters are at FluidFS v3 or previous, the source and destination cluster must have the same number of controllers/appliances. There is no requirement or limitation around physical capacity deployment or disk enclosure configuration at each site. However, the destination system should have at least as much free space as the source system, and should take into account deduplicated data that will be rehydrated when replicated.

Replication performance and hence the RPO is highly dependent on the overall change rate of the data set, which dictates the amount of data that needs to be replicated at a given time. Replication performance is also highly dependent on the performance of the back-end Storage Centers, the available performance capacity of the NAS clusters themselves and, most importantly, the available bandwidth between replication sources and destinations. FluidFS allows the administrator to configure a NAS volume to be replicated as often as once every minute. Please consult the FluidFS Support Matrix document for the maximum number of supported replications per hour per FluidFS cluster. The FluidFS Support Matrix can be found on the FluidFS TechCenter website, which is referenced in [Appendix B – Additional Resources](#).

Authentication/access control configuration

It is important that the authentication configuration of the systems be identical, including user identity databases (Active Directory, NIS, LDAP), local users, Windows/UNIX user mappings, etc. This is important

because if the DR system goes into production in a disaster scenario, the same users must be able to authenticate so they can access data. Otherwise, valuable time can be lost manually configuring authentication on the DR system during the downtime incurred during a disaster.

However, if the secondary system is only intended to be used as a backup, and not for Disaster Recovery, the authentication configuration on FluidFS is optional.

There should be no conflicting Windows-to-Unix user mapping configurations between the source and destination NAS clusters.

Quota configuration

Additionally, to avoid quota conflicts, it is suggested that no user quotas be configured on the destination NAS volume. If user quotas must be enabled at the destination NAS volume, there must be no conflicting quota rules on the source NAS volume. If the NAS volume configuration of the source volume is restored, and there are conflicting quota rules on the destination volume, this can cause problems. Furthermore, since the replication destination volume is read-only, there is not really a valid use case to put quotas on the replication destination volume. The Dell EMC recommendation is to not use quota rules on replication destination NAS volumes, but if they must be used, they should be kept identical to the quota rules on the source NAS volume.

NAS Volume Data Reduction and FluidFS Replication

Fluid Data Reduction is a valuable tool that “gives” capacity back to customers through data deduplication as well as compression. Fluid Data Reduction can be used on NAS Volumes on both the primary and DR cluster, in order to reduce the overall capacity used by NAS data. When NAS data that has been deduplicated or compressed is replicated to a DR cluster, that data is rehydrated before it is sent to the DR cluster. Consequently, the data must be deduplicated/compressed again after it has been replicated to the DR cluster.

2.3 RPO and RTO

Replicating data may be part of a complete data center disaster recovery plan, but file-based replication alone is not sufficient. A comprehensive DR plan also needs to address aspects of network recovery, application recovery and any other elements of the IT infrastructure that are not under the control of the NAS system. However, making sure an up-to-date copy of the actual data is available is a key element in any disaster recovery plan.

RPO and RTO A typical disaster recovery plan attempts to achieve two goals: a recovery point objective (RPO) and a recovery time objective (RTO).

The **RPO** is determined by the amount of time the destination system lags behind the source system (note: for the purpose of a disaster recovery plan it is assumed that the source and destination volumes reside on separate systems). For example, if the replication policy is set to run every 5 minutes, then the gap between the volumes will be at best 5-10 minutes. The gap could be more than 5 minutes if the data change rate on primary site is more than what can be transferred to the secondary site in 5 minutes.

The **RTO** determines the length of time in which the destination system can be activated once it is required. This objective depends on several components outside the FS8600 NAS system — for example, the site DNS — so the RTO is dependent upon the overall disaster recovery plan.

3 Replication topologies

FluidFS supports several topologies for replication, both single- and multiple- NAS cluster replication. The following images show the supported topologies.

3.1 Two NAS cluster replication topologies

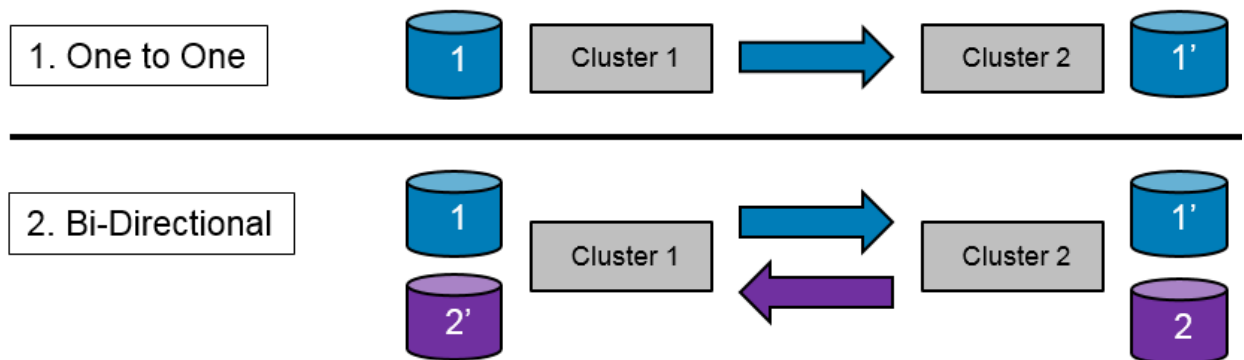


Figure 3 Single NAS cluster replication scenarios

Scenario 1 shows the typical one-to-one disaster recovery (DR) solution. In this scenario the storage administrator chooses Volume 1 in the primary site for replication to the secondary site.

Scenario 2 shows typical bi-directional DR solution when both FS8600 clusters serve as DR clusters. In this scenario the storage administrator chooses to replicate Volume 1 on the primary cluster to the secondary site, and he also chooses to replicate Volume 2 from the secondary site to the primary site. This is a great solution in the event that the data at the secondary site needs to be protected as well as the data on the primary site. However, it is important to note that a single FluidFS cluster can only contain multiple sets of SMB home shares if they are on separate tenants, so keep this in mind if bi-directional replication is in use. A single tenant cannot have two sets of SMB home shares, so if multiple sets of home shares need to be replicated, the same number of tenants will need to be created on FluidFS as you have number of sets of home shares.

3.2 Multiple NAS cluster replication topologies

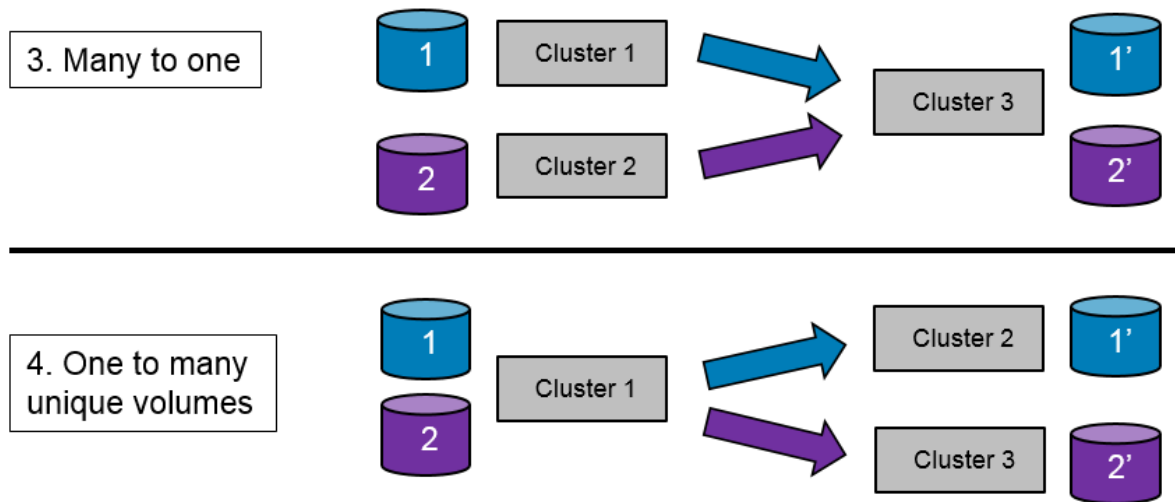


Figure 4 Multiple NAS cluster replication scenarios

Scenario 3 shows a DR solution where two separate NAS clusters replicate to one NAS cluster in a remote site. In this scenario the storage administrator chooses Volume 1 in the NAS Cluster 1 at the primary site to replicate to the secondary site, and the target volume in the remote site is Volume 1'.

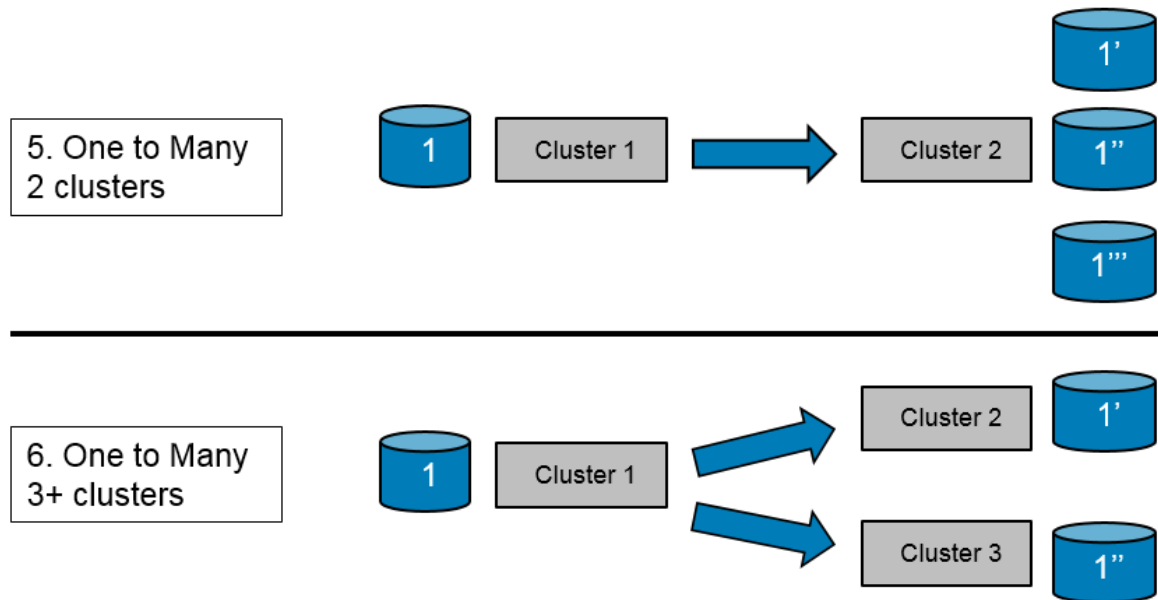
The storage administrator also chooses Volume 2 in NAS Cluster 2 in the primary site to replicate to the secondary site, and the target volume in the remote site is Volume 2'.

If multiple source clusters are utilizing home shares, the administrator will want to consider using multiple tenants on the destination/DR cluster. A single tenant cannot have more than one home share NAS Volume, so if multiple sets of home shares are needed, the same number of tenants will need to be created on the destination cluster as you have sets of home shares.

Scenario 4 shows a DR solution where one NAS cluster replicates two NAS volumes, one to each of two separate NAS clusters (Volume 1 and Volume 2) at two different DR sites. In this scenario the storage administrator chooses Volume 1 at the primary site to replicate to the FS8600 Cluster 2 at secondary site, and the target volume in the secondary site is Volume 1'.

The storage administrator also chooses Volume 2 at the primary site to replicate to the FS8600 Cluster 3 at different a DR site, and the target volume in the secondary site is Volume 2'.

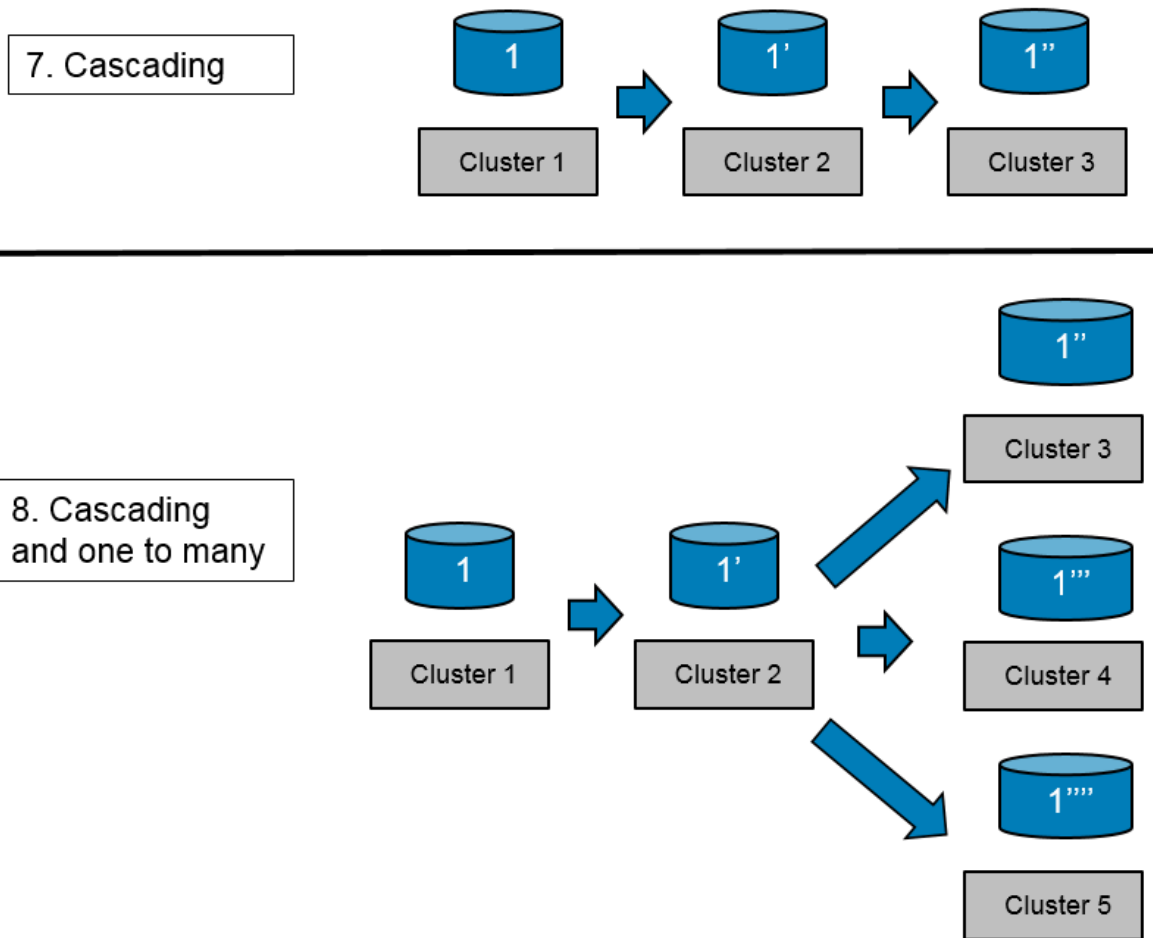
3.3 One to Many NAS Volume replication



Scenario 5 shows a typical scenario where there are 2 sites (production and DR), and one FluidFS cluster at each site. However, in this case the administrator has chosen to replicate to multiple volumes on the DR cluster. This does not provide any additional protection to the data, and would typically only be used for testing purposes.

Scenario 6 shows a scenario to implement replication utilizing multiple DR sites. In this case, Volume 1 from Cluster 1 would be asynchronously replicated to Volume 1' on Cluster 2 and Volume 1'' on Cluster 3, effectively creating an identical copy of Volume 1 on both Cluster 2 and Cluster 3.

3.4 Cascading NAS Volume replication



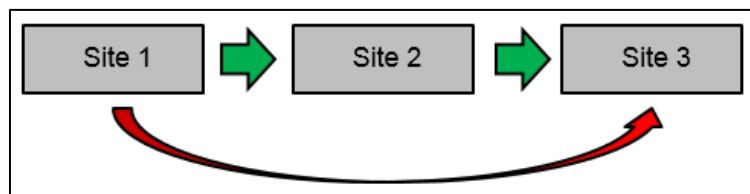
Scenario 7 shows another scenario (in addition to Scenario 6) to implement replication using multiple DR sites.

Scenario 8 shows a combination of cascading and one-to-many replication to illustrate the flexibility of FluidFS replication to meet any customers requirements.

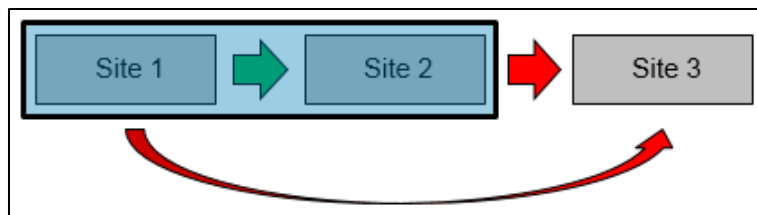
3.5 Multiple Disaster Recovery Sites best practices

For customers who wish to replicate to multiple disaster recovery sites, FluidFS offers flexibility to choose the replication topology which best suits the environment. In most cases, one-to-many replication will be the ideal choice to implement FluidFS replication across multiple disaster recovery sites. Using one to many replication will typically result in the lowest, best, and most predictable RPO. However, in cases where the link speed or latency between sites varies greatly, the administrator may want to consider cascaded replication, or a mix of cascading and one to many replication.

In some cases, the cascading replication topology will be a better choice. One example of when it might be good to use cascaded replication instead of one to many is if there is a slow network link between Site 1 and Site 3, a fast network link between Site 1 and Site 2, and a fast network link between Site 2 and Site 3. So instead of replicating Site 1 -> Site 2 and Site 1 -> Site 3 using one to many, it might be faster to replicate Site 1 -> Site 2 -> Site 3, resulting in shorter RPO.



Alternatively, if there is a fast link between Site 1 and Site 2 (if they are in the same LAN), and a slower link to Site 3 (over WAN), cascaded replication could provide some performance benefits to replicating Site 1 -> Site 2 -> Site 3 as replication from 1 to 2 can take place rapidly, while replication from 2 to 3 takes place slowly. This results in being able to replicate between Site 1 and Site 2 more frequently, giving a shorter overall RPO, while being able to provide the added redundancy of replicating to a 3rd site.



A final example of when it might be good to use cascaded replication is if there are many DR clusters/replication targets. This could put a lot of load on the primary site cluster and network. The administrator could replicate the primary sites volumes to a single DR cluster, and then replicate the volumes on that single DR cluster to the many more additional DR clusters. This would result in the primary cluster replicating to only one DR cluster, but then that single DR cluster would take on the load of replicating to many additional DR clusters. This is shown in Scenario 8 in the previous section.

4 Configuring replication

The following section will demonstrate step by step configuration of NAS replication for an FS8600 FluidFS NAS cluster.

4.1 Setup prerequisites

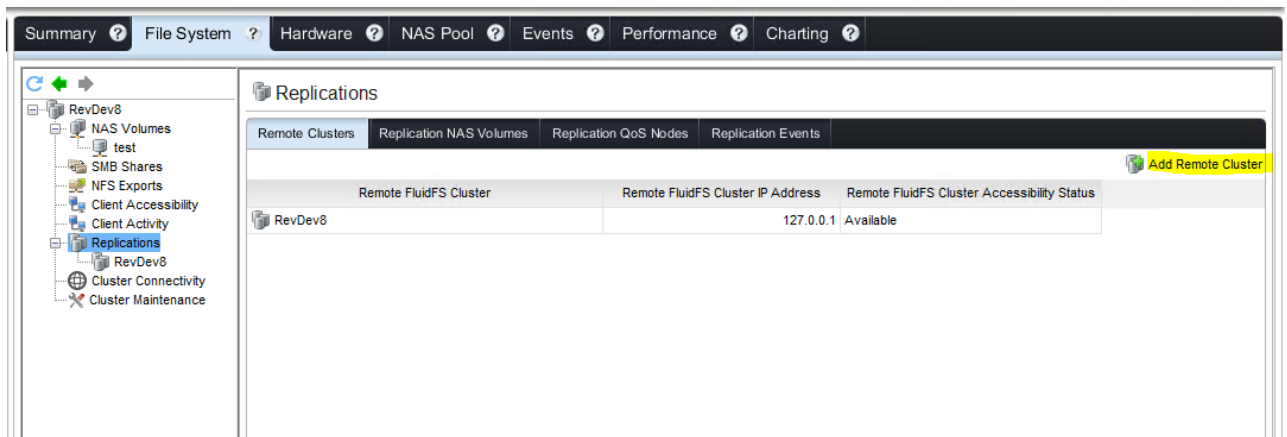
- Network connection between the primary site and the secondary site is already configured and verified to send packets in both directions. [See Section 2.2 – FluidFS Replication prerequisites](#)
- The primary and secondary clusters must both be managed by the same DSM Data Collector.

4.2 Configuring replication – One-to-one configuration

The following are step-by-step instructions for configuring NAS volume to replicate to a remote site. This example demonstrates replication between two FS8600 NAS clusters. The primary cluster is RevDev8 and the primary volume is VOL0, the secondary cluster is RevDev9 and the secondary volume will be VOL0_REP.

Step 1: Add Remote Cluster

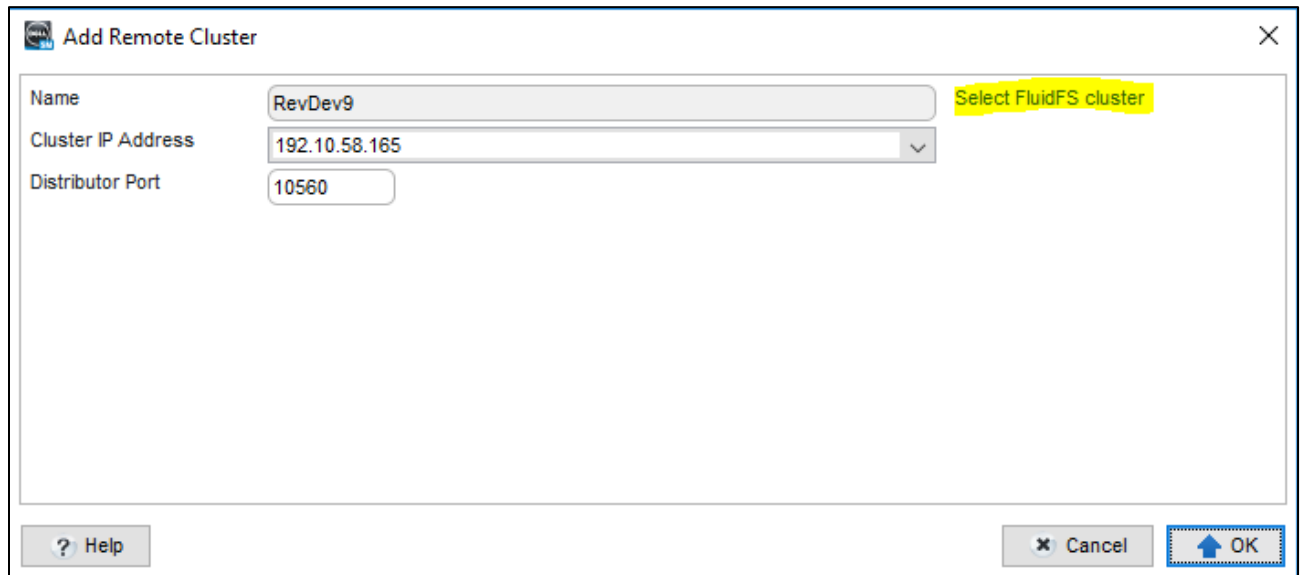
This step creates a partnership between the primary and secondary cluster. From the File System tab, click “Replications” and select “Add Remote Cluster”.



Step 2: Choose Remote Cluster

Choose the remote/secondary cluster, IP address, TCP port, and click next. The list only displays the other FS8600 clusters that are registered under your Dell Storage Manager view.

Enter the TCP port that you wish to use for FluidFS replication in the "Distributor Port" field.



The image shows a dialog box titled "Add Remote Cluster" with a close button (X) in the top right corner. The dialog contains three input fields: "Name" with the value "RevDev9", "Cluster IP Address" with the value "192.10.58.165" and a dropdown arrow, and "Distributor Port" with the value "10560". To the right of the "Name" field, there is a yellow highlighted button labeled "Select FluidFS cluster". At the bottom left, there is a "Help" button with a question mark icon. At the bottom right, there are "Cancel" and "OK" buttons. The "OK" button has a blue border and an upward arrow icon.

Name	RevDev9	Select FluidFS cluster
Cluster IP Address	192.10.58.165	
Distributor Port	10560	

? Help ✕ Cancel ↑ OK

Step 3: Verify Partnership on Secondary Cluster

Replication trusts are two way trusts. Once a trust is created from the primary FluidFS cluster, replication policies can be set up from the primary NAS cluster to the secondary NAS cluster, or from the secondary NAS cluster to the primary NAS cluster. It is a one time operation, which applies for both directions of replication.

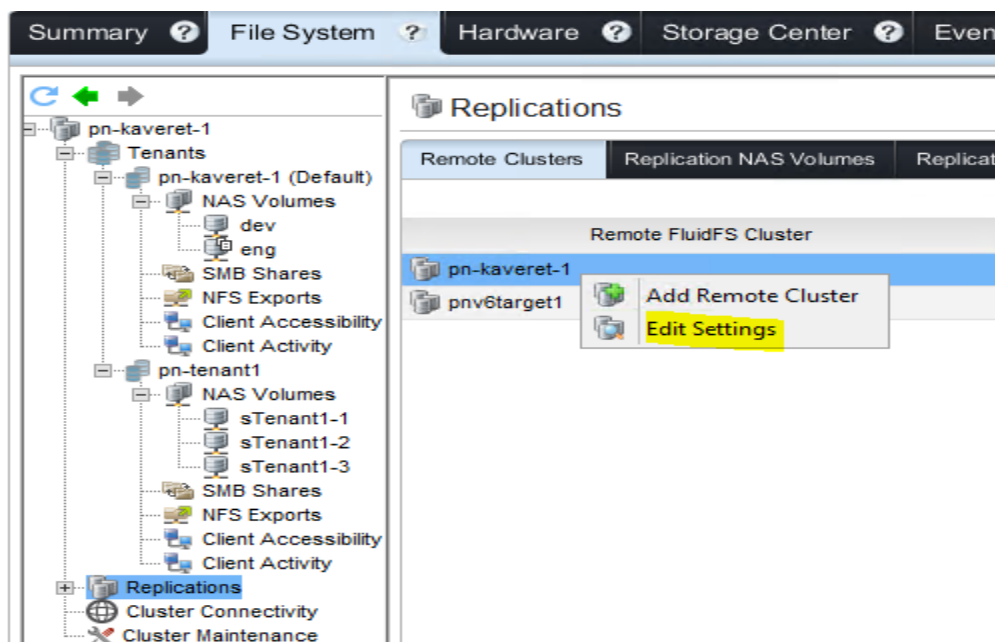
To verify the trust on the secondary cluster, look at the remote (secondary) cluster in DSM, and verify the primary cluster is listed as a partner. You can do this by clicking on the secondary cluster in DSM, and then look at the list of clusters under "Remote NAS Clusters".

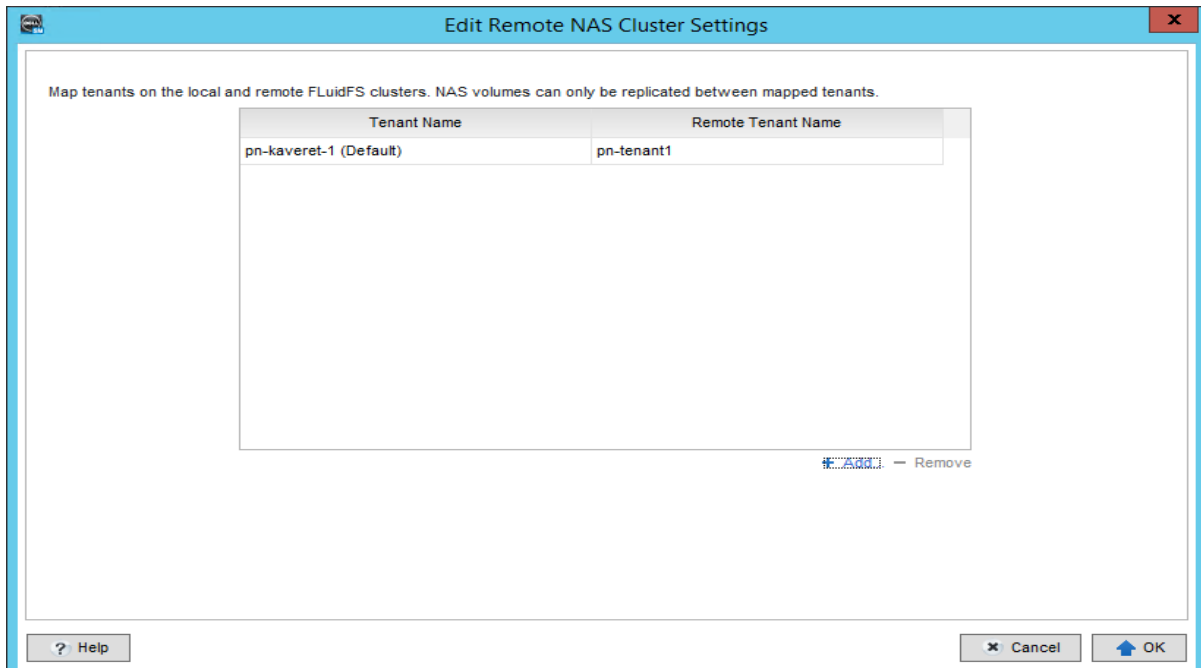
(If Multitenancy In Use) Step 3b: Create tenant partnerships

Note: This document and the screenshots inside it covers the use case of multitenancy being disabled.

If multitenancy is in use, after creating a partnership between two FluidFS clusters, a replication partnership is formed only between the default tenant on the two FluidFS clusters. If the administrator wishes to replicate to/from any of the non-default/user-created tenants, the administrator must also create partnerships between the tenants on those FluidFS clusters.

In order to create tenant partnerships, right click on the cluster-to-cluster replication partnership in DSM and click "Edit Settings".





Step 4: Create Secondary NAS Volume

Create a NAS volume on the secondary cluster (remote cluster) at least as big as the source volume. (on the primary cluster) Alternatively, the volume creation can also be done while setting up the replication in the replication wizard.

Step 5: Create Replication Policy

On the primary cluster, right-click the volume you would like to replicated to the secondary system, and select "Create Replication"

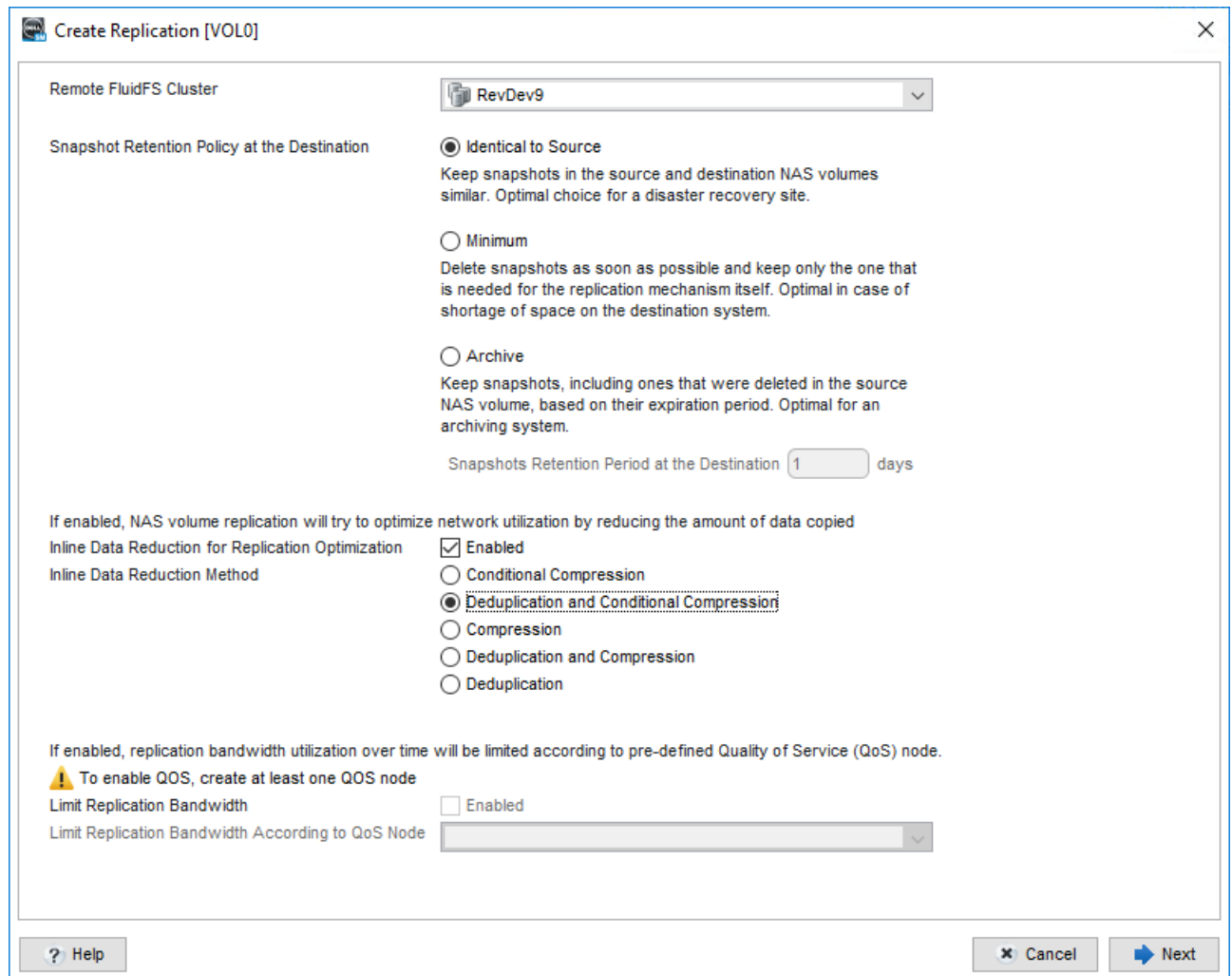
The screenshot displays the NetApp OnCommand System Manager interface. The top navigation bar includes tabs for Summary, File System, Hardware, NAS Pool, Events, and Performance. The left sidebar shows a tree view with 'RevDev8' expanded, containing 'NAS Volumes' and 'VOL0'. A right-click context menu is open over 'VOL0', with 'Create Replication' highlighted in yellow. Other menu items include 'Edit Settings', 'Create SMB share', 'Create NFS export', 'Snapshots', 'Quota', 'Restore Settings', and 'Delete'. The main panel shows the 'NAS Volume Status' for 'VOL0' with a capacity of 500 GB and a thin provisioning type. A table below lists volume details.

Volume Name	Creation Time	Cloned
VOL0	1/20/1	No

Step 6: Choose Remote Cluster, Snapshot Retention Policy, and Inline Data Reduction Type

Choose the remote NAS cluster (secondary cluster) from the drop-down list. Then decide if you would like a different snapshot retention policy on the destination volume (on the secondary cluster), or if you would like to use inline data reduction, or if you would like to use QoS, and click Next.

See [section 4.3](#) for guidance around which Snapshot Retention Policy to choose or more information about inline data reduction.



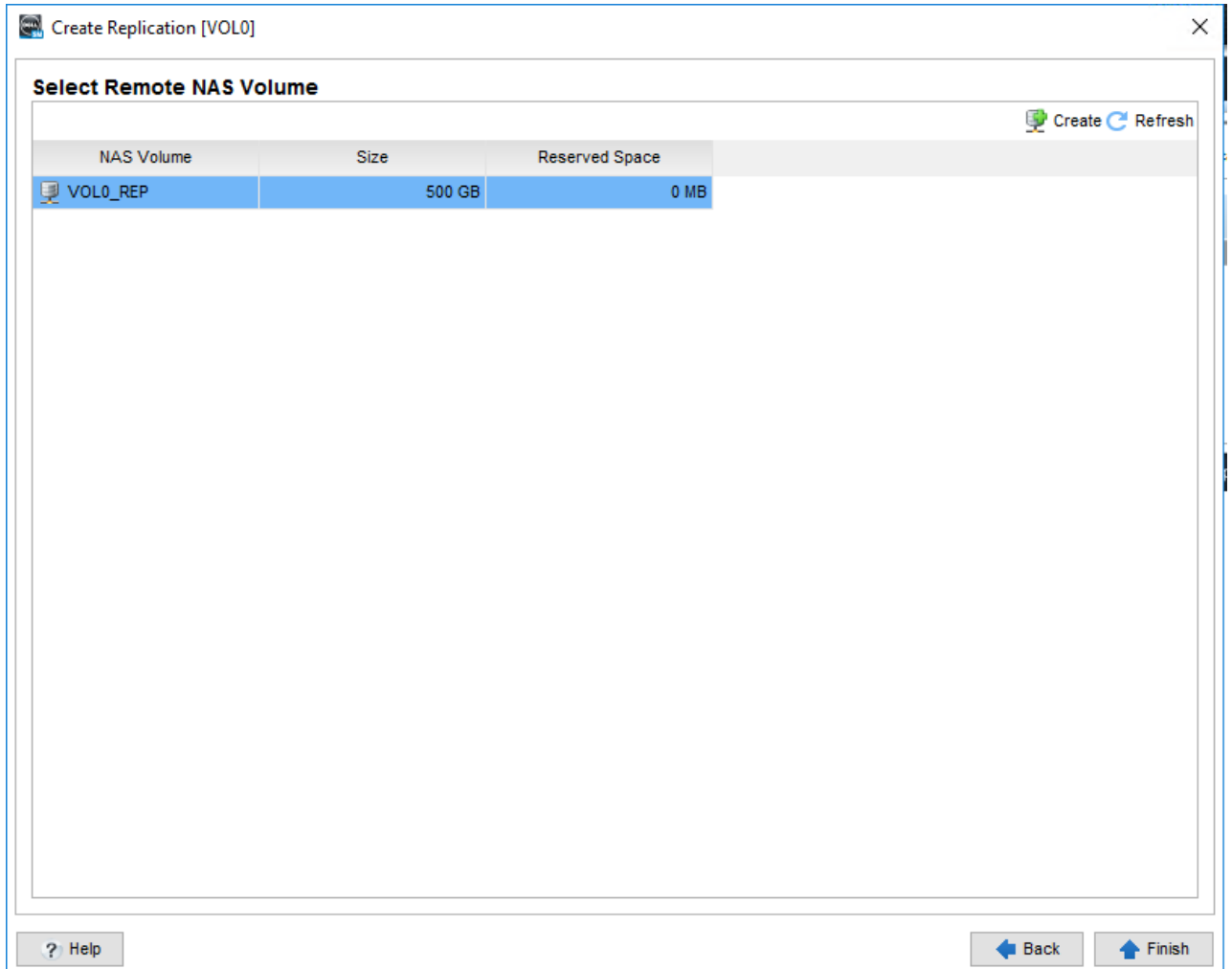
The image shows a 'Create Replication [VOL0]' dialog box with the following configuration:

- Remote FluidFS Cluster:** RevDev9
- Snapshot Retention Policy at the Destination:**
 - ☒ **Identical to Source**
Keep snapshots in the source and destination NAS volumes similar. Optimal choice for a disaster recovery site.
 - ☐ **Minimum**
Delete snapshots as soon as possible and keep only the one that is needed for the replication mechanism itself. Optimal in case of shortage of space on the destination system.
 - ☐ **Archive**
Keep snapshots, including ones that were deleted in the source NAS volume, based on their expiration period. Optimal for an archiving system.
- Snapshots Retention Period at the Destination:** 1 days
- Inline Data Reduction for Replication Optimization:** ☒ Enabled
- Inline Data Reduction Method:**
 - ☐ Conditional Compression
 - ☒ **Deduplication and Conditional Compression**
 - ☐ Compression
 - ☐ Deduplication and Compression
 - ☐ Deduplication
- Limit Replication Bandwidth:** ☐ Enabled
- Limit Replication Bandwidth According to QoS Node:** [Dropdown menu]

At the bottom, there is a **? Help** button on the left, and **Cancel** and **Next** buttons on the right.

Step 7: Select Volume to replicate to on secondary (remote) system

Select the volume previously created on the secondary (remote) NAS cluster and click Finish. If a volume on the secondary cluster has not been created yet, one can be created by clicking the "Create Remote Volume " button.



Create Replication [VOL0]

Select Remote NAS Volume

Create Refresh

NAS Volume	Size	Reserved Space
VOL0_REP	500 GB	0 MB

? Help Back Finish

Step 8: Create a schedule for the replication

On the primary cluster, click on the NAS volume, and then on the Replication tab. Click the Create button in the Replication Schedules section, as is highlighted in the image below. What is being scheduled is a replication “pulse”. At each scheduled point in time that is specified in the schedule, FluidFS will replicate all data that is new/changed since the last replication, to the secondary volume. In the case there has never been a replication between these two volumes, or there is not a common “base replica snapshot” present on both systems, all of the data on the primary volume will be replicated to the secondary volume.

The screenshot displays the FluidFS management console interface. The top navigation bar includes tabs for Summary, File System, Hardware, NAS Pool, Events, Performance, and Charting. The left sidebar shows a tree view with RevDev8 selected, containing NAS Volumes, test, SMB Shares, NFS Exports, Client Accessibility, Replications, RevDev8, RevDev9, and Cluster Maintenance. The main content area is titled 'VOL0' and shows the 'Replications' tab. The 'NAS Volume Status' section displays a progress bar for 296.5 KB (0%) of 500 GB, with details for Space Provisioning (Thin), Unused Space (500 GB (100%)), Overcommitted Space (0 MB), Used Space Threshold (90%), Unused (Reserved) Space (0 MB), and Unused (Unreserved) Space (500 GB). The 'Replications' section shows a table with columns: Role in Replication, Remote FluidFS Cluster, Remote NAS Volume, and Achieved Recon. The table contains one entry: Source, RevDev9, VOL0_REP. The 'Replication Partnership' section shows details for the partnership between Source and RevDev9, including Remote FluidFS Cluster (VOL0_REP), Snapshot Retention Policy at the Destination (Identical to Source), Inline Data Reduction for Replication Optimization Enabled (Yes), Inline Data Reduction Method (Deduplication and Conditional Compression), and Limit Replication Bandwidth Enabled (No). The 'Replication Schedules' section shows a table with columns: Replication Schedule and Frequency and Timing. A 'Create' button is highlighted in the bottom right corner of the Replication Schedules section.

Role in Replication	Remote FluidFS Cluster	Remote NAS Volume	Achieved Recon
Source	RevDev9	VOL0_REP	

Replication Schedule	Frequency and Timing
----------------------	----------------------

Step 9: Create the replication schedule and click OK

The schedule can be configured for once per minute, hour, day, or week.

Alternatively, specific days and times can be set. The "Offset by" field will result in the replications occurring at the selected times, plus the amount of minutes specified. For example, if the administrator wishes not to replicate on the hour, but wishes to replicate 15 minutes past the hour, such as at 1:15AM and 5:15AM and 9:15AM, they would enter "15" into this field, and select 1AM, 5AM, and 9AM. This would result in replicating at 1:15AM, 5:15AM, 9:15AM etc... on the days specified.

Create Replication Schedule [VOL0]

Schedule Name:

Frequency and Timing: ☒ Replicate every hours

☐ Replicate on

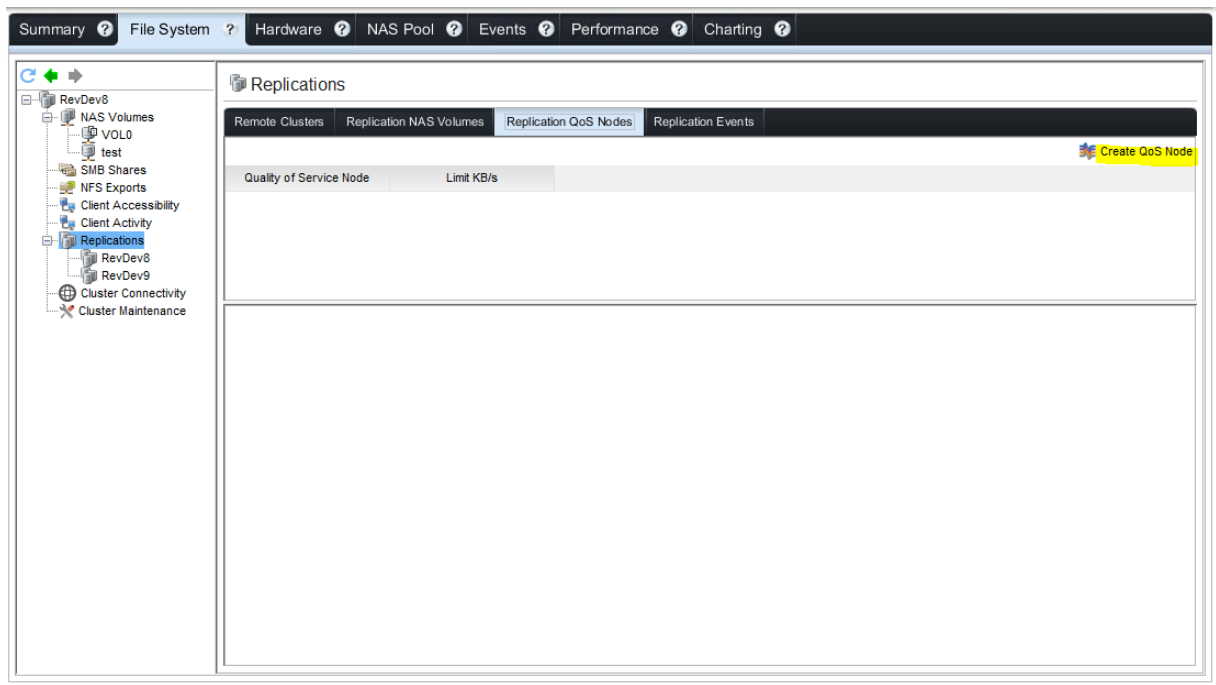
<input type="checkbox"/> Monday	<input type="checkbox"/> 1 AM	Offset by <input type="text" value="0"/> minutes
<input type="checkbox"/> Tuesday	<input type="checkbox"/> 2 AM	
<input type="checkbox"/> Wednesday	<input type="checkbox"/> 3 AM	
<input type="checkbox"/> Thursday	<input type="checkbox"/> 4 AM	
<input type="checkbox"/> Friday	<input type="checkbox"/> 5 AM	
<input type="checkbox"/> Saturday	<input type="checkbox"/> 6 AM	
<input type="checkbox"/> Sunday	<input type="checkbox"/> 7 AM	

? Help Cancel OK

OPTIONAL, Step 10, Configure QoS

Starting in FluidFS v5, the administrator can configure a Quality of Service (QoS) node in order to throttle replication during time periods that the user or application load is the highest, or when network traffic is saturating the link between sites . This feature allows the administrator to specify the maximum bandwidth of the link between the two clusters, and then build a schedule on when to throttle it and by how much.

Click [here](#) to create the QoS node



Name it, and enter the maximum speed of the link between the two sites (in Kilobytes per second)

Create Replication QoS Node

Quality of Service Node

10GigLink

Limit KB/s

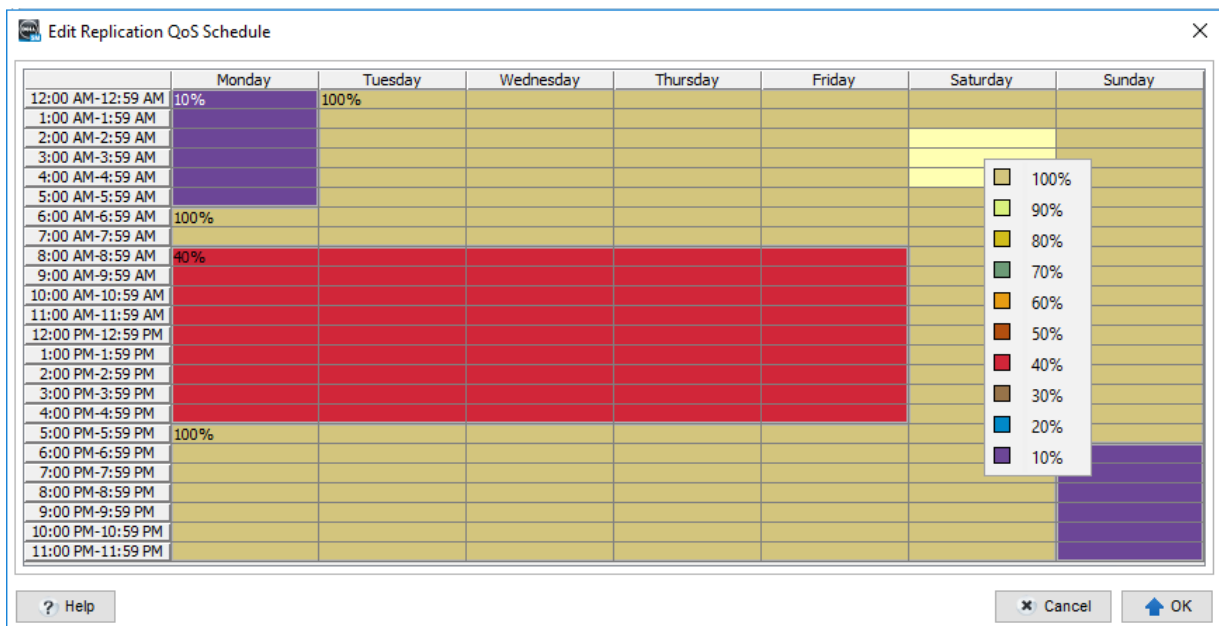
1200000

? Help

✕ Cancel

⬆ OK

Define the QoS



Apply the QoS node to a volume

The screenshot shows the NetApp ONTAP GUI with the 'VOL0' volume selected. The 'Replications' tab is active, showing a replication partnership named 'RevDev9 [VOL0_REP]'. The 'Replication Partnership' section shows the source as 'RevDev9' and the destination as 'VOL0_REP'. The 'Replication Schedules' section shows a schedule named 'ReplicationSchedule0' with a frequency of 'Every 1 hours'.

NAS Volume Status

Size	Used Space	Space Provisioning	Unused Space	Used Space Threshold	Overcommitted Space	Unused (Reserved) Space	Unused (Unreserved) Space
206.5 KB	296.5 KB (0%)	Thin	500 GB (100%)	90%	0 MB	0 MB	500 GB

Replication Partnership

Role in Replication	Source
Remote FluidFS Cluster	RevDev9
Remote NAS Volume	VOL0_REP
Snapshot Retention Policy at the Destination	Identical to Source
Inline Data Reduction for Replication Optimization Enabled	Yes
Inline Data Reduction Method	Deduplication and Conditional Compression
Limit Replication Bandwidth Enabled	No

Replication Schedules

Replication Schedule	Frequency and Timing
ReplicationSchedule0	Every 1 hours

The 'Edit Replication Partnership Settings' dialog box is shown. It contains the following settings:

- Remote FluidFS Cluster: RevDev9
- Remote NAS Volume: VOL0_REP
- Snapshot Retention Policy at the Destination: ☒ Identical to Source
Keep snapshots in the source and destination NAS volumes similar. Optimal choice for a disaster recovery site.
- ☐ Minimum
Delete snapshots as soon as possible and keep only the one that is needed for the replication mechanism itself. Optimal in case of shortage of space on the destination system.
- ☐ Archive
Keep snapshots, including ones that were deleted in the source NAS volume, based on their expiration period. Optimal for an archiving system.
- Snapshots Retention Period at the Destination: 1 days
- If enabled, NAS volume replication will try to optimize network utilization by reducing the amount of data copied
- Inline Data Reduction for Replication Optimization: ☒ Enabled
- Inline Data Reduction Method: ☒ Deduplication and Conditional Compression
- ☐ Conditional Compression
- ☐ Compression
- ☐ Deduplication and Compression
- ☐ Deduplication
- If enabled, replication bandwidth utilization over time will be limited according to pre-defined Quality of Service (QoS) node.
- Limit Replication Bandwidth: ☒ Enabled
- Limit Replication Bandwidth According to QoS Node: 10GigLink

Buttons: ? Help, Cancel, OK

4.3 Managing replication policies

Once a replication policy is set, it can always be changed or modified as follows:

- To manage a replication policy (either local or remote), click on the replication policy and select Edit Settings in the Replication Partnership section.
- Replicate on-demand lets the storage administrator initiate a replication pulse manually at any given time. This function is primarily used for the initial replication.

Other replication tasks:

- The storage administrator can pause/resume a replication, which temporarily disables the replication pulses scheduled by the administrator.
- The storage administrator can promote/demote the destination volume.
 - Promoting a destination volume makes it read+write instead of read-only, and also stops the scheduled replication pulses.
 - Demoting a volume makes it read-only, and allows replication pulses to continue on schedule (or manually initiated).
- The storage administrator can edit the Snapshot Retention Policy for the destination volume.
 - In some cases, the storage administrator wishes for the snapshot retention policy on the destination volume to be different than the source volume.
 - In some cases, there will be less storage space available in the NAS pool of the destination cluster than there is on the source cluster. In such case, space can be conserved by reducing the snapshot overhead on the destination volume. This is accomplished by using either the "No History" or "Archive" mode. Using "No History" mode only replicates the active view of the data to the destination cluster, without any snapshots. Using the "Archive" mode, snapshots can have their expiration reduced so they are expired sooner than they would naturally be expired based on their expiration time set in the snapshot schedule. For example, some administrators configure weekly snapshots to expire after 1 year, but on the destination volume this can consume space unnecessarily. If the administrator wishes to conserve space, the snapshot retention policy can be set to some low value such as 3 days. If there is a failure at the primary site, and the destination volume needs to be promoted and taken into production, as long as this is done within the 3 day window, the snapshot will still be present.
 - In some cases, the administrator will wish to retain snapshots on the destination cluster for a longer period of time than on the source, to maintain large archive of snapshots, to offer more history and granularity in restore points. In this case, "Archive" mode can be used, and set to an extended period of time, such as 90 days or 365 days. Of course, the administrator should verify that ample space is available on the destination FluidFS cluster to be able to store all of the snapshots.
- The storage administrator can use inline data reduction for replication traffic. Details of this feature are below.
- The storage administrator can apply a replication QoS node to throttle (slow down) replication during peak hours of user/application usage

Inline Data Reduction and FluidFS Replication

FluidFS NAS Replication also includes an inline data reduction feature, for replication traffic only. The deduplication and compression is for data over the wire, and is a valuable feature to reduce the amount of time it takes to complete replication jobs, as well as network overhead. The inline data reduction uses the same Rabin-Karp algorithm as NAS Volume data reduction, but the variable chunk size is between 4KB and 256KB. This feature is configured on a per-NAS-volume basis. After each replication, a FluidFS Event is generated that shows the savings statistics due to deduplication/compression.

Note: Replication inline data reduction is not related to NAS Volume data reduction whatsoever. Replication inline data reduction is for data over the wire only. The data is still rehydrated when it lands on the destination NAS Volume.

Several options are available for inline data reduction for replication:

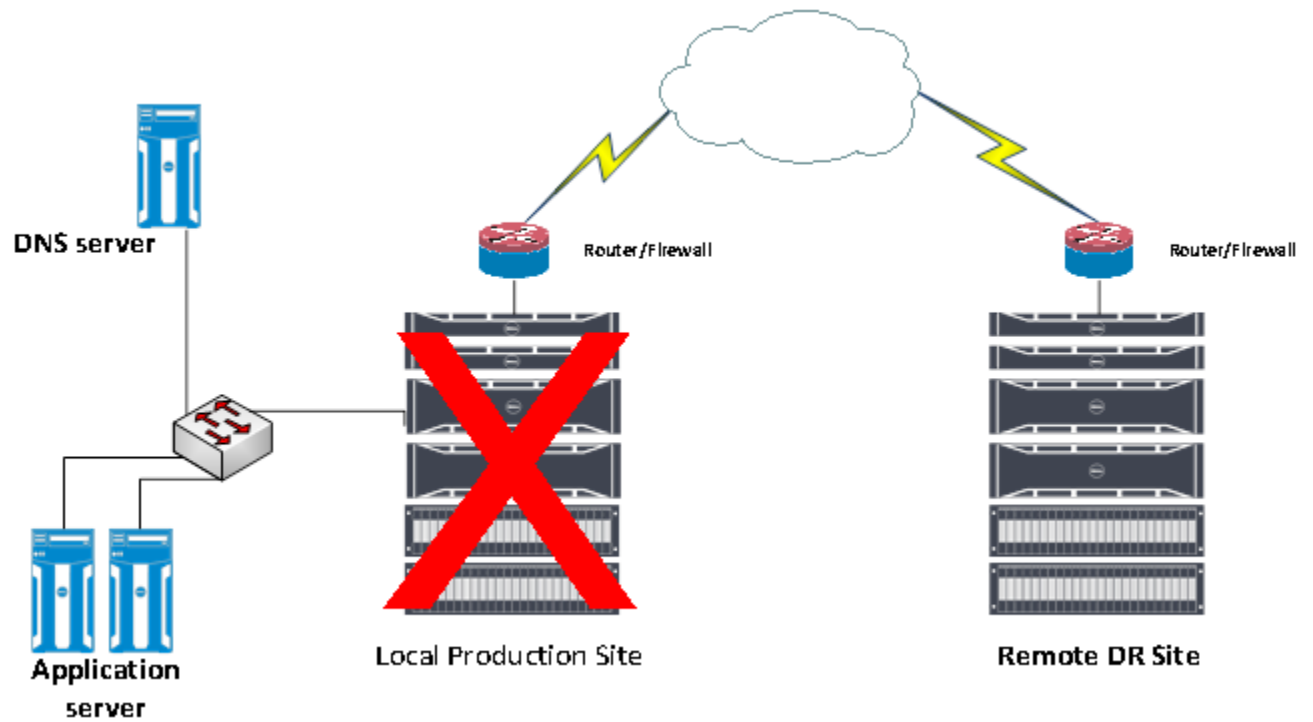
- Conditional Compression – The data is only compressed if the FluidFS NAS controllers CPU has enough free cycles. The purpose of this is to avoid a performance impact to SMB/NFS/HDFS/FTP clients due to overloading the CPU. Dell EMC recommends Conditional Compression.
- Deduplication and Conditional Compression
- Compression (not conditional – has chance to heavily load CPU)
- Deduplication and Compression
- Deduplication only

Conditional compression evaluates the load average on the CPU's every 100ms. Compression is throttled on a graduated scale in increments of 10%. For example, if the CPU is loaded 0% to 10%, conditional compression will be at 100%. If the CPU is loaded between 11% and 20%, conditional compression will be throttled to 90%, and so on.

5 Disaster Recovery Procedure

So far we've discussed the NAS replication feature and how to setup replication. Now we will discuss the necessary steps to recover from a site failure.

The diagram below shows a failed site scenario.



5.1 Failover to secondary site

When the primary site fails, the storage administrator should perform the following steps to failover to the secondary site.

It is important to note that this assumes the secondary cluster is following the best practices outlined in [Section 3.3 – Disaster Recovery Plan Best Practices](#). Namely, the secondary cluster should be configured to use the same DNS environment, NTP, Active Directory, and LDAP/NIS as the primary/production cluster. This is to avoid having to perform these time consuming configuration tasks while trying to recover from an outage.

Note: This procedure must be performed for each NAS volume that the administrator wishes to fail over. In cases where there is a high number of volumes in use, this procedure can be scripted against the FluidFS Command Line Interface. This is covered in [Appendix A](#) of this document.

Note: This document and the screenshots inside it covers the use case of multitenancy being disabled. However, the same concepts outlined here apply. This procedure must be performed for each NAS Volume, and the restore of local users/groups/mapping rules must be done for each tenant.

The high level steps of this process are as follows:

1. Promote the destination NAS volume on the secondary cluster. This will make the destination volume Read+Write and will present the latest stable replica, which is the snapshot taken during the last replication. This snapshot name always starts with "rep"
2. Restore the source NAS volume configuration on the secondary cluster. This will recreate all the SMB shares, NFS exports, snapshot schedule, and quota rules that were present on the source NAS volume.
3. Restore/Verify cluster wide configuration items
4. Redirect client systems to the secondary cluster (modify DNS and update SPN's)
5. Delete the replication on the destination NAS volume on the secondary cluster.

The detailed steps of how to perform this procedure are as follows:

Step 1: Promote the secondary volume (on secondary NAS cluster)

Promote the secondary (remote) site volume by clicking on the volume and then selecting "Promote". This will make the secondary volume read/write instead of read-only.

The screenshot shows the Veeam Backup & Replication console interface. The left sidebar displays a tree view with 'RevDev9' selected, showing 'NAS Volumes' and 'VOL0_REP'. The main pane is titled 'VOL0_REP' and shows the 'NAS Volume Status' for 'VOL0'. The status bar indicates a size of 419.5 KB and a total capacity of 500 GB. Below this, a table shows various metrics: Size (419.5 KB), Space Provisioning (Thin), Overcommitted Space (0 MB), Used Space (419.5 KB), Unused Space (500 GB), Used Space Threshold (90%), Unused (Reserved) Space (0 MB), and Unused (Unreserved) Space (500 GB). The 'Replications' tab is active, showing a table with columns: Role in Replication, Remote FluidFS Cluster, Remote NAS Volume, and Achieved Recovery Point. The table contains one entry: Destination, RevDev8, VOL0, and 1/20/17 3:16:23 PM. To the right of the table, the 'RepDev8 [VOL0]' section shows the 'Replication Status' as 'Idle' and 'Normal'. Below this, the 'Replication Partnership' section shows details for the replication from RevDev8 to RevDev9, including 'Identical to Source' and 'Deduplication and Conditional Compression'. The 'Replication Schedules' section is also visible at the bottom.

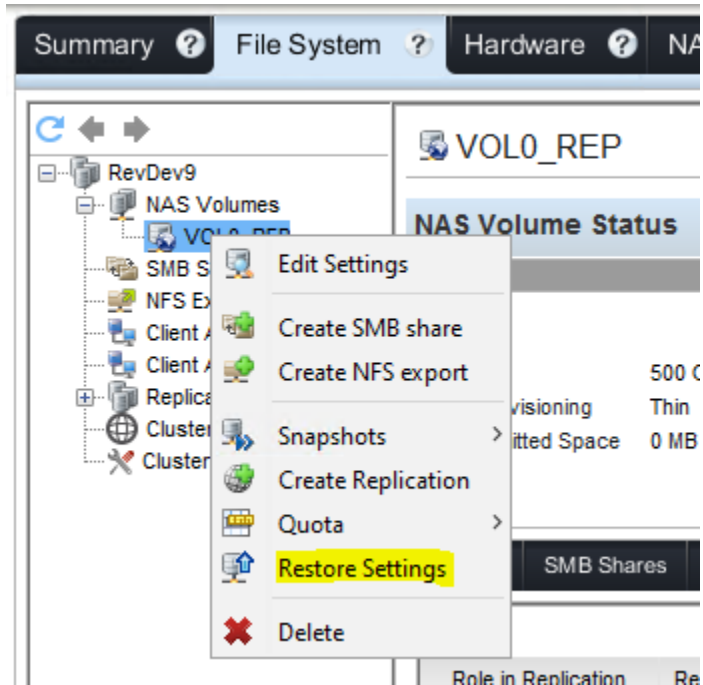
The screenshot shows a 'Promote Destination' dialog box. It contains the following information:

- Source FluidFS Cluster: RevDev8
- Source NAS Volume: VOL0
- Destination FluidFS Cluster: RevDev9
- Destination NAS Volume: VOL0_REP

Below the information, there is a warning icon and a message: "Are you sure you want to promote the destination NAS Volume? This will stop the replication." At the bottom of the dialog, there are three buttons: 'Help', 'Cancel', and 'OK'.

Step 2: Right-click on the remote site NAS volume and click "Restore Volume Config" (on secondary NAS cluster)

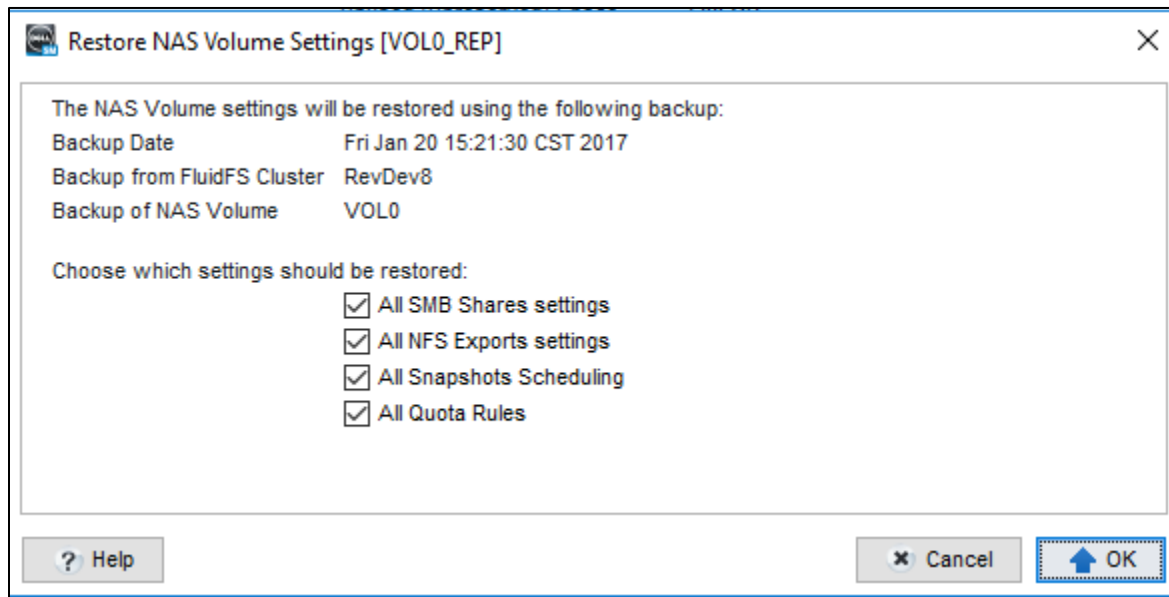
This will restore the shares, exports, snapshot schedules, and quota rules that were present on the primary site volume.



Step 3: Restore NAS Volume Configuration (on secondary NAS cluster)

By default, all available configuration files are checked. Click "OK"

Note: Directory Quotas and Redirection Folder objects do not need to be restored. The administrator can look at the replication destination volume and see that Directory Quotas and Redirection Folders are present after the first replication.



Step 4: Restore other cluster-wide configuration items (on secondary NAS cluster)

If best practices are being followed, the secondary cluster will already be configured with all environmental services such as DNS, NTP, Active Directory, LDAP/NIS, etc... But in the case that it is not, these must be configured at this stage. Additionally, if local users/groups, or manual user mappings are in place, those must be manually restored. Dell EMC recommends keeping the local users on both FluidFS clusters identical at all times. Local users and groups can be restored through Dell Storage Manager:

The screenshot shows the Dell Storage Manager interface with the 'Client Accessibility' tab selected. The 'Local Users and Groups' sub-tab is active, displaying a table of local users and a list of local groups.

Local Users

Local User	Primary Group	Allow Access	User ID	Password Never Expires
Administrator	Local Users	Enabled	500	Enabled
nobody	nobody_group	Disabled	99	Enabled

Local Users Security

Local Users Passwords Never Expires: No
Local Users Passwords Expiration Interval: 42 days

Local Groups

Local Group	Domain Type	Group ID
Administrators	Built-in Domain	500
Backup Operators	Built-in Domain	551
Local Users	Local Domain	200
nobody_group	Local Domain	99
Users	Built-in Domain	545

Any manual user mapping rules that are defined must be restored using the FluidFS Command Line Interface using the command:

```
client-access authentication mapping manual restore
```

Any networking configuration changes will have to be made manually. FluidFS does not have any automated method to restore network settings (such as IP's or static routes).

NOTE: Dell EMC recommends as a best practice to document all network settings (IP addresses, default gateway, static routes) so that if needed they can be restored onto the secondary site.

Step 5: Repoint clients to the secondary NAS cluster/NAS volume

At this point, the storage admin has two options (use one of the two options below) of how to point clients to the secondary FluidFS cluster:

1. Change the DNS entry that originally pointed to the Virtual IPs of the primary site to point to the secondary cluster's Virtual IPs. Ensure that the DNS server(s) that the secondary NAS cluster is using is the same DNS server(s) (or in the same DNS farm) as the DNS server(s) the primary NAS cluster is using. Existing client connections will break and need to be re-established. All NFS exports must be unmounted and mounted back on every client system.

Note: Lowering the TTL for these DNS entries could help with DNS cache issues when failing back.

2. Change/Add the IP's on the secondary cluster to be identical to the primary NAS clusters IPs. Choosing this option allows for NFS hosts to not have to unmount/remount all of the NFS exports.

Step 6: Update Active Directory SPN's to reflect the switch

This step must be performed for SMB access which uses Kerberos. If the cluster is being accessed via SMB using a name (such as *nas01.mycompany.com*, as opposed to IP) then odds are Kerberos is being used. In order for the secondary cluster to provide service using the primary cluster's DNS name, the Service Principle Names (SPN's) must be updated in Active Directory.

This step must be performed by an Active Directory administrator, preferably someone with Domain Administrator rights. This is done from the Windows cmd.exe

1. Remove SPNs from the PrimarySystem
 - a. `setspn -D HOST/<nas hostname> <PrimarySystem name>`
 - b. `setspn -D nfs/<nas hostname> <PrimarySystem name>`
 - c. `setspn -D nfs/<nas FQDN> <PrimarySystem name>`
 - d. `setspn -D HOST/<nas FQDN> <PrimarySystem name>`
2. Create SPNs on the SecondarySystem
 - a. `setspn -S HOST/<nas hostname> <SecondarySystem name>`
 - b. `setspn -S nfs/<nas hostname> <SecondarySystem name>`
 - c. `setspn -S nfs/<nas FQDN> <SecondarySystem name>`
 - d. `setspn -S HOST/<nas FQDN> <SecondarySystem name>`

SPN's for a computer object can be listed using `"setspn -l <ComputerObjectName>`

Example:

The primary system is *revdev5.reveille.lab*

The secondary system is *revdev8.reveille.lab*

The default SPN's for these two systems are as follows. This is set automatically when joining Active Directory

```
C:\Users\bryan_lusk.REVEILLE.000>setspn -l revdev5
Registered ServicePrincipalNames for CN=REUDEV5,CN=Computers,DC=reveille,DC=lab:

HOST/revdev5
HOST/revdev5.reveille.lab
nfs/revdev5
nfs/revdev5.reveille.lab

C:\Users\bryan_lusk.REVEILLE.000>setspn -l revdev8
Registered ServicePrincipalNames for CN=REUDEV8,CN=Computers,DC=reveille,DC=lab:

nfs/revdev8
nfs/revdev8.reveille.lab
HOST/revdev8
HOST/revdev8.reveille.lab
```

When failing over from *revdev5* to *revdev8*, the following commands will be run at cmd (either before or after updating DNS entries for *revdev5.reveille.lab* to point to the virtual IP's of *revdev8.reveille.lab*)

3. Remove SPNs from the PrimarySystem

```
setspn -D nfs/revdev5 revdev5

setspn -D HOST/revdev5 revdev5

setspn -D nfs/revdev5.reveille.lab revdev5

setspn -D HOST/revdev5.reveille.lab revdev5
```

```
C:\Users\bryan_lusk.REVEILLE.000>setspn -D HOST/revdev5 revdev5
Unregistering ServicePrincipalNames for CN=REUDEV5,CN=Computers,DC=reveille,DC=lab
Updated object

C:\Users\bryan_lusk.REVEILLE.000>setspn -D nfs/revdev5 revdev5
Unregistering ServicePrincipalNames for CN=REUDEV5,CN=Computers,DC=reveille,DC=lab
Updated object

C:\Users\bryan_lusk.REVEILLE.000>setspn -D HOST/revdev5.reveille.lab revdev5
Unregistering ServicePrincipalNames for CN=REUDEV5,CN=Computers,DC=reveille,DC=lab
Updated object

C:\Users\bryan_lusk.REVEILLE.000>setspn -D nfs/revdev5.reveille.lab revdev5
Unregistering ServicePrincipalNames for CN=REUDEV5,CN=Computers,DC=reveille,DC=lab
Updated object
```

4. Create SPNs on the SecondarySystem

```
setspn -S nfs/revdev5 revdev8
```

```
setspn -S HOST/revdev5 revdev8  
  
setspn -S nfs/revdev5.reveille.lab revdev8  
  
setspn -S HOST/revdev5.reveille.lab revdev8
```

```
C:\Users\bryan_lusk.REVEILLE.000>setspn -S HOST/revdev5 revdev8  
Checking domain DC=reveille,DC=lab  
Registering ServicePrincipalNames for CN=REUDEU8,CN=Computers,DC=reveille,DC=lab  
HOST/revdev5  
Updated object  
  
C:\Users\bryan_lusk.REVEILLE.000>setspn -S nfs/revdev5 revdev8  
Checking domain DC=reveille,DC=lab  
Registering ServicePrincipalNames for CN=REUDEU8,CN=Computers,DC=reveille,DC=lab  
nfs/revdev5  
Updated object  
  
C:\Users\bryan_lusk.REVEILLE.000>setspn -S HOST/revdev5.reveille.lab revdev8  
Checking domain DC=reveille,DC=lab  
Registering ServicePrincipalNames for CN=REUDEU8,CN=Computers,DC=reveille,DC=lab  
HOST/revdev5.reveille.lab  
Updated object  
  
C:\Users\bryan_lusk.REVEILLE.000>setspn -S nfs/revdev5.reveille.lab revdev8  
Checking domain DC=reveille,DC=lab  
Registering ServicePrincipalNames for CN=REUDEU8,CN=Computers,DC=reveille,DC=lab  
nfs/revdev5.reveille.lab  
Updated object
```

Now, users and applications are working off the secondary NAS cluster. However, this is not a permanent state, and eventually the storage administrator will want to fail back to the primary site. But first, the replication schedule and policy must be deleted, so it can be recreated in the opposite direction, replicating the secondary site to the primary.

Step 7: Delete the Replication Schedule (on the secondary NAS cluster)

FluidFS requires that the replication schedule is deleted before the replication policy can be deleted.

The screenshot displays the FluidFS management console with the 'Replications' tab selected. The main area shows the 'RevDev9 [VOL0_REP]' replication policy. On the left, a table lists the replication details:

Role in Replication	Remote FluidFS Cluster	Remote NAS Volume	Achieved Recovery Point
Source	RevDev9	VOL0_REP	1/20/17 3:24:56 PM

On the right, the 'Replication Resource Balance' is shown as 'Normal', and the 'Achieved Recovery Point' and 'Target Recovery Point' are both '1/20/17 3:24:56 PM'. Below this, the 'Replication Partnership' section shows the role as 'Source' and the remote cluster as 'RevDev9'. The 'Replication Schedules' section at the bottom shows a single schedule, 'ReplicationSchedule0', with a frequency of 'Every 1 hours'. The 'Delete' button for the schedule is highlighted in yellow.

Step 8: Delete the Replication Policy (on secondary NAS cluster)

The replication policy must be deleted, because the direction needs to be reversed to replicate the secondary site to the primary site. You can "Disconnect" the replication policy between the volumes by doing a **Delete** from Dell Storage Manager.

The screenshot displays the Dell Storage Manager interface for the VOL0_REP replication policy. The left sidebar shows a tree view with 'RevDev9' expanded, containing 'NAS Volumes' (with 'VOL0_REP' selected), 'SMB Shares', 'NFS Exports', 'Client Accessibility', 'Client Activity', 'Replications', 'Cluster Connectivity', and 'Cluster Maintenance'. The top navigation bar includes tabs for Summary, File System, Hardware, NAS Pool, Events, Performance, and Charting. The main content area is titled 'VOL0_REP' and includes an 'Edit Settings' link and a 'Create SMB share' button. Below this is the 'NAS Volume Status' section, which shows a progress bar for 2.58 MB and a table of volume statistics. The 'Replications' tab is selected, showing a table with one replication policy. The 'Delete' button is highlighted in yellow. A right-hand pane shows details for the selected replication policy.

Property	Value	Property	Value	Property	Value
Size	500 GB	Used Space	2.58 MB (0%)	Data Reduction S	
Space Provisioning	Thin	Unused Space	500 GB (100%)	Snapshot Space	
Overcommitted Space	0 MB	Used Space Threshold	90%		
		Unused (Reserved) Space	0 MB		
		Unused (Unreserved) Space	500 GB		

Role in Replication	Remote FluidFS Cluster	Remote NAS Volume	Achieved Recov
Source	RevDev8	VOL0	1/20/17 3:24:56

5.2 Failback to primary site

This procedure, at a high level, is what is covered in the previous section ([Section 5.1 – Failover to Secondary Site](#)), in reverse.

The failback from the secondary site to the primary site should occur only after all issues are fixed, and the primary site is ready to take the full production workload back.

Note: This procedure must be performed for each NAS volume that the administrator wishes to fail over. In cases where there is a high number of volumes in use, this procedure can be scripted against the FluidFS Command Line Interface. This is covered in [Appendix A](#) of this document.

Note: This document and the screenshots inside it covers the use case of multitenancy being disabled. However, the same concepts outlined here apply. This procedure must be performed for each NAS Volume, and the restore of local users/groups/mapping rules must be done for each tenant.

The procedure to fail back to the primary site follows these high level steps:

1. Choose a period of low activity to fail back to the primary site.
2. Prepare:
 - a. Promote the destination volumes on the secondary cluster, if that is not done already
 - b. Delete the replication schedules on the primary cluster and secondary cluster
3. Set up replication to replicate the NAS volume on the secondary NAS cluster back to the primary NAS cluster
4. Halt IO to the NAS volume on the secondary cluster by deleting shares or moving to NoService mode
5. Promote the NAS volume on the primary cluster, and delete the replication policy
6. Restore the NAS volume configuration on the NAS volume on the primary NAS cluster to recreate all shares, exports, snapshot schedules, and quota rules
7. Redirect clients to the primary NAS cluster
8. Re-establish replication from the primary site back to the secondary site

Step 1: Create Replication (on secondary NAS cluster)

On the secondary NAS cluster, click the secondary NAS volume and select “Create Replication”

The screenshot displays the NetApp ONTAP management interface for a secondary NAS cluster. The left sidebar shows the navigation tree with 'VOL0_REP' selected under 'NAS Volumes'. The main panel shows the 'VOL0_REP' volume details, including a progress bar for '2.58 MB' out of '500 GB'. The 'Replications' tab is active, and a 'Create Replication' button is highlighted in the top right corner. The status message at the bottom indicates 'NAS Volume is not configured for Replication'.

NAS Volume Status			
Size	500 GB	Used Space	2.58 MB (0%)
Space Provisioning	Thin	Unused Space	500 GB (100%)
Overcommitted Space	0 MB	Used Space Threshold	90%
		Unused (Reserved) Space	0 MB
		Unused (Unreserved) Space	500 GB

Replications

NAS Volume is not configured for Replication

Step 2: Choose Remote Cluster and Snapshot Retention Policy (on secondary NAS cluster)

Choose the remote NAS cluster (primary site NAS cluster) from the drop-down list, and click Next. Typically in a failback scenario the best choice is "Identical". If any unneeded snapshots are replicated this will only provide more protection of data. Snapshots can always be deleted from the source prior to replication, or the destination NAS volume after replication finishes.

You may also want to select an inline data reduction method and QoS node.

Create Replication [VOL0_REP]

Remote FluidFS Cluster: RevDev8

Snapshot Retention Policy at the Destination:

- ☒ **Identical to Source**
Keep snapshots in the source and destination NAS volumes similar. Optimal choice for a disaster recovery site.
- ☐ **Minimum**
Delete snapshots as soon as possible and keep only the one that is needed for the replication mechanism itself. Optimal in case of shortage of space on the destination system.
- ☐ **Archive**
Keep snapshots, including ones that were deleted in the source NAS volume, based on their expiration period. Optimal for an archiving system.

Snapshots Retention Period at the Destination: 1 days

If enabled, NAS volume replication will try to optimize network utilization by reducing the amount of data copied

Inline Data Reduction for Replication Optimization: ☐ **Enabled**

Inline Data Reduction Method:

- ☐ Conditional Compression
- ☐ Deduplication and Conditional Compression
- ☐ Compression
- ☐ Deduplication and Compression
- ☐ Deduplication

If enabled, replication bandwidth utilization over time will be limited according to pre-defined Quality of Service (QoS) node.

⚠ To enable QoS, create at least one QoS node

Limit Replication Bandwidth: ☐ **Enabled**

Limit Replication Bandwidth According to QoS Node:

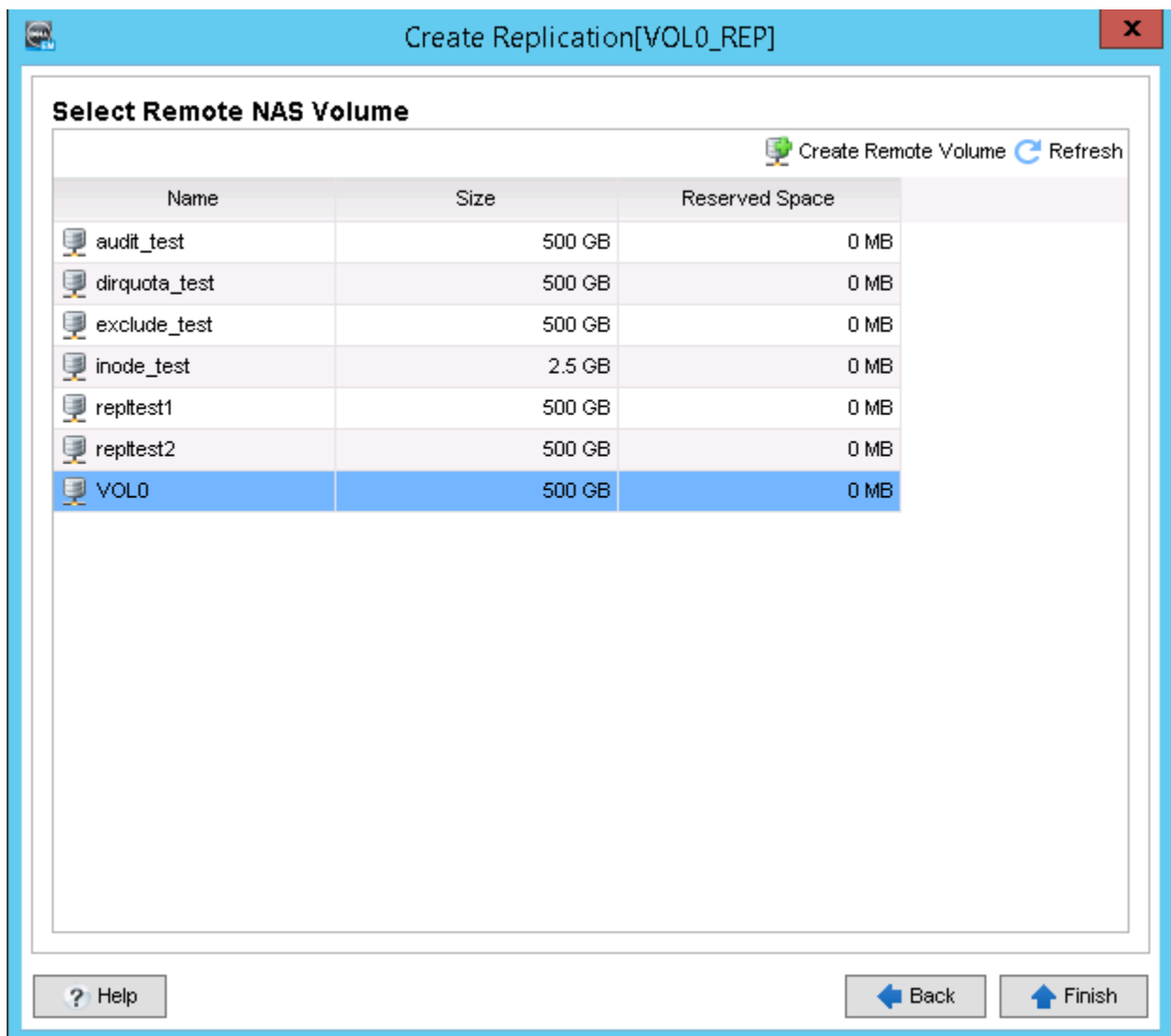
? Help Cancel Next

Step 3: Select Volume (on secondary NAS cluster)

Select the volumes previous source NAS volume, and click Finish.

If the original primary NAS volume is still present, FluidFS will only replicate the changed/new data from the secondary site back to the primary site. However, any new or changed data on the primary site, that has been changed or written after the last replication between the two NAS volumes, **will be lost**. The secondary NAS volume uses the "base replication snapshot" that is kept from the last replication, which is identical on the primary and secondary NAS volume, in order to establish a baseline between the two NAS volumes.

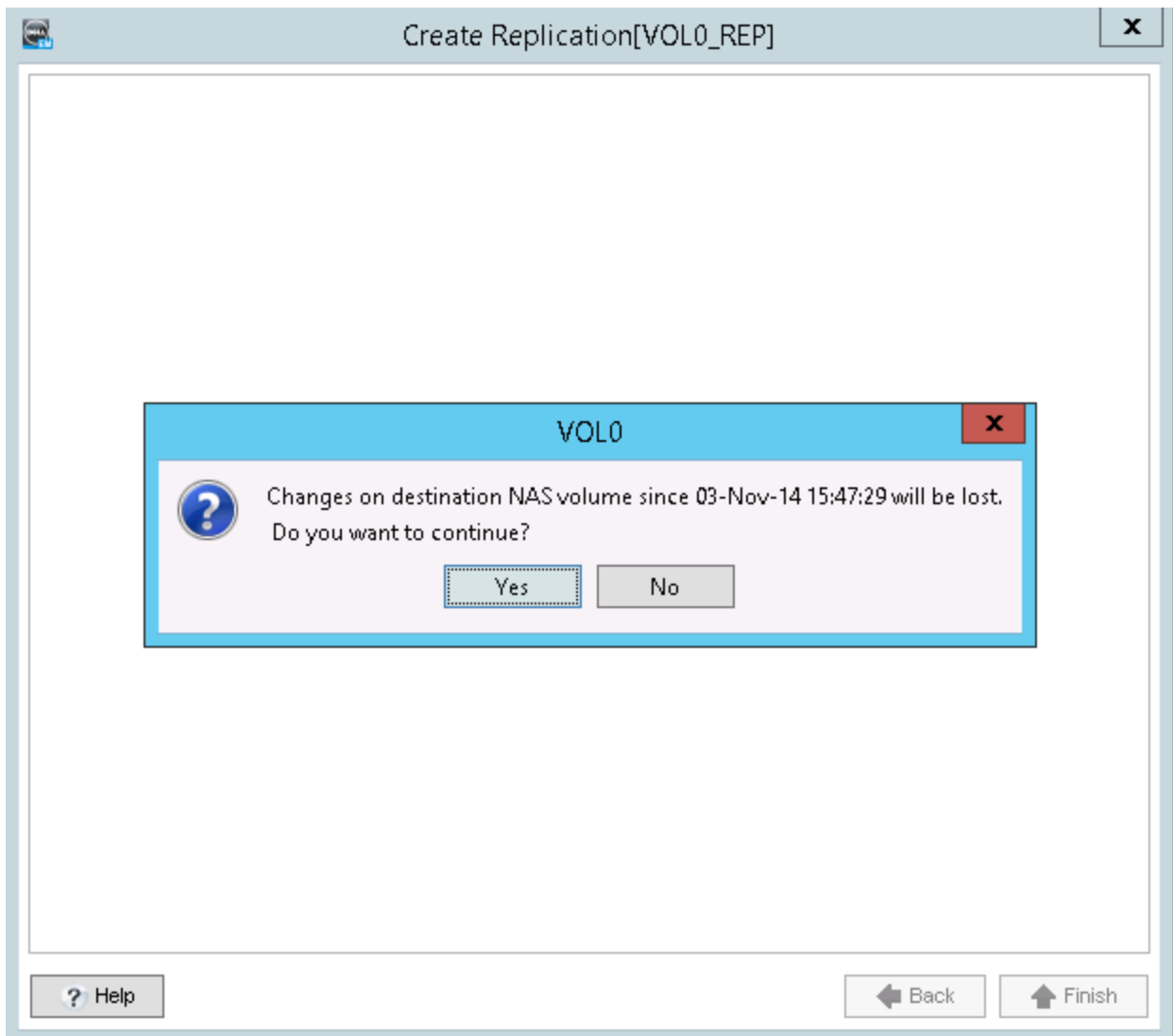
If the original primary NAS volume is no longer present, FluidFS will replicate the entire NAS volume back to the primary site. Please note that this initial replication can take a long time, depending on the amount of data that needs to be replicated from the secondary site back to the primary,



The screenshot shows a window titled "Create Replication[VOLO_REP]" with a red close button in the top right corner. Inside the window, there is a section titled "Select Remote NAS Volume". Above the table, there are two links: "Create Remote Volume" (with a green plus icon) and "Refresh" (with a blue circular arrow icon). The table has three columns: "Name", "Size", and "Reserved Space". The "VOLO" volume is selected, highlighted in blue. Below the table, there is a large empty rectangular area. At the bottom of the window, there are three buttons: "? Help", "< Back", and "Finish >".

Name	Size	Reserved Space
audit_test	500 GB	0 MB
dirquota_test	500 GB	0 MB
exclude_test	500 GB	0 MB
inode_test	2.5 GB	0 MB
reptest1	500 GB	0 MB
reptest2	500 GB	0 MB
VOLO	500 GB	0 MB

When failing back, when the original source NAS volume is selected, this message will appear below. Any changes that took place on the original source NAS volume since the last replication will be lost.



Step 4: Initiate a Manual replication from the secondary NAS volume to the primary NAS volume (on secondary NAS cluster)

Step 5: Wait for the replication to finish

Ideally, the failback procedure will take place during off hours when there is minimal I/O to the secondary NAS cluster. Manual replication can be repeatedly triggered to synchronize changes, or a replication schedule can be set up if desired.

Step 6: Promote the primary NAS volume (on primary or secondary NAS cluster)

NOTE: Once the primary site NAS volume is promoted, it will become read+write, and replications will stop. In order to avoid data loss, its important to halt all I/O to the volume on the secondary NAS cluster, so the data matches on the secondary NAS volume and the primary NAS volume.

I/O can be halted on the secondary NAS cluster by deleting shares/exports, or changing the filesystem into NoService mode.

Promote the primary site NAS volume by clicking on it and then selecting "Promote Destination". This will make the primary NAS volume read/write instead of read-only.

The screenshot displays the NetApp OnCommand System Manager interface. The left sidebar shows a tree view with 'RevDev9' selected, containing 'NAS Volumes', 'SMB Shares', 'NFS Exports', 'Client Accessibility', 'Replications', 'Cluster Connectivity', and 'Cluster Maintenance'. The main panel is titled 'VOL0_REP' and shows the 'Replications' tab. A table lists the replication details:

Role in Replication	Remote FluidFS Cluster	Remote NAS Volume	Achieved Recovery Point
Destination	RevDev8	VOL0	1/20/17 3:16:23 PM

Below the table, the 'Replication Status' section shows the status as 'Idle' and a 'Promote' button. The 'Replication Partnership' section shows details for the replication pair, including 'Role in Replication' (Destination), 'Remote FluidFS Cluster' (RevDev8), 'Remote NAS Volume' (VOL0), and various optimization settings like 'Snapshot Retention Policy' and 'Inline Data Reduction'. The 'Replication Schedules' section is also visible at the bottom.

Step 7: Delete the Replication Schedule (on secondary NAS cluster)

FluidFS requires that the replication schedule is first deleted, before the Replication Policy can be deleted.

The screenshot displays the FluidFS management console with the 'Replications' tab selected. The main content area shows the configuration for 'RevDev9 [VOL0_REP]'. On the left, a table lists the replication details:

Role in Replication	Remote FluidFS Cluster	Remote NAS Volume	Achieved Recovery Point
Source	RevDev9	VOL0_REP	1/20/17 3:24:56 PM

On the right, the 'Replication Resource Balance' is shown as 'Normal', and the 'Achieved Recovery Point' and 'Target Recovery Point' are both '1/20/17 3:24:56 PM'. Below this, the 'Replication Partnership' section shows the role as 'Source' and the remote cluster as 'RevDev9'. The 'Replication Schedules' section at the bottom shows a single schedule, 'ReplicationSchedule0', with a frequency of 'Every 1 hours'. The 'Delete' button for the schedule is highlighted in yellow.

Step 8: Delete the Replication Policy (on secondary NAS cluster)

After promoting the primary site NAS volume, you can “Disconnect” the replication policy between the NAS volumes by doing a **Delete** from Dell Storage Manager.

The screenshot displays the Dell Storage Manager web interface. The top navigation bar includes tabs for Summary, File System, Hardware, NAS Pool, Events, Performance, and Charting. The left sidebar shows a tree view with RevDev9 expanded, containing NAS Volumes, SMB Shares, NFS Exports, Client Accessibility, Client Activity, Replications, Cluster Connectivity, and Cluster Maintenance. The main content area is titled 'VOL0_REP' and shows the 'NAS Volume Status' for a 500 GB volume. Below this, the 'Replications' tab is active, displaying a table with one replication policy. The 'Delete' button is highlighted in yellow. The right sidebar shows the 'Replication' status for the selected policy.

NAS Volume Status

2.58 MB

Size	500 GB	Used Space	2.58 MB (0%)	Data Reduction S
Space Provisioning	Thin	Unused Space	500 GB (100%)	Snapshot Space
Overcommitted Space	0 MB	Used Space Threshold	90%	
		Unused (Reserved) Space	0 MB	
		Unused (Unreserved) Space	500 GB	

Replications

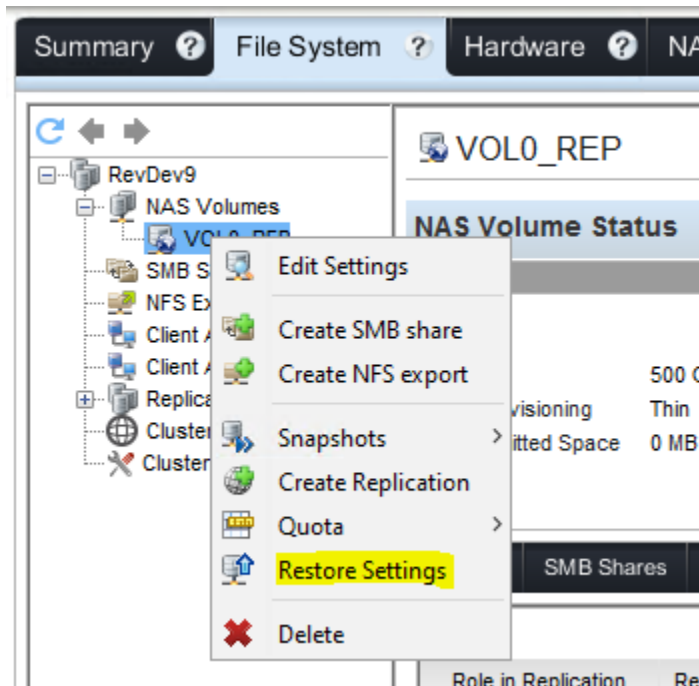
Role in Replication	Remote FluidFS Cluster	Remote NAS Volume	Achieved Recov
Source	RevDev8	VOL0	1/20/17 3:24:56

Replication

Status
Replication Res
Achieved Reco
Target Recover

Step 9: Right-click on the primary site NAS volume and click “Restore Volume Config” (on primary NAS cluster)

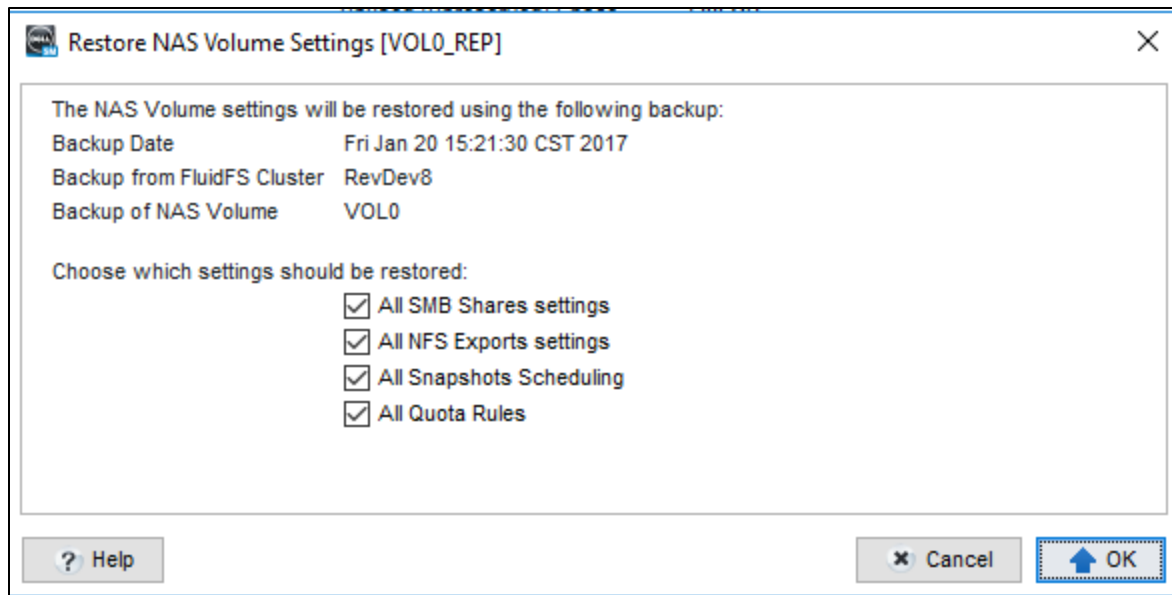
This will restore the shares, exports, snapshot schedules, and quota rules.



Step 10: Restore NAS Volume Configuration (on primary NAS cluster)

By default, all available configuration files are checked. Click “OK”

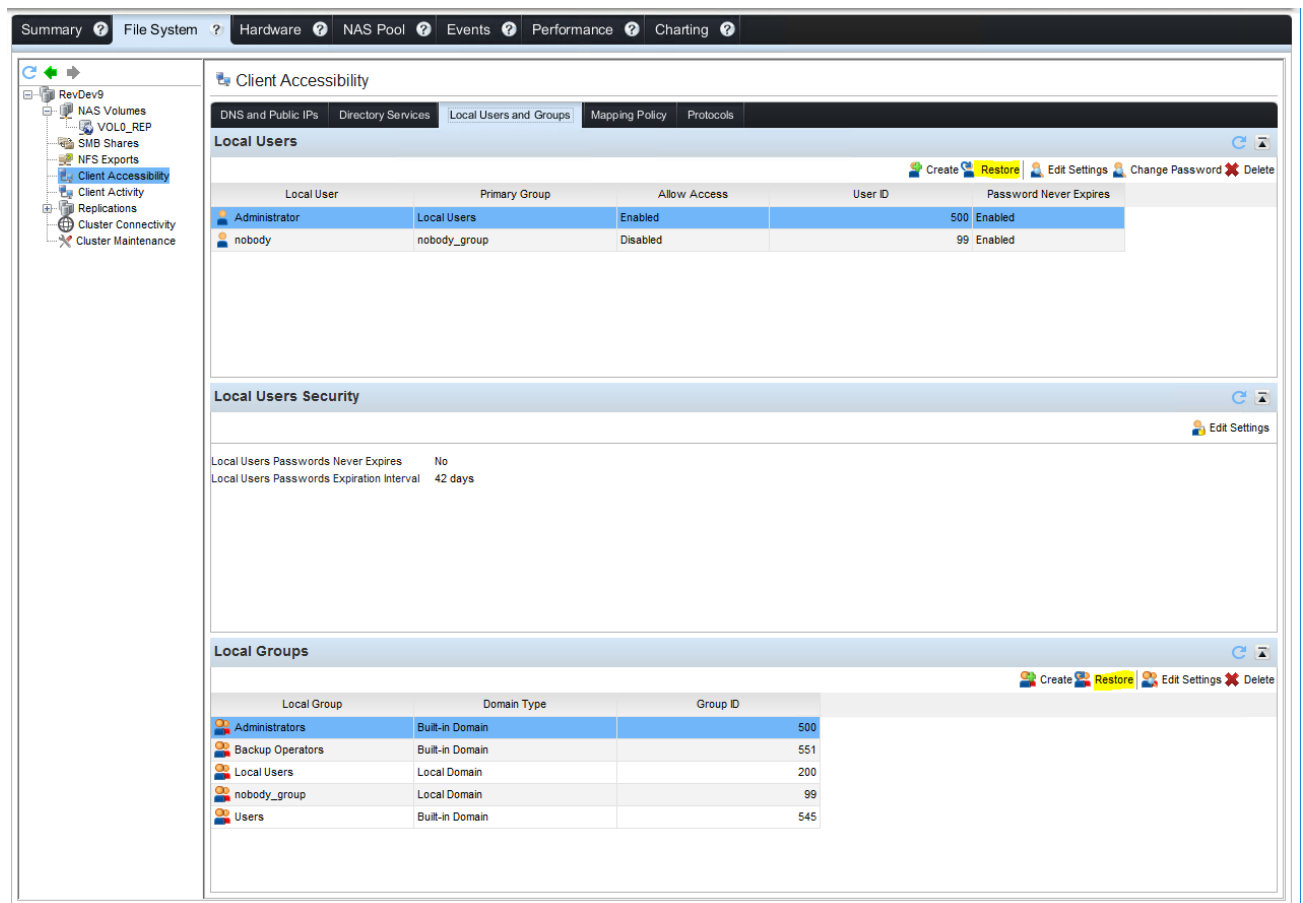
Note: Directory Quotas and Redirection folder objects do not need to be restored. The administrator can look at the replication destination volume and see that Directory Quotas and Redirection Folders are present after the first replication.



Step 11: Restore other cluster-wide configuration items (on primary NAS cluster)

If best practices are being followed, the primary NAS cluster will already be configured with all environmental services such as DNS, NTP, Active Directory, LDAP/NIS, etc... But in the case that it is not, these must be configured.

Additionally, if local users/groups, or manual user mappings are in place, those must be manually restored. Local users and groups can be restored through Dell Storage Manager:



Any manual user mapping rules that are defined must be restored using the FluidFS Command Line Interface using the command "access-control mapping manual restore".

Any networking configuration changes will have to be made manually. FluidFS does not have any automated method to restore network settings (such as IP's or static routes).

NOTE: Dell EMC recommends as a best practice to document all network settings (IP addresses, default gateway, static routes) so that if needed they can be restored onto the secondary site.

Step 12: Repoint clients to the primary NAS cluster/NAS volume

At this point, the storage admin has 2 options of how to point clients to the primary NAS cluster:

1. Change the DNS entry that originally pointed to the Virtual IPs of the secondary site to point to the primary NAS cluster's Virtual IPs. Ensure that the DNS server(s) that the primary NAS cluster is using is the same DNS server(s) (or in the same DNS farm) as the DNS server(s) the secondary NAS cluster is using. Existing client connections will break and need to be re-established. All NFS exports must be unmounted and mounted back on every client system.

2. Change the IP's on the primary NAS cluster to be identical to the secondary NAS clusters IPs. Choosing this option allows for NFS hosts to not have to unmount/remount all of the NFS exports.

Now, users and applications are working off the primary NAS cluster.

Step 13: Update Active Directory SPN's to reflect the switch

This step must be performed for SMB access which uses Kerberos. If the cluster is being accessed via SMB using a name (such as *nas01.mycompany.com*, as opposed to IP) then odds are Kerberos is being used. In order for the secondary cluster to provide service using the primary cluster's DNS name, the Service Principle Names (SPN's) must be updated in Active Directory.

This step must be performed by an Active Directory administrator, preferably someone with Domain Administrator rights. This is done from the Windows cmd.exe

1. Remove SPNs from the PrimarySystem
 - a. `setspn -D HOST/<nas hostname> <PrimarySystem name>`
 - b. `setspn -D nfs/<nas hostname> <PrimarySystem name>`
 - c. `setspn -D nfs/<nas FQDN> <PrimarySystem name>`
 - d. `setspn -D HOST/<nas FQDN> <PrimarySystem name>`
2. Create SPNs on the SecondarySystem
 - a. `setspn -S HOST/<nas hostname> <SecondarySystem name>`
 - b. `setspn -S nfs/<nas hostname> <SecondarySystem name>`
 - c. `setspn -S nfs/<nas FQDN> <SecondarySystem name>`
 - d. `setspn -S HOST/<nas FQDN> <SecondarySystem name>`
 - e. `setspn -S HOST/<nas-vip> <SecondarySystem name>`

SPN's for a computer object can be listed using "setspn -l <ComputerObjectName>

[See Step 6 in section 5.1 for an example](#)

Step 14: Re-establish replication from the primary NAS cluster to the secondary NAS cluster for all NAS volumes

6 Planned Failover Procedure

Often times, IT organizations wish to test their DR plan by conducting a planned failover of the entire NAS cluster, or maybe just a few NAS volumes (for a select number of applications). Additionally, planned maintenance may result in power outages, network outages, etc... and require a planned failover from the primary site to the secondary (DR) site. This section covers how to conduct a planned failover and failback of a full NAS cluster, as well as a planned failover and failback of individual NAS volumes.

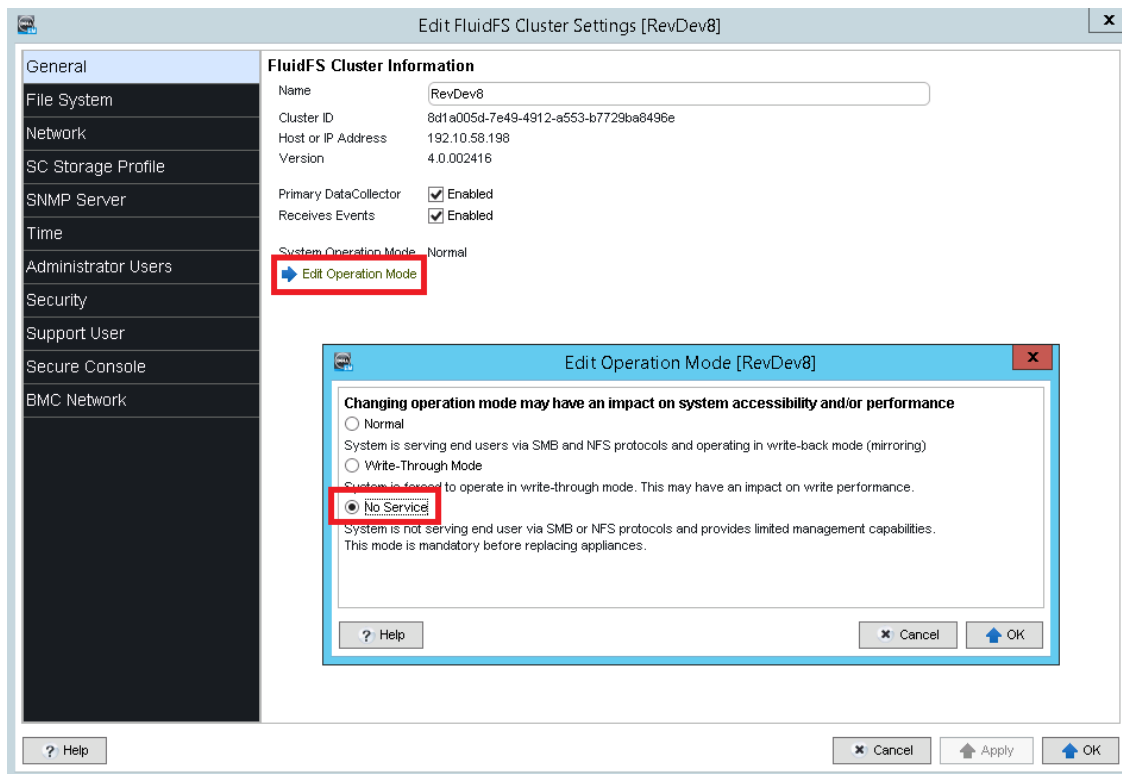
It is important to note however, that the best way to test out data on a secondary/DR volume is to use volume clones, which is detailed in [Section 7 – Testing Disaster Recovery using Volume Clones](#).

6.1 Full Cluster Planned Failover and Failback

The full cluster planned failover and failback procedure is nearly identical to the steps outlined in [Section 5 – Disaster Recovery Procedure](#). The main difference is that the primary NAS cluster must be “forced” to take all shares offline. This is accomplished by putting the primary NAS cluster into “NoService” mode. This can be done in the FluidFS CLI using the command:

```
maintenance internal service-mode set NoService
```

Alternatively, this can be done in Dell Storage Manager by right clicking on the NAS cluster, and then clicking “Edit Settings”:



The full NAS cluster **planned failover** procedure follows these high level steps:

1. (On Primary NAS Cluster) Promote the secondary NAS volume
2. (On Secondary NAS Cluster) Right-click on the remote site NAS volume and click "Restore Volume Config".
3. (On Secondary NAS Cluster) Restore NAS Volume Configuration
4. (On Secondary NAS Cluster) Restore other cluster-wide configuration items
5. (On Primary NAS Cluster) Change to "NoService" mode to bring down all shares and exports
6. (Using DNS or change IPs on secondary NAS cluster) Repoint clients to the secondary NAS cluster/NAS volume
7. Update SPN's in Active Directory
8. (On Primary NAS Cluster) Delete the Replication which is using the primary as the source and the secondary as the destination

The full NAS cluster **planned failback** procedure follows these high level steps:

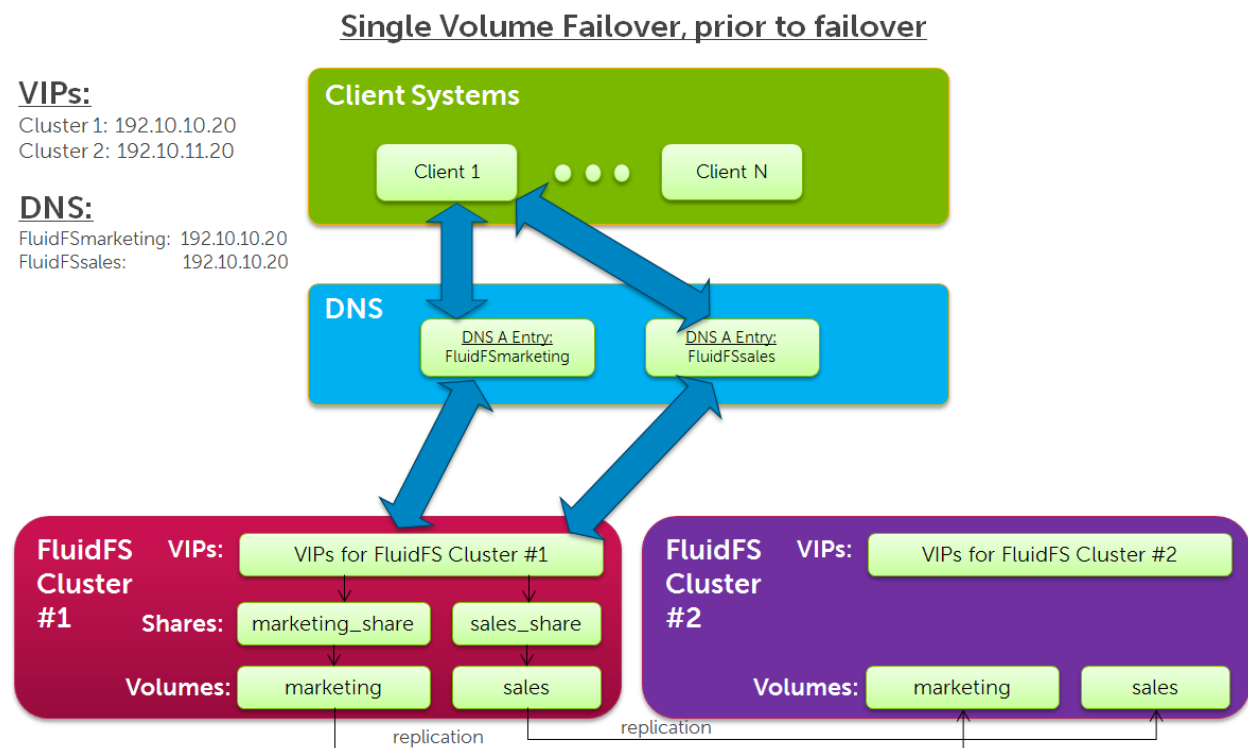
1. (On Secondary NAS Cluster) Create Replication using the secondary NAS volume as the source and the primary NAS volume as the destination
2. (On Secondary NAS Cluster) Choose Remote Cluster and Snapshot Retention Policy
3. (On Secondary NAS Cluster) Select Volume on primary NAS cluster to replicate to
4. (On Secondary NAS Cluster) Create a schedule for the replication
5. (On Secondary NAS Cluster) Create the replication schedule and click OK.
6. (On Secondary NAS Cluster) Wait for the replication to finish
7. (On Secondary NAS Cluster) Promote the primary NAS volume
8. (On Primary NAS Cluster) Right-click on the primary site NAS volume and click "Restore Volume Config".
9. (On Primary NAS Cluster) Restore NAS Volume Configuration
10. (On Primary NAS Cluster) Restore other cluster-wide configuration items
11. (On Secondary NAS Cluster) Change to "NoService" mode to bring down all shares and exports
12. (Using DNS or change IPs on primary NAS cluster) Repoint clients to the primary NAS cluster/NAS volume
13. Update SPN's in Active Directory
14. (On Secondary NAS Cluster) Delete the Replication which is using the secondary as the source and the primary as the destination
15. (On Primary NAS Cluster) Recreate replication using the primary NAS volume as the source and the secondary NAS volume as the destination

7 Single NAS Volume Planned Failover and Failback

For single NAS volume failover, it is important that the environment is set up to properly migrate clients of the NAS volumes you are failing over, without disrupting the clients of other NAS volumes you are not failing over.

When a NAS volume is failed over from one NAS cluster to another, the IP addresses that are used to access it change from NAS Cluster A's IP addresses to NAS Cluster B's IP addresses. Dell EMC recommends facilitating this change using DNS. It is recommended to set up a DNS entry to correlate to each NAS volume, and change the DNS entry for single NAS volumes when they are failed over.

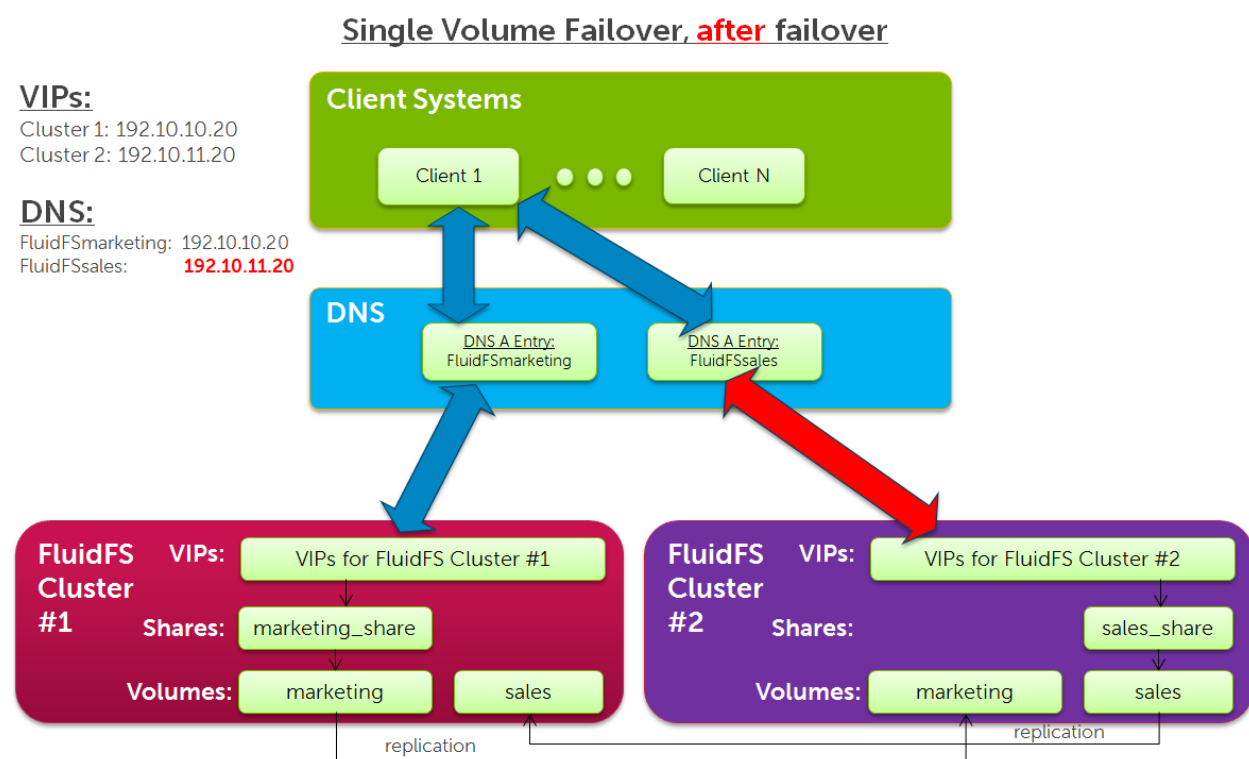
For example, suppose Marketing and Sales have their own NAS volumes, with an SMB share on the NAS volume named **marketing_share** and **sales_share** respectively. A DNS A (host) entry named **FluidFSmarketing**, is created for Marketing and another DNS A (host) entry for Sales named **FluidFSsales** is created. Both NAS volumes point to the same set of VIPs on source NAS Cluster A. Marketing can access the Marketing SMB share using **\\FluidFSmarketing\\marketing**, and Sales can access the Sales SMB share using **\\FluidFSsales\\sales**. The topology looks like this diagram below. For simplicity, only one VIP was used, but in reality there are usually more than one.



Initially, both DNS entries **FluidFSmarketing** and **FluidFSsales** point to the same set of VIPs. At this point, both the **marketing** and **sales** SMB shares can be accessed from either one of the DNS names, since FluidFS serves all shares through all VIP's by default. When you want to fail over a single NAS volume (for example **sales**) change the DNS entries for **FluidFSsales** to resolve to the VIPs on Cluster B. Client systems may need to

refresh their DNS cache. DNS entries can also be created with lower TTLs to make failing back quicker. Also, SPN's will need to be updated on active directory, as previously described in this document. To force SMB and NFS clients to NAS Cluster B, you must delete the SMB shares and NFS exports on NAS Cluster A. This forces the SMB and NFS clients to reconnect, at such time they are connected to NAS Cluster B.

After restoring the source volume's configuration on NAS Cluster B, all of the SMB shares and NFS exports will be present on the target NAS volume (on NAS Cluster B), so no SMB share/NFS export configuration information is lost. The failed over NAS volume can now be accessed using the exact same DNS name and SMB share/NFS export name as it was when hosted on NAS Cluster A, except now it is hosted on NAS Cluster B. After the single NAS volume failover for the **sales** volume, the topology will look like this:



To fail back from NAS Cluster B to NAS Cluster A, the same procedure is run in reverse.

Dell EMC recommends that you maintain accurate and detailed records/tables to track which DNS entries are used to access each NAS volume. This helps when performing failover and setting up group policies.

Throughout this process, please keep in mind that when DNS entries are changed, it is likely SPN's in Active Directory will also need to be changed (for SMB/CIFS access) as previously described in this document. For NFS access, SPN's don't come into play.

8 Testing Disaster Recovery using Volume Clones

FluidFS has the ability to create Thin Volume Clones of a NAS volume utilizing its snapshots. This feature is a powerful tool for testing disaster recovery, without affecting production volumes. Often times, administrators will have application servers that reside in a test environment, and wish to test out their DR plan, but they don't want to affect production. FluidFS Thin Volume Clones are a perfect tool for facilitating this.

As has been discussed earlier in this document, when a NAS volume is a replication secondary NAS volume, it is in a read-only state. In order to change the secondary NAS volume from read-only to read/write, it must be promoted. However, that will result in replication pausing for the time period that the secondary NAS volume is in the "promoted" state. Using Thin Volume Clones allows the replication to continue on its normal schedule, while testing DR.

The procedure to test failover and failback using Thin Volume Clones is below:

1. Select the secondary NAS cluster in Dell Storage Manager
2. On the secondary NAS cluster, select the secondary NAS volume in Dell Storage Manager
3. Navigate to the "Snapshots" tab
4. To create a thin volume clone from the last replication snapshot, right click on the snapshot that starts with "rep_". This snapshot represents the state of the source NAS volume at the time point of the last scheduled replication. Any other snapshot can be chosen as well.
5. Select "Create NAS Volume Clone" and create a NAS Volume Clone
6. Create an SMB share or NFS export on that NAS volume clone
7. Repoint the application to the DNS name of the secondary NAS cluster, and point it to the NFS export or SMB share on the clone of the secondary NAS volume.
8. If the administrator wishes to test failback, the clone of the secondary NAS volume can be replicated to a new, empty NAS volume on the primary NAS cluster. This assumes that adequate space is available on the primary NAS cluster to duplicate data. Keep in mind that if there is a large amount of data, replicating the entire dataset can take some time.
9. After the clone of the secondary NAS volume finishes replicating to the new NAS volume on the primary NAS cluster, an SMB share or NFS export will need to be created on the new NAS volume on the primary NAS cluster.
10. Repoint the application to the DNS name of the primary NAS cluster, and point it to the NFS export or SMB share on the new NAS volume on the primary NAS cluster.
11. After testing is completed, the application can be pointed back to the main/production NFS export or SMB share, if the administrator so chooses.

A Appendix A: Scripting failover/failback using the FluidFS CLI

One way to optimize the amount of time taken to perform the failover/failback procedure is to script against the FluidFS Command Line Interface. The FS8600 Administrators Guide details how to set up passwordless SSH from a Linux host. For the examples given in this Appendix, we will assume that passwordless SSH was set up using the "Administrator" user. The commands given here will follow the failover and failback procedures detailed in this document.

Note: This procedure must be performed for each NAS volume that the administrator wishes to fail over. In cases where there is a high number of volumes in use, this procedure can be scripted against the FluidFS Command Line Interface. This is covered in [Appendix A](#) of this document.

Note: This document and the screenshots inside it covers the use case of multitenancy being disabled. However, the same concepts outlined here apply. This procedure must be performed for each NAS Volume, and the restore of local users/groups/mapping rules must be done for each tenant.

The CLI commands are different depending on whether multitenancy is enabled or not. This appendix gives CLI commands assuming multitenancy is disabled.

As a reminder, the key parameters are in the table below:

Parameter	Value
Source NAS Cluster	RevDev8
Source NAS Volume	VOL0
Source NAS Cluster Virtual IP	192.168.10.50/24 – DNS Name PrimaryVIP
Destination NAS Cluster	RevDev9
Destination NAS Volume	VOL0_REP
Destination NAS Cluster Virtual IP	192.168.11.50/24 – DNS Name SecondaryVIP

A.1 Replication Setup

The script to perform the failover procedure follows these high level steps:

- Create replication partnership
- Create secondary NAS volume
- Connect source and destination NAS volume
- Create a schedule to replicate once per hour

For example, the script from the Linux client would look like this:

```
ssh Administrator@PrimaryVIP environment data-protection cluster-partnerships add  
SecondaryVIP  
ssh Administrator@SecondaryVIP NAS-volumes add-volume VOL0_REP 500GB  
ssh Administrator@PrimaryVIP NAS-volumes volumes VOL0 replication connect RevDev9 VOL0_REP
```

```
ssh Administrator@PrimaryVIP NAS-volumes volumes VOL0 replication schedules add RevDev9  
VOL0_REP Rep0 Periodic -Period 60
```

A.2 Failover CLI Scripting

The high level steps, along with the CLI commands to perform these steps, **run against the secondary cluster**, within the context of this example, are as follows:

- promote secondary NAS volume
 - NAS-volumes replication promote VOL0_REP RevDev8 VOL0
- restore NAS volume config
 - NAS-volumes configuration-backups restore-configuration VOL0_REP CifsShare,NfsExport,QuotaRule,SnapshotSchedule
- (optional)
 - restore local users
 - access-control local-users restore RevDev8
 - access-control local-groups restore RevDev8
 - restore manual user mapping
 - access-control mapping manual restore RevDev8
- Update DNS or change IPs
- delete replication
 - NAS-volumes replication disconnect VOL0_REP RevDev8 VOL0

For example, the script from the Linux client would look like this:

```
ssh Administrator@SecondaryVIP NAS-volumes volumes VOL0_REP replication promote RevDev8 VOL0  
  
ssh Administrator@SecondaryVIP NAS-volumes volumes VOL0_REP configuration-backups restore-  
configuration CifsShare,NfsExport,QuotaRule,SnapshotSchedule  
  
ssh Administrator@SecondaryVIP client-access authentication local-users restore RevDev8  
  
ssh Administrator@SecondaryVIP client-access authentication local-groups restore RevDev8  
  
ssh Administrator@SecondaryVIP client-access authentication mapping manual restore RevDev8  
  
ssh Administrator@SecondaryVIP NAS-volumes volumes VOL0_REP replication disconnect RevDev8  
VOL0
```

After the script is run, either DNS should be updated, or the IP's on the secondary NAS cluster changed to match those of the primary site. The DNS updates can be scripted in cmd or Powershell. Don't forget that the SPN's in Active Directory will need to be updated as well.

A.3 Failback CLI Scripting

The high level steps, along with the CLI commands to perform these steps, **run against the primary and secondary NAS cluster**, within the context of this example, are as follows:

- Create replication from secondary site to primary site (Run from Secondary NAS Cluster)
 - NAS-volumes replication connect VOL0_REP RevDev8 VOL0
- Trigger manual replication (Run from Secondary NAS Cluster)
 - NAS-volumes replication start VOL0_REP RevDev8 VOL0
- promote primary volume (Run from Primary NAS Cluster)
 - NAS-volumes replication promote VOL0 RevDev9 VOL0_REP
- restore volume config (Run from Primary NAS Cluster)
 - NAS-volumes configuration-backups restore-configuration VOL0 CifsShare,NfsExport,QuotaRule,SnapshotSchedule
- (optional)
 - restore local users (Run from Primary NAS Cluster)
 - access-control local-users restore RevDev9
 - access-control local-groups restore RevDev9
 - restore manual user mapping (Run from Primary NAS Cluster)
 - access-control mapping manual restore RevDev9
- Update DNS or change IPs
- delete replication (Run from Primary NAS Cluster)
 - NAS-volumes replication disconnect VOL0 RevDev9 VOL0_REP

For example, the script from the Linux client would look like this:

```
ssh Administrator@SecondaryVIP NAS-volumes volumes VOL0_REP replication connect RevDev8 VOL0
ssh Administrator@SecondaryVIP NAS-volumes volumes VOL0_REP replication start RevDev8 VOL0
```

Wait for the replication to finish...

```
ssh Administrator@PrimaryVIP NAS-volumes volumes VOL0 replication promote RevDev9 VOL0_REP
ssh Administrator@PrimaryVIP NAS-volumes volumes VOL0 configuration-backups restore-configuration CifsShare,NfsExport,QuotaRule,SnapshotSchedule
ssh Administrator@PrimaryVIP client-access authentication local-users restore RevDev9
ssh Administrator@PrimaryVIP client-access authentication local-groups restore RevDev9
ssh Administrator@PrimaryVIP client-access authentication mapping manual restore RevDev9
ssh Administrator@PrimaryVIP NAS-volumes volumes VOL0 replication disconnect RevDev9 VOL0_REP
```

After the script is run, either DNS should be updated, or the IP's on the primary NAS cluster changed to match those of the secondary site. The DNS updates can be scripted in cmd or Powershell. Don't forget that the SPN's in Active Directory will need to be updated as well.

B Appendix B: Additional resources

[All FluidFS Technical Collateral on Dell TechCenter](#)

[FluidFS Scripting Best Practices Guide](#)

[FluidFS Migration Best Practices Guide](#)

[FS8600 Disaster Recovery Best Practices Guide \(this document\)](#)

Additional resources below located at <http://kc.compellent.com>