Understanding Snapshots in Dell FluidFS Network-Attached Storage

Compellent FS8600
EqualLogic FS7600, FS7610
PowerVault NX3600, NX3610

A Dell Technical White Paper

Enterprise Storage Solutions Engineering
Dell Enterprise Solutions Group
January 2013
Acknowledgements

This white paper was produced by the Dell Enterprise Storage Solutions Engineering team.

Authors: Sharon Hanson, Raj Hosamani, and Animesh Pillai

Thanks to these Dell team members for their significant support during development and review:

Akin Akinboro, Ron Stefani and Dell Enterprise Storage Solutions Engineering

Feedback

We welcome your feedback. E-mail us at StorageSolutionsFeedback@Dell.com.

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

Disclaimer: The performance tests and results in this document were measured using specific configurations within the Dell performance labs as of October 2012. Actual performance results will vary based on the system configuration, applications, and manufacturing variability. These results should be used as a relative indicator only.

© 2013 Dell Inc. All rights reserved. Reproduction of this material in any manner whatsoever without the express written permission of Dell Inc. is strictly forbidden. For more information, contact Dell.

Dell, the DELL logo, the DELL badge, PowerVault, Compellent, and EqualLogic are trademarks of Dell Inc. Microsoft and Windows are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

January 2013
## Contents

1. Introduction ........................................................................................................................................................ 1
2. FluidFS: Architected for Data Protection ...................................................................................................... 2
   2.1 High Availability .......................................................................................................................................... 2
   2.2 Data Integrity .............................................................................................................................................. 2
   2.3 Metadata Integrity ..................................................................................................................................... 3
3. FluidFS Snapshots Overview ........................................................................................................................... 4
   3.1 FluidFS Redirect-on-Write Snapshots ................................................................................................... 4
   3.2 Configuring FluidFS Snapshots ............................................................................................................... 5
   3.3 Accessing FluidFS Snapshots ................................................................................................................... 5
   3.4 Restoring Data ........................................................................................................................................... 5
4. Understanding the Size of FluidFS Snapshots .............................................................................................. 7
   4.1 FluidFS “Snapshot Size” and “Delta Size” ................................................................................................ 7
      4.1.1 Create Snapshot 1 ............................................................................................................................ 8
      4.1.2 Update Active File System .............................................................................................................. 9
      4.1.3 Create Snapshot 2 ............................................................................................................................ 9
      4.1.4 Update Active File System and Create Snapshot 3 .................................................................. 10
      4.1.5 Delete Snapshot 1 .......................................................................................................................... 10
5. Planning For and Monitoring the Snapshot Reserve ................................................................................12
   5.1 Potential Causes of Unexpected Snapshot Growth ...........................................................................13
6. Snapshots and Performance ......................................................................................................................... 15
7. Typical Use Cases for Snapshots ................................................................................................................. 16
8. Conclusion ........................................................................................................................................................ 17

Appendix A Additional Resources .................................................................................................................. 18
Appendix B Working with FluidFS Snapshots: Compellent FS Series and PowerVault NX Series .... 19
   8.1 Creating Snapshots ................................................................................................................................. 19
      8.1.1 FluidFS Graphical User Interface ................................................................................................. 19
      8.1.2 FluidFS Command Line Interface ................................................................................................ 19
   8.2 Creating Snapshot Schedules ............................................................................................................... 19
      8.2.1 FluidFS Graphical User Interface ................................................................................................. 20
      8.2.2 FluidFS Command Line Interface ................................................................................................ 20
   8.3 Restoring from a Snapshot .....................................................................................................................21
      8.3.1 Restoring Single File....................................................................................................................... 22
1 Introduction

Snapshots are an important component of a data protection strategy because they provide instant point-in-time copy and recovery of important data, without compromising performance. Though most storage systems have built-in support for snapshots, the design criteria and usability differs from vendor to vendor.

Snapshots are part of the data protection capabilities built into the Dell™ Fluid File System (FluidFS). FluidFS underlies Dell Compellent™ FS Series, EqualLogic™ FS Series, and PowerVault™ NX Series NAS solutions. It is designed from the ground up to meet customer requirements for data availability, data integrity, high performance, scalability, and data protection. FluidFS also provides an easy-to-use interface for deployment, administration, and general management.

This paper discusses in depth the snapshot data protection capability that is built into FluidFS. The paper reviews the overall FluidFS data protection capabilities, then focuses on FluidFS redirect-on-write snapshots, including snapshot sizing, management and monitoring, performance, and typical use cases.
2 FluidFS: Architected for Data Protection

The Dell Fluid File System architecture was designed from the ground up with data protection and data integrity in mind.

2.1 High Availability

The FluidFS architecture shown in Figure 2 is built from the ground up to be a highly available and scalable enterprise NAS solution. Its no-single-point-of-failure design is enabled by specific FluidFS hardware and software features. Each NAS appliance consists of dual active-active controllers, redundant and hot-swappable power supplies and fans. Furthermore, the FluidFS firmware clusters multiple NAS appliances into a single system. This software intelligence constantly monitors cluster-wide health and provides automatic failover in the unlikely event of a failure.

The strengths of the FluidFS architecture include:

- **Designed for High Availability** — All critical system components are redundant, including hardware and software. Multiple network paths to each controller shield against network failure. In the event of a failure, the workload of a NAS controller is automatically migrated to its partner controller.
- **Mirrored Write Cache** — Write data is mirrored between NAS controllers within an appliance to assure data integrity, while delivering very high write performance.
- **Fault Management System and Automated Recovery** — FluidFS cluster services and I/O controllers are constantly monitored for system integrity. A failed or malfunctioning service triggers internal escalation policies to heal the system. If a controller detects a service failure on a peer controller, it tries to restart the controller before initiating a failover.

2.2 Data Integrity

In general, FluidFS relies on the reliability properties of the underlying storage-area network (SAN) for data-at-rest. This means that the best practices used in SAN design should also apply to designing file logical unit numbers (LUNs) or volumes. For example, RAID6 should be implemented on large-scale unstructured data repositories.

As described earlier, FluidFS also implements data integrity features for data-path protection. These features are important to the FluidFS write-back caching architecture. During normal operation, the write cache, which includes data and metadata, is mirrored between the controller pairs in the FluidFS cluster. If a controller fails, making cache mirroring impossible, the surviving controller enables journaling for all transactions, and shifts from write-back to write-through caching mode. This ensures that the file system remains consistent and that all data is protected in case of additional failures.
In the event of a power outage, the controllers use internal battery power to drain the write cache to a local disk. This approach ensures that all I/O in flight remains consistent and no data is lost. It also ensures that data consistency is not compromised, no matter how long the power outage lasts.

### 2.3 Metadata Integrity

Metadata integrity plays a crucial role in overall NAS operation, especially at the high scaling levels supported by FluidFS. FluidFS is designed with explicit protection mechanisms for metadata.

The FluidFS metadata structures are stored as normal data on the back-end SAN, inheriting the RAID properties and reliability characteristics of the SAN. In addition, FluidFS applies the following metadata protection:

- All metadata updates are journaled for reliable transaction consistency.
- Metadata is fingerprinted using hashing functions.
- Metadata is replicated across different underlying LUNs.
- Metadata replicas are periodically checked against their fingerprints to insure consistency. Soft errors are automatically corrected in-place, with proper administrative alerting.

These FluidFS capabilities provide a solid foundation for a strong data protection strategy. Additional elements built on this foundation are user-restorable snapshots; asynchronous, file-level replication; and NDMP backup capabilities. In the following sections, we explore the FluidFS snapshot capabilities.
3 FluidFS Snapshots Overview

A snapshot is a point-in-time copy of a FluidFS volume\(^1\). Snapshots present a full synthesis of the file system volume, even though only blocks that have changed since the prior image are physically retained. This makes snapshots very space efficient. When the first snapshot of a NAS volume is created, all snapshots created after the baseline snapshot are a delta from the previous snapshot. When performed at regular intervals (daily, hourly, etc.), snapshots provide a view of the file system over time.

A snapshot is not a complete copy of the file system. Instead, it consists of pointers to storage blocks that have changed. This means that snapshots can be performed practically instantaneously, but rely on the source data to restore data. The combination of the source data and snapshot presents the point-in-time copy. For this reason – and the fact that snapshots reside on the same volume as the active data they protect – snapshots are not a replacement for full backups. Instead, they excel at fast recovery of lost or corrupted files, and can also be used for testing, migration operations, replication, or as a consistent source for backup to tape or disk.

3.1 FluidFS Redirect-on-Write Snapshots

Two main methods are used for file system snapshots:

- Copy-on-write
- Redirect-on-write (used by the Dell FluidFS)

Using the copy-on-write method, when a change is written to a file system, the copy-on-write snapshot technique must make a copy of the old data block before writing the new data. First, it reads the old data from the storage block to be overwritten on the source volume. Second, it copies this old data to the snapshot volume. Third, it overwrites the old data on the source volume with the new data. The main drawback to this approach is the significant performance penalty associated with three I/O operations. Its performance overhead renders copy-on-write snapshot mechanisms unusable on production systems or other performance-sensitive systems during normal operational hours.

In contrast, the FluidFS redirect-on-write snapshot technique requires just one I/O operation when writing a change to a file system. The old data is left intact, and new data is written to a new block. Meanwhile, the snapshot still points to the original data blocks so that the snapshot view of the volume looks exactly like it did at the point in time when the snapshot was taken. This approach avoids the performance overhead typical of a copy-on-write operation.

---

\(^1\) A FluidFS volume (or container) is a virtualized volume that consumes storage space in the NAS storage pool. Administrators can create CIFS shares and NFS exports on a NAS volume and share them with authorized users. A FluidFS NAS solution supports multiple NAS volumes.
Snapshots are available to users as a read-only copy of the file system, which allows them to restore their documents without help desk or IT administrator intervention. Administrators can also easily restore very large data sets (terabyte scale) as a whole to a particular point in time. This eliminates long file copies over the network and the need for free space for the recovery process.

3.2 Configuring FluidFS Snapshots

FluidFS snapshots and snapshot policies are configured at the volume level. Snapshot data is stored on the same volume as the data. This approach differs from snapshot solutions that require a reserve space be set up on a separate, dedicated volume. Various FluidFS snapshot policies can be set, including frequency (daily, weekly, monthly, or on-demand), number of snapshots to retain, and percentage of NAS volume space to be used for snapshots. The snapshot space limit specified for a volume defines an alerting threshold, as well as the capacity point at which FluidFS begins expiring older snapshots off the system to make room for newer snapshots. FluidFS supports up to 512 snapshots per NAS volume and 10,000 snapshots per NAS cluster.

3.3 Accessing FluidFS Snapshots

FluidFS snapshots are accessible from any point in the volume in a hidden directory — /snapshots/ — under each NFS export or Windows CIFS share. Each snapshot retains the same security style as its source. Therefore, users can access only their own files based on existing permissions. The data available when accessing a particular snapshot is at the level of the specific share and its subdirectories, ensuring that users cannot access other parts of the file system.

The active file system user and permission information may change based on the change rate over time. When an entire volume is restored or an individual file/folder is copied from a snapshot, the user and permission information stored in the snapshot is restored. The copy operation for an individual file or folder follows the standard UNIX®/NTFS mechanism. This mechanism verifies that the files and folders in the active file system and snapshot have adequate permissions for the operation.

3.4 Restoring Data

There are two ways to restore data from a FluidFS snapshot:

- **Direct file restore** — To recover accidentally deleted or modified files, a user can access the hidden snapshot directory (/snapshots/), find the appropriate snapshot folder (named according to its time of creation), and copy the file(s). This method is useful for the day-to-day restore activities of individual files, testing data sets to identify the proper restore point, and bulk restores of directories.

- **Admin-level NAS volume restore** — An entire NAS volume, irrespective of its size, can be restored from a snapshot instantly using the FluidFS NAS administrative interface or the EqualLogic Group Manager interface (for EqualLogic NAS). When restoring a NAS volume, all snapshots with creation dates that are more recent than the snapshot used for the volume

---

2 Permissions can be impacted by the method the client uses to copy the data and the data’s destination.
3 In Microsoft Windows environments, FluidFS integrates with the Previous Versions tracking feature of Windows Explorer®. Using this tool, end users can directly restore files from snapshots of their home directories.
restore are deleted. In addition, restoring the entire NAS volume disconnects current connections.

The following section documents how to work with FluidFS snapshots, including creating and scheduling, restoring data from, and deleting a snapshot.
4 Understanding the Size of FluidFS Snapshots

FluidFS snapshots are "point-in-time" read-only copies of the active file system. When a snapshot is created, it consists of pointers to the actual data stored in the active file system. Initially, a snapshot does not consume any space. As the active file system blocks are updated over time, each update to an original file system block is redirected by the FluidFS redirect-on-write mechanism to a new block. The original data that has been changed is stored in the snapshot, which begins to consume snapshot capacity. The pointers associated with the active file system and snapshot are updated to reflect the new layout. Thus, the size of a snapshot can be an indication of the level of updates to the active file system since the snapshot was created.

This process is depicted in Figure 2, which shows the file system before and after a snapshot is taken — "Before Snapshot" and "After Snapshot 1." Snapshot 1 consists only of pointers to the active file system and consumes no disk space. It represents a point-in-time view of data blocks A, B, C, and D.

As shown in Figure 2, the first change is an update to block D ("After Data Modification"). Snapshot 1 continues to reference the unchanged file system, with pointers to the original unchanged blocks. The new version of block D, depicted as D1, is "owned" by the active file system, consumes additional storage space, and will become part of the next snapshot. Meanwhile, Snapshot 1 protects the previous version of the active file system, and takes ownership of block D. This process is described in more detail in the following section, "FluidFS Snapshot Size and Delta Size."

![Figure 2. Redirect-on-Write Snapshot Process](image)

4.1 FluidFS “Snapshot Size” and “Delta Size”

Because a snapshot is a "point-in-time" copy of the active file system, it can be used to return the file system to its state at the time the snapshot was created. In this way, a snapshot protects the blocks present when the snapshot was created. Blocks containing new or updated data are not protected by
the existing snapshot, but will be protected by the next new snapshot. The new snapshot and each successive snapshot only tracks changes made to the active file system since the previous snapshot.

The size of a FluidFS snapshot is expressed in two ways — logical and physical:

- **FluidFS Snapshot Size** — Snapshot size refers to the total size of the data blocks protected by the snapshot. It expresses the logical size of the snapshot. For example, Snapshot 1 shown in Figure 3 points to (i.e., protects) data blocks A, B, C, and D. If the size of each of these blocks is 100 kilobytes (KB), Snapshot 1 will have a snapshot size of 400 KB.

- **FluidFS Delta Size** — Delta size refers to the actual size of the snapshot during its life cycle, as well as the amount of space that will be reclaimed when the snapshot is deleted. For example, Snapshot 1 in Figure 3 consists only of pointers to the active file system, which means that its delta size is 0. As changes are made to the active file system, Snapshot 1 and successive snapshots may grow to a delta size greater than 0.

FluidFS snapshot size and delta size are explored in more detail in the following sections, which detail a series of three successive “cascading” snapshots. In this example, we walk through the snapshot life cycle shown in Figure 4.

![Figure 3. Active File System after First Snapshot](image)

The 100-KB block size in this example scenario is used for illustrative purposes only. FluidFS can track block sizes as small as 4 KB.

### 4.1.1 Create Snapshot 1

Returning to Figure 3, the active file system contains data blocks A, B, C, and D. Each block is 100 KB in size. Snapshot 1 has been taken of the active file system. Consisting only of pointers to data blocks A, B, C, and D, Snapshot 1 references a point-in-time view of the active file system, and is now responsible for protecting this version. As shown in Table 1, the Snapshot 1 snapshot size is 400 KB and its delta size is 0.

![Figure 4. Example Snapshot Life Cycle](image)

<table>
<thead>
<tr>
<th>View of File System</th>
<th>Snapshot Size</th>
<th>Snapshot Delta Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active file system</td>
<td>Blocks A, B, C, and D</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Snapshot 1</td>
<td>Blocks A, B, C, and D</td>
<td>A + B + C + D = 400 KB</td>
</tr>
</tbody>
</table>
4.1.2 Update Active File System

In Figure 5, an update is made to block D in the active file system. The update is shown as block D\textsuperscript{1}. The active file system now consists of blocks A, B, C, and D\textsuperscript{1}. Snapshot 1 continues to point to the view of the active file system at the time the snapshot was created: blocks A, B, C, and D. As shown in Table 2, its snapshot size remains 400 KB. However, Snapshot 1 has now taken ownership of block D, which increases the delta size of the snapshot to 100 KB.

This example highlights another way of viewing FluidFS snapshot size. In theory, if all of the data blocks in the active file system are updated before another snapshot is taken, the Snapshot 1 delta size would increase from 100 KB to 400 KB. Thus, the FluidFS snapshot size represents the maximum delta size to which the snapshot can grow.

<table>
<thead>
<tr>
<th>View of File System</th>
<th>Snapshot Size</th>
<th>Snapshot Delta Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active file system</td>
<td>A, B, C, and D</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Snapshot 1</td>
<td>A, B, C, and D</td>
<td>A + B + C + D = 400 KB</td>
</tr>
</tbody>
</table>

4.1.3 Create Snapshot 2

In Figure 6, a second snapshot of the active file system is created. Here we see the efficiency of successive snapshots under FluidFS. Snapshot 2 captures only the changes made since Snapshot 1. Snapshot 1 continues to protect blocks A, B, and C of the current active file system (as well as block D). This means that Snapshot 2 must protect only the changed data block, D\textsuperscript{1}.

In this scenario, there is no change to the active file system or Snapshot 1. Snapshot 2 consists of pointers to the same data blocks — A, B, C, and D\textsuperscript{1} — as the active file system. Once again, this means that Snapshot 2 does not consume any space and, thus, its delta size is 0. However, its snapshot size is only 100 KB, reflecting the fact that it must protect only block D\textsuperscript{1}. Table 3 summarizes snapshot size and delta size of Snapshots 1 and 2 at this point.

<table>
<thead>
<tr>
<th>View of File System</th>
<th>Snapshot Size</th>
<th>Snapshot Delta Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active File system</td>
<td>A, B, C, and D</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Snapshot 2</td>
<td>D\textsuperscript{1}</td>
<td>D\textsuperscript{1} = 100 KB</td>
</tr>
<tr>
<td>Snapshot 1</td>
<td>A, B, C, and D</td>
<td>A + B + C + D = 400 KB</td>
</tr>
</tbody>
</table>
4.1.4 Update Active File System and Create Snapshot 3

In Figure 7, block $D^1$ in the active file system block is updated to $D^2$ and a third snapshot is created. The active file system now contains blocks A, B, C, and $D^2$, which is reflected in Snapshot 3. There is no change to Snapshot 1. However, Snapshot 2 is responsible for protecting block $D^1$ and now takes ownership of it. As shown in Table 4, this increases the delta size of Snapshot 2 to 100 KB, the size of $D^2$.

![Figure 7. Active File System after Snapshot 3](image)

<table>
<thead>
<tr>
<th>View of File System</th>
<th>Snapshot Size</th>
<th>Snapshot Delta Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active File system</td>
<td>Blocks A, B, C, and $D^2$</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Snapshot 3</td>
<td>Blocks A, B, C, and $D^2$</td>
<td>$D^2 = 100$ KB</td>
</tr>
<tr>
<td>Snapshot 2</td>
<td>Blocks A, B, C, and $D^1$</td>
<td>$D^1 = 100$ KB</td>
</tr>
<tr>
<td>Snapshot 1</td>
<td>Blocks A, B, C, and D</td>
<td>$A + B + C + D = 400$ KB</td>
</tr>
</tbody>
</table>

4.1.5 Delete Snapshot 1

In typical deployments, older snapshots are deleted after a specified period of time or when space is required for new snapshots. When a snapshot is deleted, its pointer associations and the data blocks referenced by it are either released to the free pool of storage or accounted for in another existing snapshot.

Figure 8 shows how deleting Snapshot 1 impacts FluidFS snapshot size and delta size. Snapshot 1 protects blocks A, B, and C of the active file system, and it “owns” block D, which is no longer needed by the active file system. When Snapshot 1 is deleted, Block D is released to the free pool and is no longer protected. The free pool size increases by 100 KB, the delta size of Snapshot 1. The Snapshot 1 pointers to blocks A, B, and C are removed, and responsibility for their protection shifts to the closest snapshot — Snapshot 2. The delta size of Snapshot 2 does not change, but its snapshot size increases from 100 KB to 400 KB.
Table 5. FluidFS Snapshot Size and Delta Size After Snapshot 1 Deleted

<table>
<thead>
<tr>
<th>Snapshot</th>
<th>View of File System</th>
<th>Snapshot Size</th>
<th>Snapshot Delta Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active File system</td>
<td>Blocks A, B, C, and D²</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Snapshot 3</td>
<td>Blocks A, B, C, and D²</td>
<td>D² = 100 KB</td>
<td>0</td>
</tr>
<tr>
<td>Snapshot 2</td>
<td>Blocks A, B, C, and D¹</td>
<td>Blocks A, B, and C, and D¹ = 400 KB (Blocks A, B, and C added)</td>
<td>D¹ = 100 KB</td>
</tr>
<tr>
<td>Snapshot 1 Deleted</td>
<td>Pointers to blocks A, B, and C released</td>
<td>Not applicable (deleted)</td>
<td>Block D released to free pool of storage</td>
</tr>
</tbody>
</table>

If Snapshot 1 is the last remaining or most current snapshot of the active file system, its pointers to blocks A, B, and C are removed and Block D is released to the free pool.

The next section discusses how to put these sizing concepts into practice in a FluidFS snapshot environment.
5 Planning For and Monitoring the Snapshot Reserve

As discussed in the previous section, snapshots occupy space on the NAS volume. To use snapshot space efficiently, administrators can configure alerts to be generated when a predefined percentage of volume capacity has been consumed by snapshots.

The total capacity consumed by snapshots for a volume at a given point in time is the sum of the snapshot delta size of all the snapshots on the volume. The snapshot delta size increases dynamically, based on the update rate of the active file system. Only existing blocks that are updated in the active file system are accounted for in the snapshot delta size or the overall snapshot reserve. New data blocks added to the active file system do not impact the space consumption of existing snapshots.

Thus, the following factors should be considered when planning the size of the NAS volume:

1. Actual user data
2. Estimated growth of user data
3. User data update rate
4. Data retention requirements

The capacity required for actual user data and estimated growth rate of user data are accounted for in the space consumed by the active file system within the volume. The capacity required for user data update rate and data retention requirements are accounted for in the space consumed by the snapshots on the volume. Thus, it is clear that the update rate and retention requirements of a dataset are important factors when planning snapshot reserve capacity. If a precise user data update rate is not known, the size of daily incremental backups of the dataset can be used as a conservative estimate of snapshot reserve capacity. This can be used to configure daily/weekly snapshot schedules and retention policy.

The following formula provides a rough calculation of the estimated NAS volume size required per year.
January 2013

Understanding Snapshots in Dell FluidFS NAS Systems

13

Current Space Utilization = Storage capacity used by existing user data
Annual Growth in User Data = Estimated growth in user data per year
Capacity Consumed by Snapshots = Storage capacity required for snapshots

Example:
A customer has implemented a NAS system containing 10 TB of file data. The customer expects a 25% annual growth rate in this file data. The customer’s data protection policy requires nightly snapshots. An average of 1% of the data is expected to change each day. The business plans to retain each snapshot for 30 days.

Current Space Utilization = 10 TB. Customer has 10 TB of NAS data today.
Annual Growth in User Data = Growth rate * Current Space Utilization = 2.5 TB.
Customer estimates 25% data growth per year, which equates to 2.5 TB (25% of 10 TB).
Capacity Consumed by Snapshots = Change Rate * (Current Space Utilization + Annual Growth in User Data) * Number of snapshots retained = 3.75 TB.
Customer has 1% update rate between successive snapshots, which equates to .125 TB per snapshot (1% of [10 TB + 2.5 TB]).
Customer retains 30 snapshots for 30 days. Total capacity used by snapshots is 3.75 TB (.125 TB per snapshot x 30 snapshots).

Estimated Total NAS Volume Space Required Per Year:
10 + 2.5 + 3.75 = 16.25 TB

As a best practice, it is recommended that an additional headroom allowance of, say, 10 percent be added to this estimate. Administrators should also keep in mind potential causes of unexpected snapshot growth that are identified in the next section.

5.1 Potential Causes of Unexpected Snapshot Growth
There are scenarios in which IT administrators may see unexpected growth in snapshots. A few of these scenarios are presented in Table 6.
<table>
<thead>
<tr>
<th>Scenario</th>
<th>Action</th>
<th>Impact on Snapshot Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Accidental deletion of files/folders from active file system (#rm -rf * on root of export).</td>
<td>This action causes all data blocks to be removed from the active file system. This causes any snapshot pointing to these blocks to begin consuming space for the blocks, increasing to the maximum defined snapshot size.</td>
</tr>
<tr>
<td>2</td>
<td>Reorganization effort that spans multiple NAS volumes.</td>
<td>These operations cause block-level changes to the active file system that have the same impact on snapshot size as Scenario 1.</td>
</tr>
<tr>
<td>3</td>
<td>Snapshot retention is not configured to the correct value based on sizing.</td>
<td>In this scenario, the sizing exercise assumes a particular snapshot retention period that is not matched by the actual snapshot retention period configured for the ‘periodic,” “hourly,” “daily,” and “weekly” policies. It is possible that the snapshots may consume more than the planned-for space on the NAS volume</td>
</tr>
<tr>
<td>4</td>
<td>Manually created snapshots are not deleted after use.</td>
<td>This practice causes snapshot space to unnecessarily increase over time. The impact can be reduced by properly configuring snapshot alerts and auto-delete.</td>
</tr>
</tbody>
</table>

Table 6. Potential Causes of Unexpected Snapshot Growth
6 Snapshots and Performance

To gauge the impact of creating snapshots on performance, we simulated a simple file server workload on a Dell PowerVault™ NX3500 FluidFS system. The workload was run under three scenarios:

- No snapshots configured.
- One snapshot configured.
- Ten snapshots configured.

For each test run, we ensured that the FluidFS controllers did not cache data from the previous run. The workload size used for the test was 10 gigabytes (GB) and consisted of 10,000 files, an average directory width of 20, and average directory depth of 3.

Figure 9 presents the results. The performance of the base configuration with no snapshots is compared to the performance with one and ten snapshots enabled. Operations per second, throughput, and latency are measured. As shown, FluidFS snapshots have little impact on performance, mainly due to the efficiency of its redirect-on-write design.

Figure 9. Performance Impact of Snapshots

<table>
<thead>
<tr>
<th>Snapshots</th>
<th>Operations/s</th>
<th>Throughput</th>
<th>Latency</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Snapshot</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>1 Snapshot</td>
<td>101%</td>
<td>101%</td>
<td>99%</td>
</tr>
<tr>
<td>10 Snapshots</td>
<td>99%</td>
<td>99%</td>
<td>102%</td>
</tr>
</tbody>
</table>

Note: This simple test run in Dell performance labs October 2012 was designed to characterize the performance impact of FluidFS snapshots. It is not intended to provide a detailed performance analysis of FluidFS or its snapshot functionality under different scenarios.
**7 Typical Use Cases for Snapshots**

FluidFS snapshots can be leveraged in a variety of use cases. Some of the most common scenarios are listed in the table below.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Typical Snapshot Use Cases</th>
<th>Challenge</th>
<th>How Dell FluidFS Snapshots Address Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Improve recovery point objective (RPO)</td>
<td>Traditional backup methods that leverage external backup software, disk pools, and/or tapes are less flexible in their ability to perform frequent backups. As a result, the RPO is typically higher than most organizations would prefer. The primary reason is that these resources are shared across the enterprise and must service not only NAS backups, but all other data repositories. Traditional backup approaches also have performance overhead associated with moving data across storage tiers. This overhead renders them ineffective as backup frequency increases, so are typically limited to daily backups. Daily backups may not adequately protect data that is updated many times daily.</td>
<td>FluidFS snapshots are designed to provide more frequent and space-efficient point-in-time copies of data, while minimizing performance overhead. Because snapshots reside on the same NAS volume as active data, data does not move across storage tiers. Snapshots can be scheduled as frequently as required — every 5 minutes or hourly. A common approach is to run hourly snapshots of user directories, combined with daily and weekly snapshots. Overall, snapshots help improve RPO.</td>
</tr>
<tr>
<td>2</td>
<td>End-user controlled recovery</td>
<td>Traditional backup methods typically require administrator invention for restores, which can cause delays in recovering lost data.</td>
<td>FluidFS snapshots allow an end user to restore data without administrative intervention. The snapshots are read-only to protect the data, while allowing user access.</td>
</tr>
<tr>
<td>3</td>
<td>Full copy of data that can be used for development environments or to test software patches and upgrades.</td>
<td>Traditionally, a full backup is taken of customer data before patches are applied to client systems or applications are upgraded to newer versions. In addition, quality/test/development environments continuously generate different versions of data that must be protected. These traditional backups have performance and flexibility limitations that impact productivity.</td>
<td>FluidFS snapshots provide point-in-time copies instantaneously and online. These snapshots can be used to revert to pre-patch or pre-upgrade versions, if required. Snapshots can also protect different versions of data in quality assurance, test, and development environments.</td>
</tr>
<tr>
<td>4</td>
<td>Tier 0 of data protection strategy.</td>
<td>Traditionally, disk pools attached to external backup software have been considered Tier 0 of a data protection strategy, with tape libraries and archives constituting the lower tiers. Backup and restore data must flow from the NAS system to the external disk pool.</td>
<td>FluidFS snapshots are a fast and reliable alternative Tier 0. Backup and restore operations can occur within the FluidFS system for volume snapshot create and volume revert operations.</td>
</tr>
</tbody>
</table>
8 Conclusion

FluidFS snapshots are simple to use and can be automated to address enterprise data protection requirements and storage capacity limitations. The ability to create up to 512 snapshots per volume and up to 10,000 snapshots across the entire FluidFS storage system gives IT administrators a powerful component of the data protection strategy.

FluidFS snapshots are built into the Dell Fluid File System, which is a core component of the Dell NAS storage solutions shown in Figure 10. The Fluid File System includes the following data protection capabilities:

- Data integrity and high-availability features built into the NAS file system.
- Snapshots for short-term, quick backup and recovery of important user files.
- Replication for protection of data on NAS appliances, particularly for failover in a disaster-recovery scenario.
- Full backups using Network Data Management Protocol (NDMP)-compliant backup application for complete backup protection to meet disaster recovery, compliance, and off-site storage requirements.

Figure 10. Dell FluidFS NAS Solutions
Appendix A Additional Resources

Dell online support resources:

- Dell technical support site: http://support.dell.com
- Dell TechCenter is an online IT community where IT professionals connect with Dell customers and employees to share knowledge, best practices, and other information about Dell products and installations: http://DellTechCenter.com

Dell Fluid File System resources:

The FluidFS graphical user interface (GUI) and command line interface (CLI) should be used to configure Compellent FS8600 series and PowerVault NX3500 and NX3600 series NAS systems.

### 8.1 Creating Snapshots

The following sections describe how to create a FluidFS snapshot using the FluidFS graphical user interface (GUI) and the FluidFS command line interface (CLI).

#### 8.1.1 FluidFS Graphical User Interface

From the FluidFS GUI, Data Protection → Snapshots → List → Create. Select the NAS volume, specify the snapshot name, and click Create, as shown below. The snapshot is created.

![Create Snapshot](image)

#### 8.1.2 FluidFS Command Line Interface

From the FluidFS CLI, enter the following command:

```
#ssh admin@<FluidFS-Management-IP> "data-protection snapshots actions create <Volume-Name> <Snapshot Name>"
```

### 8.2 Creating Snapshot Schedules

The following sections describe how to create a FluidFS snapshot schedule using the FluidFS GUI and the FluidFS CLI.

---

8.2.1 FluidFS Graphical User Interface

From the FluidFS GUI, Data Protection -> Snapshots → Policies. Select the NAS volume and specify the alert threshold. Set the snapshot schedule to periodic, hourly, daily, or weekly, as shown below.

8.2.2 FluidFS Command Line Interface

The following CLI commands are used to configure the snapshot alert and auto-delete thresholds, create various snapshot schedules.

- **Snapshot Alert Threshold** — When the snapshot size as a percentage of the total volume size exceeds this threshold, an alert is generated.

  ```bash
  #ssh admin@<FluidFS-Management-IP> "data-protection snapshots policies set-Snapshot space-thresholds <Volume-Name> -alert %"
  ```
- **Auto-delete Threshold** — When snapshot size as a percentage of total volume size exceeds this threshold, older snapshots are automatically deleted.

```
#ssh admin@<FluidFS-Management-IP> "data-protection snapshots policies set-Snapshot space-thresholds <Volume-Name> -autodelete %
```

- **Create Periodic Snapshot Schedule** — This schedule creates a snapshot at regular intervals in minutes (5, 10, 15, 20 or 30 minutes) and retains a fixed number of the latest snapshots, based on the specified options parameter.

```
#ssh admin@<FluidFS-Management-IP> "data-protection snapshots policies set-periodic-policy <Volume-Name> on -periodicinterval 30 -periodickeep 16
```

- **Create Hourly Snapshot Schedule** — This schedule creates a snapshot every hour or at any hour:minute specified in the command. It also retains a fixed number of latest snapshots, based on the command options.

```
#ssh admin@<FluidFS-Management-IP> "data-protection snapshots policies set-hourly-policy <Volume-Name> on -hourlyall

#ssh admin@<FluidFS-Management-IP> "data-protection snapshots policies set-hourly-policy <Volume-Name> on -hourlyat (0-23) -hourlystartmin (0-59) -hourlykeep 24
```

- **Create Daily Snapshot Schedule** — This schedule creates snapshots every day or at any hour:minute specified as arguments. It also retains a fixed number of the latest snapshots, based on the command options.

```
#ssh admin@<FluidFS-Management-IP> "data-protection snapshots policies set-daily-policy <Volume-Name> on -dailyall

#ssh admin@<FluidFS-Management-IP> "data-protection snapshots policies set-daily-policy <Volume-Name> on -dailyat (0-6) -dailystarttimehour (0-23) -dailystarttimemin (0-59) -dailykeep 5
```

- **Create Weekly Snapshot Schedule** — This schedule creates snapshots every week or at any hour:minute specified as arguments. It also retains a fixed number of latest snapshots, based on the command options.

```
#ssh admin@<FluidFS-Management-IP> "data-protection snapshots policies set-weekly-policy <Volume-Name> on -weeklyday (0-6) -weeklystarttimehour (0-23) -weeklystarttimemin (0-59) -weeklykeep 12
```

### 8.3 Restoring from a Snapshot

This section describes how to restore data from a snapshot:

- Restoring a single file
- Restoring a single folder using Microsoft® Windows® Server Volume Shadow Copy Service
• Restoring an entire container

8.3.1 Restoring Single File
FluidFS creates a hidden snapshot directory called .snapshots under each directory. The .snapshots directory contains a list of all snapshots. Under each snapshot is the directory structure with files and folders. A single file can be restored from a snapshot by simply copying it from the snapshot location to the active file system with no NAS service disruption.

Windows:

![Snapshot Directory](image)

<table>
<thead>
<tr>
<th>Name</th>
<th>Date Modified</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snap1</td>
<td>04/03/12 11:54</td>
<td>File folder</td>
</tr>
<tr>
<td>snap2</td>
<td>04/03/12 11:56</td>
<td>File folder</td>
</tr>
</tbody>
</table>

Linux/UNIX:

```
[root@node0-derby-sup1 /Marketing/.snapshots]# ls -latr
total 12
drwxrwxrwx 1 root root 76 Mar 4 07:59 snap2
drwxrwxrwx 1 root root 76 Mar 4 07:59 ..
```

8.3.2 Restoring Single Folder using Windows Server Volume Shadow Copy Service

• Right click on the directory to be restored and select Properties.
• Select Previous Version tab.
• Select Folder version.
• Click Restore.
8.3.3 Restoring Entire Container

The entire NAS volume can also be restored from a snapshot instantly, irrespective of the size of the volume. When restoring an entire NAS volume, FluidFS deletes all snapshots with a creation date later than the snapshot used for the restore. In addition, restoring the entire volume disconnects current connections. The GUI and CLI method to restore a NAS volume follows.

FluidFS GUI:

From the FluidFS GUI, Data Protection → Snapshots → Restore. Select the NAS volume to be restored and the snapshot to be used for the restore, as shown below. Click Next.

The warning below is displayed. Click Yes to restore the volume from the snapshot.
8.4 Deleting a Snapshot

This section describes how to delete a FluidFS snapshot using the FluidFS GUI or CLI.

**FluidFS GUI:**

From the FluidFS GUI, Data Protection → Snapshots → List. Select the snapshot to be deleted and click Delete, as shown below.

**FluidFS CLI:**

From the FluidFS CLI, enter the following command:

```
#ssh admin@<FluidFS-Management-IP> "data-protection snapshots revert <Volume-Name> <Snapshot-Name>"
```
FluidFS CLI:

```
#ssh admin@<FluidFS-Management-IP> "data-protection snapshots actions
delete <Volume-Name> <Snapshot-Name>"
```

8.5 Monitoring the Size of Snapshots

The following sections document how to monitor FluidFS snapshot size, delta size, and reserve size.

8.5.1 Monitoring Snapshot Size

As described earlier, snapshot size refers to the total size of the data blocks protected by the snapshot. It expresses the logical size of the snapshot. Expressed another way, snapshot size refers to the space allocated to (not consumed by) the snapshot at the time it was created. This value is dynamic; it is adjusted over time as older snapshots are deleted and additional blocks must be accounted for by the snapshot.

Snapshot size can be monitored using the FluidFS GUI or CLI.

**FluidFS GUI:**

From the FluidFS GUI, **Data Protection → Snapshots → List**. The **Snapshots List** shows all snapshots, the volumes to which they belong, creation date and time, and snapshot size in megabytes (MBs).

![Snapshots List](image)

FluidFS CLI:

```
#ssh admin@<FluidFS-Management-IP> "data-protection snapshots actions
list"
```

8.5.2 Monitoring Snapshot Delta Size

The snapshot delta size refers to the actual space consumed by the snapshot at a given point in time. Thus, it is also the amount of space that can be reclaimed if the snapshot is deleted.

The snapshot delta size can be monitored using the FluidFS GUI or CLI.

**FluidFS GUI:**
From the FluidFS GUI, **Data Protection → Snapshots → List**. The resulting list shows all snapshots, the volumes to which they belong, creation date and time, and snapshot size in megabytes (MBs). Click on the required snapshot. The **Edit Snapshot** window displays information about the snapshot. Click on **Calculate Snapshot Delta Size**.

![Edit Snapshot](image)

**FluidFS CLI:**

```
# ssh admin@<FluidFS-Management-IP> "data-protection snapshots actions
view-delta <Volume-Name> <Snapshot-Name>"
```

### 8.5.3 Monitoring Snapshot Reserve Utilization

The total capacity used by snapshots for a volume can be monitored using the FluidFS GUI or the CLI.

**FluidFS GUI:**

From the FluidFS GUI, **User Access → NAS Volumes → Configuration**. The resulting screen shows the total space consumed in gigabytes by the snapshots on each NAS volume.

![NAS Volumes Configuration](image)

An alternative approach using the FluidFS GUI is: **Monitor → Capacity → Space Utilization**. The resulting screen shows total space consumed by snapshots as a percentage of the total NAS volume capacity.
FluidFS CLI:

```bash
# ssh admin@<FluidFS-Management-IP> "access nas-volumes list"
```
Appendix C  Working with FluidFS Snapshots on EqualLogic FS Series

The EqualLogic Group Manager GUI should be used to configure EqualLogic FS series of NAS solutions. Use Group Manager to select NAS controllers and to configure and manage a NAS cluster. When configuring a NAS cluster, specify the network configuration for the service and the amount of storage pool space for the NAS reserve. The NAS reserve is the percentage of the container size that can be used to store snapshots. The snapshot reserve is consumed from the NAS reserve space allocated to the container. Therefore, user data and snapshots compete for the same container space. Note that data takes precedence over snapshots. If the container begins to run out of space, it will take space from the snapshot reserve. The oldest snapshots are deleted first.

C.1 Creating Snapshots

Group Manager Interface

To create a snapshot of a NAS container:

1. Click NAS, then expand NAS containers, and then select the NAS container name.
2. Click Create snapshot.
3. Specify a snapshot name. If you do not assign a snapshot name, the NAS cluster generates a name automatically, based on the NAS container name and the timestamp. A snapshot name can contain up to 127 characters: letters, numbers, and underscores. Fewer characters are accepted for this field if you enter the value as a Unicode character string, which takes up a variable number of bytes, depending on the specific character.
4. Click OK.

The snapshot appears (identified by its timestamp) when you expand the NAS container name in the far-left panel.

C.2 Creating Snapshot Schedules

To create a NAS container snapshot schedule:

1. Click NAS, then expand NAS containers, and then select the NAS container name.
2. Click Create schedule. The Create Schedule wizard starts.
3. In the Create Schedule - Schedule Settings dialog box:
   a) Specify the schedule name.
   b) Select the type of schedule or whether to create the new schedule based on an existing schedule.
   c) Specify whether to enable the schedule. You can enable or disable a schedule at a later time, if desired.
4. Click Next.
5. If you are creating a Run Once, Run Hourly, or Run Daily schedule type, specify when and how often to create snapshots and click Next.
6. If you are creating a schedule based on an existing schedule, select the existing schedule and click Next. Then, modify the configuration settings for the new schedule, as needed, and click Next.
7. In the Create Schedule - Summary dialog box, click Finish if the schedule is correct. Click Back to make changes.

C.3 Restoring from a Snapshot
When an administrator creates a snapshot of a NAS container, the NAS cluster creates a hidden directory named .snapshot in each NFS export and CIFS share in the NAS container. Within the .snapshots directory are directories that are named for each snapshot. Within each snapshot directory are the files that represent the delta (difference) between the current NAS container data and the data that existed when the administrator created the snapshot.

Snapshots retain the same security style as the base NAS container; therefore, clients can access only their own files, based on existing permissions.

C.3.1 Restoring Single File
1. Locate the snapshot directory in the affected NFS export or CIFS share.
2. Locate the file in the appropriate snapshot directory.
3. Copy the file to the desired location.

C.3.2 Restoring Entire Container
1. Click NAS, then expand NAS containers, and then select the NAS container name.
2. Click Restore NAS container.
3. Select the snapshot.
4. Confirm that you want to restore the NAS container from the snapshot.

After the restore operation completes, the NAS cluster deletes any snapshots created after the snapshot from which you restored the NAS container. Snapshots created before the snapshot from which you restored the NAS container are not affected.

C.3.3 Deleting a Snapshot
To delete a NAS container snapshot:

1. Click NAS, then expand NAS containers, and then select the NAS container name.
2. Click the Snapshots tab.
3. Select the snapshot in the Snapshots panel and click Delete snapshot.
4. Confirm that you want to delete the snapshot.

C.4 Monitoring Snapshot Size
To display all the snapshots for a NAS container:

1. Click NAS, then expand NAS containers, and then select the NAS container name.
2. Click the Snapshots tab.

The Snapshots Panel lists all the snapshots for the NAS container.
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created</td>
<td>Date and time the snapshot was created.</td>
</tr>
<tr>
<td>Name</td>
<td>Snapshot name. If you did not specify a snapshot name, the NAS cluster generates a snapshot name, based on the NAS container name and the snapshot timestamp.</td>
</tr>
<tr>
<td>Size</td>
<td>Snapshot size.</td>
</tr>
<tr>
<td>Schedule</td>
<td>Name of the schedule by which the snapshot was created, if any.</td>
</tr>
</tbody>
</table>

### C.5 Monitoring Delta Size

Because Group Manager does not present snapshot delta size, use the FluidFS CLI to monitor delta size.

```
#ssh admin@<FluidFS-Management-IP> "data-protection snapshots actions view-delta <Volume-Name> <Snapshot Name>"
```

### C.6 Monitoring Snapshot Reserve Utilization

To display all snapshots for a volume:

1. Click **Volumes**.
2. Expand **Volumes** and select the volume name.
3. Click the **Snapshots** tab.

The **Snapshot Summary Panel** shows the following data fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snapshot Reserve</td>
<td>Percentage of the volume reserve allocated for snapshots.</td>
</tr>
<tr>
<td>In-use space warning level</td>
<td>Percentage of the snapshot reserve that, when reached by in-use snapshot reserve, results in an event message. The default is 90% of the snapshot reserve. For example, if snapshot reserve space is 200 MB and the warning level is 90%, a warning occurs when in-use snapshot reserve equals or exceeds 180 MB.</td>
</tr>
<tr>
<td>Space recovery</td>
<td>Space recovery policy for when the snapshot reserve is full: delete oldest snapshot or set volume and snapshots offline.</td>
</tr>
<tr>
<td>Snapshot reserve</td>
<td>Capacity of the Snapshot Reserve.</td>
</tr>
<tr>
<td>Free reserve</td>
<td>Unused capacity in the snapshot reserve, in MB or GB, and unused percentage of the snapshot reserve.</td>
</tr>
<tr>
<td>Snapshots</td>
<td>Number of snapshots of the volume.</td>
</tr>
<tr>
<td>Snapshot schedules</td>
<td>Number of snapshot schedules created for the volume.</td>
</tr>
<tr>
<td>Running schedules</td>
<td>Number of snapshot schedules for the volume that are enabled.</td>
</tr>
<tr>
<td>Next snapshot</td>
<td>Next scheduled time for a snapshot operation on the volume.</td>
</tr>
</tbody>
</table>

**Note:** Move the pointer over a snapshot to display a context message showing its name, the current snapshot status, and the requested snapshot status.