FS8600 Snapshot and Volume Cloning Best Practices

Dell Storage Technical Solutions
April 2014

A Dell Best Practices
Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 2013</td>
<td>Initial release. Authors: Sharon Hanson, Raj Hosamani, and Animesh Pillai</td>
</tr>
<tr>
<td>April 2014</td>
<td>Updated for FluidFS v3 Volume Cloning and FS8600. Author: Andrew Smith</td>
</tr>
</tbody>
</table>

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.

© 2014 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.


Performance of network reference architectures discussed in this document may vary with differing deployment conditions, network loads, and the like. Third party products may be included in reference architectures for the convenience of the reader. Inclusion of such third party products does not necessarily constitute Dell’s recommendation of those products. Please consult your Dell representative for additional information.

Trademarks used in this text:

Dell™, the Dell logo, Dell Boomi™, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™ and Vostro™ are trademarks of Dell Inc. Other Dell trademarks may be used in this document. Cisco Nexus®, Cisco MDS®, Cisco NX-OS®, and other Cisco Catalyst® are registered trademarks of Cisco System Inc. EMC VNX®, and EMC Unisphere® are registered trademarks of EMC Corporation. Intel®, Pentium®, Xeon®, Core® and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™ and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® and Active Directory® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries. VMware®, Virtual SMP®, vMotion®, vCenter® and vSphere® are registered trademarks or trademarks of VMware, Inc. in the United States or other countries. IBM® is a registered trademark of International Business Machines Corporation. Broadcom® and NetXtreme® are registered trademarks of Broadcom Corporation. Qlogic is a registered trademark of QLogic Corporation. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and/or names or their products and are the property of their respective owners. Dell disclaims proprietary interest in the marks and names of others.
# Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revisions</td>
<td>2</td>
</tr>
<tr>
<td>1 Introduction</td>
<td>4</td>
</tr>
<tr>
<td>2 FluidFS: Architected for data protection</td>
<td>5</td>
</tr>
<tr>
<td>2.1 High Availability</td>
<td>5</td>
</tr>
<tr>
<td>2.2 Data integrity</td>
<td>6</td>
</tr>
<tr>
<td>2.3 Metadata integrity</td>
<td>6</td>
</tr>
<tr>
<td>3 FluidFS snapshots overview</td>
<td>7</td>
</tr>
<tr>
<td>3.1 FluidFS redirect-on-write snapshots</td>
<td>7</td>
</tr>
<tr>
<td>3.2 Configuring FluidFS snapshots</td>
<td>8</td>
</tr>
<tr>
<td>3.3 Accessing FluidFS snapshots</td>
<td>8</td>
</tr>
<tr>
<td>3.4 Restoring data</td>
<td>9</td>
</tr>
<tr>
<td>4 Understanding the size of FluidFS snapshots</td>
<td>10</td>
</tr>
<tr>
<td>4.1 FluidFS snapshot size and delta size</td>
<td>10</td>
</tr>
<tr>
<td>4.1.1 Create Snapshot 1</td>
<td>12</td>
</tr>
<tr>
<td>4.1.2 Update active file system</td>
<td>12</td>
</tr>
<tr>
<td>4.1.3 Create Snapshot 2</td>
<td>13</td>
</tr>
<tr>
<td>4.1.4 Update Active File System and Create Snapshot 3</td>
<td>14</td>
</tr>
<tr>
<td>4.1.5 Delete Snapshot 1</td>
<td>14</td>
</tr>
<tr>
<td>5 Planning for and monitoring the snapshot reserve</td>
<td>16</td>
</tr>
<tr>
<td>5.1 Potential causes of unexpected snapshot growth</td>
<td>17</td>
</tr>
<tr>
<td>6 Typical use cases for snapshots</td>
<td>18</td>
</tr>
<tr>
<td>7 FluidFS volume cloning overview</td>
<td>19</td>
</tr>
<tr>
<td>7.1 Benefits of a cloned volume</td>
<td>19</td>
</tr>
<tr>
<td>7.2 Creating a volume clone</td>
<td>19</td>
</tr>
<tr>
<td>7.3 Configuring volume clones</td>
<td>24</td>
</tr>
<tr>
<td>7.4 Cloned volume integration rules and restrictions</td>
<td>24</td>
</tr>
<tr>
<td>8 Typical use cases for volume clones</td>
<td>25</td>
</tr>
<tr>
<td>9 Conclusion</td>
<td>26</td>
</tr>
<tr>
<td>10 Additional Resources</td>
<td>27</td>
</tr>
</tbody>
</table>
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. Volume Cloning provides the ability to create a writable copy of a NAS volume. Though most storage systems have built-in support for snapshots and clones, the design criteria and usability differs from vendor to vendor.

Snapshots and volume clones are part of the data protection capabilities built into the Dell Fluid File System (FluidFS). FluidFS underlies Dell Compellent FS 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 and volume clone data protection capability that is built into FluidFS. The paper reviews the overall FluidFS data protection capabilities and 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 1 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.

![FluidFS logical architecture](image)

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 ensure 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 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. A snapshot is a point-in-time copy of a FluidFS volume. 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 (for example, daily or hourly), 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 creates the point-in-time copy. For this reason, and because 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.

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. As shown in Figure 2, 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.

![Figure 2](image.png)

Figure 2  Configuring a snapshot schedule

3.3 Accessing FluidFS snapshots
FluidFS snapshots are accessible from any point in the volume. From Windows server version 7 or greater,
the snapshot can be accessed by using the “Restore previous version” function. From a Linux client, the
snapshot can be seen by accessing a hidden directory called .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.
Permissions can be impacted by the method the client uses to copy the data and the destination of the
data. 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 using a Linux client, 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). In Microsoft Windows environments, FluidFS integrates with the Previous Versions (Figure 3) tracking feature of Windows Explorer. Using this tool, end users can directly restore files from snapshots of their home directories. 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.

![Figure 3](image)

Using Windows previous versions to restore files from snapshots

- 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 available through the Dell Compellent Enterprise Manager Client. When restoring a NAS volume, all snapshots with creation dates that are more recent than the snapshot used for the volume 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 4, which shows the file system before and after a Snapshot 1 is taken. 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 4 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 Section 4.1, FluidFS snapshot size and delta size.

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

**Figure 4** Redirect-on-Write Snapshot Process

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 track 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 (that is, 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 5 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.

![After Snapshot 1](image)

Figure 5  Active File System after first Snapshot

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 6.

![Example snapshot life cycle](image)

Figure 6  Example snapshot life cycle

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 5, 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.

<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 D1. The active file system now consists of blocks A, B, C, and D1. 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.

Figure 7   After Data Modification

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 2   FluidFS Snapshot Size and Delta Size of Snapshot 1 After Data Modification
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, D1.

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 D1) 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 D1. Table 3 summarizes snapshot size and delta size of Snapshots 1 and 2 at this point.

Table 3 FluidFS Snapshot Size and Delta Size After Snapshot 2

<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 D1</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>
<tr>
<td>Snapshot 2</td>
<td>Blocks A, B, C, and D1</td>
<td>D1 = 100 KB</td>
</tr>
</tbody>
</table>

Figure 8 Active file system after Snapshot 2
4.1.4 Update Active File System and Create Snapshot 3

In Figure 7, block D1 in the active file system block is updated to D2 and a third snapshot is created. The active file system now contains blocks A, B, C, and D2, which is reflected in Snapshot 3. There is no change to Snapshot 1. However, Snapshot 2 is responsible for protecting block D1 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 D2.

Figure 9  Active file system after Snapshot 3

Table 4  FluidFS Snapshot Size and Delta Size After Snapshot 3

<table>
<thead>
<tr>
<th></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>D1 = 100 KB</td>
<td>D1 = 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>
<td>D = 100 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 10 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, which is Snapshot 2. The delta size of Snapshot 2 does not change, but its snapshot size increases from 100 KB to 400 KB.

<table>
<thead>
<tr>
<th></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 D</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Snapshot 3</td>
<td>Blocks A, B, C, and D</td>
<td>D = 100 KB</td>
<td>0</td>
</tr>
<tr>
<td>Snapshot 2</td>
<td>Blocks A, B, C, and D</td>
<td>Blocks A, B, and C, and D</td>
<td>D' = 100 KB</td>
</tr>
<tr>
<td><strong>Snapshot 1 Deleted</strong></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.
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.

\[
\text{Estimated NAS Volume Space Required Per Year} = \text{Current Space Utilization} + \text{Annual Growth in User Data} + \text{Capacity Consumed by Snapshots}
\]

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 about 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 6  Potential causes of unexpected snapshot growth

<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>
## 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 Table 7 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 they 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, for example, 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>
7 FluidFS volume cloning overview

Snapshots of volumes are very useful for creating point-in-time copies of data that are read only, however it is sometimes useful to have the ability to create a read-writeable copy (Clone) of a NAS volume. These clones can then be accessed through shares and exports and are functionally separate from the original. Cloning a volume creates an identical copy of a volume in seconds, making it easy to create multiple production data sets without affecting the original. Clones do not take up any additional space from the NAS pool until a change is made in the cloned volume.

7.1 Benefits of a cloned volume

The ability to create a clone quickly means that the administrator can provide a copy of a volume and present it as if it were an original volume. An example of this could be the ability to provide a copy of production data such as a database or application data to run tests or modifications against without having to change the original production data set.

When a NAS volume clone is created, it is created as a thin clone. That is, it uses the same re-direct on write method as a snapshot. No space is consumed until data in the clone is modified. Once new data is written to the clone, only the new or changed blocks are written. Figure 11 shows that the clone still points to the original snapshot for the unchanged blocks of data.

![Figure 11 Cloning uses re-direct on write](image)

7.2 Creating a volume clone

In order to create a clone, a snapshot of the volume must be created first, or you can use an existing snapshot. This snapshot will become the base snapshot. This snapshot cannot be deleted until all clones created out of it are deleted as well. Once a snapshot of the volume has been created, the clone can then be created. The following scenario demonstrates a clone being created and shows the difference in size as data is moved into the newly created clone.
Dell Compellent Enterprise Manager is used to administer the FS8600 appliance. All administrative functions, such as creating snapshots and clones are configured and executed here. Figure 12 shows a volume called **Projects Volume** that is currently using 1.06 GB of its 500 GB capacity.

![Figure 12 Properties of a volume](image)

A snapshot of the volume is created and named **Projects Volume Snapshot**.

![Figure 13 Create a snapshot](image)

Once the snapshot is created, the clone can now be created. Figure 14 shows a clone being created named **Projects Volume Clone**.
Figure 14  Creating a clone

Once the clone has been created, the new clone appears. Figure 15 shows the new clone summary information and shows that the space used within the clone is 0%. Note that the new clone appears on the left side of the screen along with the original volume from which it was created. The icon has also changed to reflect its status as a clone.

Figure 15  Created clone summary page
A CIFS Share is now created within the new clone called **Project Volume Clone CIFS**. Once the CIFS share is created, the data within the clone may now be viewed.

![Create CIFS Share within the new clone](image)

**Figure 16**  Create a CIFS Share within the new clone

Using Windows Explorer, the newly created CIFS share can now view the files within the share. Note that the total size of files within the share is approximately the same as the original volume from which the clone was created.

![Properties page of created share in Windows Explorer](image)

**Figure 17**  Properties page of created share in Windows Explorer

In Figure 18, approximately 410MB is copied to the share.
Figure 18  Copying new files to project clone CIFS Share

Figure 19 shows the **Projects Volume Clone** summary page. Note that the size of the clone has grown by approximately 410MB. There is some additional space consumed that is used for metadata (properties and configuration information about the clone).

Figure 19  Clone increased in size
Note that in Figure 12, the original volume that was cloned was 1.06GB, however, the size of the cloned volume (Figure 19) after the copying additional files into it is only 427MB. The share created in the cloned volume shows the total amount of storage consumed (Figure 18) by the original volume plus the added additional files. This scenario is meant to show how a clone only grows from 0MB when data is added to it. It uses the original blocks of unchanged data that came from the original volume.

7.3 Configuring volume clones
A new NAS volume is created with the exact same data as the base snapshot, but now this data can be modified. The new clone also has the same quota usage as the original volume. It also uses the same interoperability policy and Access time granularity definition as the base snapshot. When deleting a clone the same rules apply as when deleting a volume. You must delete all shares and snapshots first. Also, base snapshots and volumes cannot be deleted if a clone exists.

7.4 Cloned volume integration rules and restrictions
Observe the following restrictions when planning to use volume clones. As a best practice, always check the latest FluidFS FS8600 Administrators guide.

- A Cloned volume cannot be created on source replication snapshots. These are temporary snapshots meant for replication. These are temporary and are removed after the next replication succeeds.
- Cloned volumes cannot have data reduction enabled.
- Once a NAS volume is cloned, data reduction cannot be re-enabled until all clone NAS volumes have been deleted.
- Nested clones (a clone of a clone) are not allowed.
- Snapshot space accounting (snapshot quota, global snapshot space, alerting) is not available for clones.
- A clone NAS volume contains user and group recovery information, but not the NAS volume configuration.
- Clone NAS volumes count towards the total number of NAS volumes (1024) in the FluidFS cluster.
- You cannot create a clone NAS volume of a clone NAS volume (nested clones) unless a clone NAS volume is replicated to another FluidFS cluster and then cloned.
- You cannot delete a base volume until all of its clone NAS volumes have been deleted.
- A snapshot cannot be deleted as long as there are clone NAS volumes based on it.
- Restoring to an older snapshot fails if it would result in a base snapshot getting deleted.
- You can replicate a clone NAS volume only after the base volume is replicated. If the base snapshot in the base volume is removed, and a clone NAS volume exists on the replication target FluidFS cluster, replication between NAS volumes will stop. To resume replication, the cloned NAS volume on the target FluidFS cluster must be deleted.
Typical use cases for volume clones

FluidFS volume clones can be leveraged in a variety of use cases. Some of the most common scenarios are listed in Table 8 below.

Table 8  Use cases for volume clones

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Typical volume clone use cases</th>
<th>Challenge</th>
<th>How Dell FluidFS volume clones address challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Databases</td>
<td>The need to run reports against a production database without affecting the performance of the production database environment.</td>
<td>A clone of the database could be used to provide a copy of the production database for the purpose of running reports without affecting the performance of the production database.</td>
</tr>
<tr>
<td>2</td>
<td>Virtual Desktop Infrastructure (VDI)</td>
<td>Creating and copying virtual desktop images can become a cumbersome time consuming task.</td>
<td>Virtual desktop Images could be created and then cloned to provide read/write copies of virtual desktop images.</td>
</tr>
<tr>
<td>3</td>
<td>Disaster recovery for production applications</td>
<td>Providing a DR copy of a production environment.</td>
<td>Clones could be used to provide read/write copies of production environments and replicated to DR sites for protection and possible use in the event of a disaster.</td>
</tr>
</tbody>
</table>
Conclusion

FluidFS snapshots and volume clones 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 and volume clones are built into version 3 of the Dell Fluid File System, which is a core component of the Dell FS8600 NAS storage solutions. 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.
- The ability to clone volumes to create read/write copies for multiple purposes.
- 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.
10 Additional Resources

Dell online support resources:

Dell technical support site: [http://support.dell.com](http://support.dell.com)

Dell Tech Center 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](http://DellTechCenter.com)

Dell Fluid File System resources:

