Dell EMC PowerFlex: Secure Snapshots
Overview and Basic Configuration

Abstract
Dell EMC PowerFlex™ version 3.5 adds the option for time-based Secure Snapshots. This paper provides an overview of this new feature, its uses and restrictions in the overall context of PowerFlex’s snapshot architecture.

July 2020
Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 2020</td>
<td>Initial release</td>
</tr>
</tbody>
</table>

Acknowledgements

Co-author: Neil Gerren, Senior Principal Engineer, Storage Technical Marketing
Co-author: Brian Dean, Senior Principal Engineer, Storage Technical Marketing

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © 2020 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. [7/13/2020] [Technical White Paper] [H18393]
Table of contents

Revisions ........................................................................................................................................... 2
Acknowledgements ................................................................................................................................. 2
Table of contents ................................................................................................................................. 3
Executive summary ............................................................................................................................... 4
1 Introduction ......................................................................................................................................... 5
2 PowerFlex 3.5 New Features ............................................................................................................... 6
   2.1 Native Asynchronous Replication ................................................................................................. 6
   2.2 Protected Maintenance Mode .......................................................................................................... 6
   2.3 SDC Authentication ......................................................................................................................... 6
   2.4 New WebUI ..................................................................................................................................... 7
   2.5 Secure Snapshots ............................................................................................................................ 7
   2.6 Core Improvements ......................................................................................................................... 7
3 PowerFlex Snapshots ......................................................................................................................... 8
   3.1 Max snapshot count ......................................................................................................................... 8
   3.2 Snapshot Consistency Groups ......................................................................................................... 8
   3.3 Snapshot Independence ................................................................................................................... 10
   3.4 Snapshot Policies ............................................................................................................................ 12
4 Secure Snapshots .............................................................................................................................. 13
   4.1 General Behavior ............................................................................................................................ 13
   4.2 Creating a Secure Snapshot .............................................................................................................. 14
   4.3 Extending Retention Period of Secure Snapshot ............................................................................. 16
   4.4 Deleting Secure Snapshots on or after Expiration ........................................................................ 16
   4.5 Deleting Secure Snapshot before Expiration .................................................................................. 16
   4.6 Creating a Write-enabled Version of a Secured Snapshot .............................................................. 16
5 Summary ............................................................................................................................................. 17
Executive summary

Sarbanes-Oxley and other business drivers led customers to ask for new ways to secure data, protecting it not only from deletion, but also from alteration. PowerFlex 3.5 offers this and a variety of other core features. Snapshot creation now provides the ability to prescribe an expiration date at creation time. This paper will discuss this feature in detail, describing the behavior of Secure Snapshots, how they're created, and how they can eventually be deleted.
Introduction

PowerFlex (formerly VxFlex OS) is a software-defined storage platform designed to significantly reduce operational and infrastructure complexity empowering organizations to move faster by delivering flexibility, elasticity, and simplicity with predictable performance and resiliency at scale. The PowerFlex family provides a foundation that combines compute as well as high performance storage resources in a managed unified fabric. Flexibility is offered as it comes in multiple hardware deployment options such as integrated rack, appliance or ready nodes, all of which provide Server SAN, HCI and storage only architectures.

![PowerFlex Overview](image)

PowerFlex provides the flexibility and scale demanded by a range of application deployments, whether they’re on bare metal, virtualized, or containerized.

It provides the performance and resiliency required by the most demanding enterprises, demonstrating six 9s or greater of mission-critical availability with stable and predictable latency.

Easily providing millions of IOPs at sub-millisecond latency, PowerFlex is ideal for both high performance applications and for private clouds that desire a flexible foundation with synergies into public and hybrid cloud. It’s also great for organizations consolidating heterogeneous assets into a single system with a flexible, scalable architecture that provides the automation to manage both storage and compute infrastructure.
2 PowerFlex 3.5 New Features

There is much more to this release than Secure Snapshots, so it is worth mentioning some additional features included in the release.

![Image of new features: Native Asynchronous Replication, New HTML5-based Web UI, Protected Maintenance Mode, Secure Snapshots, SDC Authentication, Core Improvements*](image.png)

Figure 2  New Features

2.1 Native Asynchronous Replication

The flagship feature in version 3.5 is native asynchronous replication. Implemented as a journaling-based replication architecture, PowerFlex replication continues the tradition of vastly scalable, performant, and elastic systems. For additional information see the white papers on Dell EMC PowerFlex: Introduction to Replication as well as Dell EMC PowerFlex: Networking Best Practices and Design Considerations.

2.2 Protected Maintenance Mode

Protected Maintenance Mode, or PMM, offers better data protection over Instant Maintenance Mode. While Instant Maintenance Mode, or IMM, offered the ability to perform node maintenance very quickly, there was some exposure to potential data unavailability or loss should an additional device or node experience failure. PMM creates a temporary third copy of the node’s data throughout the system spare capacity during the maintenance period. When maintenance is complete, the deltas are synced back to the maintained node. While it takes longer to perform than IMM, it preserves full data protection throughout the maintenance period and vastly reduces concern for data loss and availability.

2.3 SDC Authentication

Authentication of SDCs is better secured with CHAP, or Challenge-Handshake Authentication Protocol. It allows the MDM to validate the authenticity of each SDC when it’s first attached and to establish secrets between the SDCs and SDSs to regulate access to volumes. The MDM regularly refreshes the secrets, forcing the SDCs and SDSs to re-authenticate on a regular basis.
2.4 New WebUI

The PowerFlex 3.5 release offers a new, streamlined HTML5-based user interface which is consistent with other Dell Technologies product solutions.

![Image](image.png)

Figure 3 This primary dashboard view displays the majority of system activity at a single glance while also preserving the ability to drill into all PowerFlex elements to view or manage them.

2.5 Secure Snapshots

The subject of this paper, and it will be covered in detail.

2.6 Core Improvements

There are several core improvements in 3.5, but a few merit special mentions. Release 3.5 adds a Fine Granularity Metadata cache which eliminates the two-step metadata lookup required for FG volume read I/Os. Up to 32GB of FG pool metadata can be cached per SDS. The cache is not persistent, it resides in DRAM, and it is updated either on new reads after an SDS reboot or upon a cache-miss. This dramatically improves FG read performance for recent and frequently read I/Os.

Data resiliency has been improved with two new features. Persistent checksum is now available for data residing on Medium Granularity storage pools, and this is enabled by default on volumes created after the upgrade to 3.5. Additionally, new Partial Disk Error handling prevents immediate ejections and rebuild of entire drives when only a few sectors fail. This provides a longer useful life of your media.

For more information on the PowerFlex 3.5 release, refer to the Getting to Know document in the product documentation bundle found on the Dell EMC support site.
3 PowerFlex Snapshots

Snapshots are a block image in the form of a storage volume or LUN used to instantaneously capture the state of a volume at a specific point in time. PowerFlex snapshots are thin-provisioned and writable. Once a snapshot is taken, it becomes a new, unmapped volume in the system. It can be manipulated just like any other volume exposed by the storage system: mapped, unmapped, renamed, resized, etc.

PowerFlex snapshots can be initiated manually through any of the clients: the WebUI, CLI or REST API. Snapshots can also be managed by any of these clients. The CLI and REST API, however, offer the ability to create snapshot policies, which automate the creation and deletion of snapshots according to a defined schedule.

Snapshots and their source volume are organized into a Volume Tree, or V-Tree. Stated differently, a V-Tree includes the root volume and all of the descendant snapshots resulting from that volume. This includes not only snapshots taken of the root volume at different points in time, but also descendants that are snapshots of snapshots. The following diagram depicts a small V-Tree with both types of descendant.

![V-Tree Diagram]

Figure 4 V-Tree where S111 and S112 are snapshots of volume V1 at different times, and S121 is a snapshot of another snapshot – S111.

3.1 Max snapshot count

In PowerFlex (VxFlex OS) 3.0 and later, each V-Tree can have up to 128 members. One member is the root volume itself, and another is reserved by the system for use when overwriting a member of the V-Tree with the contents of another member. The reserved V-Tree member isn't visible in the system, but it deducts from the total possible snapshot count. This means that for any root volume we start with, it can have up to 126 usable descendants, or snapshots, in the V-Tree.

3.2 Snapshot Consistency Groups

PowerFlex Snapshots can also have relations across different V-Trees. When you take a snapshot, multiple volumes can be selected simultaneously. All snapshots taken together like this form a Consistency Group.

The snapshots in a consistency group are guaranteed to be from precisely the same point in time. They can be used to capture a crash-consistent snapshot-based backup across multiple volumes.
In the PowerFlex WebUI, select the checkbox next to all of the volumes you wish to snap and click **More > Create Snapshot**

![Configuration: Volumes]

Figure 5  Create snapshot of multiple volumes for snapshot consistency group

Once created, all of the members of the consistency group will appear in the Details for any single member.

![Details]

Because they were all taken at the same time, together, there is a contextual relationship among the members, and the consistency group can be manipulated together as a set. For example, the entire consistency group can be deleted as a single action.

![Diagram]

Figure 6  Snapshots S112 and S211 are taken together and form a Consistency Group, C1

However, PowerFlex does not enforce the relationship, and does not try to preserve it as originally created. A user can remove a member of a consistency group, or resize it, overwrite its contents, or otherwise alter it. Snapshot consistency groups are for convenience purposes only.
### 3.3 Snapshot Independence

PowerFlex does not rigidly enforce the parent-child relationships in a V-Tree. It is possible to overwrite the contents of one snapshot with the contents from any other snapshot. In the following example, we have a root volume, a snapshot of the root volume, and a snapshot of the snapshot.

![Snapshot Independence Diagram](image)

**Figure 7**

We can remove the root (or source) volume and choose whether or not to delete the descendent snapshots.

![Remove Volume Source](image)

**Figure 8**

Alternatively, we might choose to overwrite the contents of the root volume with the contents of a child or ‘grandchild’ snapshot. Select the root volume as our target.

![Overwrite Volume Content](image)
Then select the volume whose contents you wish to use for the overwrite. Note that you can select broad time frames in which to search for the snapshot you desire. In this case, we’ll use the snapshot of a snapshot.

Then proceed to do the overwrite. The UI will warn of the destructiveness of the process.

In general, there are few if any limits on the possible manipulations of members of a V-Tree. This sort of flexibility is very useful in development scenarios wherein a gold copy might be used to develop and test many iterations and versions.

Figure 9  Images showing sequence for snapshot overwrite
3.4 Snapshot Policies

Of the 126 available snapshots per volume, sixty (60) of these can be used for policy-based snapshot scheduling. Any given root volume can only participate in one snapshot policy, but a policy can apply to multiple source volumes simultaneously.

First a rule is created and then source volumes are attached to the rule. The rule itself defines the interval between snapshots and the number of them to keep. For example, take a snapshot every 60 minutes and keep 24 of them. This ensures you have a snapshot for every hour of the past 24 hours. The rule can also be created in a multi-level retention structure (up to six levels), where the intervals build upon one another as minutes/hours/days/weeks. For example, setting the base interval at 60 minutes, we keep 24 (as before) and then define another retention level to keep one of these for 7 days, thereby keeping one daily copy for a week. If we set another retention level to keep one of the daily copies for 4 weeks, we ensure that the system maintains (on a rotating basis):

- Hourly snapshots for a day (24)
- A daily snapshot for a week (7)
- And a weekly snapshot for a month (4)

In Version 3.5, there is no graphical user interface for the policy scheduling. Rather, it is something to be handled programmatically via the CLI or REST API.

For more information see the section on Snapshot Policies in Getting to Know Dell EMC PowerFlex v3.5.

To create the policy described above with the CLI, the following command would be used:

```
scli --add_snapshot_policy --snapshot_policy_name snap_policy_hourly \   --snapshot_creation_cadence 60 --number_of_snapshots_per_retention_level 24,7,4
```

**Note:** the snapshot_creation_cadence is set in minutes.

To add a source volume to this policy we would use, for example:

```
scli --add_source_volume_to_snapshot_policy --snapshot_policy_name snap_policy_hourly \   --source_vol_id 3b21a36600000003
```

For details on the CLI and the options available, see the section on snapshots in Dell EMC PowerFlex v3.5 CLI Reference Guide.
4 Secure Snapshots

The volume snapshot functionality in PowerFlex 3.5 has been expanded again. We now have the option to mark snapshots as "secure", thereby enabling customers to meet business and statutory requirements for data retention. This is especially important in financial sectors.

![Create snapshot of volume source- fg-vol-2](image)

Figure 10 Secure snapshot with 1 year expiration time.

Once a snapshot is created with the secure option, it cannot be deleted until the assigned expiration time is reached. For cases where secure snapshots are created by mistake, or must be removed for other reasons, there is a formal process integrated with Dell support that must be followed in order to delete them.

It should be noted that Secure Snapshots are, by default, Read Only. The general ability to create snapshots with Read Only access is new in version 3.5, whether they are marked as secure or not.

4.1 General Behavior

A snapshot can be created initially with or without the secure flag and expiration time. If it is initially created without the secure flag, the expiration time can be added later with the set_snapshot_security CLI command. (The REST API can also be used to add this marker.)

Secure snapshots cannot be altered before their expiration time. When a secure snapshot is mapped to an SDC, regardless of how it’s mounted, it will be forced into the read-only option. We saw above that PowerFlex snapshots can be deleted or overwritten with the contents of another V-Tree member. These operations are not possible for secure snapshots.

It is possible to mark snapshots created through a scheduling policy as secure. However, any secure snapshots that exist in a policy-generated set will remain in place regardless of what is done to the snapshot policy. Pausing, altering, or deleting the policy will not delete the snapshots marked as secure.

The snapshot policy engine itself has been enhanced to enable the automatic creation of secure snapshots using the secure_snapshots flag. In this case, the snapshots created for and during each interval cannot be manually deleted until the normal intervals have occurred. At that point, the policy engine will remove the snapshots per the defined rule.
4.2 Creating a Secure Snapshot

Secure Snapshots can be created:

1. Via the WebUI
2. Via the PowerFlex command line interface
3. With the Rest APIs
4. With a pre-defined snapshot policy
5. By issuing a CLI or REST command to secure a previously created snapshot

The easiest approach is with the WebUI. We visit the Configuration → Volumes menu, select the desired volume, and click the MORE menu.

Figure 11

This opens a pop-up form which allows us to name the snapshot and to set its properties (read-only; secure):

Figure 12

For this example, we will set the expiration time to 15 minutes. But the interval can be set in the UI for minutes, hours, days, or weeks.
Secure Snapshots

After creating the snapshot of our source volume, it appears and is marked both secure and read only.

![Configuration: Volumes](image)

**Figure 13**

If we try to delete it or overwrite the contents, we receive the following sort of error:

![Failed to remove Volume source-fg-vol-1-snap-1](image)

**Figure 14**

From the CLI, we would do something like the following to create a secure snapshot:

```bash
scli --snapshot_volume --volume_name source-fg-vol-1 \       --snapshot_name source-fg-vol-1-snap-1 --retention_period 15m
```

You are prompted to confirm the decision to create a secure snapshot:

```
[root@mx182R4 ~]# scli --snapshot_volume --volume_name source-fg-vol-1 --snapshot_name source-fg-vol-1-snap-1 --retention_period 15m
You are about to create secure snapshots that cannot be removed during the retention period. Press 'y' and then Enter to confirm: y
```

Alternatively, users can preemptively approve the creation by adding the `--i_am_sure` flag to the command.

Specifying a retention period denotes the snapshot as secure, and this includes the read-only attribute. The time period is specified using `m` | `h` | `D` | `W` | `M` | `Y` respectively indicating minutes, hours, days, weeks, months, or years. Examples: 30m (thirty minutes), 5D (five days), 1M (one month, which equals 31 days)
4.3 Extending Retention Period of Secure Snapshot

While it is not possible to reduce the retention period of a snapshot, it is possible to use the CLI to extend the retention period. This operation cannot be performed from the WebUI.

```
scli --set_snapshot_security --volume_name source-fg-vol-1-snap-1 \  --retention_period 30m --i_am_sure
```

This command will alter the retention period and reset the expiration time to 30 minutes from the time the command is run.

Attempting to set a retention period shorter than the remaining time already defined will receive an error:

```
[root@me-1029-a /]# scli --set_snapshot_security --volume_name source-fg-vol-1-snap-1 --retention_period 5m --i_am_sure
Error: NDM failed command. Status: The snapshot retention period cannot be reduced
```

4.4 Deleting Secure Snapshots on or after Expiration

Secure snapshot deletion is not automatic after the expiration time has been reached. But once the time period for the secure flag has expired, users are free to alter or delete the snapshot. In the WebUI, the date and time of the retention policy expiration are shown next to the snapshot.

4.5 Deleting Secure Snapshot before Expiration

There is no mechanism provided for customers to delete secured snapshots if they are mistakenly created, or created with the wrong expiration date, or if system capacity issues might benefit from the deletion of secured snapshots. Instead, there is a multi-step business-approval workflow with specific documentation requirements (including two business leader signatures). Subsequently, a support ticket is created. The required documentation is reviewed and a login session with support is facilitated in which the snapshot’s retention period is reset. After this, the snapshot in question can be deleted.

4.6 Creating a Write-enabled Version of a Secured Snapshot

While the secure snapshot’s data protection is guaranteed, if application testing or other needs arise that would require write access to the secured data, it is possible to create a snapshot of the secured snapshot, and by default, this copy will be writable.
Summary

The addition of Secure Snapshots adds yet another feature to the data protection and management tool set in PowerFlex software-defined storage. Dell Technologies is passionate about meeting customer needs and expectations. This new feature accommodates business needs and government requirements while adding flexibility to the management of PowerFlex storage clusters.

You should now have a better understanding of the secure snapshots and their limits and consequences. Creating secure snapshots should be done carefully, but there are ways to deal with snapshots that were created by mistake.