

Dell EMC PowerMax and VMAX All Flash: Snapshot Policies

January 2022

H18432.1

White Paper

Abstract

Snapshot policies on Dell EMC PowerMax and VMAX All Flash storage arrays provide automated scheduling of SnapVX snapshots through a highly available and flexible policy. This document discusses snapshot policy use cases and implementation best practices using Unisphere for PowerMax, REST API, and command line with Solutions Enabler.

Dell Technologies

Copyright

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 © 2020-2022 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. Intel, the Intel logo, the Intel Inside logo and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries. Other trademarks may be trademarks of their respective owners.

Published in the USA January 2022 H18432.1.

Dell Inc. believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

Contents

Executive summary	4
Snapshot policies	5
Default policies	11
Creating policies	14
Associating snapshot policies with SGs	15
Policy snapshots	19
Compliance	24
Alerts	29
Cloud mobility for Dell EMC PowerMax	30
Legacy Unisphere snapshot scheduler	31
Summary	31
Appendix A: Solutions Enabler command examples	32
Appendix B: REST API examples	34
Appendix C: Technical support and resources	37

Executive summary

Overview

In today's digital age, the growth of data being stored increases the importance of data-protection and recovery options. The high frequency of online transactions magnifies the implications of an outage. During a data-availability issue due to accidental or malicious activity, the ability to quickly and surgically recover from data loss is critical. Applications must be able to recover from a large selection of granular, point-in-time images.

As important as these recovery options are, many business leaders cannot afford to dedicate valuable resources to creating, maintaining, and monitoring backup data. Protecting applications must be done as easily as possible and with confidence that protection is provided as expected.

Designed to address these challenges, the snapshot policies feature is included with the PowerMaxOS Q3 2020 release for Dell EMC PowerMax and VMAX All Flash storage arrays. This feature provides automated scheduling of SnapVX snapshots using a highly available and flexible policy engine that runs internally on the storage array. Snapshot policies can be managed through Dell EMC Unisphere for PowerMax, REST API, and Solutions Enabler.

Snapshot policies can be customized with rules that specify when to take snapshots, how many snapshots to take, and how long to keep each snapshot. Compliance requirements can also be specified to send alerts if the rules of a policy are not being met. Applications can be protected by multiple policies with differing schedules and retention parameters according to the requirements of the business. Each policy can protect many applications, even protecting a mix of open systems and mainframe applications.

Snapshot policies provide reliable protection for applications in an automated fashion that requires little to no maintenance by the business. Administrators can manually take snapshots of applications that are protected by snapshot policies to satisfy on-demand requirements

Revisions

Date	Description
September 2020	Initial release: PowerMaxOS Q3 2020
January 2022	Template update

We value your feedback

Dell Technologies and the authors of this document welcome your feedback on this document. Contact the Dell Technologies team by [email](#).

Author: Mike Bresnahan

Contributors: Dell EMC Storage Technical Marketing Engineering Team

Note: For links to other documentation for this topic, see the [PowerMax and VMAX Info Hub](#).

Snapshot policies

Snapshot policies overview

Snapshot policies minimize the effort required to maximize application protection. They provide regularly scheduled, crash-consistent snapshots that are based on application requirements.

Snapshot policies create and retain SnapVX snapshots according to the rules within each policy. These customizable rules include the frequency of snapshots, snapshot retention time or count, and compliance-based alerts. Policies are applied to storage groups (SGs) to protect applications with crash-consistent snapshots at regularly scheduled intervals.

Up to four policies can be assigned to each SG. This ability allows applications to be protected with a combination of frequent snapshots and snapshots taken at specified times that are important to the business. There is no limit to the number of SGs that can be assigned to a single policy. Each array supports up to 20 policies.

Child SGs inherit policies that are assigned to its parent SG. This ability enables taking snapshots of an entire database with the option of performing link and restore operations on the entire database or on subsets of a database. When a policy is assigned to a parent SG, the policy takes a snapshot at the parent-SG level and the snapshot is consistent across all child SGs. Conversely, if the policy is individually assigned to each child SG, the child SGs are snapped separately, and the snapshots are not consistent across all child SGs. If a child SG and its parent SG are assigned to the same policy, the policy ignores the child SG.

When assigning parent and child SGs to snapshot policies, be aware of the RPO Interval and Offset values to ensure that the 10-minute minimum RPO is not continually exceeded. This factor must be considered when assigning volumes to multiple SGs. However, users do not have to configure all policies so that snapshots are never taken within 10 minutes of each other. We recommend not intentionally overlapping policies, which would cause applications to be continually snapped every two to three minutes.

Three default policies are automatically populated in the array. These default policies are available for immediate use, but their parameters should be modified according to the requirements of the applications that they will protect. New policies with custom settings can also be created.

Role-based access controls (RBAC) can be implemented, requiring users to have StorageAdmin rights to create, modify, and delete policies, and to associate or disassociate snapshot policies with SGs.

Snapshot policies parameters

The following parameters are defined within each policy. You can modify all parameters on active policies, except for the **Policy Type (Local or Cloud)** and **Secure Snaps** options which are only selectable during policy creation.

- Policy Name
 - 1 to 32 characters
 - Can contain letters, digits, dashes, and underscores
 - Not case sensitive
- Policy Type
 - Local (on array)

- Cloud (off array)
- Secure Snaps
 - May only be terminated after they expire or by customer-authorized Dell Support
 - See Dell Support knowledge base article [498316](#) before implementing Secure Snaps
- Recovery Point Objective (RPO)
 - Interval:
 - By the minute, hour, day, or week
 - Minimum RPO interval is 10 minutes
 - Offset
 - Timeframe within the RPO interval
- Snapshots to keep
 - Timeframe or snapshot count
- Compliance Alerting
 - Based on snapshot count and scheduled interval

Workflow examples

The document discusses snapshot policies using examples from Unisphere for PowerMax. Examples from Solutions Enabler ([Appendix A: Solutions Enabler command examples](#)) and REST API ([Appendix B: REST API examples](#)) are included at the end of the document.

This section explains the implementation and best practices surrounding Snapshot Policies using a typical implementation workflow. The following figure shows a high-level example of a typical implementation procedure.

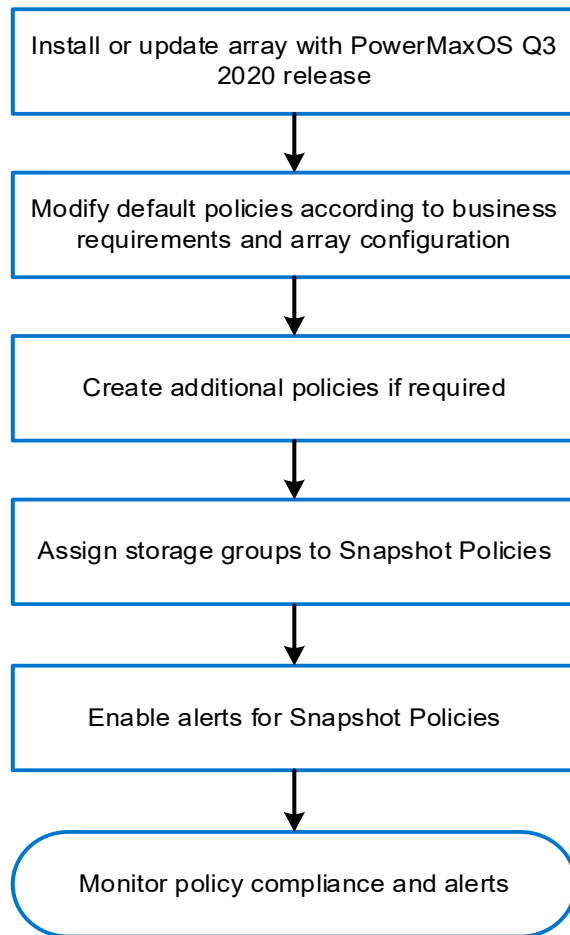


Figure 1. High-level workflow example

Snapshot policy requirements

The following are requirements for using snapshot policies:

- PowerMax and VMAX All Flash storage platforms
- PowerMaxOS Q3 2020 release or later
- Unisphere for PowerMax V9.2 or later
- Solutions Enabler V9.2 or later

TimeFinder session limits

The following table lists the per-source-volume session limit of the various TimeFinder modes. Each SnapVX source volume can have up to 1024 SnapVX linked targets.

Table 1. TimeFinder session limits

TimeFinder mode	Maximum sessions per source volume
Total sessions, combination of all modes	1024
Snapshot policies SnapVX snapshots	1024
Data Protector for z Systems (zDP) SnapVX snapshots	1024
Solutions Enabler SnapVX snapshots	256

TimeFinder mode	Maximum sessions per source volume
Unisphere for PowerMax SnapVX snapshots	256
Dell EMC Mainframe Enablers SnapVX snapshots	256
AppSync SnapVX snapshots	256
PowerProtect Storage Direct SnapVX snapshots	256
RecoverPoint SnapVX snapshots	256
TimeFinder/VP Snap	32
TimeFinder/Clone	8
TimeFinder/Mirror (BCV)	8

There is no hard limit on the number of sessions in a single array. The total sessions within an array depend on the configured and available resources. Include snapshot use in the overall sizing and planning of new systems to ensure that each array is configured with required resources. After deployment, monitor system resources as usage grows. These best practice recommendations are applicable to all features and applications on a storage array and are not specific to snapshots.

Terminology

The following tables provide definitions for some of the terms that are used in this document.

Table 2. Traditional SnapVX terminology

Term	Definition
Source volume	A LUN or mainframe CKD volume that is protected by snapshots or clones.
Snapshot	A preserved, point-in-time image of a source volume.
Targetless snapshot	A snapshot used by SnapVX that does not require a target LUN or CKD volume.
Source snap	An optional setting for SnapVX targetless snapshots that prevents a user from deleting snapshots accidentally or intentionally. Secure snapshots may only be terminated after they expire or by customer-authorized Dell Support. See the Dell Support knowledge base article 498316 for more information.
Snapshot delta	A point-in-time version of a source volume track that was preserved during a host write to a source volume that had an active snapshot.
Replication cache	A portion of the metadata in cache that is dedicated for replication data pointers (RDP) which track the snapshot deltas in the SRP. Replication cache usage increases as SnapVX and VP snap source devices are written to, as there is more point-in-time data to manage.
Linked target volume	A LUN that is linked to a SnapVX snapshot to make the point-in-time of the snapshot accessible to a host.

Term	Definition
zDP	Data Protector for Z Systems (zDP) is a Dell EMC z/OS-based application that uses TimeFinder SnapVX snapshots to enable rapid recovery from logical data corruption on IBM z Systems. zDP achieves this functionality by providing multiple, frequent, and consistent point-in-time copies of data in an automated fashion across multiple volumes from which an application-level recovery can be conducted. For more information about zDP, see the document Dell EMC PowerMax and VMAX All Flash: Data Protector for z Systems (zDP) Essentials .
Coordinated Universal Time (UTC)	The primary time standard by which the world regulates clocks and time. It is not adjusted for daylight saving time .

Table 3. Snapshot policies terminology

Term	Definition
Effective policies	Snapshot policies that are operating (not suspended) on a storage group (SG) on the PowerMax or VMAX All Flash (AF) array.
Inherited	Term that describes how a snapshot policy that applied to a parent SG is inherited by all child SGs.
Recovery point objective (RPO)	<p>Unisphere for PowerMax definitions for the frequency at which a Snapshot Policy takes snapshots, and when the snapshots should be taken. Solutions Enabler refers to these settings as the Interval and the Offset, respectively.</p> <ul style="list-style-type: none"> Interval can be defined by the minute, hourly, daily, or weekly. The minimum Interval is 10 minutes. Intervals must be evenly divisible into 7 days. For example, when defining an interval in minutes, acceptable values include the following: 10, 12, 15, 20, 30, 60, 120, 180, 240, 360, 480, 720, 1440, and 10080 minutes. Unisphere for PowerMax offers a selection of supported interval values. The Offset defines when to take the snaps during the Interval, and therefore, the Offset value must be less than the Interval value. For example, if the interval is every two hours, the offset indicates when within each 2-hour interval the snapshots will be taken.
Max mount	The maximum number of snapshots that should be maintained for a specified Snapshot Policy. The maximum count must be between 1 and 1024.
Warning compliance	User-defined snapshot count at which warning alerts are posted. The user sets the attribute on each Snapshot Policy. The compliance count cannot be set to 0 and must be less than or equal to the maximum count of the Snapshot Policy. If the critical compliance count is also set, the warning compliance count must be greater than or equal to that.
Critical compliance	User-defined snapshot count at which critical alerts are posted. The user sets the attribute on each Snapshot Policy. The compliance count cannot be set to 0 and must be less than or equal to the maximum count of the Snapshot Policy. If the warning compliance count is also set, the critical compliance count must be less than or equal to that count.

Term	Definition
Persistent policy snapshots	Setting a policy snapshot to persistent excludes it from being automatically recycled by the policy parameters. A persistent snapshot is not automatically terminated until the user clears the persistent setting and the policy retention time has passed, or if the snapshot is manually terminated by the user.
Orphaned	When a policy is deleted, snapshots that the policy created are renamed to _Orphaned . The expiration date is set earlier when the SG was removed from the policy. Orphaned snapshots can be used for link and restore operations and can be manually terminated.
Cloud snapshots	Cloud Mobility for Dell EMC PowerMax provides open-systems snapshot movement to and from private and public clouds (Dell EMC ECS, AWS, Microsoft Azure) for recovering data back to the array and consumed it directly in AWS.
Out-of-window exception	Indication that a SnapSet has a policy snapshot with a timestamp that is outside of the policy window. Possible reasons include modification of a policy or snapshots prevented from being terminated as scheduled due to being set as persistent, being in a restore state, or linked to a target.
Gap exception	Indication that a SnapSet has policy snapshots that were taken at intervals that are larger than defined in the policy. Possible reasons include failure to create a regularly scheduled snapshot, termination of a snapshot, or modification of a policy.

The following SnapVX terms are introduced in the PowerMaxOS Q3 2020 release. These terms are applicable to all snapshots and are not unique to snapshot policies.

Table 4. Other SnapVX terminology

Term	Definition
SnapSet	A set of consistent snapshots that are taken together. For example, when a snapshot is taken of an SG that contains 10 devices, the resulting SnapSet consists of 10 consistent snapshots.
SnapSet ID	A system-generated number that is applied to consistent snapshots across the volumes in a SnapSet. When a snapshot is taken of an SG, all resulting snapshots have the same SnapSet ID. The SnapSet ID is an absolute value that does not adjust as other snapshots are created or terminated.
Bulk terminate	A Unisphere term for functionality that allows termination of many snapshots of an SG in a single operation.

Default policies

Each array is automatically populated with three default policies: HourlyDefault, DailyDefault, and WeeklyDefault. The default policies can be used with their preset values if they meet the business requirements of applications that are assigned to each policy, and the array resource limits. Otherwise, the RPO rules of the policy should be modified accordingly.

Whether using the default policies as-is, modifying the default policies, or creating policies, you must size the array configuration to meet the expected snapshot usage. The sizing requirements must consider the capacity of the applications that will be protected, the snapshot count, the snapshot retention requirements, and several other capacity- and performance-requirement metrics.

When a policy is modified to reduce the number of snapshots to keep, existing snapshots that exceed the new count are terminated. This action is performed according to the previous count, and not immediately after the count has been reduced. This behavior prevents accidental changes from immediately affecting protection.

Figure 2 is an example of the initial card view of the Snapshot Policies dashboard before SGs have been assigned to the default policies and before any new policies have been created. Figure 3 is the list view of the Snapshot Policies dashboard.

Select the pencil icon as shown on the DailyDefault policy to open a window that displays the parameters of the policy. The parameters can be edited from the resulting window.

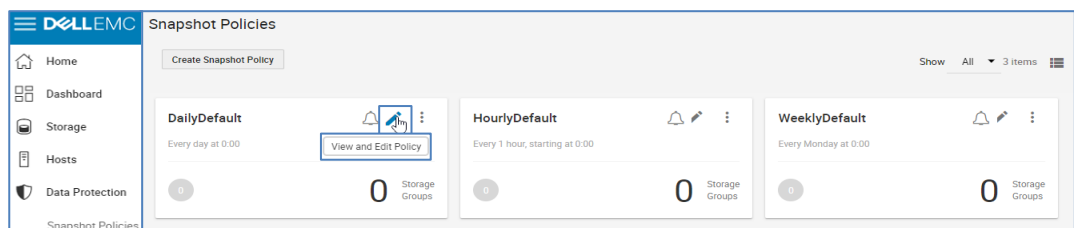


Figure 2. Snapshot Policies dashboard

Policy Name	Storage Groups	Compliance	State	Type	Secure
DailyDefault Every day at 0:00	0	0	✓	Local	—
HourlyDefault Every 1 hour, starting at 0:00	0	0	✓	Local	—
WeeklyDefault Every Monday at 0:00	0	0	✓	Local	—

Figure 3. Snapshot Policies dashboard > list view

The following three figures show the parameters of the default policies. Modifying a policy affects all SGs that are associated with that policy.

View & Modify Policy | DailyDefault

Properties

Name

DailyDefault

Type

☐ Secure Snapshots

Last Execution Time

N/A

Description

Every day at 0:00

Recovery Point Objective (RPO)

Create a snapshot

Daily

at

00:00

Keep


14

Snapshots

Total 14 Snapshots (Max 1024)

Compliance


Show as

 if fewer than

N/A

▼

snapshots are created

 if fewer than

10 (71%)

▼

snapshots are created

?

CANCEL

MODIFY

Figure 4. DailyDefault policy

View & Modify Policy | HourlyDefault

Properties

Name

HourlyDefault

Location

☒ Local ☐ Cloud

Type

☐ Secure

Last Execution Time

Wed Jul 29 2020 11:58:53

Description

Every 1 Hour, starting at :00

Recovery Point Objective (RPO)

Create a snapshot

Hourly

every

1

hour at

:00

↓into the interval

Keep


24

Snapshots

Total 24 Snapshots (Max 1024)

Compliance


Show as

 If fewer than

N/A

▼

snapshots are created

 If fewer than

18 (75%)

▼

snapshots are created

?

CANCEL

MODIFY

Figure 5. HourlyDefault policy

View & Modify Policy | WeeklyDefault

Properties

NameWeeklyDefault

Type☐ Secure Snapshots

Last Execution TimeN/A

DescriptionEvery Monday at 0:00

Recovery Point Objective (RPO)

Create a snapshotWeeklyonMondayat00:00

Keep13SnapshotsTotal 13 Snapshots (Max 1024)

Compliance

Show as⚠ if fewer thanN/Asnapshots are created

⛔ if fewer than10 (77%)snapshots are created

?

CANCELMODIFY

Figure 6. WeeklyDefault policy

The displayed **Create a snapshot** time adjusts according to the time zone of the user's local workstation. When the policy is created, the system takes this value and stores it on the array in UTC format.

UTC does not adjust for seasonal time changes. Systems that are in regions where seasonal time changes occur do not automatically adjust the snapshot creation time. Depending on when the policy was created, snapshots may be taken one hour before or one hour after the target time during seasonal time changes.

Whenever possible, create policies with focus on the frequency of snapshots rather than the exact time that the snapshots are taken. This best practice eliminates the need to modify policies during seasonal time changes. This practice is likely to be more acceptable for policies that create snapshots at a high frequency.

For policies that take snapshots at specific times according to business requirements, you may need to modify them to account for seasonal time changes. This requirement is more common for policies that create snapshots at a lower frequency, such as end-of-week or end-of-month processing.

Creating policies

You can create policies on the Snapshot Policies dashboard (Figure 7) and the Data Protection dashboard (Figure 8).

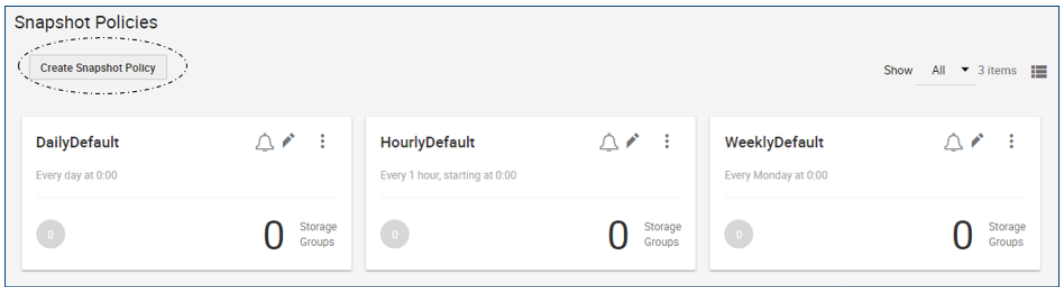


Figure 7. Snapshot Policies dashboard

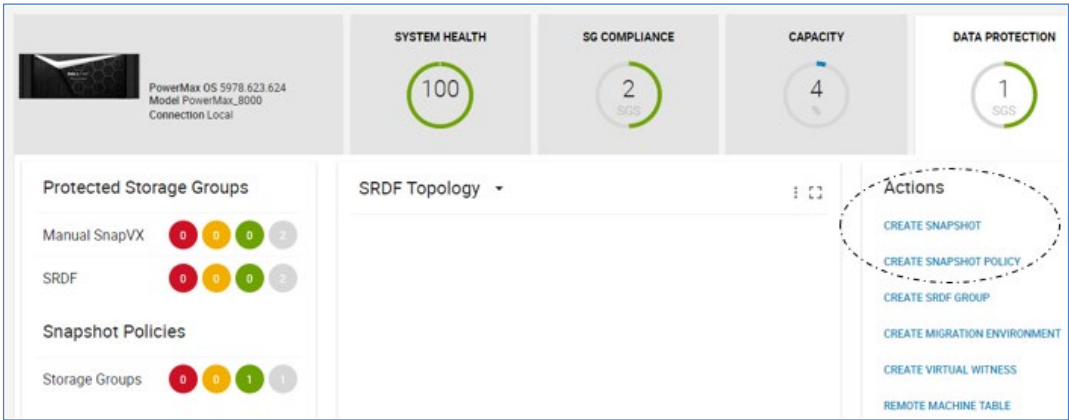


Figure 8. Data Protection dashboard

Both workflows open the same Create Snapshot Policy window. This window has the same parameters for modifying a policy (shown in Figure 4, Figure 5, and Figure 6) with the other options of selecting Secure Snaps. Creating a Cloud Snapshot Policy is also available when creating a policy from Embedded Management.

The following figure shows the Create Snapshot Policy window from embedded Unisphere for PowerMax.

Create Snapshot Policy

Properties

Name:

Location: ☒ Local ☐ Cloud

Type: ☐ Secure

Recovery Point Objective (RPO)

Create a snapshot: By The Minute every 15 mins at :00

Keep 2 Hour(s) Total 8 Snapshots (Max 1024)

Compliance

Show as: If fewer than 7 (88%) snapshots are created

If fewer than 6 (75%) snapshots are created

? CANCEL CREATE

Figure 9. Create Snapshot Policy window

Associating snapshot policies with SGs

Introduction

There are multiple methods for associating snapshot policies with SGs. Each of the workflows described in this section requires the snapshot policy to be created. Other than the Provisioning Wizard process in [Provision Storage wizard](#), the workflows also require the SG to be created.

You can assign up to four policies to each SG. There is no limit to the number of SGs that can be assigned to a single policy.

The child SGs inherit the policies assigned to a parent SG. When a policy is assigned to a parent SG, the policy takes a snapshot at the parent-SG level and the snapshot is consistent across all child SGs. Conversely, if the policy is individually assigned to each child SG, the child SGs are snapped separately, and the snapshots are not consistent across all child SGs.

SGs that contain common volumes should not be assigned to the same policy because only one SG will be snapped.

CKD SGs can be assigned to snapshot policies. For CKD volumes on z Systems, the best practice is to protect the volumes with either zDP or snapshot policies, but not both.

Snapshot Policies dashboard

You can associate multiple SGs to a specific snapshot policy from the Snapshot Policies dashboard. Click the button shown in Figure 10 to open the window shown in Figure 11.

Figure 10 to disassociate policies from an SG, which opens a window that is similar to the screen shown in Figure 11.

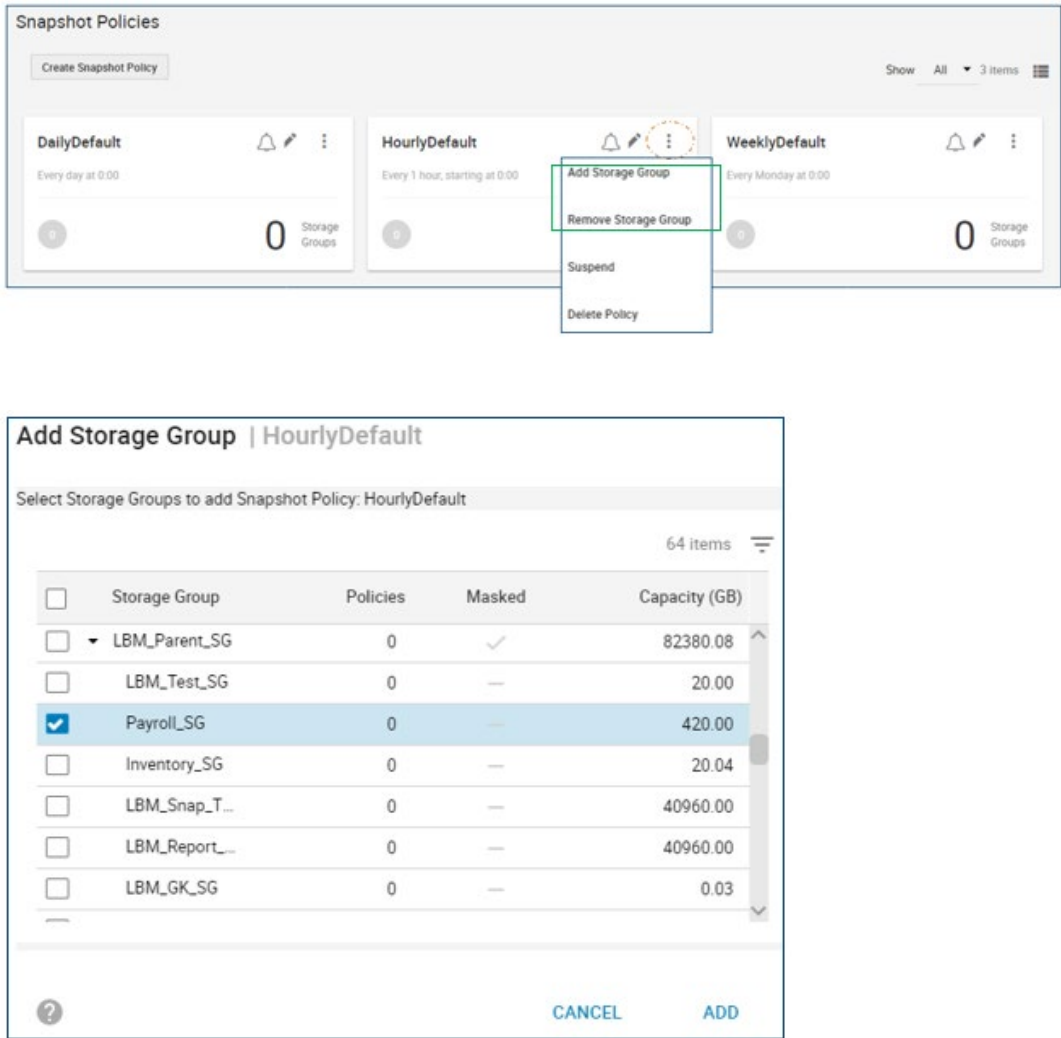


Figure 11. Add Storage Group window

After assigning an SG, the policy tile shows the number of SGs assigned as seen in the following figure.

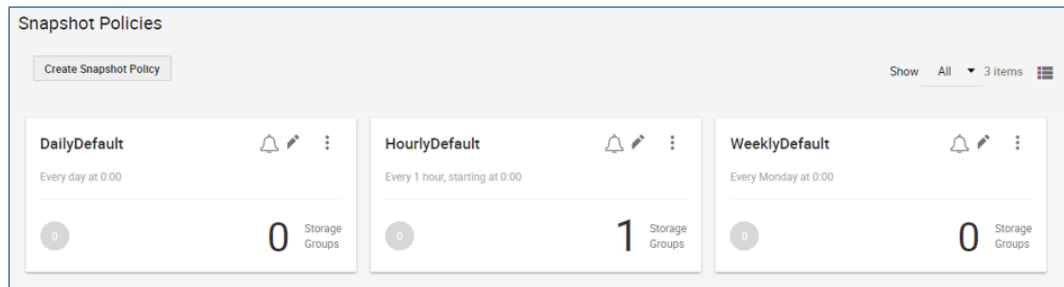


Figure 12. One SG assigned to HourlyDefault policy

Storage Group dashboard

You can associate multiple snapshot policies to a specific SG from the **Storage Group** view > **Data Protection** tab. Click the **Add Snapshot Policy** button in Figure 13 to open the **Select Snapshot Policy(s)** window shown in Figure 14.

Figure 13 to disassociate policies from an SG, which opens a window that is similar to the one shown in Figure 14.

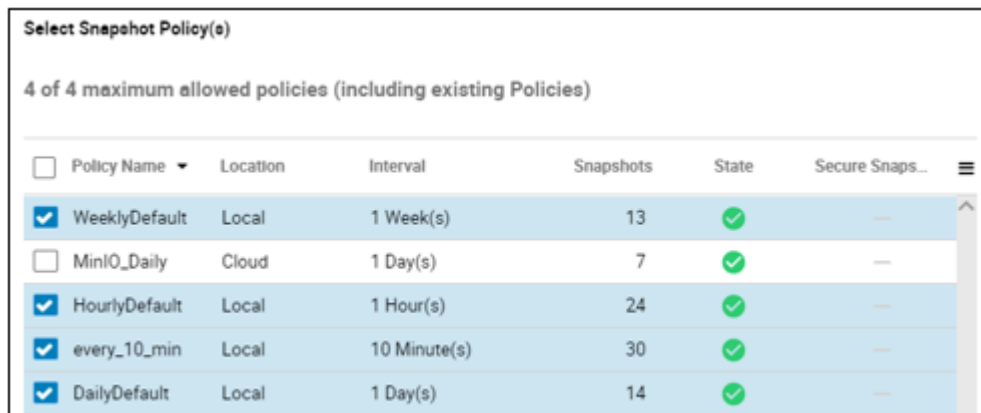
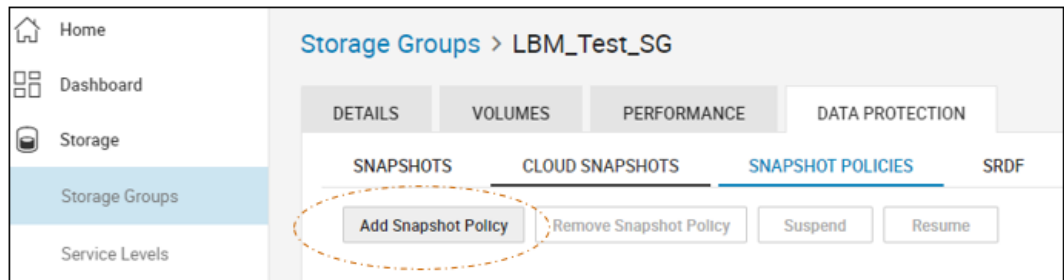


Figure 14. Select Snapshot Policy(s) window

The number of policies that can be selected in Figure 14 depends on the number of policies already associated with the SG. In this example, four policies can be selected because the SG is not already associated with any policies. If the SG was already associated with one policy, only three policies could be selected.

Protect wizard

You can use the Protect wizard from the Storage Group dashboard to associate multiple policies to an SG.

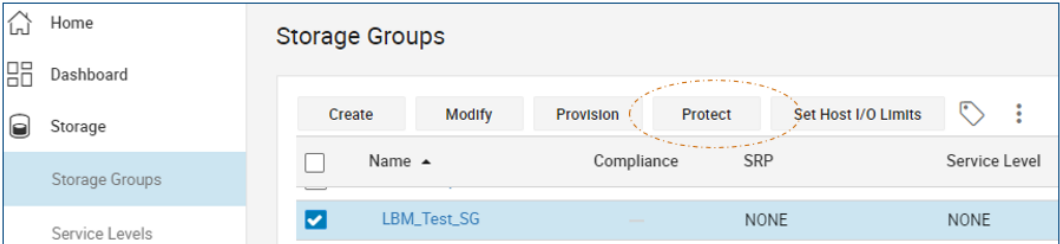


Figure 15. Storage Groups dashboard

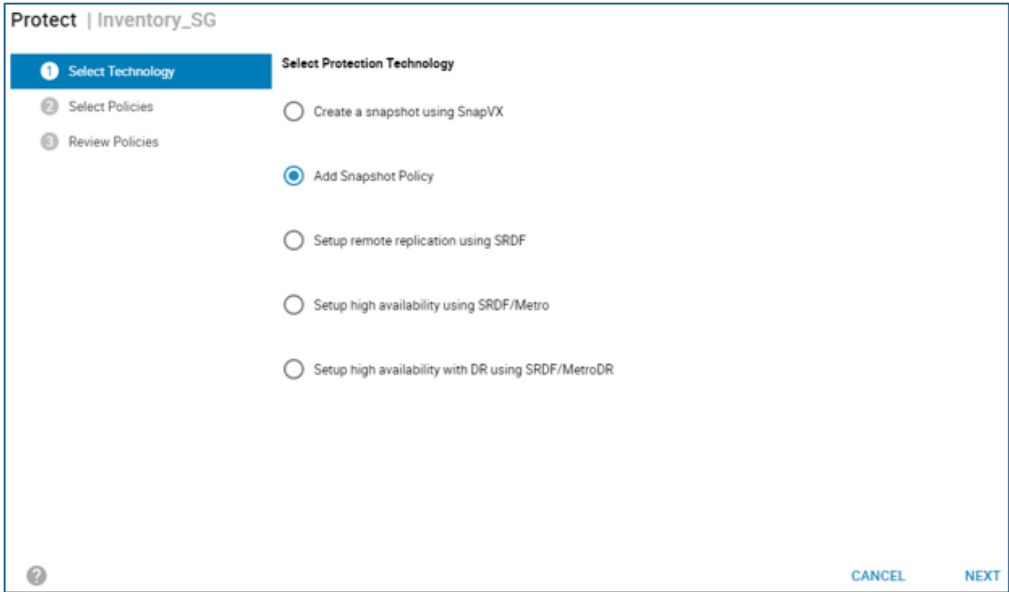
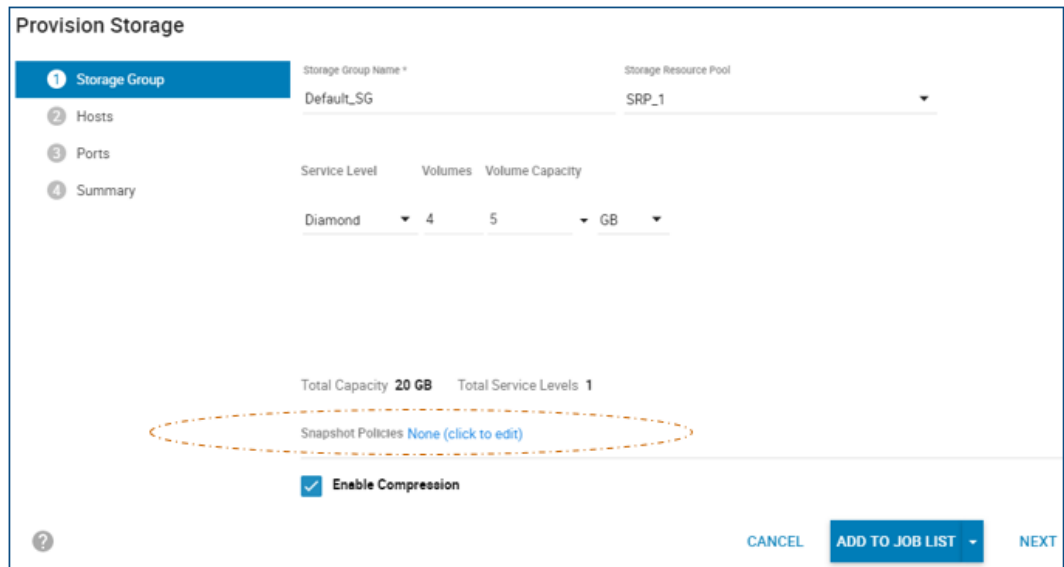


Figure 16. Protect wizard

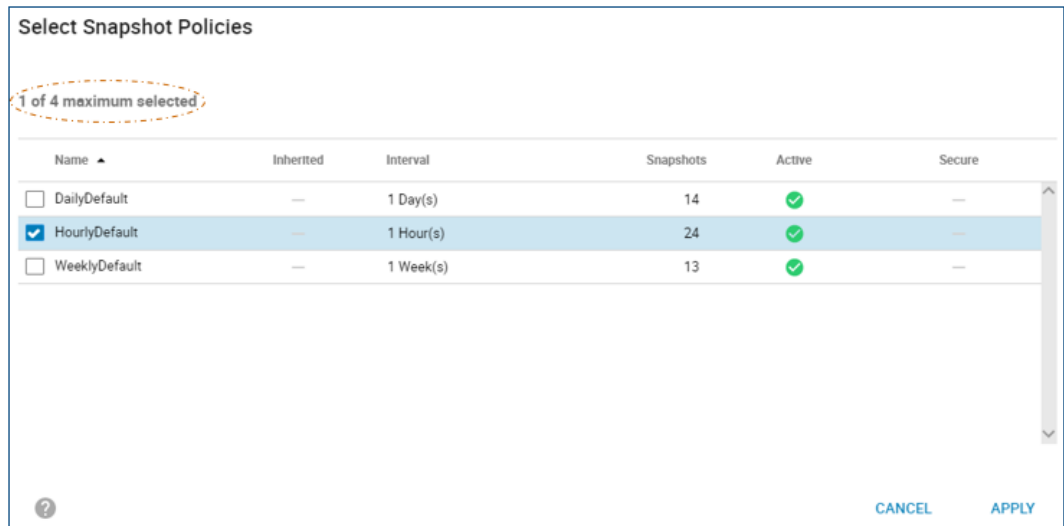
Provision Storage wizard

Use the Provision Storage wizard shown in the following figure to associate multiple snapshot policies to a specific SG when provisioning storage. Click the area shown in the figure to open the **Select Snapshot Policies** window.



The screenshot shows the 'Provision Storage' wizard. On the left, a sidebar lists steps: 1 Storage Group (selected), 2 Hosts, 3 Ports, and 4 Summary. The main area shows configuration for 'Storage Group Name' (Default_SG) and 'Storage Resource Pool' (SRP_1). Below this, 'Service Level' is set to 'Diamond', 'Volumes' to '4', and 'Volume Capacity' to '5 GB'. At the bottom, 'Total Capacity' is 20 GB and 'Total Service Levels' is 1. A dashed orange oval highlights the 'Snapshot Policies' section, which currently shows 'None (click to edit)'. Below this is a checked checkbox for 'Enable Compression'. At the bottom right are buttons for 'CANCEL', 'ADD TO JOB LIST', and 'NEXT'.

Figure 17. Provision Storage wizard



The screenshot shows the 'Select Snapshot Policies' window. A dashed orange oval highlights the text '1 of 4 maximum selected'. Below this is a table with columns: Name, Inherited, Interval, Snapshots, Active, and Secure. Three policies are listed: DailyDefault, HourlyDefault (selected with a blue checkmark), and WeeklyDefault. All three are active (green checkmarks) and secure (dash). At the bottom right are buttons for 'CANCEL' and 'APPLY'.

Name	Inherited	Interval	Snapshots	Active	Secure
<input type="checkbox"/> DailyDefault	—	1 Day(s)	14	✓	—
<input checked="" type="checkbox"/> HourlyDefault	—	1 Hour(s)	24	✓	—
<input type="checkbox"/> WeeklyDefault	—	1 Week(s)	13	✓	—

Figure 18. Select Snapshot Policies window

Policy snapshots

Introduction

The name of a snapshot created by a policy matches the policy name. The following figure shows a list of snapshots that the HourlyDefault policy created.

Modifying the name of a policy also modifies the name of snapshots that were already taken.

The **Snapshot type** column indicates the snapshot was taken by a policy. Snapshots that were created manually have a snapshot type of **Manual**.

The screenshot shows the 'Storage Groups > LBM_Test_SG' page with the 'SNAPSHOTS' tab selected. A table lists 24 snapshots, all of type 'Policy'. The first snapshot is selected. A side panel on the right shows details for the selected snapshot.

Snapshot	Creation Time	Linked	Restored	Expired	Secured	Persistent	Snapshot type
<input checked="" type="checkbox"/> HourlyDefault	Wed Mar 04 2020 12:00:17	---	---	---	---	---	Policy
<input type="checkbox"/> HourlyDefault	Wed Mar 04 2020 11:00:23	---	---	---	---	---	Policy
<input type="checkbox"/> HourlyDefault	Wed Mar 04 2020 10:00:20	---	---	---	---	---	Policy
<input type="checkbox"/> HourlyDefault	Wed Mar 04 2020 09:00:26	---	---	---	---	---	Policy
<input type="checkbox"/> HourlyDefault	Wed Mar 04 2020 08:00:22	---	---	---	---	---	Policy
<input type="checkbox"/> HourlyDefault	Wed Mar 04 2020 07:00:18	---	---	---	---	---	Policy
<input type="checkbox"/> HourlyDefault	Wed Mar 04 2020 06:00:24	---	---	---	---	---	Policy

Name: HourlyDefault

Snapset ID: 115887421697

Creation Time: Wed Mar 04 2020

Expiry Date: ---

State: Established

Secured: No

Figure 19. Snapshot list

SnapSet and SnapSet ID

A SnapSet is a set of consistent snapshots that are taken together across a group of volumes. For example, when a snapshot is taken of an SG that contains 10 devices, the resulting SnapSet consists of 10 consistent snapshots.

Beginning with the PowerMaxOS Q3 2020 release, snapshots are assigned a SnapSet ID. The SnapSet ID is an absolute value that remains the same regardless of creation or deletion of other snapshot generations. When a snapshot is taken across a SnapSet, the snapshots that are created on the individual TDEVs in the SnapSet have the same SnapSet ID. SnapSet IDs are assigned to all snapshot types.

This is a zoomed-in view of the side panel from Figure 19, showing the SnapSet ID for the selected snapshot. The SnapSet ID is 115887421697.

Name	HourlyDefault
Snapset ID	115887421697
Creation Time	Wed Mar 04 2020
Expiry Date	---
State	Established
Secured	No

Figure 20. SnapSet ID

The generation ID of a snapshot is relative to the number of snapshots at the time the snapshots are viewed. However, the SnapSet ID remains the same throughout the life of the snapshot. Since the introduction of SnapVX, the standard method to control or view details of a snapshot is to use the relative generation number, and this method continues to be supported.

However, using snapshot policies can increase the snapshot frequency and snapshot count. This usage also increases the probability that the relative generation number is changed shortly before the user issues a control command to a snapshot. This scenario would issue the control command to the incorrect snapshot.

Creating and terminating snapshots on subsets of the devices in a group could also cause snapshots of the group to have different generation IDs on the individual snapshots. The SnapSet ID would remain constant.

The best practice is to use the SnapSet ID rather than the generation ID. We do not recommend correlating the SnapSet ID of a snapshot to the generation ID. The generation ID will change the next time another snapshot is created and or terminated.

Setting a policy snapshot to persistent

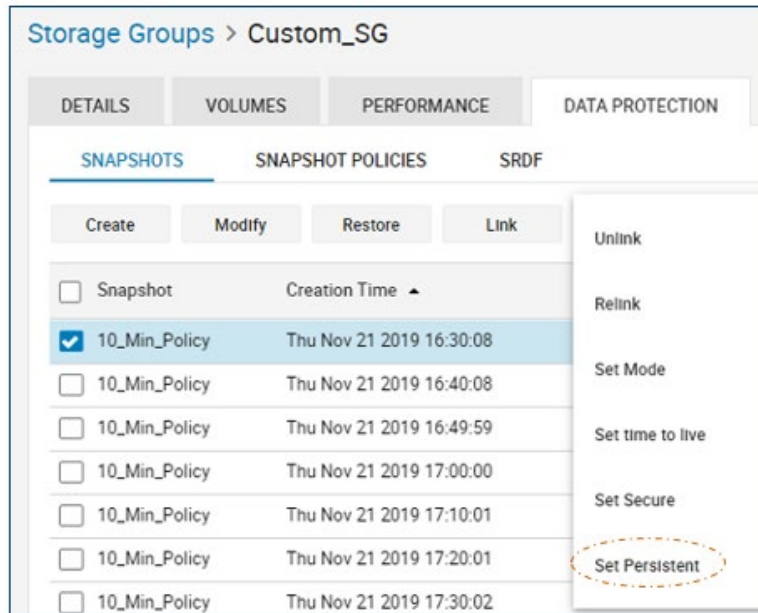


Figure 21. Setting a policy snapshot to the persistent state

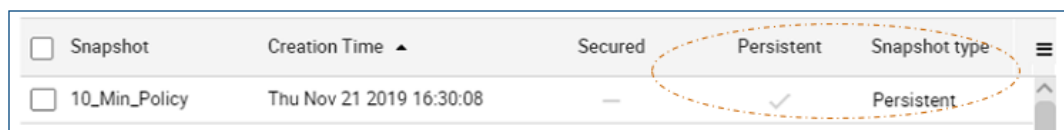


Figure 22. Persistent policy snapshot

After setting a snapshot to persistent, the policy continues to take regularly scheduled snapshots and maintain compliance. When a persistent snapshot passes the point when it would be recycled, the maximum count of the policy may be exceeded.

In one example, persistence is set on the newest snapshot of a running policy that calls for one snapshot per day with a maximum of 10 snapshots. Over the next 10 days, the application always has 10 snapshots of this policy. After day 10, and until persistence is removed from the snapshot, there is a total 11 snapshots created by the policy.

This behavior guarantees the application always has snapshots of the required intervals. However, users must be aware of the potential increase in resource usage.

Note: A persistent policy snapshot can be terminated manually without removing the persistent setting. The persistent setting only prevents the policy from recycling the snapshot.

Linking targets and restoring from a snapshot

Link and restore operations are performed in the same way on policy snapshots and manual snapshots. The operations are performed through standard SnapVX interfaces, not through the policies.

When a snapshot with targets linked or in a restored state passes the retention rule of the policy, it is marked as EXPIRED but will not be recycled by the policy. The policy will continue to take snapshots at the scheduled intervals in addition to retaining the linked or restored snapshot. The snapshot is automatically terminated when the target is unlinked or the restore session is terminated.

Manually terminating snapshots

The PowerMaxOS Q3 2020 release introduces options to terminate multiple snapshots simultaneously. System performance is not affected by snapshot termination because the back-end deltas are deallocated by a low-priority background task after the snapshots have been terminated.

The Bulk Terminate options allow the user to terminate a sequential range of snapshots from a **single SG** with the following options:

- Terminate all snapshots
- Terminate all versions of a specific snapshot
- Terminate oldest versions of a snapshot by specifying which to keep
- Terminate oldest versions of a snapshot by specifying which to terminate

The Bulk Terminate options are not exclusive to policy snapshots and can be used on manual snapshots too. However, snapshots that are linked, in a restored state, or created by Cloud Mobility, are not terminated by the Bulk Terminate options.

Note: The **Bulk Terminate** options are intended to simplify deletion of multiple snapshots. The operations will terminate as many snapshots as possible even if some cannot be terminated. This behavior differs from standard snapshot snapshot-deletion and other snapshot operations which must be successful across the entire set of LUNs. After a Bulk Terminate operation completes, verify that all intended snapshots were successfully terminated.

The following figures show examples of the snapshot Bulk Terminate options.

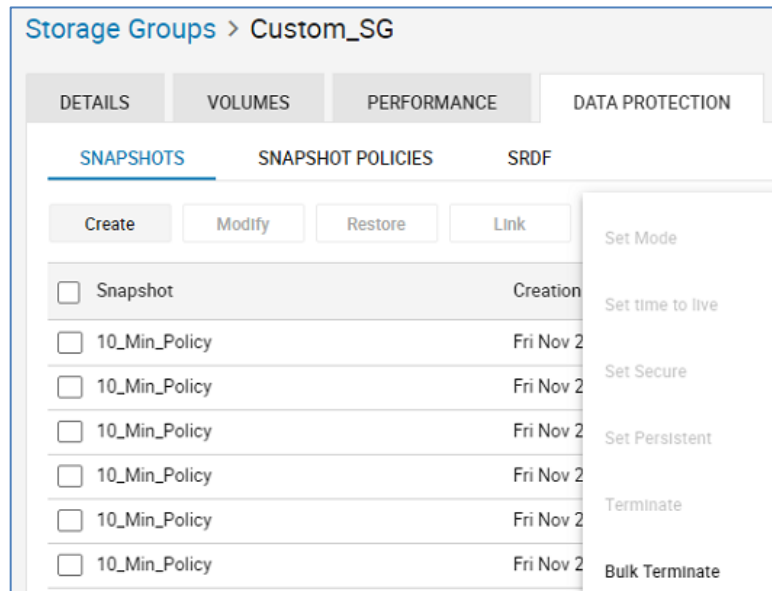


Figure 23. Bulk Terminate operation

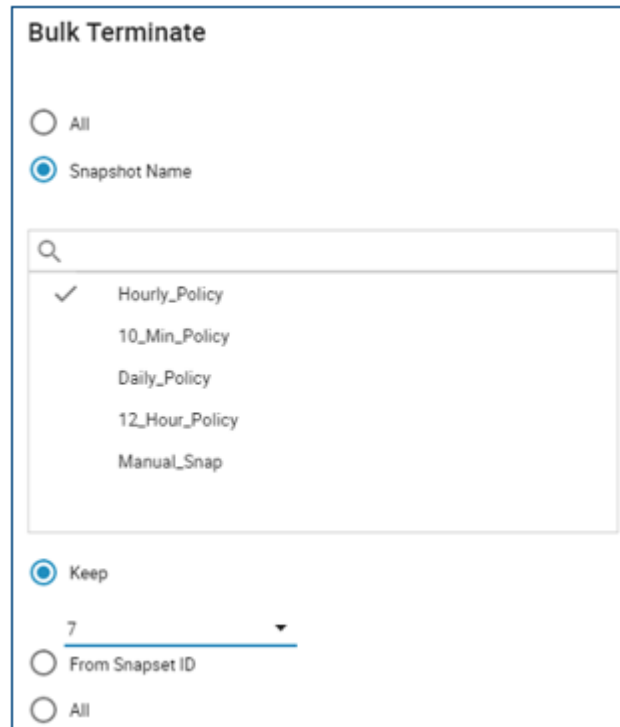


Figure 24. Bulk Terminate

In addition to the Bulk Terminate options, you can use Unisphere to manually select multiple snapshots of an SG and terminate them with a single operation.

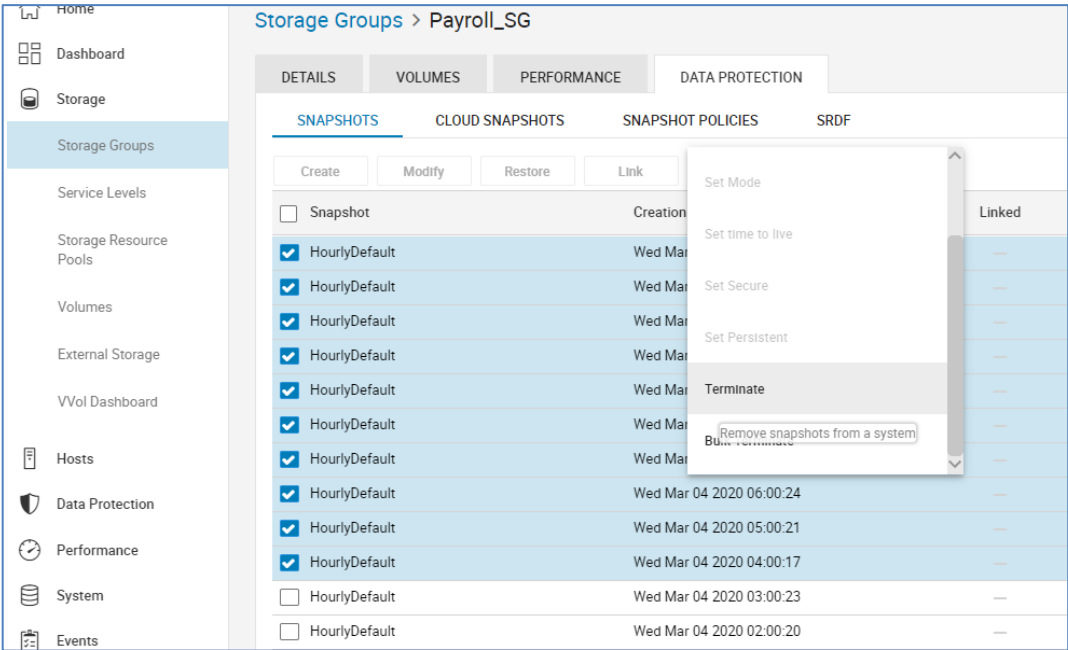


Figure 25. Manually selected snapshots to Terminate

Compliance

Introduction

Policy compliance is measured against the count and intervals of the existing snapshots of the SGs that are assigned to the policy.

The snapshots must exist and be available for user action such as a restore or link operation. The existing snapshots must have been taken at the expected scheduled time and in a valid, non-failed state.

Policy compliance is available in Unisphere for PowerMax and the REST API. However, some Solutions Enabler outputs contain information that is related to policy compliance.

Unisphere for PowerMax reports high-level, color-coded policy compliance in multiple locations. In each location, you can obtain further information by clicking the color-coded icon.

Unisphere automatically runs a compliance check each hour. Changes that affect policy compliance may not be immediately displayed in the dashboard. If a true failure condition is detected, for example if a new snapshot creation fails, the array calls home before the next compliance check. This behavior is important to consider, especially during feature testing.

Data Protection dashboard

Click the color-coded circles in the Data Protection dashboard (see Figure 26) to view the SG list shown in Figure 27. This list shows a breakdown of compliance for each policy on each SG.

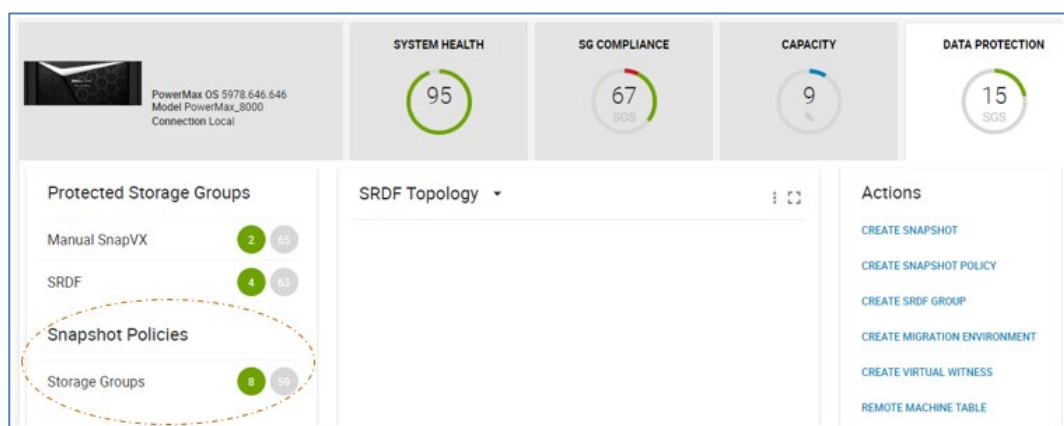


Figure 26. Data Protection dashboard

Select an entry to display other information in the right pane, as shown in the following figure.

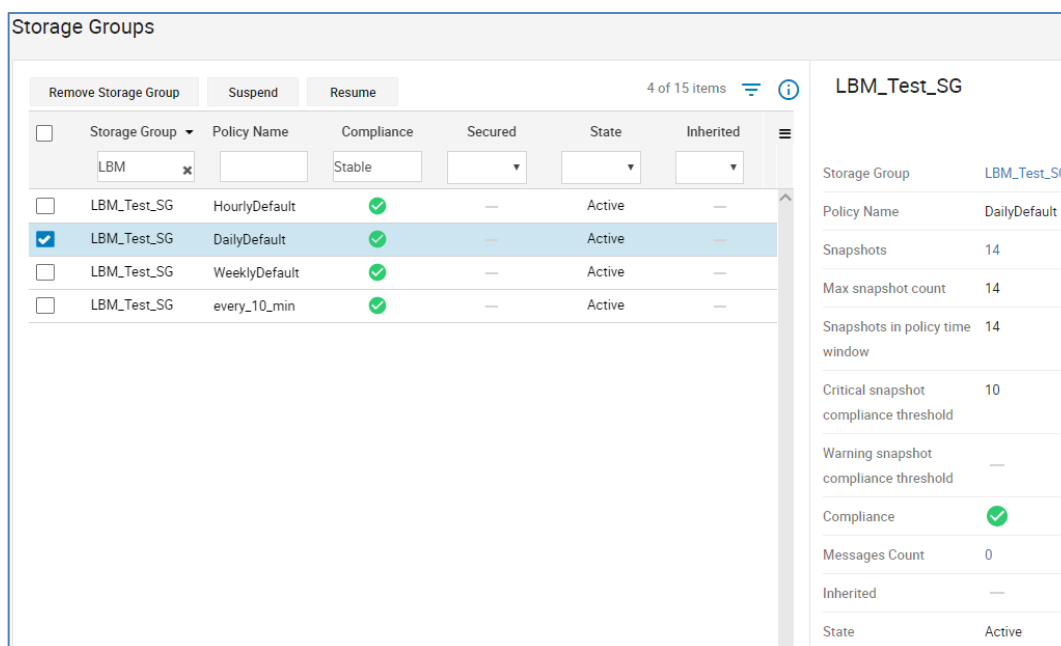


Figure 27. Storage Groups dashboard

In right pane that is shown in Figure 27, click the compliance circle to open the Snapshot Policies page shown in the following figure. This page shows the SG with a trending graph for each policy that associated with the SG.

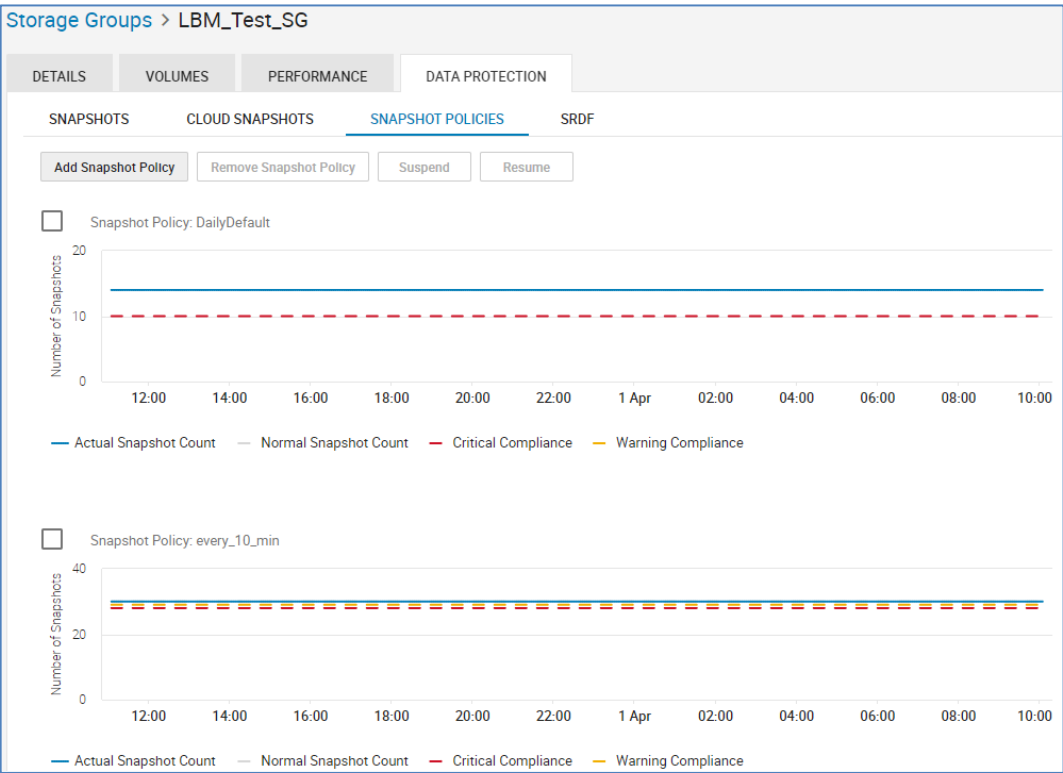


Figure 28. Snapshot Policies page of a specific SG

Snapshot Policies dashboard

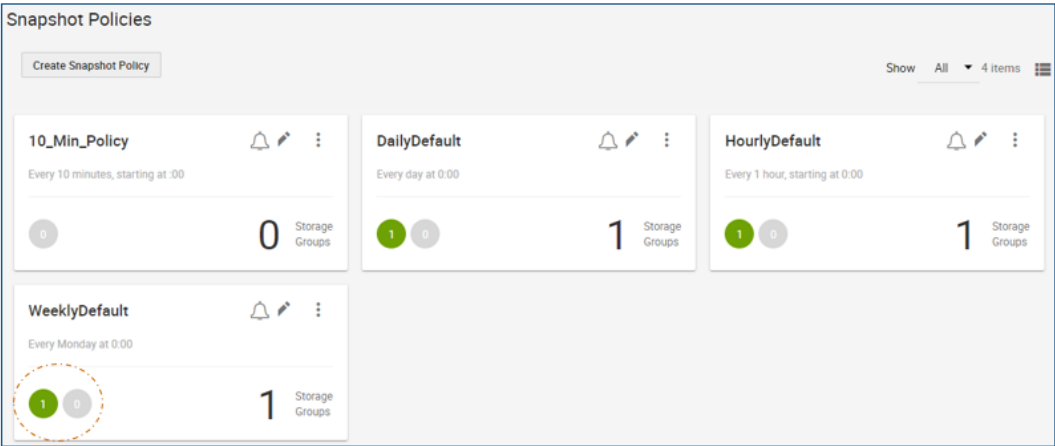


Figure 29. Snapshot Policies dashboard

Select the indicator shown in Figure 29 to open the SG list page for the specific policy shown in Figure 30.

Select one of the entries in Figure 30 to display other information in the right pane. Select the Compliance circle in the right pane to open the same Snapshot Policies page shown in Figure 28.

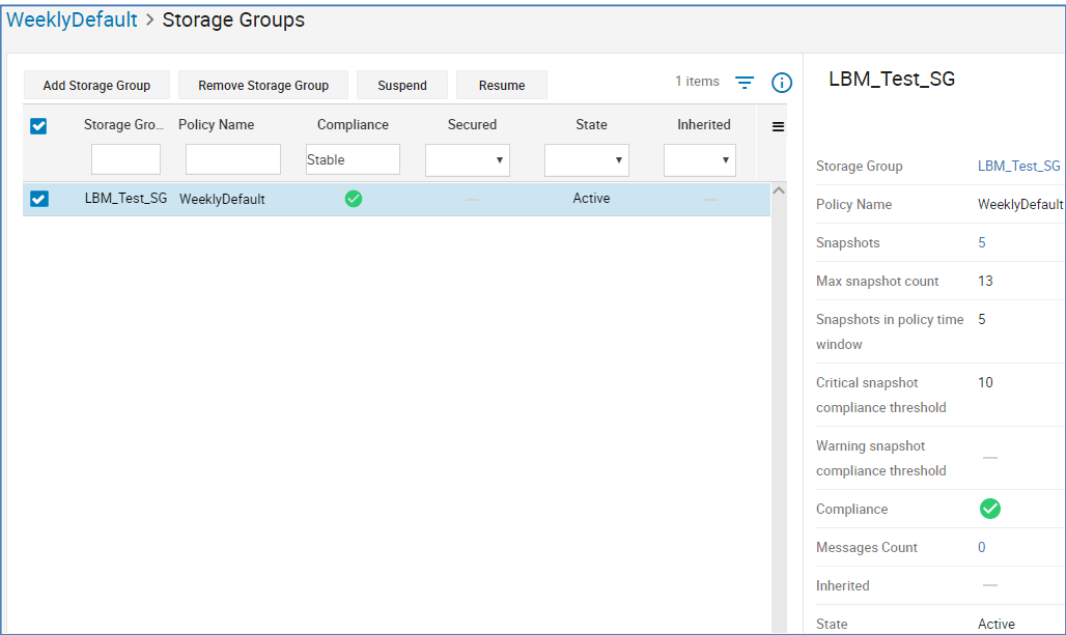


Figure 30. SG list page for a snapshot policy

Compliance messages

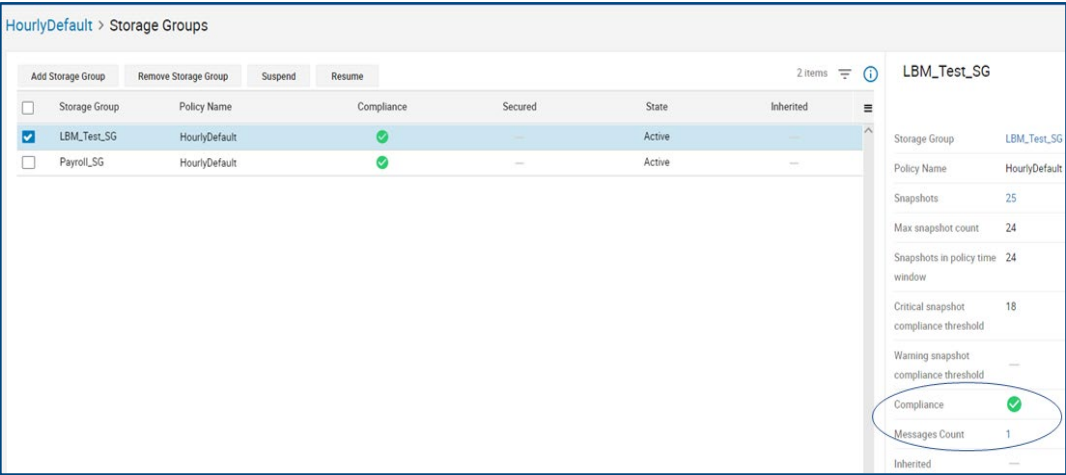


Figure 31. Policy SG list

The following figure shows an example of a compliance message due to an out-of-window snapshot.

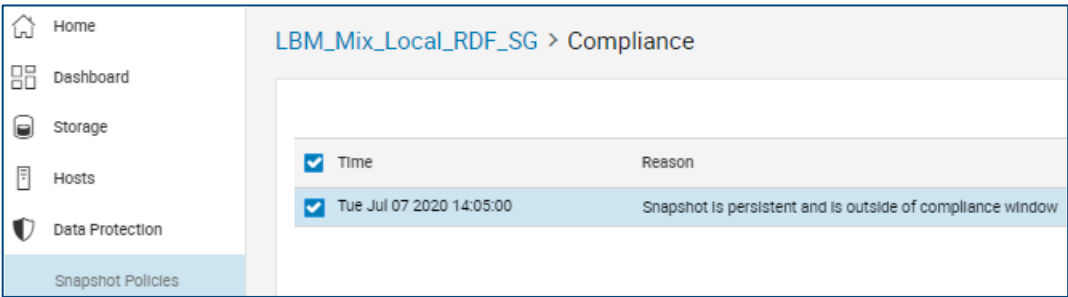


Figure 32. Compliance message

Suspend or resume policies

Figure 33, or on specified SGs, as seen in Figure 34.

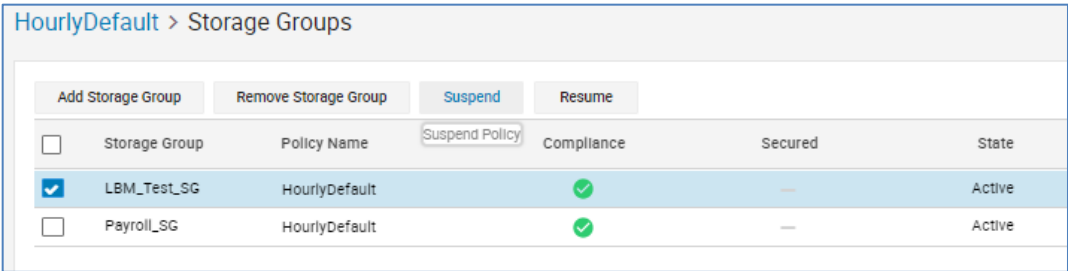


Figure 34. Suspend a policy on SGs

The Storage Groups page (Figure 35) also has an option to suspend policies on a specific SG.

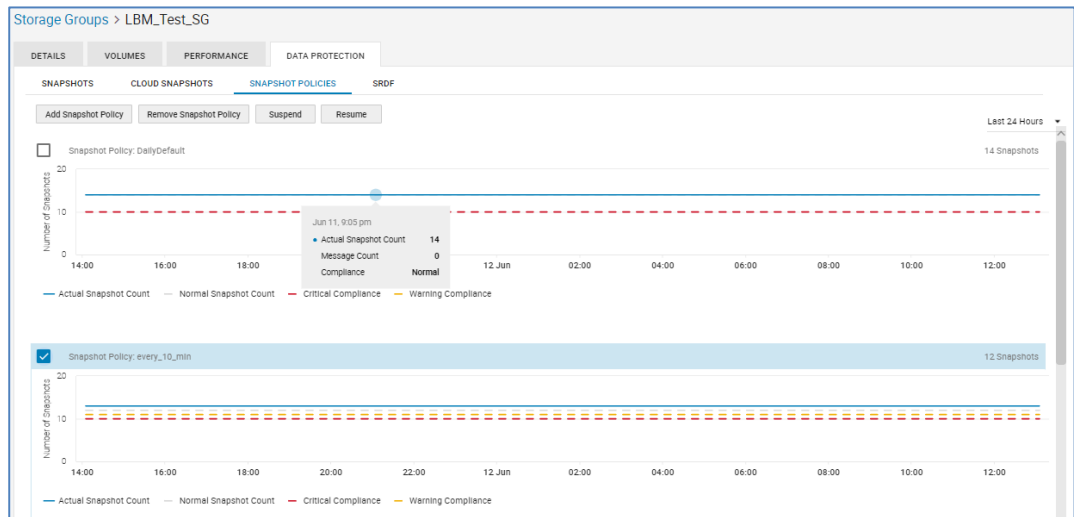


Figure 35. Suspend policies on an SG

Alerts

The alerts shown in the following figure are related to snapshot policies. Not all alerts are enabled by default. Enable alerts of interest when implementing snapshot policies.

Alerts

ALERT POLICIES

Select Array: **All**

90 items

Name	Type	Enabled	Notifications
Initiated delete of expired snapset	Array	✓	NONE
Snap shipping job was completed successfully	Array	✓	NONE
Snapset deleted	Array	✓	NONE
Snapshot Policy Created	Array	✓	NONE
Snapshot Policy Deleted	Array	✓	NONE
Snapshot Policy Modified	Array	✓	NONE
Snapshot Policy added to Storage Group	Array	✓	NONE
Snapshot Policy removed from Storage Group	Array	✓	NONE
Snapshot compliance for Storage Group degraded	Array	✓	NONE
Snapshot compliance for Storage Group improved	Array	✓	NONE

Figure 36. Unisphere alerts

The notification settings must be configured according to the environment (see Figure 37).

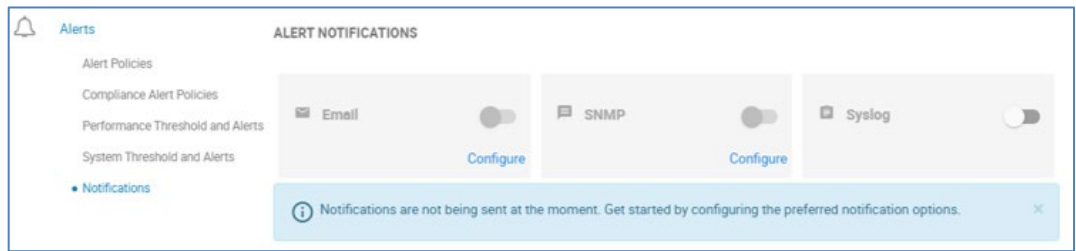


Figure 37. Unisphere Alert Notifications

Cloud mobility for Dell EMC PowerMax

Cloud Mobility for Dell EMC PowerMax provides application-level protection for block devices through snapshot shipping to private and public clouds (Dell EMC ECS, AWS, Azure). Data that is moved to the cloud can be used to restore data to the array and can be consumed directly in AWS.

Cloud Mobility offers the following benefits:

- Reduces array capacity usage
- Data repurposing: Data analytics, reporting
- Space-efficient snapshot shipping: Full initial copy and differential updates
- Cloud-system-independent compression and encryption
- Separation from PowerMax data services
- In-flight and Data at Rest Encryption (on cloud provider)

Cloud Mobility snapshot policies can be managed through Unisphere for PowerMax and REST API, and the policies can only be created with Embedded Management for Unisphere. Cloud Mobility policy parameters include:

- Cloud provider selection
- RPO options:
 - Daily or weekly
- Keep snapshots for:
 - 3 days
 - 1 week
 - 1, 3, or 6 months
 - 1 to 14 years

Figure 38. Creating a Cloud Mobility policy

For more information, see the Cloud Mobility for PowerMax white paper.

Legacy Unisphere snapshot scheduler

When upgrading to Unisphere for PowerMax 9.2, snapshot schedules that were created with previous versions of Unisphere continue to run as scheduled. However, the snapshots cannot be modified other than being deleted, and new schedules cannot be created using the legacy method.

Do not assign an SG to snapshot policies and legacy snapshot schedules simultaneously. In general, delete legacy schedules and end their snapshots before assigning the SG to a policy.

However, the legacy schedules and snapshots can remain if required to support business cases as snapshot policies are implemented and approach compliance. Use care to ensure that system resources are not exhausted, including ensuring the automatic expiration date is set on the snapshots.

Summary

Snapshot policies give businesses the high-level protection that their applications require while involving minimal effort to configure and maintain that protection. The combination of multiple policies per array and multiple policies per application allows businesses to scale snapshot protection according to application importance. Organizations can be confident that they will receive alerts if requirements are not being met, and do not need to dedicate valuable time and resources to monitoring and managing snapshots.

Appendix A: Solutions Enabler command examples

List snapshot policies:

```
symcfg -sid <sid> list -policy -type snap
```

```
symcfg -sid <sid> list -policy -type snap -detail
```

View a policy:

```
symcfg -sid <sid> show -policy <name> -type snap
```

Create a policy:

```
symcfg -sid <sid> create -policy <name> -type snap -interval  
<dd:hh:mm>
```

```
-offset <dd:hh:mm> -max_count <count> -warning_compliance <count>
```

```
-critical_compliance <count>
```

Delete a policy:

```
symcfg -sid <sid> delete -policy <name> -type snap
```

Modify a policy:

```
symcfg -sid <sid> set -policy <name> -type <snap> <[-interval  
[[<D>:]<HH>:]<MM>] [-max_count <#>] [-offset [[<D>:]<HH>:]<MM>]
```

```
[-critical_compliance <#> | -no_critical_compliance]
```

```
[-warning_compliance <#> | -no_warning_compliance] [-new_name  
<Name>]>
```

Suspend a policy:

```
symcfg -sid <sid> suspend -policy <name> -type snap -sg <name>
```

Resume a policy:

```
symcfg -sid <sid> resume -policy <name> -type snap -sg <name>
```

Assign an SG to a policy:

```
symmsg -sid <sid> -sg <name> add -policy <name> -type snap
```

Remove an SG from a policy:

```
symmsg -sid <sid> -sg <name> remove -policy <name> -type snap
```

List SGs that are associated with a snapshot policy:

```
symmsg -sid <sid> list -policy -type snap
```


List policy snapshots (also shows persistent policy snapshots and Cloud Mobility snapshots):

```
symsnapvx -sid <sid> list -policy
```

List manual snapshots:

```
symsnapvx -sid <sid> list -manual:
```

List snapshots on an SG and display the SnapSet ID:

```
symsnapvx -sid <sid> -sg <name> list -snapshot_name <name> -detail  
-snapid
```

List the most recent versions of snapshot on a specified SG:

```
symsnapvx -sid <sid> list -sg <sg_name> -snapshot_name  
<snapshot_name> -detail -last_n <count>
```

List aggregate summary of the snapshots on an SG:

```
symsnapvx -sid <sid> list -sg <sg_name> -aggregate
```

Set a policy snapshot to persistent:

```
symsnapvx -sid <sid> -sg <name> -snapshot_name <name> -snapid <id>  
set persistent
```

List persistent policy snapshots (also shows Cloud Mobility snapshots):

```
symsnapvx -sid <sid> list -persistent
```

Unset persistence from a policy snapshot:

```
symsnapvx -sid <sid> -sg <name> -snapshot_name <name> -snapid <id>  
set nopersistent
```

Terminate all snapshots on specified SG:

```
symsnapvx -sid <sid> -sg <name> terminate -all -force
```

Terminate all versions of a snapshot on an SG:

```
symsnapvx -sid <sid> -sg <name> -snapshot_name <name> terminate -all  
-force
```

Terminate all versions of a snapshot on an SG while keeping most recent count:

```
symsnapvx -sid <sid> -sg <name> -snapshot_name <name> terminate -  
keep_count <count> -force
```

Terminate all versions of a snapshot on an SG after the specified SnapSet ID:

```
symsnapvx -sid <sid> -sg <name> -snapshot_name <name> terminate  
-older_than -snapid <id> -force
```

Appendix B: REST API examples

To help set up and manage snapshots using the REST API, Unisphere 9.2 adds new endpoints and additional REST parameters to new versions of existing REST calls.

The versioned calls are all under the new branch of the API at the following URI:

`https://{IPAddress|hostname}:8443/univmax/restapi/92/`

Note: The Dell EMC REST API officially supports up to three versions of the API in a release of Unisphere with N-2 version support. Version 9.2 supports API versions 9.2, 9.1, and 9.0. When Unisphere is upgraded, REST API continues to work the same. However, newer versions of a call may provide extra functionality. Check the REST API change log available on [Dell.com/support](https://dell.com/support).

Provisioning calls for service-level provisioning can now assign a policy when SGs are created. The other parameters are highlighted in the following screenshot.

Note: It is possible to assign multiple policies at the time of SG creation. The following POST example associates the hourly, daily, and weekly default policies while creating an SG with 5 volumes.

URL : `https://unisphere:8443/univmax/restapi/92/sloprovisioning/symmetrix/000197900 /storagegroup`

Method : POST

Request Parameters

- custom_cascaded_storageGroupid :
- snapshot_protection_policy_id :
- slold :
- workloadSelection :
- * volumeAttributes :
 - * capacityUnit :
 - * volume_size :
 - * num_of_vols :
- volumeIdentifier :
- allocate_capacity_for_each_vol :
- persist_preallocated_capacity_through_reclaim_or_co :
- noCompression :
- enable_mobility_id :
- setHostIOLimitsParam :
 - emulation :

Request Generated JSON

```
{
  "storageGroupid": "newsg",
  "sloBasedStorageGroupParam": [
    {
      "slold": "Diamond",
      "snapshot_protection_policy_id": [
        "DailyDefault",
        "HourlyDefault",
        "WeeklyDefault"
      ],
      "volumeAttributes": [
        {
          "num_of_vols": 5,
          "volume_size": "1",
          "capacityUnit": "GB"
        }
      ]
    }
  ],
  "enable_mobility_id": true
}
```

Create a snapshot policy REST API (POST): Snapshot policies can also be created or modified with REST POST and PUT calls under `https://{ipaddress|hostname}:8443/univmax/restapi/92/replication/symmetrix/{symmetrixId}/snapshot_policy` calls. The following screen shows an example to create a 15-minute policy with a retention of 5 snapshots.

URL:

Method: POST Send

Request Parameters	Request Generated JSON
▼ * snapshotPolicyCreate : snapshot_policy_name : <input type="text" value="15_minute_policy"/> ▶ cloud_snapshot_policy_details : ▼ local_snapshot_policy_details : secure : <input type="text" value=""/> snapshot_count : <input type="text" value="5"/> interval : <input type="text" value="15 Minutes"/> offset_mins : <input type="text" value=""/> compliance_count_warning : <input type="text" value="2"/> compliance_count_critical : <input type="text" value="4"/>	<pre>{ "compliance_count_warning": 2, "local_snapshot_policy_details": { "snapshot_count": 5 }, "interval": "15 Minutes", "compliance_count_critical": 4, "snapshot_policy_name": "15_minute_policy" }</pre>

View a snapshot policy REST API (GET):

/restapi/92/replication/symmetrix/ 000297600 /snapshot_policy/ 10_Minute_Policy /storagegroup/ Snap_SL_PM_1

URL:

Method: GET

```
{
  "snapshots_in_time_window": 0,
  "symmetrixID": "000297600",
  "compliance": "NONE",
  "snapshot_policy_id": "10_Minute_Policy",
  "storage_group_id": "Snap_SL_PM_1",
  "suspended": false
}
```

Modify, Suspend, or Add an SG to a snapshot policy:

Method: PUT

Request Parameters
▼ * snapshotPolicyUpdate : * action : <input type="text" value=""/> ▶ modify : Modify ▶ associate : Suspend ▶ disassociate : Resume AssociateToStorageGroups DisassociateFromStorageGroups

Python SDK

In addition to the method of calling the API directly, the Python SDK from Dell Technologies helps users create their own scripts with minimal effort. The SDK PyU4V is available on [PyPI](#).

We have added a new functional module for snapshot-policy management and support for assigning policies when creating or modifying a storage group. The following functions are present in the `snapshot_policy.py` function library:

- `get_snapshot_policy_list`: Lists all policies on a PowerMax array
- `get_snapshot_policy`: Shows details for a snapshot policy
- `create_snapshot_policy`: Creates a new snapshot policy
- `modify_snapshot_policy`: Changes the characteristics of existing snapshot policy, and enables associating and disassociating storage groups to a policy
- `delete_snapshot_policy`: Deletes a snapshot policy; all storage groups must be disassociated from the policy for the delete function to succeed

Provisioning functions also enable associating policies to storage groups upon creation or later.

- `create_storage_group`: New parameters in version 9.2 `snapshot_policy_ids`

Sample python script to create a new storage group and assign DailyDefault and HourlyDefault existing snapshot policies.

```
"""SnapShot_Policy_Example.py"""

import PyU4V

# Initialise PyU4V Unisphere connection
conn = PyU4V.U4VConn(server_ip='UnisphereServerIP', port=8443,
                     verify=False, username='SecretUser',
                     password='DontTellAnyone', array_id='000297600 ')

print (conn.provisioning.create_storage_group(
    srp_id='SRP_1', storage_group_id='REST_Example',
    service_level='Diamond', workload=None, num_vols=50, vol_size=1,
    cap_unit='GB', snapshot_policy_ids=['DailyDefault', 'HourlyDefault']))
```

Appendix C: Technical support and resources

[Dell.com/support](https://dell.com/support) is focused on meeting customer needs with proven services and support.

[Storage and data protection technical white papers and videos](#) provide expertise that helps to ensure customer success with Dell EMC storage and data protection products.

For more information, see the following related resources:

- [TimeFinder SNAPVX Local Replication](#)
- [Frequently Asked Questions about TimeFinder SnapVX on VMAX All Flash Arrays](#)
- [Dell EMC PowerMax and VMAX All Flash: Data Protector for z Systems \(zDP\) Essentials](#)
- [Dell EMC PowerMax Family Overview](#)
- [Dell EMC PowerMax: Reliability, Availability, and Serviceability](#)